Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Directoraat-generaal Overheidsorganisatie
Directie Informatiesamenleving en Overheid

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
http://www.rijksoverheid.nl

Kenmerk
2016-0000328613

Bijlage(n)
17

Datum 9 juni 2016
Betreft Beslissing op uw Wob-verzoek

Geachte

Bij brief van 28 maart 2016 heeft u bij het ministerie een verzoek ingediend als bedoeld in artikel 3, eerste lid, van de Wet openbaarheid van bestuur (hierna ook: Wob) met betrekking tot, kort gezegd, DigiNotar.

Bij brief van 31 maart 2016 heb ik u erop geattendeerd dat de stukken met betrekking tot DigiNotar op de website van de rijksoverheid staan naar aanleiding van eerdere verzoeken op grond van de Wet openbaarheid van bestuur. De stukken zijn daarmee reeds openbaar. Ik heb u in die brief de directe vindplaatsen gegeven.
Bij brief van 5 april 2016 heeft u uw verzoek in verband hiermee desgevraagd gespecificeerd, en deels beperkt.

Uw nader gespecificeerde en deels beperkte verzoek betreft het onderzoek dat het bedrijf Fox-IT in 2011 in opdracht van het ministerie heeft ingesteld naar DigiNotar.
Concreet verzoekt u:
"Het eindrapport van dit onderzoek is openbaar, maar ik verzoek om openbaarmaking van onderliggende documenten, e-mails en notities op basis waarvan dit rapport tot stand is gekomen. Ook verzoek ik om eventuele eerdere versie van dit rapport openbaar te maken. Daaronder valt ook de analyse die Fox-IT heeft gemaakt over de gecompromitteerde systemen en informatie over de mogelijke dader(s)".

Bij brief van 7 april 2016 heb ik de ontvangst op 7 april 2016 van uw gespecificeerde en ingeperkte verzoek Wob-verzoek aan u bevestigd.

Bij brief van 26 april 2016 is de termijn om op uw verzoek te beslissen met vier weken verlengd (tot en met 3 juni 2016).

Bij brief van 25 mei 2016 is aan u meegedeeld dat de beslistermijn is opgeschort vanwege het vragen van zienswijzen aan een derde.

Directoraat-generaal Overheidsorganisatie
Directie Informatiesamenleving en Overheid

Datum
9 juni 2016

Kenmerk
2016-0000328613

Bij brief van 3 juni 2016 bent u geïnformeerd over de beëindiging van de opschorting van de beslistermijn en heb ik meegedeeld dat u met circa twee weken doch uiterlijk op 17 juni 2016 een beslissing op uw verzoek tegemoet kunt zien.

Door de derde belanghebbende zijn geen bedenkingen ingediend.

In de eerste plaats attendeer ik u erop dat de Wet openbaarheid van bestuur niet van toepassing is op informatie die reeds openbaar is.

Met betrekking tot uw verzoek zijn de volgende e-mails, e-mailwisselingen en overige documenten zoals conceptversies van het rapport, aangetroffen.

No	***Onderwerp***	***Begindatum***	***Einddatum***	***Naam document***
1.	FOX-IT rapport	14-9-2011	14-9-2011	
2.		14-9-2011	14-9-2011	Diginotar Rapport Outline v01.docx
3.	rapport 1.1	19-9-2011	19-9-2011	
4.		19-9-2011	19-9-2011	Diginotar public report (draft) v1 1 1.docx
5.	Rapport 1.1 draft 2	22-9-2011	4-10-2011	
6.		22-9-2011	3-10-2011	
7.		22-9-2011	22-9-2011	Diginotar public report (draft) v1 1 2.docx
8.	Black Tulip Report 1.1	10-10-2011	10-10-2011	
9.		10-10-2011	10-10-2011	Operation Black Tulip v1.1.pdf
10.		10-10-2011	10-10-2011	Operation Black Tulip v1.1_with diff to 1.0.pdf
11.	concept fox-it	8-12-2011	8-12-2011	
12.		8-12-2011	8-12-2011	HH-Operation Black Tulip Update (draft) 0.1-1207b[1].pdf
13.	laatste versie van het Fox-rapport	19-12-2011	19-12-2011	
14.		19-12-2011	19-12-2011	HH-Operation Black Tulip Update (draft) 0.1-1215a.pdf
15.	het rapport!	4-7-2012	25-7-2012	
16.		4-7-2012	4-7-2012	REP_MinBZK_pr-110202_Operation_Black_Tulip_Update_0.9.pdf
17.	Definitieve versie DigiNotar rapport	13-8-2012	13-8-2012	
18.		13-8-2012	13-8-2012	REP_MinBZK_pr-110202_Operation_Black_Tulip_Update_1.0.pdf

Directoraat-generaal
Overheidsorganisatie
Directie
Informatiesamenleving en
Overheid

Datum
9 juni 2016

Kenmerk
2016-0000328613

Document 18 is reeds openbaar. De Wob is daarop dan ook niet van toepassing. Als service geef ik u de vindplaats. U vindt dit stuk via https://www.rijksoverheid.nl/documenten/rapporten/2012/08/13/black-tulip-update.

Ik heb besloten om aan uw Wob-verzoek tegemoet te komen door de overige 17 bij mij berustende documenten openbaar te maken. U treft de documenten 1 tot en met 17 bijgaand aan.
U zult zien dat op enkele plaatsen in deze documenten gegevens onleesbaar (zwart) zijn gemaakt. Deze gegevens maak ik niet openbaar. Dit betreft in alle gevallen uitsluitend (voor)namen, handtekeningen en directe contactgegevens zoals telefoonnummers en e-mailadressen van individuele ambtenaren en/of andere individuele personen. Deze gegevens maak ik niet openbaar in verband met het belang van de eerbiediging van de persoonlijke levenssfeer van de betrokken individuele personen. Dit belang, dat wordt vermeld in artikel 10, tweede lid, aanhef en onder e, van de Wob acht ik hier zwaarwegender dan het algemene belang van openbaarmaking van deze tot individuele personen herleidbare gegevens.

Graag geef ik u nog de volgende toelichting op de openbaar gemaakte documenten.

1. U vraagt naar openbaarmaking van onderliggende documenten, e-mails en notities op basis waarvan het rapport tot stand is gekomen.
   Het eerste contact tussen Fox-IT en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties over het rapport vond plaats op 14 september 2011. U treft de e-mailwisseling en de bijbehorende eerste opzet van het onderzoek in de bijlagen aan.
   Over dit onderzoek is uitsluitend per e-mail gecommuniceerd tussen Fox-IT en het ministerie. Gedurende de (korte) looptijd van het onderzoek heeft geen formele besluitvorming plaatsgevonden. Ambtelijke nota's, memo's of andere notities hierover berusten dan ook niet bij het ministerie.

2. Ook vraagt u om eventuele eerdere versies van dit rapport openbaar te maken, waaronder "de analyse die Fox-IT heeft gemaakt over de gecompromitteerde systemen en informatie over de mogelijke dader(s)".
   Tussen het ministerie en de opdrachtnemer zijn tussen 14 september 2011 en de publicatie op 13 augustus 2012 in totaal zes conceptversies van het rapport gewisseld. Deze treft u, met de bijbehorende e-mailwisselingen, bijgaand aan. Behalve deze e-mailwisselingen en tussenliggende versies berusten bij het ministerie geen e-mailwisselingen of andere documenten op basis waarvan dit rapport tot stand is gekomen.
   De door u genoemde analyse die Fox-IT zou hebben gemaakt over de gecompromitteerde systemen en informatie over de mogelijke dader(s), anders dan die blijkt uit de bijgevoegde tussenversies van de rapporten is, als die al is gemaakt, niet met de directie in wier opdracht de rapporten zijn gemaakt, gedeeld en ook overigens niet bij het ministerie aangetroffen. De

Directoraat-generaal
Overheidsorganisatie
Directie
Informatiesamenleving en
Overheid

Datum
9 juni 2016

Kenmerk
2016-0000328613

conclusie is dan ook dat een dergelijk document, indien al bestaand, niet bij het ministerie berust.

Tot slot wijs ik u erop dat omdat voor de totstandkoming van de (MS-Word-)documenten macro's zijn gebruikt, het zo kan zijn dat bij het afdrukken ten behoeve van de openbaarmaking, de documentdatum automatisch is vervangen door de datum waarop de afdruk is vervaardigd. In de gevallen dat gelijkluidende PDF- en Word-versies zijn gewisseld, sluit ik alleen de PDF-versie bij.

Dit Wob-besluit en de stukken die hiermee voor een ieder openbaar worden gemaakt, worden zo spoedig mogelijk na toezending gepubliceerd op de website www.rijksoverheid.nl.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
De minister van Binnenlandse Zaken en Koninkrijksrelaties,
namens deze,

Richard van Zwol
Secretaris-generaal

Bijlagen:
1 t/m 17

Belanghebbenden kunnen binnen zes weken na bekendmaking van dit besluit daartegen per brief bezwaar maken bij de minister van Binnenlandse Zaken en Koninkrijksrelaties, DGOO/DIO, Postbus 20011, 2500 EA Den Haag. Het bezwaarschrift moet zijn ondertekend, voorzien zijn van een datum alsmede de naam en het adres van de indiener en dient vergezeld te gaan van de gronden waarop het bezwaar berust en, zo mogelijk, een afschrift van het besluit waartegen het bezwaar is gericht.

Van: [redacted]@fox-it.com]
Verzonden: woensdag 14 september 2011 16:25
Aan: [redacted]; [redacted] (Fox-IT)
CC: [redacted]
Onderwerp: RE: FOX-IT rapport
Bijlagen: Diginotar Rapport Outline v01.docx

Beste allemaal,

Bijgesloten een rapport over de outline van het eindrapport... Met name de lijst van onderzoeksvragen kunnen we in het overleg morgen gebruiken als leidraad.

Met vriendelijke groet/ With kind regards,

[redacted]
Security Expert

Fox-IT Experts in IT Security!

T +31 (0)15 2847[redacted]
F +31 (0)15 2847990
I www.fox-it.com

Van: [redacted] - Logius [mailto[redacted]@logius.nl]
Verzonden: woensdag 14 september 2011 11:25
Aan: [redacted]; [redacted] (Fox-IT)
CC: [redacted]
Onderwerp: RE: FOX-IT rapport

15:00 bij BZK wordt het dus ([redacted]kan ook). Ik stuur straks de definitieve locatie (vergaderzaal) e.d. rond.

[redacted]

Van: [redacted] [mailto[redacted]@fox-it.com]
Verzonden: woensdag 14 september 2011 11:13
Aan: [redacted] (Fox-IT); [redacted] - Logius
CC: [redacted]
Onderwerp: RE: FOX-IT rapport

Wat mij betreft prima!

[redacted]

Van: [redacted] (Fox-IT)
Verzonden: woensdag 14 september 2011 11:09
Aan: [redacted] - Logius
CC: [redacted]
Onderwerp: RE: FOX-IT rapport

Helemaal goed. Doen we dat [redacted]lukt dat ook?

From: [redacted] - Logius [mailto[redacted]@logius.nl]
Sent: woensdag 14 september 2011 10:59
To: [redacted](Fox-IT)
Cc: [redacted]
Subject: RE: FOX-IT rapport

[redacted]

Wat mij betreft kunnen het ook om 15:00 bij BZK in Den Haag doen. Ben je in ieder geval al in de buurt.

[redacted]

Van: [redacted](Fox-IT) [mailto[redacted]@fox-it.com]
Verzonden: woensdag 14 september 2011 10:51
Aan: [redacted] - Logius
CC: [redacted]
Onderwerp: RE: FOX-IT rapport

Hoi [redacted]

Ja, ik krijg lange brieven van hun advocaat met opmerkingen dus laten we daar ook maar wat mee gaan doen. Het zijn punten over het proces en punten over de inhoud. Die zou ik uit elkaar willen trekken.

We zitten in een zeer vreemde situatie natuurlijk. We zijn ingehuurd om te publiceren dat het allemaal wel goed zat. Van te voren is afgesproken dat het een publiek rapport zou worden. Normaal gesproken heeft een klant die ons vraagt een oordeel te vellen ook de ruimte om een concept in te zien en daar aanpassingen in te suggeren. Dat is nu ook gebeurd. Wij houden de vrijheid om dat al dan niet mee te nemen. Het gaat dan meestal over feitelijke slordigheden en of het schetsen van een context. Bij een snelle glimp over hun opmerkingen denk ik we een zeer beperkt aantal zaken mogelijk aanpassen (data als die echt niet blijken te kloppen etc). Andere nuanceringen ga ik niet zo maar in mee.
Als ze daar iets mee willen zouden ze zelf hun reactie kunnen publiceren.

Ik heb [redacted] gevraagd een en ander voor te bereiden en morgenmiddag heb ik tijd ingeruimd om het te bespreken. We moeten misschien nadenken over verschillende rapporten. Een aan de hand waarvan bzk en opta conclusies kan trekken over de werkelijke veiligheidssituatie bij DN, en een die voor de opsporing meer relevant is. Verschillende spelers zullen verschillende vragen hebben. Heeft de OPTA misschien nog bijzondere vragen. Heeft MinBZ nog vragen over de schade voor het Iraanse volk. Gaat MinBZK dat allemaal coordineren.

Ik moet om 1800 uur bij de hoorzitting in de Tweede Kamer zijn. Zullen we om 1500 uur de conference call doen?

From: [redacted] - Logius [mailto[redacted]@logius.nl]
Sent: woensdag 14 september 2011 8:39
To: [redacted](Fox-IT)
Cc: [redacted]
Subject: FOX-IT rapport

[redacted]

Op 5-9 is een tussenrapportage uitgebracht door FOX-it.

Ik heb begrepen dat er ook met Diginotar nog over onderwerpen wordt gesproken (of dat men een reactie heeft gegeven). Verder staan er nog wat vragen open.

Lijkt me handig om op korte termijn even met elkaar bij te praten hoe te komen tot een definitief rapport. Zou het evt lukken om donderdagmiddag even elkaar te spreken (evt conference call) hierover?

[redacted]

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

FOX-IT
EXPERTS IN IT SECURITY

Diginotar Rapport Outline

Black Tulip

Classificatie **VERTROUWELIJK**

Opdrachtgever [opdrachtgever]
[adres]

Betreft [onderwerp]

Project Nr./ Ref. nr. xxxxx
Datum 14 september 2011
Versie 0.1
Auteur [redacted]
Business Unit Cybercrime
Pagina's 9

VERTROUWELIJK
Dit document is geclassificeerd als vertrouwelijk. De informatie die in dit document en bijbehorende bijlagen gepubliceerd is, is alleen bedoeld voor de geadresseerde(n) in de distributielijst op de pagina Document Management. Het gebruik van het document door een andere partij dan de geadresseerde(n) is niet toegestaan, tenzij deze partij hiertoe expliciet geautoriseerd is door een geadresseerde. De informatie in dit document is mogelijkerwijs vertrouwelijk van aard en valt eventueel onder de bepalingen van een geheimhoudingsverklaring of -plicht.

Indien u het voorliggende document foutief heeft ontvangen en/of geen toestemming heeft tot inzage van het document, verzoekt Fox-IT u om het document direct te sluiten en te retourneren aan Fox-IT.

Enig misbruik van dit document of de informatie in het document is niet toegestaan. Fox-IT aanvaardt geen aansprakelijkheid voor enig ongeautoriseerd gebruik of misbruik van voorliggend document door een derde partij of schade ontstaan door de inhoud van het document.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Telefoon: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: fox@fox-it.com
Internet: www.fox-it.com

Document Management

Versiebeheer

Projectnaam:	PROJECTNAAM
Klant:	[opdrachtgever]
Onderwerp:	[onderwerp]
Datum:	14 september 2011
Versie:	[versie]
Status:	[status]
Auteur(s):	[redacted]

Deze versie vervangt alle voorgaande versies van dit document. Vernietig a.u.b. alle voorgaande versies!

Distributielijst

Kopie	Verspreiding (versie)	Naam/functie/opmerking

Reviews

Review door	Functie	Datum	Versie

Wijzigingen

Versie	Datum	Door	Opmerkingen	Goedkeuring

Gerelateerde documenten

Versie	Datum	Omschrijving	Opmerkingen

Inhoudsopgave

1 Inleiding

Dit is niet het definitieve rapport over de hack zaak van DigiNotar maar in dit rapport staat wat er in het rapport komt te staan.

2 Rapport indeling

In het rapport wordt de volgende indeling gemaakt:

2.1 Introductie

Hierin staat een korte inleiding, scope van het rapport en een leeswijzer

2.2 Betrokken partijen

Hierin staan de betrokken de partijen die betrokken zijn geweest bij het onderzoek en die geïnteresseerd zijn de resultaten.

2.3 Situatie

Omschrijving van de situatie zoals die bij DigiNotar is aangetroffen.
Hoe zag het netwerk eruit, hoe werkte de systemen bij DigiNotar globaal e.d.

2.4 Onderzoeksvragen

Welke onderzoeksvragen zijn er gesteld en waar wordt een antwoord op gegeven in het rapport.
{Discussiepunt: Er kunnen meerdere rapportages zijn die verschillende onderzoeksvragen antwoorden.}

2.5 Onderzoek

Welke systemen zijn onderzocht, wat globaal de aanpak geweest, welke zaken zijn niet onderzocht, welke open eindjes kunnen nog verder worden onderzocht

Afhankelijk van de onderzoeksvragen bevat dit:

- Servers en andere systemen binnen de infrastructuur van DigiNotar
- Servers en andere (log) informatie buiten DigiNotar (b.v. voor opsporing van de dader, of de effecten van de inbraak)

2.6 Resultaten

Samenvattend hoofdstuk waarin de gevonden sporen en onderzoeksresultaten worden gekoppeld aan de vraagstelling. Hier wordt dus de onderzoeksvraag beantwoord of zal de onderzoeksvraag door andere mee kunnen beantwoordt worden. Hier wordt ook aangegeven hoe betrouwbaar de antwoorden zijn.

Ook de openeindjes en (nog) niet onderzochte issues worden aangegeven.

3 Rapport inhoud

3.1 Algemeen

Het rapport zal in het Engels worden opgesteld.

In het rapport zullen alleen technische feiten worden weergegeven op basis van onderzoek gedaan door Fox-IT.

Feiten uit technisch onderzoek van andere partijen zullen zoveel mogelijk worden geverifieerd door Fox-IT. Er zal naar documenten of email worden gerefereerd.

Niet technische feiten zullen als zodanig worden genoemd. Er zal naar documenten of email worden gerefereerd.

Details over de manier waarop het onderzoek is gedaan wordt niet in het rapport opgenomen. Het rapport bevat alleen de relevante resultaten van het onderzoek.

Er zullen geen conclusies worden getrokken m.u.v. technisch gevolgtrekkingen zoals: uit sporen blijkt dat de aanvaller op xxx actief is geweest op systeem yyy, dit betekend dat de beveiliging van yyy is doorbroken.
{punt ter discussie: we kunnen wel een aantal conclusies trekken!}

3.2 Betrokken partijen

Betrokken partijen en hun doelen:

DigiNotar:	
Fox-IT:	Bijdrage aan een veiligere digitale samenleving. Leren van de aanval om betere producten te ontwikkelen en betere advies te kunnen geven aan klanten.
KLPD:	Opsporing en onderzoek naar dader(s).
AIVD:	Vaststellen dreiging voor de Nationale Veiligheid.
GOVCERT.NL:	Uitvoeren van respons, damage control en woordvoering.
OM:	Vervolging dader(s).
OPTA:	Toezicht op en monitoren van geregistreerde CSP's. (waar DigiNotar een voorbeeld is).
PWC:	Uitvoerende audit partij.
Hoffman Bedrijfsrech.:	
De mensen in Iran:	Wat waren de gevolgen voor de slachtoffers van de nep google.com certificaat.
De internet gemeenschap:	Wat zijn de mogelijke gevolgen van deze diefstal voor andere gebruikers
DigiNotar klanten:	De klanten die een certificaat uitgegeven van DigiNotar gebruiken.
Andere target bedrijven:	
Fabrikanten:	Web browser fabrikanten, Adobe en andere?
RSA software:	Mogelijkheden om hun product te verbeteren of advies daarin

3.3 Onderzoeksvragen

Opsporing
- Zoeken naar informatie die kunnen leiden naar de arrestatie van de aanvaller

Wat is er gestolen?
- Welke certificaten zijn uitgegeven door de aanvaller (incl. serienummers)?
- Welke private keys zijn gestolen?
- Welke andere zaken zijn gestolen (persoonsgegevens, email, broncode, contracten, e.d.)?

Aanvaller
- Hoe ging de hacker te werk?

    - Welke exploits zijn gebruikt?
    - Welke tools?
    - Wat waren de aanvalspaden? (Was e-mail gebruikt?)
- Welke systemen buiten DigiNotar zijn gebruikt?
- Hoe geraffineerd was the aanval?
    - Hoeveel personen?
    - Welke kennis was vereist?
- Wat zijn de overeenkomsten/ verschillen met andere TTP aanvallen?
- Wat zijn de motieven van de aanvaller?

Consequenties (internetgebruikers algemeen)
- Wat zijn consequenties voor de burgers van Iran?
    - Welke extra inspanning zijn er gedaan?
- Wat zijn andere potentiële gevolgen voor internetgebruikers?
    - Welke andere inspanningen moeten daarvoor worden gedaan?

Consequenties (Klanten DigiNotar)
- Wat zijn de gevolgen van de gestolen sleutels voor de klanten van DigiNotar?
- Wat zijn de gevolgen van het intrekken van de CA's voor de klanten van DigiNotar?

Detectie en preventie
- Hoe kon de aanval (eerder) gedetecteerd worden?
- Hoe kon de aanval tegengehouden worden?

Huidige beveiliging status DigiNotar
- Welke maatregelen zijn er sinds de ontdekking genomen
- Wat is de huidige beveiligingsstatus van de systemen van DigiNotar

Wet- en regelgeving (Compliancy)
- Voldeden de beveiligingsmaatregelen aan de gestelde eisen?

Gepaste ijver (Due diligence)
- Heeft DigiNotar gepaste ijver getoond in hun beveiligmaatregelen?
- Heeft DigiNotar juist gehandeld sinds hun bekendheid van de aanval?
- Heeft de overheid juist gehandeld sinds hun bekendheid met de aanval?

4 Status onderzoek

Het onderzoek heeft zich tot nu toe gericht op de opsporing. Het was zaak zo snel mogelijk in beeld krijgen wat er is gebeurd en wat de impact daarvan is geweest.

Van: [redacted]@fox-it.com]
Verzonden: maandag 19 september 2011 16:57
Aan: [redacted] (Fox-IT); [redacted]; [redacted]
Onderwerp: rapport 1.1
Bijlagen: Diginotar public report (draft) v1.1.1.docx

Hallo,

Bijgevoegd wat kleine aanpassingen in het rapport met track changes. In het rapport van de OPTA staat nog wel iets meer aan info dan in ons rapport (OPTA punt 25). Als we echter deze info ook in ons rapport willen opnemen moeten we wel meer wat meer van het lopende onderzoek toevoegen, wat wellicht meer vragen of onduidelijkheden gaat oproepen.

PS: ik weet niet aan wie we deze versie nog meer moeten sturen ter review.

Met vriendelijke groet,

[redacted]
Security Expert

Fox-IT Experts in IT Security!

Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands

T +31 (0)15 28479[redacted]
F +31 (0)15 2847990
I www.fox-it.com

KvK Haaglanden 27301624

Interim Report

September 5, 2011

DigiNotar Certificate Authority breach
"Operation Black Tulip"

Classification **PUBLIC**

Customer DigiNotar B.V.

Subject: Investigation DigiNotar Certificate Authority Environment

Date 19 September 2011
Version 1.1
Author J.R. Prins (CEO Fox-IT)
Business Unit Cybercrime
Pages 13

Verwijderd: 5
Verwijderd: 0

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

1 Introduction

1.1 Background

The company DigiNotar B.V. provides digital certificate services; it hosts a number of Certificate Authorities (CA's). Certificates issued include default SSL certificates, Qualified Certificates and 'PKIoverheid' (Government accredited) certificates.

On the evening of Monday August 29th it became public knowledge that a rogue *.google.com certificate was presented to a number of Internet users in Iran. This false certificate had been issued by DigiNotar B.V. and was revoked[1] that same evening.

On the morning of the following Tuesday, Fox-IT was contacted and asked to investigate the breach and report its findings before the end of the week.

Fox-IT assembled a team and started the investigation immediately. The investigation team includes forensic IT experts, cybercrime investigators, malware analysts and a security expert with PKI experience. The team was headed by CEO J.R. Prins directly.

It was communicated and understood from the outset, that Fox-IT wouldn't be able to complete an in-depth investigation of the incident within this limited timeframe. This is due to the complexity of the PKI environment and the uncommon nature of the breach.

Rather, due to the urgency of this matter, Fox-IT agreed to prepare an interim report at the end of the week with its preliminary findings, which would be published.

1.2 Investigation questions

The investigation predominately focused on following questions:

1. How did the perpetrators access the network?

2. What is the scope and status of the breach?
   - *Have other DigiNotar CA environments been breached?*
   - *Do we still see hacker activity on the network of DigiNotar?*
   - *Are rogue certificates actively being used by hackers?*

3. Can we discover anything about the impact of the incident?
   - *What certificates were issued without knowledge of DigiNotar?*
   - *What other (rogue) certificates might have been generated?*
   - *How many rogue connections were made using rogue certificates?*
   - *What was the nature of these connections?*

In order to address these questions we (basically) (i) implemented specialized monitoring to be able to detect, analyse and follow up on active misuse, and (ii) analysed digital traces on hard disks, and in databases and log files to investigate the origin and impact of the breach.

[1] Revoked: A certificate is irreversibly revoked if, for example, it is discovered that the certificate authority (CA) had improperly issued a certificate, or if a private-key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements such as publication of false documents, mis-representation of software behavior, or violation of any other policy specified by the CA operator or its customer. The most common reason for revocation is the user no longer being in sole possession of the private key (*e.g.*, the token containing the private key has been lost or stolen).

1.3 This report

The goal of this report is to share relevant information with DigiNotar stakeholders (such as the Dutch Government and the Internet community), based on which they can make their own risk analysis. Because this is a public report, some investigation results and details cannot be included for privacy and/ or security reasons.

Since the investigation has been more of a fact finding mission thus far, we will not draw any conclusions with regards to the network-setup and the security management system. In this report we will not give any advice to improve the technical infrastructure for the long term. Our role is to investigate the incident and give a summary of our findings until now. We leave it to the reader in general and other responsible parties in the PKI- and internet community to draw conclusions, based on these findings. We make a general reservation, as our investigations are still ongoing.

Verwijderd:

2 Investigations

2.1 Prior investigations

Some investigations were conducted before we started.

Fox-IT was given access to a report produced by another IT-security firm which performs the regular penetration testing and auditing for DigiNotar. The main conclusions from this report dated July 27th were:

> A number of servers were compromised. The hackers have obtained administrative rights to the outside webservers, the CA server "Relaties-CA" and also to "Public-CA". Traces of hacker activity started on June 17th and ended on July 22nd.

Furthermore, staff from DigiNotar and the parent company Vasco performed their own security investigation. E-mail communication and memos with further information were handed over to us.

This information gave us a rough overview of what happened:

- The signing of 128 rogue certificates was detected on July 19th during the daily routine security check. These certificates were revoked immediately;
- During analysis on July 20th the generation of another 129 certificates was detected. These were also revoked on July 21th;
- Various security measures on infrastructure, system monitoring and OCSP validation have been taken immediately to prevent further attacks.
- More fraudulent issued certificates were discovered during the investigation and 75 more certificates were revoked on July 27th.
- DigiNotar found evidence on July 28th that rogue certificates were verified by internet addresses originating from Iran.
- On August 29th a *.google.com certificate issued was discovered that was not revoked before. This certificate was revoked on August 29th.

Verwijderd: <#>On July 29th a *.google.com certificate issued was discovered that was not revoked before. This certificate was revoked on July 29th.¶

On August 30th Fox-IT was asked investigate the incident and recommend and implement new security measures. Fox-IT installed a specialized incident response network sensor to assist in the investigation. Furthermore we created images of several other servers.

2.2 Monitoring

The rogue certificate found by Google was issued by the DigiNotar Public CA 2025. The serial number of the certificate was, however, not found in the CA system's records. This leads to the conclusion that it is unknown how many certificates were issued without any record present. In order to identify these unknown certificates and to prevent them from being used by victims, the OCSP responder[2] requests were monitored.

Current browsers perform an OCSP check as soon as the browser connects to an SSL protected website through the https-protocol[3]. The serial number of the certificate presented by the website a user visits is sent to the issuing CA OCSP-responder. The OCSP-responder can only answer either with 'good', 'revoked' or 'unknown'. If a certificate serial number is presented to the OCSP-responder and no record of this serial is found, the normal OCSP-responder answer would be 'good'[4]. The OCSP-responder answer 'revoked' is only returned when the serial is revoked by the CA. In order to prevent misuse of the unknown issued serials the OCSP-responder of DigiNotar has been set to answer 'revoked' when presented any unknown certificate serial it has authority over. This was done on September 1st.

Verwijderd: d

The incident response sensor immediately informs if a serial number of a known fraudulently issued certificate is being misused. Also, all unknown serial number requests can be analysed and used in the investigation. A large number of requests to a single serial number is suspicious and will be detected.

Verwijderd: ll

[2] The **Online Certificate Status Protocol** (**OCSP**) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
[3] Other applications using certificates can also use the OCSP verification method.
[4] According to the RFC2560

Note that advanced methods for misusing the rogue certificates are possible by which a thorough attacker can circumvent our detection method.

The incident response sensor logged all network traffic since August 30th. Current analyses still show hacking attempts on the web server originating from Iran. During monitoring, we also saw unusual traffic after the company F-Secure announced its findings of a possible earlier breach of the website.[5] We haven't investigated this breach yet in detail. In August, DigiNotar installed a new web server. It's fair to assume these hacker traces where copied from the previous web server install.

2.3 CA servers investigation

DigiNotar hosts several CA services on different servers. Earlier reports indicated two of these servers where compromised and misused by the attacker(s). It was essential to verify the status of the other CA systems and investigate if they were compromised or misused. Forensic disk images were made of all the CA servers for investigation.

Because of security implications, the details of these results are not shared in this public report. More generally, we found traces of hacker activity with administrator rights on the Qualified and PKIoverheid CA server as well as on other CA servers. Furthermore, we can share that on September 3rd more rogue certificates were discovered. The list of certificates is in the Annex 5.1.

The log files on the Qualified & PKI Overheid CA server do not show traces of deleted entries. These traces are present on other CA servers, where rogue certificates were produced. During further investigation however, we encountered several serial numbers of certificates that cannot be related to trusted certificates. Two of these were found on the Qualified & PKI Overheid CA server. It might be possible that these serial numbers have been temporarily generated by the CA software without being used. Alternatively, these serials were generated as a result of a bug of the software. However, we cannot rule out the possibility that these serial numbers relate to rogue certificates. Further investigation needs to be done to confirm or contradict this. The list of serials is in the Annex 5.2; this list has been communicated with the web browser vendors.

2.4 Firewall investigation

The firewall log files have not been analysed yet.

2.5 Malicious software analyses

A number of malicious/hacker software tools was found. These vary from commonly used tools such as the famous Cain & Abel tool[6] to tailor made software.

Specifically developed software probably enabled the hackers to upload the generated certificates to a dropbox. Both the IP-addresses of an internal DigiNotar server and the IP-address of the dropbox were hardcoded in the software. Possibilities are being explored to investigate this server, as (parts of) the uploaded rogue certificates might be still available there.

A script was found on CA server public 2025. The script was written in a special scripting language only used to develop PKI software. The purpose of the script was to generate signatures by the CA for certificates which have been requested before. The script also contains English language which you can find in Annex 5.3. In the text the hacker left his fingerprint: *Janam Fadaye Rahbar*[7]*.* The same text was found in the Comodo hack in March of this year[8]. This breach also resulted in the generation of rogue certificates.

[5] The IT-Security company F-Secure blogs about a breach of the webserver of DigiNotar in May 2009. http://www.f-secure.com/weblog/archives/00002228.html

[6] Cain&Abel is a very powerful hackers toolkit. It's capable of sniffing and breaking passwords. Most anti-virus software will detect C&A and flag it as malicious.

[7] Supposedly meaning: "I will sacrifice my soul for my leader"

[8] http://www.wired.com/threatlevel/2011/03/comodo_hack/

Verwijderd: s

3 Provisional results

3.1 Fraudulent issued certificates

In total 531 fraudulent certificates have been issued. We have no indication that more certificate were issued by the attacker(s). 344 Of these contain a domain name in the common name. 187 Certificates have in the common name 'Root CA'. We have reason to believe these certificates are not real CA certificates but normal end user certificates.

3.2 Compromised CAs

The attacker(s) had acquired the domain administrator rights. Because all CA servers were members of the same Windows domain, the attacker had administrative access to all of them. Due to the limited time of the ongoing investigation we were unable to determine whether all CA servers were used by the attacker(s). Evidence was found that the following CAs *were* misused by the attacker(s):

- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- Koninklijke Notariele Beroepsorganisatie CA
- Stichting TTP Infos CA

The security of the following CAs was compromised, but no evidence of misuse was found (this list is incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Qualified CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association
- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TU Delft CA

For some of these CAs extra security measures were in place (like the CCV CA). This makes it more unlikely they were misused.

3.3 Misuse

We investigated the OCSP responder log files around the time of the *.google.com incident. That incident was detected on August 27th. The first known public mention was a posting in a google forum. The user (from Iran) was warned by the Google Chrome browser that there was something wrong with the certificate. The corresponding rogue certificate was created on July 10th.

Based on the logging mentioned above from the OCSP responder, we were able to extract the following information. On August 4th the number of request rose quickly until the certificate was revoked on August 29th at 19:09. Around 300.000 unique requesting IPs to google.com have been identified. Of these IPs >99% originated from Iran, as illustrated in figure 1.[9]

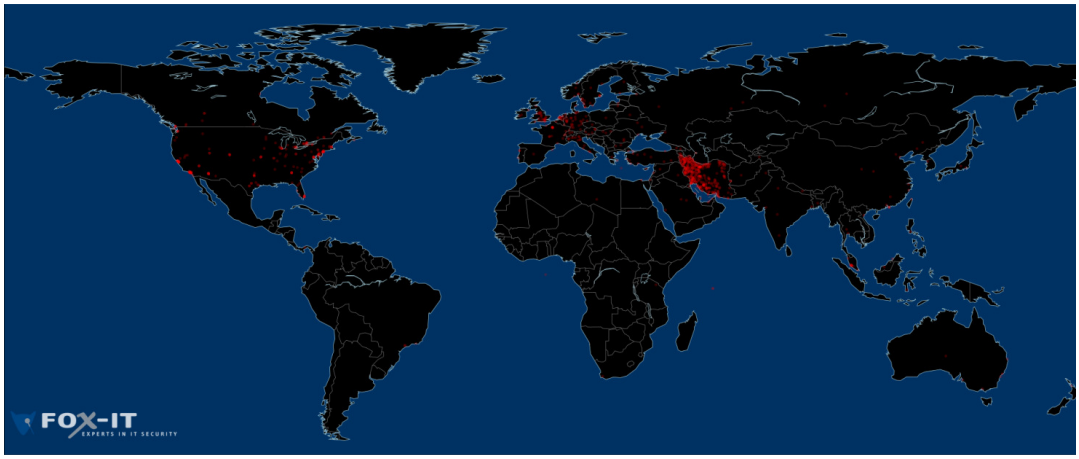


Figure 1: OCSP requests for the rogue *.google.com certificate

A sample of the IP's outside of Iran showed mainly to be TOR-exit nodes, proxies and other (VPN) servers, and almost no direct subscribers.

The list of IP-addresses will be handed over to Google. Google can inform their users that during this period their e-mail might have been intercepted. Not only the e-mail itself but also a login cookie could have been intercepted. Using this cookie the hacker is able to log in directly to the Gmail mailbox of the victim and also read the stored e-mails. Besides that, he is able to log in all other services Google offers to users like stored location information from Latitude or documents in GoogleDocs. Once the hacker is able to receive his targets' e-mail he is also able to reset passwords of others services like Facebook and Twitter using the lost password button. The login cookie stays valid for a longer period. It would be wise for all users in Iran to at least logout and login but even better change passwords.

Other OSCP request logs show some activity on August the 30th with a misused *.torproject.org certificate. None of these originated from Iran. However this does not prove that rogue certificates weren't abused between the issue date and revocation date of the certificates based on the OCSP logs because some applications might not use the OCSP protocol for revocation checking.

[9] This static image shows all IP-addresses detected. On http://www.youtube.com/watch?v=wZsWoSxxwVY you can see the interception of Google users taking place in a timeline.

Verwijderd: http://www.youtube.com/watch?v=_eIbNWUyJWQ

4 Discussion

4.1 Skills and goal of the hackers

We found that the hackers were active for a longer period of time. They used both known hacker tools as well as software and scripts developed specifically for this task. Some of the software gives an amateurish impression, while some scripts, on the other hand, are very advanced. In at least one script, fingerprints from the hacker are left on purpose, which were also found in the Comodo breach investigation of March 2011. Parts of the log files, which would reveal more about the creation of the signatures, have been deleted.

The list of domains and the fact that 99% of the users are in Iran suggest that the objective of the hackers is to intercept private communications in Iran.

4.2 Other possible rogue certificates

Using the OCSP responder requests we verify if the requested serial belongs to a known certificate. We have seen requests for unknown serials that cannot be matched against a known certificate. It's possible that these serials belong to a "rogue" certiticate or are just bogus OCSP requests, for instance done by security researchers. It's still possible other unknown[10] rogue certificates have been produced.

OCSP logging could still catch other possible rogue certificates based on the number of requests for an unknown serial, although it's difficult to match the common name with that serial if the certificate in question is not known.

4.3 Trust in the PKIoverheid and Qualified environment

Although all CA-servers have been accessed by a hacker with full administrative access rights and attempts have been made to use the running PKI-software we have no proof of generated rogue Qualified or PKIoverheid certificates. The log files of these CA-Servers validate as correct and no deleted log files have been found on these CA-servers. This is in contrast to our findings on the other breached CA servers.

Investigators encountered two (2) serial numbers of certificates on the Qualified or PKIoverheid server that cannot be related to trusted certificates[11]. Based on this, we cannot rule out the possibility that these relate to rogue certificates.

4.4 Current network infrastructure at DigiNotar

The successful hack implies that the current network setup and / or procedures at DigiNotar are not sufficiently secure to prevent this kind of attack.

The most critical servers contain malicious software that can normally be detected by anti-virus software. The separation of critical components was not functioning or was not in place. We have strong indications that the CA-servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the management LAN.

The network has been severely breached. All CA servers were members of one Windows domain, which made it possible to access them all using one obtained user/password combination. The password was not very strong and could easily be brute-forced.

The software installed on the public web servers was outdated and not patched.

No antivirus protection was present on the investigated servers.

An intrusion prevention system is operational. It is not clear at the moment why it didn't block some of the outside web server attacks. No secure central network logging is in place.

[10] Unknown as in, that we haven't been able to revoke them yet because we don't know their existence.
[11] OCSP requests to these serial numbers will result in a 'revoke' reply.

5 Appendix

5.1 Fraudulent issued certificates

The following list of Common Names in certificates are presumed to be generated by the attacker(s):

Common Name	Number of certs issued
CN=*.*.com	1
CN=*.*.org	1
CN=*.10million.org	2
CN=*.JanamFadayeRahbar.com	1
CN=*.RamzShekaneBozorg.com	1
CN=*.SahebeDonyayeDigital.com	1
CN=*.android.com	1
CN=*.aol.com	1
CN=*.azadegi.com	1
CN=*.balatarin.com	3
CN=*.comodo.com	3
CN=*.digicert.com	2
CN=*.globalsign.com	7
CN=*.google.com	26
CN=*.logmein.com	1
CN=*.microsoft.com	3
CN=*.mossad.gov.il	2
CN=*.mozilla.org	1
CN=*.skype.com	22
CN=*.startssl.com	1
CN=*.thawte.com	6
CN=*.torproject.org	14
CN=*.walla.co.il	2
CN=*.windowsupdate.com	3
CN=*.wordpress.com	14
CN=Comodo Root CA	20
CN=CyberTrust Root CA	20
CN=DigiCert Root CA	21
CN=Equifax Root CA	40
CN=GlobalSign Root CA	20
CN=Thawte Root CA	45
CN=VeriSign Root CA	21
CN=addons.mozilla.org	17
CN=azadegi.com	16
CN=friends.walla.co.il	8
CN=login.live.com	17
CN=login.yahoo.com	19
CN=my.screenname.aol.com	1
CN=secure.logmein.com	17
CN=twitter.com	19
CN=wordpress.com	12
CN=www.10million.org	8
CN=www.Equifax.com	1
CN=www.balatarin.com	16
CN=www.cia.gov	25
CN=www.cybertrust.com	1
CN=www.facebook.com	14
CN=www.globalsign.com	1
CN=www.google.com	12
CN=www.hamdami.com	1
CN=www.mossad.gov.il	5
CN=www.sis.gov.uk	10
CN=www.update.microsoft.com	4

Met opmaak: Aantal kolommen: 1

5.2 Unknown serial numbers

Root-CA server

On the 'Root-CA' server the following serials were encountered:

```
83120A023016C9E1A59CC7D146619617
68E32B2FE117DFE89C905B1CCBE22AB7
711CE18C04232184255l0EF51513B7B8
B7ABEFC8A1F844207B774C782E5385B3
6E0088D11C7E4E98CC9E0694D32A0F6B
80C990D339F177CA9FDAC258105882AB
7F73EC0A14C4BA065BECFAD69DC5A61D
```

Qualified-CA server

On the 'Qualified-CA' server the following serials were encountered:

```
C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4
```

These serials might have been issued by the following CAs:

- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven

'Taxi-CA

On the 'Taxi-CA' server the following serials were encountered:

```
25B6CA311C52F0E4F72A1BD53774B5B3
A0CF459D0D1EA9A946861A0A02783D88
71A10FA4C491D3A72D18D33E3CCF576C
FE456B099700A6C428A193FE5968C9FD
E7E2B46B8C9AA64679E03841F88CA5A0
AEC9F2324D80020B6E2B2A1103D6A4E8
CB20C25F14583AFC86465F14E621FBC1
947FF1DB66A41D809A9BC7E7344E342A
90BCA541B4DF5E77FB1349684F84A930
AB4967CE8B94FCF8DA7691922E6FD59C
BA479991C9103C005726FAB83088A8D6
363E9AAF4DAC7085F31B89B2AC49059A
8A63042B8A8FA256035773BC9417435A
963CCB2601B15C73DCA821F4BC4C7458
6B7057D5DE0170842C372821D3F17DB2
C391438C15FF31BD89544A7F68DDF3B3
7278CB2A8270A3E66A021A7CD75F1211
F401D4C50FCA9161A70ED9D91D40E684
6C396359C423417E20C54CFC6690F3FF
9916C8350225BB607857375A02B6DC72
0F48A14121370B5CF4828EF826749FBC
DB43E2CE6110750785FCBBE9A8EAE061
C641E4B7F19B63C4FF1EA6D3833FC874
D8B771F90BC01C9ED1333C23EF24CFC1
```

'Public-CA server

On the 'Public-CA' server the following serials were encountered:

```
79C03FE0C81A3022DBF8143B27E40223    8B0EABAF922D4C6E6917FCBE365DD64A    82C42F0EDC18BD751727BE5C54413EF7
FCCF53CB3D0A71494AF9664690FFCF84    4FC2D72D6427CABBE3E859453865F43B    03124C25849D9E49BC2A2FAD3E10C8A4
82BC18B1AA5D59C61D0EFDBEA7664C08    53B53BF2F74997EBEB2577D63DA692B7    EFF0DD4B4927DF64232C5D2FF280C1E4
5D4352671C39616670B2F34C173A1F63    ABB21F43553F2695031A1C85355D7F1C    9EDCB5E1FE1255A2F1D7FC52C4AFA3B1
6FA3C48173B3B289943F113A8CD9DB8C    5563605FDC2DC865E2A1C32995B5A086    3A32AAA9DFE2CA7F9E003885E316944B
CFAF9BE4E5BD0F5A75F628E45E0178C9    5DD6A72747D90C018B63F959DFE7C976    4455B43B9173CBAE4E247272EE2573D5
4ADA28D281D3D14D19FB782D64086D0C    CAB736FFE7DCB2C47ED2FF88842888E7    B95F62E86194734C9F68D4BF8B200C49
0B41ABEE6F4168D3CDE5A7D223B58BC1    9C79C9FE16727BAC407B4AA21B153A54    FE873B742B230B22AE540E840490A2F4
13548FC160BC5C9F315AE28CDB490E36    2D711C9CB79EC15445747BFE3F8BC92F    8779917563EC38B7746B8ECAFE239BE6
5D8D0D43611275982E6A5490E7F87BD7    752A2D0325A3D34D9F5198C2F5C92A6C    72CBC4824C6215B139FDE6BA10DAC6AD
C880AE4D7927E6A8FA7D456CB03E9763    39936336286F843756FC4BC296D7A8E0    8D09D4B98DE67C9E9C7C18CB72AD2418
82072FC8F8DD7E6C0ECE9B47185F0521    4A6D90618A5CA6797C768C03C860C4F8    07BC72A463D4DE33B2BE733D6FAC991D
90DB656E273476CC8367782555582FA8B   0954E1AB9141ED7E8B640FE681046451    D3E2205C3B899FC99D77FE802985283F
171A8599EDE711A3315BC7D694CEBEC6    8259C3E1DB6C2C9B7FCD6A305EADEFE4    A5029D6A057D50D20ECFE0E528EDA067
E9EB8075F7FE3683B431552C2D962CB0    BC01852405D3F4E22C486002666550 26    C8B2487ADFAF969E34306029AC934406
E6F9E095464F64448840A832FB3443DB    9F7DDFE3CAAD224EC6BD68B60DE78550    5F3C1BDC7A2BCD47ABAF0C8E62D9F757
C83D16E9CB29DCF35F3B351CB942FE0D    A67C22A6E1F9D87799548EBFC7D5527E    601315BB085FECF29538DA3F9B7BA1CE
39B5DD0ECC85C3F62A72391DC055F561    11661878CCE9DC337CEEBB16E30F9A3A    30170F15A240446E6B482E0A364E3CCA
DF3FD6AFBBFBC30C9AD80BF764A102DB    6BF3BEB26AFF31116200B14F4378C33B    0590B310AEFC7A3EDC03ECA2A6F6624F
327B9A443C49018D7B0A97B6EC2254B8    7A61A7778842E502E2291166C4574485    FDEB145AAC81B8CD29B8DA018E71456F
```

```
C3F9F45F19E334C8303F44288856D843
028CF7556F8BE27026800448FA6AA527
E93B28B47C34B243EBA62E58FE2FF46F
F89F5DE575755A3B4C0DECC6EDA7C804
5D8F8D78B0C19EF4479F744DECBD84BC
EAACDC2F46D4A86F39B035B793F4A94F
9D06313F21A4EDF734C324FFBCB9E2B5
35C54E845AE855F818504C8C189F52C7
E3E120935934CBD77E1DA7F00431F745
0A6DFACFDEAE74A816031534BE90B75A
9AD82BE2FED538B10BDFBD229A8A5AEA
C0F216CA8197AD00F0D98927EAE29E64
DE76B17BFB1B6D6D6634C8C104A6E59F
A90F1BB43E9DB5EDFC60C15FB897C593
8625B32398C2722D96E7B972580A0238
D1FDE3A78C9D2E80C2303CC4E3E92A4C
B355E909FD55C5E9EF1A6E67E9C18203
ADB59A303C6260DBE466F0149AB11A4A
5CEBD524469A075FB6B42D06C9BF27AD
0E0886EEAA119CF14F1C54387060929A
B4F9299F05A327E60543C4CDE3277FC0
E4B2F09505726306314DF05B734FD9D0
4DD0497CBAABBA058574A611B26151BA
7073C6C01DEE4E158F554555F697F7D9
EB72415ECD0B4AACBDEEA3734F4349BF
BED90D98FA3A1E0A5BD78AD54E55774D
3CDCD81930F91AC0B990664931E5412E
763B0C2A7B83066A9D995C8C4FD9E35E
720DF591261D710ADC73127C1BC4303D
C06C12DBBC7055FE40950803238EC104
62BF5A170CC779ADE7EF0090F395D5E6
61BF9A0FF2CE9D55D86BC063839F72F4
B5D7A148CA6C1F9693A2C16ACDD66226
35FBDCDF923F99B5E1C5FF4423B715B8
F1EBE73557546DC8B21E0A2DE5E3A33E
EBE7561CA573DA5DBB8EFAA250A40FD3
6BACB6C5B74FA747A3CF375EC3095035
6C1950AA83F4663F1BA063B5275C25EC
56EF1EE54D65EF7B39AF541E95BB45A9
2B1EA767EC59E46364BC2DF9B1F30B97
3913B1E1C35BDDF02CE03C916E8AA638
AFA2F7E964280B36DB0D714B86256F54
022E35B1ACD40F040C444DF32A7B8DE6
170370B60D515F164119BE54FD55E1ED
CBFE437C9B62805C4353516699E44649
5FFA79AB76CE359089A2F729A1D44B31
5298BCBD11B3952E3FDDC6FDD6711F5C
1836289F75F74A0BA5E769561DE3E7CD
DEB427AC9F1E8A0D0237049C80DF7E7F
FD8FE350325318C893AFE03F9DFC7096
A8031D608F6549941879981764674DD7
DDAD29B8B1215191E7EB5AAEE0219338
3F8A5EA1756DDF4A6B6F2645B4911486
30DF96D87EEC8CA77A135ECCAB1AD25E
7DD8E0E1906C1754E11E901927CCABBD
DAC51C3D23B163601305AF99DF129689
D77EC92400AE0D9FA57DEF4DD8CFA4D4
09369288E36D7AFFEE94EA81998FA316
EEBE1885532234328919191 3F6D769EB
C00132DA154BDEE361EDEE727226D0F5
6580BE22A0566352B9622777BFCB7164
7352C61297D6B04E874EDAD12480F78E
F658C0D52B3EEF71DDE6C284E7E1B337
E1253D04A17AB8E47F4A5916B9BF9D23
8922A9A23BE960FFE9707A0B3F4D75BD
EAE97F465015E49A14F3B23403ACFA11
13A757022817C0514A5C142FE9BF143A
5132F0FCB3F8DCAA501C620575D33FEE
39953BF6383A00D29BEB377568E3DE7A
67887932934DFF086153CA905E7DE9EE
DCD1072719692871126E4159D80EFDA8
C6741E3D08C0FFD4617B94E654DD89F1
D0BA58BA609CC1A001F612987A822BEF
6B339433956F1505104BB231314A153E
C1366C7246041A3089E1C244C5DC42E7
61D11B35765ECB85890D5349786D9FCA
44C287C1C3697367B0E6CB78A78C1DF5
DAACF72BC91FB6DA90A804933CB72E23
2ACBA14BB6F65F7BD0A485BFCB6D023F
84BE5D762F37E9018D623C8E91F4D924
1A89324D6D3E6DE6726C688BFF225DDD
F5FA42A5B421705E4803DA93C4F7E099
A869B96BCDF1D474C0714763AA34A8C9
3EA0F90DE57187FC7E1AC45AE44D16C6
F7DE638B76C3958AA3413A9785A19900
3F8C9CDAACBB533AE94F47456819FA0E
209920C169512D3EB4A1ED7CAD17D033
B2F57BD01BAAF7AF01EF442910CEBBA0
C0766829AA4D2E1A5D97213A4E4A654E
FC9993EA7A4E761B6CB79ABE2BD3CDE1
4D556B338FAA020979A740B4C3AEE28C
8ED896B9A622FF24559A3429E5888E0A
8CF1F45323EC5AB449451E7A9476CFDC
D1718E9BD91257D2169C81197D508A67
E4A691D60266784968DF971D6BF473AF
B3B64F1925F759A2E145190333D1D6D2
ED4C2EBC14B85F46A9A75F159DF8BEB3
CDBC0441C10DB5ABA43120E63A048425
DC1665266A0198728861AC99ED368928
706BBC770C62D41DD799721ABD1868AB
B2205D8CBDDFE49D7C5F0F95D506718F
901F30DB86EEB1666F5A8CAE1C7BD08B
9A3A951BE27E0729726FD8B80060E7E1
6410577C738133297472F6C22C2BB397
C8C06B0C6B7FE7CA66BCFE617AB6C4E6
58C18B290620E18B8C78AC1912E5DCD7
2F5ABFDCCAB1A2927E54283296F19FB8
A07CB7881E35C91FD9C5D20F6102572C
05E2E6A4CD09EA54D665B075FE22A256
8BA800DDDD865B6BF3A85ADEC4C29730
07B546E8E002FC5854651BE31802F96D
DF2AD7F766E2EEFAF0FD1FB5C6883AB4
1C6EA2DA6ECED5C5C761BCA9CA4C5308
A640A29E706AF38557B86619EAF45E7A
F88885670C3D55EBA52096A65310DACA
B85E7BB83667097F15D8A3DEAAA1B198
A5F6F149B468683318DC178F4208E237
04841B82A9D81E44CB4F2D98CFE7C374
A81686CEFDEFFCE82B8DBF100E1395F1
9952073595776A3D7A8101664A56AB96
A076DA72A8C8E2137F05FE3FA59870EB
121378A6DE0A13DDB295106E912A4E14
65A925E578098658FADA30E9FB67B5E4
5B8E5202EC6769F2389605D33DC245B2
EA71F746BD17D1B05450329818572F2E
DD8C315D2CA61870CBCF9D56ED7474E2
F346A1E62FED476F472560C6DDE0CADC
CBBCB9E06F9FC92C533B2F2A5284BA22
79DCFDA2700E06F8EAA640BA9B827810
17CF5474D5A8B4E735E69E017CEC2F37
7034FBF641CEB257FC109A6819D19DA0
6E6D052B5ABC015C779EA3500FA11A28
FAB79682C8EAE556F11ECF6DAD7121BA
0370390E48A7F26AA62188A79E612DC3
59F8BDDA3F56D8026FAB6E3130F5D843
C731140FAA7690918BABF17BECB7938D
8C605DFAA0EC88CDB7D12F7250C9F53A
68F252CD36F2798A2182F6406A31A5A2
BD7CB0D124DFDE784CD5B9EF288C304E
3D2BC95A85EF539A68DAC84542A1AE7A
8CC74931E64061491652CC169C8BAAB3
4157D99E46A3E45E6130A95645410DAC
E34C4FC7488C4DFEF0EA475A17AF2C7B
```

These serials might have been issued by the following CAs (list incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- DigiNotar Qualified CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- Koninklijke Notariele Beroepsorganisatie CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association

- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- Stichting TTP Infos CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TU Delft CA

5.3 Plain text left in script to generate signatures on rogue certificates

```
I know you are shocked of my skills, how i got access to your network
to your internal network from outside
how I got full control on your domain controller
how I got logged in into this computer
HoW I LEARNED XUDA PROGRAMMING
HOW I got this IDEA to write such XUDA code
How I was sure it's going to work?
How i bypassed your expensive firewall, routers, NetHSM, unbreakable hardware keys
How I did all xUDA programming without 1 line of resource, got this idea, owned your
 network accesses your domain controlled, got all your passwords, signed my certificates
 and received them shortly
THERE IS NO ANY HARDWARE OR SOFTWARE IN THIS WORLD EXISTS WHICH COULD STOP MY HEAVY
 ATTACKS
MY BRAIN OR MY SKILLS OR MY WILL OR MY EXPERTISE
That's all ok! EVerything I do is out of imagination of people in world
I know you'll see this message when it is too late, sorry for that
I know it's not something you or any one in this world have thought about
But everything is not what you see in material world, when God wants something to happen


My signature as always: Janam Fadaye Rahbar


Rahbare azizam mesle hamishe asoode bash, ta vaghti ke man va amsale man baraye in marzo
 boom
va baraye barafrashte negah dashtane parchame velayate faghih kar mikonand
daste har doshmano mozdouri ghat khahad bood
Rahbaram, Tamame vojoodam fadaye to ke ham jani o ham janani
```

5.4 Timeline

06-Jun-2011	Possibly first exploration by the attacker(s)
17-Jun-2011	Servers in the DMZ in control of the attacker(s)
02-Jul-2011	First attempt creating a rogue certificate
10-Jul-2011	The first succeeded creation of rogue certificate (*.Google.com)
19-Jul-2011	Incident detected by DigiNotar by daily audit procedure
20-Jul-2011	Last known succeeded rogue certificate was created
22-Jul-2011	Last outbound traffic to attacker(s) IP (not confirmed)
22-Jul-2011	Start investigation by IT-security firm (not confirmed)
27-Jul-2011	Delivery of security report of IT-security firm
27-Jul-2011	First rogue *.google.com OSCP request
28-Jul-2011	First seen that rogue certificates were verified from Iran
04-Aug-2011	Start massive activity of *.google.com on OCSP responder
27-Aug-2011	First mention of *.google.com certificate in blog
29-Aug-2011	GOVCERT.NL is notified by CERT-Bund
29-Aug-2011	The *.google.com certificate is revoked
30-Aug-2011	Start investigation by Fox-IT
30-Aug-2011	Incident response sensor active
01-Sep-2011	OSCP responder based on white list

Verwijderd: 19-Jun-2011 ... [1]

Verwijderd: UND

19-Jun-2011 Incident detected by DigiNotar by daily audit procedure

Van: [redacted]@fox-it.com]
Verzonden: dinsdag 4 oktober 2011 7:58
Aan: [redacted]
CC: [redacted](Fox-IT);[redacted]
Onderwerp: RE: Rapport 1.1 draft 2

Beste [redacted]

We zullen deze vraag expliciet meenemen in de vraagstelling. In deze versie van het rapport kunnen we die echter niet meenemen omdat we nog met het onderzoek daarover bezig zijn.

Mvg,

[redacted]

Van: [redacted]- Logius [mailto:[redacted]@logius.nl]
Verzonden: maandag 3 oktober 2011 16:37
Aan: [redacted]
CC: [redacted](Fox-IT);[redacted]
Onderwerp: RE: Rapport 1.1 draft 2

[redacted]

In deze versie van het rapport graag ook expliciet een passage opnemen over de WBP aspecten. Waar men zich vanuit het CBP zorgen over maakt is in hoeverre klant informatie (mogelijk) naar buiten is gegaan. Kun je hier ook apart wat over opnemen?

[redacted]

Van: [redacted] Logius
Verzonden: woensdag 28 september 2011 17:07
Aan: [redacted]
CC: [redacted](Fox-IT);[redacted]
Onderwerp: RE: Rapport 1.1 draft 2

[redacted]

Zoals net besproken blijkt het voorliggende rapport niet dezelfde informatie te bevatten als die OPTA heeft gebruikt in haar besluitvorming. In de rechtzaak gisteren gaf men aan dat er vanaf de qualified CA's is gecopieerd. In het rapport staat echter dat er geen bewijs is dat er wat verwijderd is.

Subtiel verschil, maar er blijkt dus een verschil in info te zijn die OPTA heeft ontvangen van Fox-it t.o.v. de voorliggende versie.

Gaarne deze discrepantie zsm gelijktrekken.

[redacted]

Van: [redacted][mailto:[redacted]@fox-it.com]
Verzonden: donderdag 22 september 2011 15:18
Aan: [redacted]- Logius;[redacted](Fox-IT);[redacted]@diginotar.nl);[redacted]

[redacted]@diginotar.nl); [redacted]
Onderwerp: Rapport 1.1 draft 2

Hallo,

Bijgevoegd wat kleine aanpassingen in het rapport met track changes. Het betreft de correctie op de datums en een kleine toevoeging van informatie die ook aan OPTA is verstrekt. Graag jullie opmerkingen of aanvullingen.

Met vriendelijke groet,

[redacted]
Security Expert

Fox-IT Experts in IT Security!

Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands

T +31 (0)15 2847[redacted]
F +31 (0)15 2847990
I www.fox-it.com

KvK Haaglanden 27301624

Van: [redacted]@diginotar.nl]
Verzonden: vrijdag 23 september 2011 11:25
Aan: [redacted]
CC:
Onderwerp: RE: Rapport 1.1 draft 2

Ik denk niet dat het nog de taak is van [redacted] of mij om te reageren op deze aanpassingen.
Dat is kennelijk in handen van de curator.
Ik zou de curator willen aanraden bezwaar te maken tegen publicatie van nog meer vertrouwelijke security gegevens zoals aan deze (publieke) versie is toegevoegd.

[redacted]
Manager [redacted]

DigiNotar
A GD VASCO COMPANY

T +31 (0)251 268888
F +31 (0)251 268800
M+31 (0)6 [redacted]
info@diginotar.nl
www.diginotar.nl

Van: [redacted] [mailto:[redacted]@fox-it.com]
Verzonden: donderdag 22 september 2011 15:18
Aan: [redacted] - Logius; [redacted] (Fox-IT); [redacted]
Onderwerp: Rapport 1.1 draft 2

Hallo,

Bijgevoegd wat kleine aanpassingen in het rapport met track changes. Het betreft de correctie op de datums en een kleine toevoeging van informatie die ook aan OPTA is verstrekt. Graag jullie opmerkingen of aanvullingen.

Met vriendelijke groet,

[redacted]
Security Expert

Fox-IT Experts in IT Security!

Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands

T +31 (0)15 28479[redacted]
F +31 (0)15 2847990
I www.fox-it.com

KvK Haaglanden 27301624

FOX-IT
EXPERTS IN IT SECURITY

Interim Report

September 5, 2011

DigiNotar Certificate Authority breach
"Operation Black Tulip"

Classification **PUBLIC**

Customer DigiNotar B.V.

Subject: Investigation DigiNotar Certificate Authority Environment

Date 19 September 2011
Version 1.1
Author J.R. Prins (CEO Fox-IT)
Business Unit Cybercrime
Pages 16

Verwijderd: 5
Verwijderd: 0
Verwijderd: 13

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

1 Document Management

Version management

This version replaces all previous version of this document. Please destroy all previous copies!

Distribution list

Copy	Distribution (version)	Name/function/remarks

Review management

Review by	Function	Date	Version

Change management

Version	Date	By	Remarks	Approval
1.0	05-sep-2011	J.R. Prins		
1.0a	05-sep-2011	J.R. Prins	Minor layout changes	
1.1		J.R. Prins	Rectification of dates, minor addition of details	

Related documents

Version	Date	Description	Remarks

Table of Contents

Met opmaak: Standaard

2 Introduction

2.1 Background

The company DigiNotar B.V. provides digital certificate services; it hosts a number of Certificate Authorities (CA's). Certificates issued include default SSL certificates, Qualified Certificates and 'PKIoverheid' (Government accredited) certificates.

On the evening of Monday August 29th it became public knowledge that a rogue *.google.com certificate was presented to a number of Internet users in Iran. This false certificate had been issued by DigiNotar B.V. and was revoked[1] that same evening.

On the morning of the following Tuesday, Fox-IT was contacted and asked to investigate the breach and report its findings before the end of the week.

Fox-IT assembled a team and started the investigation immediately. The investigation team includes forensic IT experts, cybercrime investigators, malware analysts and a security expert with PKI experience. The team was headed by CEO J.R. Prins directly.

It was communicated and understood from the outset, that Fox-IT wouldn't be able to complete an in-depth investigation of the incident within this limited timeframe. This is due to the complexity of the PKI environment and the uncommon nature of the breach.

Rather, due to the urgency of this matter, Fox-IT agreed to prepare an interim report at the end of the week with its preliminary findings, which would be published.

2.2 Investigation questions

The investigation predominately focused on following questions:

1. How did the perpetrators access the network?

2. What is the scope and status of the breach?
   - *Have other DigiNotar CA environments been breached?*
   - *Do we still see hacker activity on the network of DigiNotar?*
   - *Are rogue certificates actively being used by hackers?*

3. Can we discover anything about the impact of the incident?
   - *What certificates were issued without knowledge of DigiNotar?*
   - *What other (rogue) certificates might have been generated?*
   - *How many rogue connections were made using rogue certificates?*
   - *What was the nature of these connections?*

In order to address these questions we (basically) (i) implemented specialized monitoring to be able to detect, analyse and follow up on active misuse, and (ii) analysed digital traces on hard disks, and in databases and log files to investigate the origin and impact of the breach.

[1] Revoked: A certificate is irreversibly revoked if, for example, it is discovered that the certificate authority (CA) had improperly issued a certificate, or if a private-key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements such as publication of false documents, mis-representation of software behavior, or violation of any other policy specified by the CA operator or its customer. The most common reason for revocation is the user no longer being in sole possession of the private key (*e.g.*, the token containing the private key has been lost or stolen).

2.3 This report

The goal of this report is to share relevant information with DigiNotar stakeholders (such as the Dutch Government and the Internet community), based on which they can make their own risk analysis. Because this is a public report, some investigation results and details cannot be included for privacy and/ or security reasons.

Since the investigation has been more of a fact finding mission thus far, we will not draw any conclusions with regards to the network-setup and the security management system. In this report we will not give any advice to improve the technical infrastructure for the long term. Our role is to investigate the incident and give a summary of our findings until now. We leave it to the reader in general and other responsible parties in the PKI- and internet community to draw conclusions, based on these findings. We make a general reservation, as our investigations are still ongoing.

Verwijderd:

3 Investigations

3.1 Prior investigations

Some investigations were conducted before we started.

Fox-IT was given access to a report produced by another IT-security firm which performs the regular penetration testing and auditing for DigiNotar. The main conclusions from this report dated July 27th were:

> A number of servers were compromised. The hackers have obtained administrative rights to the outside webservers, the CA server "Relaties-CA" and also to "Public-CA". Traces of hacker activity started on June 17th and ended on July 22nd.

Furthermore, staff from DigiNotar and the parent company Vasco performed their own security investigation. E-mail communication and memos with further information were handed over to us.

This information gave us a rough overview of what happened:

- The signing of 128 rogue certificates was detected on July 19th during the daily routine security check. These certificates were revoked immediately;
- During analysis on July 20th the generation of another 129 certificates was detected. These were also revoked on July 21th;
- Various security measures on infrastructure, system monitoring and OCSP validation have been taken immediately to prevent further attacks.
- More fraudulent issued certificates were discovered during the investigation and 75 more certificates were revoked on July 27th.
- DigiNotar found evidence on July 28th that rogue certificates were verified by internet addresses originating from Iran.
- On August 29th a *.google.com certificate issued was discovered that was not revoked before. This certificate was revoked on August 29th.

Verwijderd: <#>On July 29th a *.google.com certificate issued was discovered that was not revoked before. This certificate was revoked on July 29th.¶

On August 30th Fox-IT was asked investigate the incident and recommend and implement new security measures. Fox-IT installed a specialized incident response network sensor to assist in the investigation. Furthermore we created images of several other servers.

3.2 Monitoring

The rogue certificate found by Google was issued by the DigiNotar Public CA 2025. The serial number of the certificate was, however, not found in the CA system's records. This leads to the conclusion that it is unknown how many certificates were issued without any record present. In order to identify these unknown certificates and to prevent them from being used by victims, the OCSP responder[2] requests were monitored.

Current browsers perform an OCSP check as soon as the browser connects to an SSL protected website through the https-protocol[3]. The serial number of the certificate presented by the website a user visits is sent to the issuing CA OCSP-responder. The OCSP-responder can only answer either with 'good', 'revoked' or 'unknown'. If a certificate serial number is presented to the OCSP-responder and no record of this serial is found, the normal OCSP-responder answer would be 'good'[4]. The OCSP-responder answer 'revoked' is only returned when the serial is revoked by the CA. In order to prevent misuse of the unknown issued serials the OCSP-responder of DigiNotar has been set to answer 'revoked' when presented any unknown certificate serial it has authority over. This was done on September 1st.

Verwijderd: d

The incident response sensor immediately informs if a serial number of a known fraudulently issued certificate is being misused. Also, all unknown serial number requests can be analysed and used in the investigation. A large number of requests to a single serial number is suspicious and will be detected.

Verwijderd: ll

[2] The **Online Certificate Status Protocol** (**OCSP**) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
[3] Other applications using certificates can also use the OCSP verification method.
[4] According to the RFC2560

Note that advanced methods for misusing the rogue certificates are possible by which a thorough attacker can circumvent our detection method.

The incident response sensor logged all network traffic since August 30th. Current analyses still show hacking attempts on the web server originating from Iran. During monitoring, we also saw unusual traffic after the company F-Secure announced its findings of a possible earlier breach of the website.[5] We haven't investigated this breach yet in detail. In August, DigiNotar installed a new web server. It's fair to assume these hacker traces where copied from the previous web server install.

3.3 CA servers investigation

DigiNotar hosts several CA services on different servers. Earlier reports indicated two of these servers where compromised and misused by the attacker(s). It was essential to verify the status of the other CA systems and investigate if they were compromised or misused. Forensic disk images were made of all the CA servers for investigation.

Because of security implications, the details of these results are not shared in this public report. More generally, we found traces of hacker activity with administrator rights on the Qualified and PKIoverheid CA server as well as on other CA servers. On the CA systems a web page has been accessed on a server in the demilitarized zone (DMZ) that contained several hacker tools and malware. This web page was also accessible to anyone on the internet making it a stepping stone for the attacker. Furthermore, we can share that on September 3rd more rogue certificates were discovered. The list of certificates is in the Annex 5.1.

The log files on the Qualified & PKI Overheid CA server do not show traces of deleted entries. These traces are present on other CA servers, where rogue certificates were produced. During further investigation however, we encountered several serial numbers of certificates that cannot be related to trusted certificates. Two of these were found on the Qualified & PKI Overheid CA server. It might be possible that these serial numbers have been temporarily generated by the CA software without being used. Alternatively, these serials were generated as a result of a bug of the software. However, we cannot rule out the possibility that these serial numbers relate to rogue certificates. Further investigation needs to be done to confirm or contradict this. The list of serials is in the Annex 5.2; this list has been communicated with the web browser vendors.

3.4 Firewall investigation

The firewall log files have not been analysed yet.

3.5 Malicious software analyses

A number of malicious/hacker software tools was found. These vary from commonly used tools such as the famous Cain & Abel tool[6] to tailor made software.

Specifically developed software probably enabled the hackers to upload the generated certificates to a dropbox. Both the IP-addresses of an internal DigiNotar server and the IP-address of the dropbox were hardcoded in the software. Possibilities are being explored to investigate this server, as (parts of) the uploaded rogue certificates might be still available there.

A script was found on CA server public 2025. The script was written in a special scripting language only used to develop PKI software. The purpose of the script was to generate signatures by the CA for certificates which have been requested before. The script also contains English language which you can find in Annex 6.3. In the text the hacker left his fingerprint: *Janam Fadaye Rahbar*[7]. The same text was found in the Comodo hack in March of this year[8]. This breach also resulted in the generation of rogue certificates.

Verwijderd: 5.3

[5] The IT-Security company F-Secure blogs about a breach of the webserver of DigiNotar in May 2009. http://www.f-secure.com/weblog/archives/00002228.html

[6] Cain&Abel is a very powerful hackers toolkit. It's capable of sniffing and breaking passwords. Most anti-virus software will detect C&A and flag it as malicious.

Verwijderd: s

[7] Supposedly meaning: "I will sacrifice my soul for my leader"

[8] http://www.wired.com/threatlevel/2011/03/comodo_hack/

4 Provisional results

4.1 Fraudulent issued certificates

In total 531 fraudulent certificates have been issued. We have no indication that more certificate were issued by the attacker(s). 344 Of these contain a domain name in the common name. 187 Certificates have in the common name 'Root CA'. We have reason to believe these certificates are not real CA certificates but normal end user certificates.

4.2 Compromised CAs

The attacker(s) had acquired the domain administrator rights. Because all CA servers were members of the same Windows domain, the attacker had administrative access to all of them. Due to the limited time of the ongoing investigation we were unable to determine whether all CA servers were used by the attacker(s). Evidence was found that the following CAs *were* misused by the attacker(s):

- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- Koninklijke Notariele Beroepsorganisatie CA
- Stichting TTP Infos CA

The security of the following CAs was compromised, but no evidence of misuse was found (this list is incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Qualified CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association
- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TU Delft CA

For some of these CAs extra security measures were in place (like the CCV CA). This makes it more unlikely they were misused.

4.3 Misuse

We investigated the OCSP responder log files around the time of the *.google.com incident. That incident was detected on August 27th. The first known public mention was a posting in a google forum. The user (from Iran) was warned by the Google Chrome browser that there was something wrong with the certificate. The corresponding rogue certificate was created on July 10th.

Based on the logging mentioned above from the OCSP responder, we were able to extract the following information. On August 4th the number of request rose quickly until the certificate was revoked on August 29th at 19:09. Around 300.000 unique requesting IPs to google.com have been identified. Of these IPs >99% originated from Iran, as illustrated in figure 1.[9]

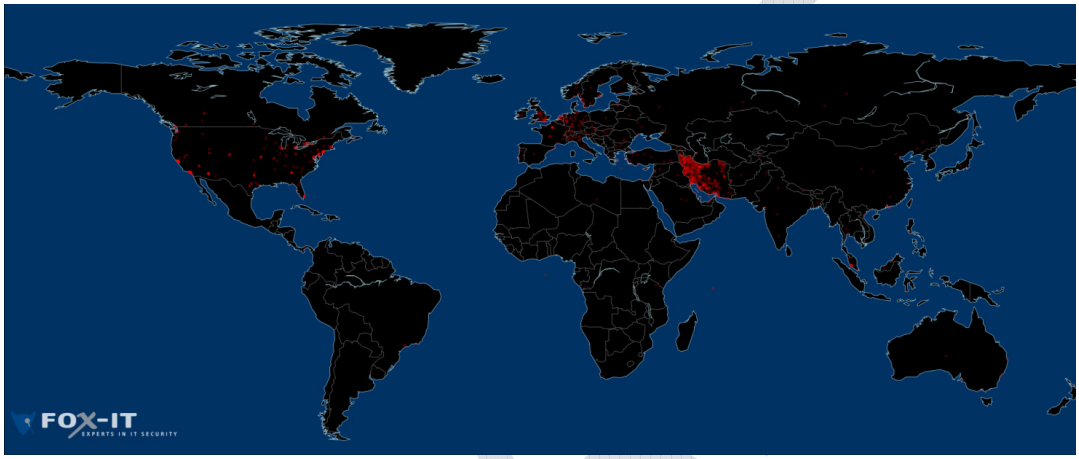


Figure 1: OCSP requests for the rogue *.google.com certificate

A sample of the IP's outside of Iran showed mainly to be TOR-exit nodes, proxies and other (VPN) servers, and almost no direct subscribers.

The list of IP-addresses will be handed over to Google. Google can inform their users that during this period their e-mail might have been intercepted. Not only the e-mail itself but also a login cookie could have been intercepted. Using this cookie the hacker is able to log in directly to the Gmail mailbox of the victim and also read the stored e-mails. Besides that, he is able to log in all other services Google offers to users like stored location information from Latitude or documents in GoogleDocs. Once the hacker is able to receive his targets' e-mail he is also able to reset passwords of others services like Facebook and Twitter using the lost password button. The login cookie stays valid for a longer period. It would be wise for all users in Iran to at least logout and login but even better change passwords.

Other OSCP request logs show some activity on August the 30th with a misused *.torproject.org certificate. None of these originated from Iran. However this does not prove that rogue certificates weren't abused between the issue date and revocation date of the certificates based on the OCSP logs because some applications might not use the OCSP protocol for revocation checking.

[9] This static image shows all IP-addresses detected. On http://www.youtube.com/watch?v=wZsWoSxxwVY you can see the interception of Google users taking place in a timeline.

Verwijderd: http://www.youtube.com/watch?v=_eIbNWUyJWQ

5 Discussion

5.1 Skills and goal of the hackers

We found that the hackers were active for a longer period of time. They used both known hacker tools as well as software and scripts developed specifically for this task. Some of the software gives an amateurish impression, while some scripts, on the other hand, are very advanced. In at least one script, fingerprints from the hacker are left on purpose, which were also found in the Comodo breach investigation of March 2011. Parts of the log files, which would reveal more about the creation of the signatures, have been deleted.

The list of domains and the fact that 99% of the users are in Iran suggest that the objective of the hackers is to intercept private communications in Iran.

5.2 Other possible rogue certificates

Using the OCSP responder requests we verify if the requested serial belongs to a known certificate. We have seen requests for unknown serials that cannot be matched against a known certificate. It's possible that these serials belong to a "rogue" certiticate or are just bogus OCSP requests, for instance done by security researchers. It's still possible other unknown[10] rogue certificates have been produced.

OCSP logging could still catch other possible rogue certificates based on the number of requests for an unknown serial, although it's difficult to match the common name with that serial if the certificate in question is not known.

5.3 Trust in the PKIoverheid and Qualified environment

Although all CA-servers have been accessed by a hacker with full administrative access rights and attempts have been made to use the running PKI-software we have no proof of generated rogue Qualified or PKIoverheid certificates. The log files of these CA-Servers validate as correct and no deleted log files have been found on these CA-servers. This is in contrast to our findings on the other breached CA servers.

Investigators encountered two (2) serial numbers of certificates on the Qualified or PKIoverheid server that cannot be related to trusted certificates[11]. Based on this, we cannot rule out the possibility that these relate to rogue certificates.

5.4 Current network infrastructure at DigiNotar

The successful hack implies that the current network setup and / or procedures at DigiNotar are not sufficiently secure to prevent this kind of attack.

The most critical servers contain malicious software that can normally be detected by anti-virus software. The separation of critical components was not functioning or was not in place. We have strong indications that the CA-servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the management LAN.

The network has been severely breached. All CA servers were members of one Windows domain, which made it possible to access them all using one obtained user/password combination. The password was not very strong and could easily be brute-forced.

The software installed on the public web servers was outdated and not patched.

No antivirus protection was present on the investigated servers.

An intrusion prevention system is operational. It is not clear at the moment why it didn't block some of the outside web server attacks. No secure central network logging is in place.

[10] Unknown as in, that we haven't been able to revoke them yet because we don't know their existence.
[11] OCSP requests to these serial numbers will result in a 'revoke' reply.

6 Appendix

6.1 Fraudulent issued certificates

The following list of Common Names in certificates are presumed to be generated by the attacker(s):

Common Name	Number of certs issued
CN=*.*.com	1
CN=*.*.org	1
CN=*.10million.org	2
CN=*.JanamFadayeRahbar.com	1
CN=*.RamzShekaneBozorg.com	1
CN=*.SahebeDonyayeDigital.com	1
CN=*.android.com	1
CN=*.aol.com	1
CN=*.azadegi.com	1
CN=*.balatarin.com	3
CN=*.comodo.com	3
CN=*.digicert.com	2
CN=*.globalsign.com	7
CN=*.google.com	26
CN=*.logmein.com	1
CN=*.microsoft.com	3
CN=*.mossad.gov.il	2
CN=*.mozilla.org	1
CN=*.skype.com	22
CN=*.startssl.com	1
CN=*.thawte.com	6
CN=*.torproject.org	14
CN=*.walla.co.il	2
CN=*.windowsupdate.com	3
CN=*.wordpress.com	14
CN=Comodo Root CA	20
CN=CyberTrust Root CA	20
CN=DigiCert Root CA	21
CN=Equifax Root CA	40
CN=GlobalSign Root CA	20
CN=Thawte Root CA	45
CN=VeriSign Root CA	21
CN=addons.mozilla.org	17
CN=azadegi.com	16
CN=friends.walla.co.il	8
CN=login.live.com	17
CN=login.yahoo.com	19
CN=my.screenname.aol.com	1
CN=secure.logmein.com	17
CN=twitter.com	19
CN=wordpress.com	12
CN=www.10million.org	8
CN=www.Equifax.com	1
CN=www.balatarin.com	16
CN=www.cia.gov	25
CN=www.cybertrust.com	1
CN=www.facebook.com	14
CN=www.globalsign.com	1
CN=www.google.com	12
CN=www.hamdami.com	1
CN=www.mossad.gov.il	5
CN=www.sis.gov.uk	10
CN=www.update.microsoft.com	4

Met opmaak: Aantal kolommen: 1

6.2 *Unknown serial numbers*

Root-CA server

On the 'Root-CA' server the following serials were encountered:

```
83120A023016C9E1A59CC7D146619617
68E32B2FE117DFE89C905B1CCBE22AB7
711CE18C04232184255l0EF51513B7B8
B7ABEFC8A1F844207B774C782E5385B3
6E0088D11C7E4E98CC9E0694D32A0F6B
80C990D339F177CA9FDAC258105882AB
7F73EC0A14C4BA065BECFAD69DC5A61D
```

Qualified-CA server

On the 'Qualified-CA' server the following serials were encountered:

```
C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4
```

These serials might have been issued by the following CAs:

- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven

'Taxi-CA

On the 'Taxi-CA' server the following serials were encountered:

```
25B6CA311C52F0E4F72A1BD53774B5B3
A0CF459D0D1EA9A946861A0A02783D88
71A10FA4C491D3A72D18D33E3CCF576C
FE456B099700A6C428A193FE5968C9FD
E7E2B46B8C9AA64679E03841F88CA5A0
AEC9F2324D80020B6E2B2A1103D6A4E8
CB20C25F14583AFC86465F14E621FBC1
947FF1DB66A41D809A9BC7E7344E342A
90BCA541B4DF5E77FB1349684F84A930
AB4967CE8B94FCF8DA7691922E6FD59C
BA479991C9103C005726FAB83088A8D6
363E9AAF4DAC7085F31B89B2AC49059A
8A63042B8A8FA256035773BC9417435A
963CCB2601B15C73DCA821F4BC4C7458
6B7057D5DE0170842C372821D3F17DB2
C391438C15FF31BD89544A7F68DDF3B3
7278CB2A8270A3E66A021A7CD75F1211
F401D4C50FCA9161A70ED9D91D40E684
6C396359C423417E20C54CFC6690F3FF
9916C8350225BB607857375A02B6DC72
0F48A14121370B5CF4828EF826749FBC
DB43E2CE6110750785FCBBE9A8EAE061
C641E4B7F19B63C4FF1EA6D3833FC874
D8B771F90BC01C9ED1333C23EF24CFC1
```

'Public-CA server

On the 'Public-CA' server the following serials were encountered:

```
79C03FE0C81A3022DBF8143B27E40223    8B0EABAF922D4C6E6917FCBE365DD64A    82C42F0EDC18BD751727BE5C54413EF7
FCCF53CB3D0A71494AF9664690FFCF84    4FC2D72D6427CABBE3E859453865F43B    03124C25849D9E49BC2A2FAD3E10C8A4
82BC18B1AA5D59C61D0EFDBEA7664C08    53B53BF2F74997EBEB2577D63DA692B7    EFF0DD4B4927DF64232C5D2FF280C1E4
5D4352671C39616670B2F34C173A1F63    ABB21F43553F2695031A1C85355D7F1C    9EDCB5E1FE1255A2F1D7FC52C4AFA3B1
6FA3C48173B3B289943F113A8CD9DB8C    5563605FDC2DC865E2A1C32995B5A086    3A32AAA9DFE2CA7F9E003885E316944B
CFAF9BE4E5BD0F5A75F628E45E0178C9    5DD6A72747D90C018B63F959DFE7C976    4455B43B9173CBAE4E247272EE2573D5
4ADA28D281D3D14D19FB782D64086D0C    CAB736FFE7DCB2C47ED2FF88842888E7    B95F62E86194734C9F68D4BF8B200C49
0B41ABEE6F4168D3CDE5A7D223B58BC1    9C79C9FE16727BAC407B4AA21B153A54    FE873B742B230B22AE540E840490A2F4
13548FC160BC5C9F315AE28CDB490E36    2D711C9CB79EC15445747BFE3F8BC92F    8779917563EC38B7746B8ECAFE239BE6
5D8D0D43611275982E6A5490E7F87BD7    752A2D0325A3D34D9F5198C2F5C92A6C    72CBC4824C6215B139FDE6BA10DAC6AD
C880AE4D7927E6A8FA7D456CB03E9763    39936336286F843756FC4BC296D7A8E0    8D09D4B98DE67C9E9C7C18CB72AD2418
82072FC8F8DD7E6C0ECE9B47185F0521    4A6D90618A5CA6797C768C03C860C4F8    07BC72A463D4DE33B2BE733D6FAC991D
90DB656E273476CC8367782555582FA8B   0954E1AB9141ED7E8B640FE681046451    D3E2205C3B899FC99D77FE802985283F
171A8599EDE711A3315BC7D694CEBEC6    8259C3E1DB6C2C9B7FCD6A305EADEFE4    A5029D6A057D50D20ECFE0E528EDA067
E9EB8075F7FE3683B431552C2D962CB0    BC01852405D3F4E22C48600266655026    C8B2487ADFAF969E34306029AC934406
E6F9E095464F64448840A832FB3443DB    9F7DDFE3CAAD224EC6BD68B60DE78550    5F3C1BDC7A2BCD47ABAF0C8E62D9F757
C83D16E9CB29DCF35F3B351CB942FE0D    A67C22A6E1F9D87799548EBFC7D5527E    601315BB085FECF29538DA3F9B7BA1CE
39B5DD0ECC85C3F62A72391DC055F561    11661878CCE9DC337CEEBB16E30F9A3A    30170F15A240446E6B482E0A364E3CCA
DF3FD6AFBBFBC30C9AD80BF764A102DB    6BF3BEB26AFF31116200B14F4378C33B    0590B310AEFC7A3EDC03ECA2A6F6624F
327B9A443C49018D7B0A97B6EC2254B8    7A61A7778842E502E2291166C4574485    FDEB145AAC81B8CD29B8DA018E71456F
```

```
C3F9F45F19E334C8303F44288856D843
028CF7556F8BE27026800448FA6AA527
E93B28B47C34B243EBA62E58FE2FF46F
F89F5DE575755A3B4C0DECC6EDA7C804
5D8F8D78B0C19EF4479F744DECBD84BC
EAACDC2F46D4A86F39B035B793F4A94F
9D06313F21A4EDF734C324FFBCB9E2B5
35C54E845AE855F818504C8C189F52C7
E3E120935934CBD77E1DA7F00431F745
0A6DFACFDEAE74A816031534BE90B75A
9AD82BE2FED538B10BDFBD229A8A5AEA
C0F216CA8197AD00F0D98927EAE29E64
DE76B17BFB1B6D6D6634C8C104A6E59F
A90F1BB43E9DB5EDFC60C15FB897C593
8625B32398C2722D96E7B972580A0238
D1FDE3A78C9D2E80C2303CC4E3E92A4C
B355E909FD55C5E9EF1A6E67E9C18203
ADB59A303C6260DBE466F0149AB11A4A
5CEBD524469A075FB6B42D06C9BF27AD
0E0886EEAA119CF14F1C54387060929A
B4F9299F05A327E60543C4CDE3277FC0
E4B2F09505726306314DF05B734FD9D0
4DD0497CBAABBA058574A611B26151BA
7073C6C01DEE4E158F554555F697F7D9
EB72415ECD0B4AACBDEEA3734F4349BF
BED90D98FA3A1E0A5BD78AD54E55774D
3CDCD81930F91AC0B990664931E5412E
763B0C2A7B83066A9D995C8C4FD9E35E
720DF591261D710ADC73127C1BC4303D
C06C12DBBC7055FE40950803238EC104
62BF5A170CC779ADE7EF0090F395D5E6
61BF9A0FF2CE9D55D86BC063839F72F4
B5D7A148CA6C1F9693A2C16ACDD66226
35FBDCDF923F99B5E1C5FF4423B715B8
F1EBE73557546DC8B21E0A2DE5E3A33E
EBE7561CA573DA5DBB8EFAA250A40FD3
6BACB6C5B74FA747A3CF375EC3095035
6C1950AA83F4663F1BA063B5275C25EC
56EF1EE54D65EF7B39AF541E95BB45A9
2B1EA767EC59E46364BC2DF9B1F30B97
3913B1E1C35BDDF02CE03C916E8AA638
AFA2F7E964280B36DB0D714B86256F54
022E35B1ACD40F040C444DF32A7B8DE6
170370B60D515F164119BE54FD55E1ED
CBFE437C9B62805C4353516699E44649
5FFA79AB76CE359089A2F729A1D44B31
5298BCBD11B3952E3FDDC6FDD6711F5C
1836289F75F74A0BA5E769561DE3E7CD

DEB427AC9F1E8A0D0237049C80DF7E7F
FD8FE350325318C893AFE03F9DFC7096
A8031D608F6549941879981764674DD7
DDAD29B8B1215191E7EB5AAEE0219338
3F8A5EA1756DDF4A6B6F2645B4911486
30DF96D87EEC8CA77A135ECCAB1AD25E
7DD8E0E1906C1754E11E901927CCABBD
DAC51C3D23B163601305AF99DF129689
D77EC92400AE0D9FA57DEF4DD8CFA4D4
09369288E36D7AFFEE94EA81998FA316
EEBE1885532234328919191 3F6D769EB
C00132DA154BDEE361EDEE727226D0F5
6580BE22A0566352B9622777BFCB7164
7352C61297D6B04E874EDAD12480F78E
F658C0D52B3EEF71DDE6C284E7E1B337
E1253D04A17AB8E47F4A5916B9BF9D23
8922A9A23BE960FFE9707A0B3F4D75BD
EAE97F465015E49A14F3B23403ACFA11
13A757022817C0514A5C142FE9BF143A
5132F0FCB3F8DCAA501C620575D33FEE
39953BF6383A00D29BEB377568E3DE7A
67887932934DFF086153CA905E7DE9EE
DCD1072719692871126E4159D80EFDA8
C6741E3D08C0FFD4617B94E654DD89F1
D0BA58BA609CC1A001F612987A822BEF
6B339433956F1505104BB231314A153E
C1366C7246041A3089E1C244C5DC42E7
61D11B35765ECB85890D5349786D9FCA
44C287C1C3697367B0E6CB78A78C1DF5
DAACF72BC91FB6DA90A804933CB72E23
2ACBA14BB6F65F7BD0A485BFCB6D023F
84BE5D762F37E9018D623C8E91F4D924
1A89324D6D3E6DE6726C688BFF225DDD
F5FA42A5B421705E4803DA93C4F7E099
A869B96BCDF1D474C0714763AA34A8C9
3EA0F90DE57187FC7E1AC45AE44D16C6
F7DE638B76C3958AA3413A9785A19900
3F8C9CDAACBB533AE94F47456819FA0E
209920C169512D3EB4A1ED7CAD17D033
B2F57BD01BAAF7AF01EF442910CEBBA0
C0766829AA4D2E1A5D97213A4E4A654E
FC9993EA7A4E761B6CB79ABE2BD3CDE1
4D556B338FAA020979A740B4C3AEE28C
8ED896B9A622FF24559A3429E5888E0A
8CF1F45323EC5AB449451E7A9476CFDC
D1718E9BD91257D2169C81197D508A67
E4A691D60266784968DF971D6BF473AF
B3B64F1925F759A2E145190333D1D6D2

ED4C2EBC14B85F46A9A75F159DF8BEB3
CDBC0441C10DB5ABA43120E63A048425
DC1665266A0198728861AC99ED368928
706BBC770C62D41DD799721ABD1868AB
B2205D8CBDDFE49D7C5F0F95D506718F
901F30DB86EEB1666F5A8CAE1C7BD08B
9A3A951BE27E0729726FD8B80060E7E1
6410577C738133297472F6C22C2BB397
C8C06B0C6B7FE7CA66BCFE617AB6C4E6
58C18B290620E18B8C78AC1912E5DCD7
2F5ABFDCCAB1A2927E54283296F19FB8
A07CB7881E35C91FD9C5D20F6102572C
05E2E6A4CD09EA54D665B075FE22A256
8BA800DDDD865B6BF3A85ADEC4C29730
07B546E8E002FC5854651BE31802F96D
DF2AD7F766E2EEFAF0FD1FB5C6883AB4
1C6EA2DA6ECED5C5C761BCA9CA4C5308
A640A29E706AF38557B86619EAF45E7A
F88885670C3D55EBA52096A65310DACA
B85E7BB83667097F15D8A3DEAAA1B198
A5F6F149B468683318DC178F4208E237
04841B82A9D81E44CB4F2D98CFE7C374
A81686CEFDEFFCE82B8DBF100E1395F1
9952073595776A3D7A8101664A56AB96
A076DA72A8C8E2137F05FE3FA59870EB
121378A6DE0A13DDB295106E912A4E14
65A925E578098658FADA30E9FB67B5E4
5B8E5202EC6769F2389605D33DC245B2
EA71F746BD17D1B05450329818572F2E
DD8C315D2CA61870CBCF9D56ED7474E2
F346A1E62FED476F472560C6DDE0CADC
CBBCB9E06F9FC92C533B2F2A5284BA22
79DCFDA2700E06F8EAA640BA9B827810
17CF5474D5A8B4E735E69E017CEC2F37
7034FBF641CEB257FC109A6819D19DA0
6E6D052B5ABC015C779EA3500FA11A28
FAB79682C8EAE556F11ECF6DAD7121BA
0370390E48A7F26AA62188A79E612DC3
59F8BDDA3F56D8026FAB6E3130F5D843
C731140FAA7690918BABF17BECB7938D
8C605DFAA0EC88CDB7D12F7250C9F53A
68F252CD36F2798A2182F6406A31A5A2
BD7CB0D124DFDE784CD5B9EF288C304E
3D2BC95A85EF539A68DAC84542A1AE7A
8CC74931E64061491652CC169C8BAAB3
4157D99E46A3E45E6130A95645410DAC
E34C4FC7488C4DFEF0EA475A17AF2C7B
```

These serials might have been issued by the following CAs (list incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- DigiNotar Qualified CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- Koninklijke Notariele Beroepsorganisatie CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association

- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- Stichting TTP Infos CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TU Delft CA

6.3 Plain text left in script to generate signatures on rogue certificates

```
I know you are shocked of my skills, how i got access to your network
to your internal network from outside
how I got full control on your domain controller
how I got logged in into this computer
HoW I LEARNED XUDA PROGRAMMING
HOW I got this IDEA to write such XUDA code
How I was sure it's going to work?
How i bypassed your expensive firewall, routers, NetHSM, unbreakable hardware keys
How I did all xUDA programming without 1 line of resource, got this idea, owned your
 network accesses your domain controlled, got all your passwords, signed my certificates
 and received them shortly
THERE IS NO ANY HARDWARE OR SOFTWARE IN THIS WORLD EXISTS WHICH COULD STOP MY HEAVY
 ATTACKS
MY BRAIN OR MY SKILLS OR MY WILL OR MY EXPERTISE
That's all ok! EVerything I do is out of imagination of people in world
I know you'll see this message when it is too late, sorry for that
I know it's not something you or any one in this world have thought about
But everything is not what you see in material world, when God wants something to happen


My signature as always: Janam Fadaye Rahbar


Rahbare azizam mesle hamishe asoode bash, ta vaghti ke man va amsale man baraye in marzo
 boom
va baraye barafrashte negah dashtane parchame velayate faghih kar mikonand
daste har doshmano mozdouri ghat khahad bood
Rahbaram, Tamame vojoodam fadaye to ke ham jani o ham janani
```

6.4 Timeline

06-Jun-2011	Possibly first exploration by the attacker(s)
17-Jun-2011	Servers in the DMZ in control of the attacker(s)
02-Jul-2011	First attempt creating a rogue certificate
10-Jul-2011	The first succeeded creation of rogue certificate (*.Google.com)
19-Jul-2011	Incident detected by DigiNotar by daily audit procedure
20-Jul-2011	Last known succeeded rogue certificate was created
22-Jul-2011	Last outbound traffic to attacker(s) IP (not confirmed)
22-Jul-2011	Start investigation by IT-security firm (not confirmed)
27-Jul-2011	Delivery of security report of IT-security firm
27-Jul-2011	First rogue *.google.com OSCP request
28-Jul-2011	First seen that rogue certificates were verified from Iran
04-Aug-2011	Start massive activity of *.google.com on OCSP responder
27-Aug-2011	First mention of *.google.com certificate in blog
29-Aug-2011	GOVCERT.NL is notified by CERT-Bund
29-Aug-2011	The *.google.com certificate is revoked
30-Aug-2011	Start investigation by Fox-IT
30-Aug-2011	Incident response sensor active
01-Sep-2011	OSCP responder based on white list

Verwijderd: 19-Jun-2011 ... [1]

Verwijderd: UND

19-Jun-2011 Incident detected by DigiNotar by daily audit procedure

Van: [redacted]- Logius[redacted]@logius.nl]
Verzonden: maandag 10 oktober 2011 17:18
Aan: [redacted]
Onderwerp: FW: Black Tulip Report 1.1
Bijlagen: Operation Black Tulip v1.1_with diff to 1.0.pdf; Operation Black Tulip v1.1.pdf; Diginotar public report (final) v1.1_with diff to 1.0.docx; Diginotar public report (final) v1.1_final.docx

Bijgaand in ieder geval het aangepaste rapport met daarin verwerkt :

- Feitelijke onjuistheden
- Info Opta
- Commentaar Diginotar

Volgende versie bevat CPB info.

Meest spannende aanpassing (agv OPTA info):

Because of security implications, the details of these results are not shared in this public report. More generally, we found traces of hacker activity with administrator rights on the Qualified and PKIoverheid CA server as well as on other CA servers. On the CA systems a web page has been accessed on a server in the demilitarized zone (DMZ) that contained several hacker tools and malware. This web page was also accessible from the internet with a password making it a stepping stone for the attacker. Logs show that outside office hours on 1 and 2 July files were transferred. Furthermore, we can share that on September 3rd more rogue certificates were discovered. The list of certificates is in the Annex 5.1.

Gegeven het feit dat eind van de week het volledige rapport beschikbaar komt lijkt het me niet handig om deze versie breed te verspreiden.

[redacted]

Van: [redacted] [mailto:[redacted]@fox-it.com]
Verzonden: maandag 10 oktober 2011 15:45
Aan: [redacted]- Logius
CC: DigiBZK
Onderwerp: Black Tulip Report 1.1

Beste[redacted]

Hierbij de (final) versie van het 1.1 rapport. Wat ons betreft is deze nu conform met de informatie die wij ook aan de OPTA hebben verstrekt.

Met vriendelijke groet,

[redacted]
Security Expert

Fox-IT Experts in IT Security!

Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands

T +31 (0)15 2847[redacted]

F +31 (0)15 2847990
I www.fox-it.com

KvK Haaglanden 27301624

FOX-IT
EXPERTS IN IT SECURITY

Interim Report

September 5, 2011
(rectifications)

DigiNotar Certificate Authority breach
"Operation Black Tulip"

Classification **PUBLIC**

Customer DigiNotar B.V.

Subject: Investigation DigiNotar Certificate Authority Environment

Date 10 October 2011
Version 1.1
Author J.R. Prins (CEO Fox-IT)
Business Unit Cybercrime
Pages 15

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

1 Document Management

Version management

This version replaces all previous version of this document. Please destroy all previous copies!

Distribution list

Copy	Distribution (version)	Name/function/remarks

Review management

Review by	Function	Date	Version

Change management

Version	Date	By	Remarks	Approval
1.0	05-sep-2011	J.R. Prins		
1.0a	05-sep-2011	J.R. Prins	Minor layout changes	
1.1	10-oct-2011	J.R. Prins	Rectification of dates, minor addition of details	

Related documents

Version	Date	Description	Remarks

Table of Contents

2 Introduction

2.1 Background

The company DigiNotar B.V. provides digital certificate services; it hosts a number of Certificate Authorities (CA's). Certificates issued include default SSL certificates, Qualified Certificates and 'PKIoverheid' (Government accredited) certificates.

On the evening of Monday August 29th it became public knowledge that a rogue *.google.com certificate was presented to a number of Internet users in Iran. This false certificate had been issued by DigiNotar B.V. and was revoked[1] that same evening.

On the morning of the following Tuesday, Fox-IT was contacted and asked to investigate the breach and report its findings before the end of the week.

Fox-IT assembled a team and started the investigation immediately. The investigation team includes forensic IT experts, cybercrime investigators, malware analysts and a security expert with PKI experience. The team was headed by CEO J.R. Prins directly.

It was communicated and understood from the outset, that Fox-IT wouldn't be able to complete an in-depth investigation of the incident within this limited timeframe. This is due to the complexity of the PKI environment and the uncommon nature of the breach.

Rather, due to the urgency of this matter, Fox-IT agreed to prepare an interim report at the end of the week with its preliminary findings, which would be published.

2.2 Investigation questions

The investigation predominately focused on following questions:

1. How did the perpetrators access the network?

2. What is the scope and status of the breach?
   - *Have other DigiNotar CA environments been breached?*
   - *Do we still see hacker activity on the network of DigiNotar?*
   - *Are rogue certificates actively being used by hackers?*

3. Can we discover anything about the impact of the incident?
   - *What certificates were issued without knowledge of DigiNotar?*
   - *What other (rogue) certificates might have been generated?*
   - *How many rogue connections were made using rogue certificates?*
   - *What was the nature of these connections?*

In order to address these questions we (basically) (i) implemented specialized monitoring to be able to detect, analyse and follow up on active misuse, and (ii) analysed digital traces on hard disks, and in databases and log files to investigate the origin and impact of the breach.

[1] Revoked: A certificate is irreversibly revoked if, for example, it is discovered that the certificate authority (CA) had improperly issued a certificate, or if a private-key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements such as publication of false documents, mis-representation of software behavior, or violation of any other policy specified by the CA operator or its customer. The most common reason for revocation is the user no longer being in sole possession of the private key (*e.g.*, the token containing the private key has been lost or stolen).

2.3 This report

The goal of this report is to share relevant information with DigiNotar stakeholders (such as the Dutch Government and the Internet community), based on which they can make their own risk analysis. Because this is a public report, some investigation results and details cannot be included for privacy and/ or security reasons.

Since the investigation has been more of a fact finding mission thus far, we will not draw any conclusions with regards to the network-setup and the security management system. In this report we will not give any advice to improve the technical infrastructure for the long term. Our role is to investigate the incident and give a summary of our findings until now. We leave it to the reader in general and other responsible parties in the PKI- and internet community to draw conclusions, based on these findings. We make a general reservation, as our investigations are still ongoing.

3 Investigations

3.1 Prior investigations

Some investigations were conducted before we started.

Fox-IT was given access to a report produced by another IT-security firm which performs the regular penetration testing and auditing for DigiNotar. The main conclusions from this report dated July 27th were:

> A number of servers were compromised. The hackers have obtained administrative rights to the outside webservers, the CA server "Relaties-CA" and also to "Public-CA". Traces of hacker activity started on June 17th and ended on July 22nd.

Furthermore, staff from DigiNotar and the parent company Vasco performed their own security investigation. E-mail communication and memos with further information were handed over to us.

This information gave us a rough overview of what happened:

- The signing of 128 rogue certificates was detected on July 19th during the daily routine security check. These certificates were revoked immediately;
- During analysis on July 20th the generation of another 129 certificates was detected. These were also revoked on July 21th;
- Various security measures on infrastructure, system monitoring and OCSP validation have been taken immediately to prevent further attacks.
- More fraudulent issued certificates were discovered during the investigation and 75 more certificates were revoked on July 27th.
- DigiNotar found evidence on July 28th that rogue certificates were verified by internet addresses originating from Iran.
- On August 29th a *.google.com certificate issued was discovered that was not revoked before. This certificate was revoked on August 29th.

On August 30th Fox-IT was asked investigate the incident and recommend and implement new security measures. Fox-IT installed a specialized incident response network sensor to assist in the investigation. Furthermore we created images of several other servers.

3.2 Monitoring

The rogue certificate found by Google was issued by the DigiNotar Public CA 2025. The serial number of the certificate was, however, not found in the CA system's records. This leads to the conclusion that it is unknown how many certificates were issued without any record present. In order to identify these unknown certificates and to prevent them from being used by victims, the OCSP responder[2] requests were monitored.

Current browsers perform an OCSP check as soon as the browser connects to an SSL protected website through the https-protocol[3]. The serial number of the certificate presented by the website a user visits is sent to the issuing CA OCSP-responder. The OCSP-responder can only answer either with 'good', 'revoked' or 'unknown'. If a certificate serial number is presented to the OCSP-responder and no record of this serial is found, the normal OCSP-responder answer would be 'good'[4]. The OCSP-responder answer 'revoked' is only returned when the serial is revoked by the CA. In order to prevent misuse of the unknown issued serials the OCSP-responder of DigiNotar has been set to answer 'revoked' when presented any unknown certificate serial it has authority over. This was done on September 1st.

The incident response sensor immediately informs if a serial number of a known fraudulently issued certificate is being misused. Also, all unknown serial number requests can be analysed and used in the investigation. A large number of requests to a single serial number is suspicious and will be detected.

---

[2] The **Online Certificate Status Protocol** (**OCSP**) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
[3] Other applications using certificates can also use the OCSP verification method.
[4] According to the RFC2560

Note that advanced methods for misusing the rogue certificates are possible by which a thorough attacker can circumvent our detection method.

The incident response sensor logged all network traffic since August 30th. Current analyses still show hacking attempts on the web server originating from Iran. During monitoring, we also saw unusual traffic after the company F-Secure announced its findings of a possible earlier breach of the website.[5] We haven't investigated this breach yet in detail. In August, DigiNotar installed a new web server. It's fair to assume these hacker traces where copied from the previous web server install.

3.3 CA servers investigation

DigiNotar hosts several CA services on different servers. Earlier reports indicated two of these servers where compromised and misused by the attacker(s). It was essential to verify the status of the other CA systems and investigate if they were compromised or misused. Forensic disk images were made of all the CA servers for investigation.

Because of security implications, the details of these results are not shared in this public report. More generally, we found traces of hacker activity with administrator rights on the Qualified and PKIoverheid CA server as well as on other CA servers. On the CA systems a web page has been accessed on a server in the demilitarized zone (DMZ) that contained several hacker tools and malware. This web page was also accessible from the internet with a password making it a stepping stone for the attacker. Logs show that outside office hours on 1 and 2 July files were transferred. Furthermore, we can share that on September 3rd more rogue certificates were discovered. The list of certificates is in the Annex 5.1.

The log files on the Qualified & PKI Overheid CA server do not show traces of deleted entries. These traces are present on other CA servers, where rogue certificates were produced. During further investigation however, we encountered several serial numbers of certificates that cannot be related to trusted certificates. Two of these were found on the Qualified & PKI Overheid CA server. It might be possible that these serial numbers have been temporarily generated by the CA software without being used. Alternatively, these serials were generated as a result of a bug of the software. However, we cannot rule out the possibility that these serial numbers relate to rogue certificates. Further investigation needs to be done to confirm or contradict this. The list of serials is in the Annex 5.2; this list has been communicated with the web browser vendors.

3.4 Firewall investigation

The firewall log files have not been analysed yet.

3.5 Malicious software analyses

A number of malicious/hacker software tools was found. These vary from commonly used tools such as the famous Cain & Abel tool[6] to tailor made software.

Specifically developed software probably enabled the hackers to upload the generated certificates to a dropbox. Both the IP-addresses of an internal DigiNotar server and the IP-address of the dropbox were hardcoded in the software. Possibilities are being explored to investigate this server, as (parts of) the uploaded rogue certificates might be still available there.

A script was found on CA server public 2025. The script was written in a special scripting language only used to develop PKI software. The purpose of the script was to generate signatures by the CA for certificates which have been requested before. The script also contains English language which you can find in Annex 6.3. In the text the hacker left his fingerprint: *Janam Fadaye Rahbar*[7]*.* The same text was found in the Comodo hack in March of this year[8]. This breach also resulted in the generation of rogue certificates.

[5] The IT-Security company F-Secure blogs about a breach of the webserver of DigiNotar in May 2009. http://www.f-secure.com/weblog/archives/00002228.html
[6] Cain&Abel is a very powerful hackers toolkit. It's capable of sniffing and breaking passwords. Most anti-virus software will detect C&A and flag it as malicious.
[7] Supposedly meaning: "I will sacrifice my soul for my leader"
[8] http://www.wired.com/threatlevel/2011/03/comodo_hack/

4 Provisional results

4.1 Fraudulent issued certificates

In total 531 fraudulent certificates have been issued. We have no indication that more certificate were issued by the attacker(s). 344 Of these contain a domain name in the common name. 187 Certificates have in the common name 'Root CA'. We have reason to believe these certificates are not real CA certificates but normal end user certificates.

4.2 Compromised CAs

The attacker(s) had acquired the domain administrator rights. Because all CA servers were members of the same Windows domain, the attacker had administrative access to all of them. Due to the limited time of the ongoing investigation we were unable to determine whether all CA servers were used by the attacker(s). Evidence was found that the following CAs *were* misused by the attacker(s):

- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- Koninklijke Notariele Beroepsorganisatie CA
- Stichting TTP Infos CA

The security of the following CAs was compromised, but no evidence of misuse was found (this list is incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Qualified CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association
- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TU Delft CA

For some of these CAs extra security measures were in place (like the CCV CA). This makes it more unlikely they were misused.

4.3 Misuse

We investigated the OCSP responder log files around the time of the *.google.com incident. That incident was detected on August 27th. The first known public mention was a posting in a google forum. The user (from Iran) was warned by the Google Chrome browser that there was something wrong with the certificate. The corresponding rogue certificate was created on July 10th.

Based on the logging mentioned above from the OCSP responder, we were able to extract the following information. On August 4th the number of request rose quickly until the certificate was revoked on August 29th at 19:09. Around 300.000 unique requesting IPs to google.com have been identified. Of these IPs >99% originated from Iran, as illustrated in figure 1.[9]

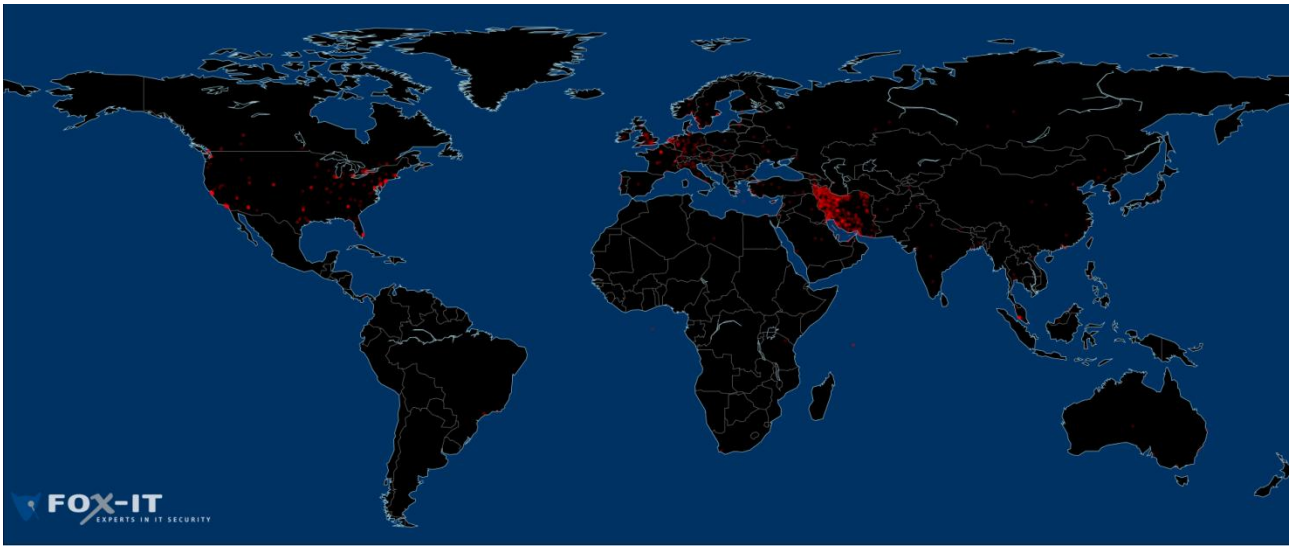


Figure 1: OCSP requests for the rogue *.google.com certificate

A sample of the IP's outside of Iran showed mainly to be TOR-exit nodes, proxies and other (VPN) servers, and almost no direct subscribers.

The list of IP-addresses will be handed over to Google. Google can inform their users that during this period their e-mail might have been intercepted. Not only the e-mail itself but also a login cookie could have been intercepted. Using this cookie the hacker is able to log in directly to the Gmail mailbox of the victim and also read the stored e-mails. Besides that, he is able to log in all other services Google offers to users like stored location information from Latitude or documents in GoogleDocs. Once the hacker is able to receive his targets' e-mail he is also able to reset passwords of others services like Facebook and Twitter using the lost password button. The login cookie stays valid for a longer period. It would be wise for all users in Iran to at least logout and login but even better change passwords.

Other OSCP request logs show some activity on August the 30th with a misused *.torproject.org certificate. None of these originated from Iran. However this does not prove that rogue certificates weren't abused between the issue date and revocation date of the certificates based on the OCSP logs because some applications might not use the OCSP protocol for revocation checking.

[9] This static image shows all IP-addresses detected. On http://www.youtube.com/watch?v=wZsWoSxxwVY you can see the interception of Google users taking place in a timeline.

5 Discussion

5.1 Skills and goal of the hackers

We found that the hackers were active for a longer period of time. They used both known hacker tools as well as software and scripts developed specifically for this task. Some of the software gives an amateurish impression, while some scripts, on the other hand, are very advanced. In at least one script, fingerprints from the hacker are left on purpose, which were also found in the Comodo breach investigation of March 2011. Parts of the log files, which would reveal more about the creation of the signatures, have been deleted.

The list of domains and the fact that 99% of the users are in Iran suggest that the objective of the hackers is to intercept private communications in Iran.

5.2 Other possible rogue certificates

Using the OCSP responder requests we verify if the requested serial belongs to a known certificate. We have seen requests for unknown serials that cannot be matched against a known certificate. It's possible that these serials belong to a "rogue" certiticate or are just bogus OCSP requests, for instance done by security researchers. It's still possible other unknown[10] rogue certificates have been produced.

OCSP logging could still catch other possible rogue certificates based on the number of requests for an unknown serial, although it's difficult to match the common name with that serial if the certificate in question is not known.

5.3 Trust in the PKIoverheid and Qualified environment

Although all CA-servers have been accessed by a hacker with full administrative access rights and attempts have been made to use the running PKI-software we have no proof of generated rogue Qualified or PKIoverheid certificates. The log files of these CA-Servers validate as correct and no deleted log files have been found on these CA-servers. This is in contrast to our findings on the other breached CA servers.

Investigators encountered two (2) serial numbers of certificates on the Qualified or PKIoverheid server that cannot be related to trusted certificates[11]. Based on this, we cannot rule out the possibility that these relate to rogue certificates.

5.4 Current network infrastructure at DigiNotar

The successful hack implies that the current network setup and / or procedures at DigiNotar are not sufficiently secure to prevent this kind of attack.

The most critical servers contain malicious software that can normally be detected by anti-virus software. The separation of critical components was not functioning or was not in place. We have strong indications that the CA-servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the management LAN.

The network has been severely breached. All CA servers were members of one Windows domain, which made it possible to access them all using one obtained user/password combination. The password was not very strong and could easily be brute-forced.

The software installed on the public web servers was outdated and not patched.

No antivirus protection was present on the investigated servers.

An intrusion prevention system is operational. It is not clear at the moment why it didn't block some of the outside web server attacks. No secure central network logging is in place.

[10] Unknown as in, that we haven't been able to revoke them yet because we don't know their existence.
[11] OCSP requests to these serial numbers will result in a 'revoke' reply.

6 Appendix

6.1 Fraudulent issued certificates

The following list of Common Names in certificates are presumed to be generated by the attacker(s):

Common Name	Number of certs issued
CN=*.*.com	1
CN=*.*.org	1
CN=*.10million.org	2
CN=*.JanamFadayeRahbar.com	1
CN=*.RamzShekaneBozorg.com	1
CN=*.SahebeDonyayeDigital.com	1
CN=*.android.com	1
CN=*.aol.com	1
CN=*.azadegi.com	1
CN=*.balatarin.com	3
CN=*.comodo.com	3
CN=*.digicert.com	2
CN=*.globalsign.com	7
CN=*.google.com	26
CN=*.logmein.com	1
CN=*.microsoft.com	3
CN=*.mossad.gov.il	2
CN=*.mozilla.org	1
CN=*.skype.com	22
CN=*.startssl.com	1
CN=*.thawte.com	6
CN=*.torproject.org	14
CN=*.walla.co.il	2
CN=*.windowsupdate.com	3
CN=*.wordpress.com	14
CN=Comodo Root CA	20
CN=CyberTrust Root CA	20
CN=DigiCert Root CA	21
CN=Equifax Root CA	40
CN=GlobalSign Root CA	20
CN=Thawte Root CA	45
CN=VeriSign Root CA	21
CN=addons.mozilla.org	17
CN=azadegi.com	16
CN=friends.walla.co.il	8
CN=login.live.com	17
CN=login.yahoo.com	19
CN=my.screenname.aol.com	1
CN=secure.logmein.com	17
CN=twitter.com	19
CN=wordpress.com	12
CN=www.10million.org	8
CN=www.Equifax.com	1
CN=www.balatarin.com	16
CN=www.cia.gov	25
CN=www.cybertrust.com	1
CN=www.facebook.com	14
CN=www.globalsign.com	1
CN=www.google.com	12
CN=www.hamdami.com	1
CN=www.mossad.gov.il	5
CN=www.sis.gov.uk	10
CN=www.update.microsoft.com	4

6.2 Unknown serial numbers

Root-CA server

On the 'Root-CA' server the following serials were encountered:

```
83120A023016C9E1A59CC7D146619617
68E32B2FE117DFE89C905B1CCBE22AB7
711CE18C0423218425510EF51513B7B8
B7ABEFC8A1F844207B774C782E5385B3
6E0088D11C7E4E98CC9E0694D32A0F6B
80C990D339F177CA9FDAC258105882AB
7F73EC0A14C4BA065BECFAD69DC5A61D
```

Qualified-CA server

On the 'Qualified-CA' server the following serials were encountered:

```
C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4
```

These serials might have been issued by the following CAs:

- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven

'Taxi-CA

On the 'Taxi-CA' server the following serials were encountered:

```
25B6CA311C52F0E4F72A1BD53774B5B3
A0CF459D0D1EA9A946861A0A02783D88
71A10FA4C491D3A72D18D33E3CCF576C
FE456B099700A6C428A193FE5968C9FD
E7E2B46B8C9AA64679E03841F88CA5A0
AEC9F2324D80020B6E2B2A1103D6A4E8
CB20C25F14583AFC86465F14E621FBC1
947FF1DB66A41D809A9BC7E7344E342A
90BCA541B4DF5E77FB1349684F84A930
AB4967CE8B94FCF8DA7691922E6FD59C
BA479991C9103C005726FAB83088A8D6
363E9AAF4DAC7085F31B89B2AC49059A
8A63042B8A8FA256035773BC9417435A
963CCB2601B15C73DCA821F4BC4C7458
6B7057D5DE0170842C372821D3F17DB2
C391438C15FF31BD89544A7F68DDF3B3
7278CB2A8270A3E66A021A7CD75F1211
F401D4C50FCA9161A70ED9D91D40E684
6C396359C423417E20C54CFC6690F3FF
9916C8350225BB607857375A02B6DC72
0F48A14121370B5CF4828EF826749FBC
DB43E2CE6110750785FCBBE9A8EAE061
C641E4B7F19B63C4FF1EA6D3833FC874
D8B771F90BC01C9ED1333C23EF24CFC1
```

'Public-CA server

On the 'Public-CA' server the following serials were encountered:

```
79C03FE0C81A3022DBF8143B27E40223    8B0EABAF922D4C6E6917FCBE365DD64A    82C42F0EDC18BD751727BE5C54413EF7
FCCF53CB3D0A71494AF9664690FFCF84    4FC2D72D6427CABBE3E859453865F43B    03124C25849D9E49BC2A2FAD3E10C8A4
82BC18B1AA5D59C61D0EFDBEA7664C08    53B53BF2F74997EBEB2577D63DA692B7    EFF0DD4B4927DF64232C5D2FF280C1E4
5D4352671C39616670B2F34C173A1F63    ABB21F43553F2695031A1C85355D7F1C    9EDCB5E1FE1255A2F1D7FC52C4AFA3B1
6FA3C48173B3B289943F113A8CD9DB8C    5563605FDC2DC865E2A1C32995B5A086    3A32AAA9DFE2CA7F9E003885E316944B
CFAF9BE4E5BD0F5A75F628E45E0178C9    5DD6A72747D90C018B63F959DFE7C976    4455B43B9173CBAE4E247272EE2573D5
4ADA28D281D3D14D19FB782D64086D0C    CAB736FFE7DCB2C47ED2FF88842888E7    B95F62E86194734C9F68D4BF8B200C49
0B41ABEE6F4168D3CDE5A7D223B58BC1    9C79C9FE16727BAC407B4AA21B153A54    FE873B742B230B22AE540E840490A2F4
13548FC160BC5C9F315AE28CDB490E36    2D711C9CB79EC15445747BFE3F8BC92F    8779917563EC38B7746B8ECAFE239BE6
5D8D0D43611275982E6A5490E7F87BD7    752A2D0325A3D34D9F5198C2F5C92A6C    72CBC4824C6215B139FDE6BA10DAC6AD
C880AE4D7927E6A8FA7D456CB03E9763    39936336286F843756FC4BC296D7A8E0    8D09D4B98DE67C9E9C7C18CB72AD2418
82072FC8F8DD7E6C0ECE9B47185F0521    4A6D90618A5CA6797C768C03C860C4F8    07BC72A463D4DE33B2BE733D6FAC991D
90DB656E273476CC8367782555582FA8B   0954E1AB9141ED7E8B640FE681046451    D3E2205C3B899FC99D77FE802985283F
171A8599EDE711A3315BC7D694CEBEC6    8259C3E1DB6C2C9B7FCD6A305EADEFE4    A5029D6A057D50D20ECFE0E528EDA067
E9EB8075F7FE3683B431552C2D962CB0    BC01852405D3F4E22C48600266655026    C8B2487ADFAF969E34306029AC934406
E6F9E095464F64448840A832FB3443DB    9F7DDFE3CAAD224EC6BD68B60DE78550    5F3C1BDC7A2BCD47ABAF0C8E62D9F757
C83D16E9CB29DCF35F3B351CB942FE0D    A67C22A6E1F9D87799548EBFC7D5527E    601315BB085FECF29538DA3F9B7BA1CE
39B5DD0ECC85C3F62A72391DC055F561    11661878CCE9DC337CEEBB16E30F9A3A    30170F15A240446E6B482E0A364E3CCA
DF3FD6AFBBFBC30C9AD80BF764A102DB    6BF3BEB26AFF31116200B14F4378C33B    0590B310AEFC7A3EDC03ECA2A6F6624F
327B9A443C49018D7B0A97B6EC2254B8    7A61A7778842E502E2291166C4574485    FDEB145AAC81B8CD29B8DA018E71456F
```

```
C3F9F45F19E334C8303F44288856D843
028CF7556F8BE27026800448FA6AA527
E93B28B47C34B243EBA62E58FE2FF46F
F89F5DE575755A3B4C0DECC6EDA7C804
5D8F8D78B0C19EF4479F744DECBD84BC
EAACDC2F46D4A86F39B035B793F4A94F
9D06313F21A4EDF734C324FFBCB9E2B5
35C54E845AE855F818504C8C189F52C7
E3E120935934CBD77E1DA7F00431F745
0A6DFACFDEAE74A816031534BE90B75A
9AD82BE2FED538B10BDFBD229A8A5AEA
C0F216CA8197AD00F0D98927EAE29E64
DE76B17BFB1B6D6D6634C8C104A6E59F
A90F1BB43E9DB5EDFC60C15FB897C593
8625B32398C2722D96E7B972580A0238
D1FDE3A78C9D2E80C2303CC4E3E92A4C
B355E909FD55C5E9EF1A6E67E9C18203
ADB59A303C6260DBE466F0149AB11A4A
5CEBD524469A075FB6B42D06C9BF27AD
0E0886EEAA119CF14F1C54387060929A
B4F9299F05A327E60543C4CDE3277FC0
E4B2F09505726306314DF05B734FD9D0
4DD0497CBAABBA058574A611B26151BA
7073C6C01DEE4E158F554555F697F7D9
EB72415ECD0B4AACBDEEA3734F4349BF
BED90D98FA3A1E0A5BD78AD54E55774D
3CDCD81930F91AC0B990664931E5412E
763B0C2A7B83066A9D995C8C4FD9E35E
720DF591261D710ADC73127C1BC4303D
C06C12DBBC7055FE40950803238EC104
62BF5A170CC779ADE7EF0090F395D5E6
61BF9A0FF2CE9D55D86BC063839F72F4
B5D7A148CA6C1F9693A2C16ACDD66226
35FBDCDF923F99B5E1C5FF4423B715B8
F1EBE73557546DC8B21E0A2DE5E3A33E
EBE7561CA573DA5DBB8EFAA250A40FD3
6BACB6C5B74FA747A3CF375EC3095035
6C1950AA83F4663F1BA063B5275C25EC
56EF1EE54D65EF7B39AF541E95BB45A9
2B1EA767EC59E46364BC2DF9B1F30B97
3913B1E1C35BDDF02CE03C916E8AA638
AFA2F7E964280B36DB0D714B86256F54
022E35B1ACD40F040C444DF32A7B8DE6
170370B60D515F164119BE54FD55E1ED
CBFE437C9B62805C4353516699E44649
5FFA79AB76CE359089A2F729A1D44B31
5298BCBD11B3952E3FDDC6FDD6711F5C
1836289F75F74A0BA5E769561DE3E7CD
DEB427AC9F1E8A0D0237049C80DF7E7F
FD8FE350325318C893AFE03F9DFC7096
A8031D608F6549941879981764674DD7
DDAD29B8B1215191E7EB5AAEE0219338
3F8A5EA1756DDF4A6B6F2645B4911486
30DF96D87EEC8CA77A135ECCAB1AD25E
7DD8E0E1906C1754E11E901927CCABBD
DAC51C3D23B163601305AF99DF129689
D77EC92400AE0D9FA57DEF4DD8CFA4D4
09369288E36D7AFFEE94EA81998FA316
EEBE1885532234328919191 3F6D769EB
C00132DA154BDEE361EDEE727226D0F5
6580BE22A0566352B9622777BFCB7164
7352C61297D6B04E874EDAD12480F78E
F658C0D52B3EEF71DDE6C284E7E1B337
E1253D04A17AB8E47F4A5916B9BF9D23
8922A9A23BE960FFE9707A0B3F4D75BD
EAE97F465015E49A14F3B23403ACFA11
13A757022817C0514A5C142FE9BF143A
5132F0FCB3F8DCAA501C620575D33FEE
39953BF6383A00D29BEB377568E3DE7A
67887932934DFF086153CA905E7DE9EE
DCD1072719692871126E4159D80EFDA8
C6741E3D08C0FFD4617B94E654DD89F1
D0BA58BA609CC1A001F612987A822BEF
6B339433956F1505104BB231314A153E
C1366C7246041A3089E1C244C5DC42E7
61D11B35765ECB85890D5349786D9FCA
44C287C1C3697367B0E6CB78A78C1DF5
DAACF72BC91FB6DA90A804933CB72E23
2ACBA14BB6F65F7BD0A485BFCB6D023F
84BE5D762F37E9018D623C8E91F4D924
1A89324D6D3E6DE6726C688BFF225DDD
F5FA42A5B421705E4803DA93C4F7E099
A869B96BCDF1D474C0714763AA34A8C9
3EA0F90DE57187FC7E1AC45AE44D16C6
F7DE638B76C3958AA3413A9785A19900
3F8C9CDAACBB533AE94F47456819FA0E
209920C169512D3EB4A1ED7CAD17D033
B2F57BD01BAAF7AF01EF442910CEBBA0
C0766829AA4D2E1A5D97213A4E4A654E
FC9993EA7A4E761B6CB79ABE2BD3CDE1
4D556B338FAA020979A740B4C3AEE28C
8ED896B9A622FF24559A3429E5888E0A
8CF1F45323EC5AB449451E7A9476CFDC
D1718E9BD91257D2169C81197D508A67
E4A691D602667849 68DF971D6BF473AF
B3B64F1925F759A2E145190333D1D6D2
ED4C2EBC14B85F46A9A75F159DF8BEB3
CDBC0441C10DB5ABA43120E63A048425
DC1665266A0198728861AC99ED368928
706BBC770C62D41DD799721ABD1868AB
B2205D8CBDDFE49D7C5F0F95D506718F
901F30DB86EEB1666F5A8CAE1C7BD08B
9A3A951BE27E0729726FD8B80060E7E1
6410577C738133297472F6C22C2BB397
C8C06B0C6B7FE7CA66BCFE617AB6C4E6
58C18B290620E18B8C78AC1912E5DCD7
2F5ABFDCCAB1A2927E54283296F19FB8
A07CB7881E35C91FD9C5D20F6102572C
05E2E6A4CD09EA54D665B075FE22A256
8BA800DDDD865B6BF3A85ADEC4C29730
07B546E8E002FC5854651BE31802F96D
DF2AD7F766E2EEFAF0FD1FB5C6883AB4
1C6EA2DA6ECED5C5C761BCA9CA4C5308
A640A29E706AF38557B86619EAF45E7A
F88885670C3D55EBA52096A65310DACA
B85E7BB83667097F15D8A3DEAAA1B198
A5F6F149B468683318DC178F4208E237
04841B82A9D81E44CB4F2D98CFE7C374
A81686CEFDEFFCE82B8DBF100E1395F1
9952073595776A3D7A8101664A56AB96
A076DA72A8C8E2137F05FE3FA59870EB
121378A6DE0A13DDB295106E912A4E14
65A925E578098658FADA30E9FB67B5E4
5B8E5202EC6769F2389605D33DC245B2
EA71F746BD17D1B05450329818572F2E
DD8C315D2CA61870CBCF9D56ED7474E2
F346A1E62FED476F472560C6DDE0CADC
CBBCB9E06F9FC92C533B2F2A5284BA22
79DCFDA2700E06F8EAA640BA9B827810
17CF5474D5A8B4E735E69E017CEC2F37
7034FBF641CEB257FC109A6819D19DA0
6E6D052B5ABC015C779EA3500FA11A28
FAB79682C8EAE556F11ECF6DAD7121BA
0370390E48A7F26AA62188A79E612DC3
59F8BDDA3F56D8026FAB6E3130F5D843
C731140FAA7690918BABF17BECB7938D
8C605DFAA0EC88CDB7D12F7250C9F53A
68F252CD36F2798A2182F6406A31A5A2
BD7CB0D124DFDE784CD5B9EF288C304E
3D2BC95A85EF539A68DAC84542A1AE7A
8CC74931E64061491652CC169C8BAAB3
4157D99E46A3E45E6130A95645410DAC
E34C4FC7488C4DFEF0EA475A17AF2C7B
```

These serials might have been issued by the following CAs (list incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- DigiNotar Qualified CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- Koninklijke Notariele Beroepsorganisatie CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association

- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- Stichting TTP Infos CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TU Delft CA

6.3 Plain text left in script to generate signatures on rogue certificates

```
I know you are shocked of my skills, how i got access to your network
to your internal network from outside
how I got full control on your domain controller
how I got logged in into this computer
HoW I LEARNED XUDA PROGRAMMING
HOW I got this IDEA to write such XUDA code
How I was sure it's going to work?
How i bypassed your expensive firewall, routers, NetHSM, unbreakable hardware keys
How I did all xUDA programming without 1 line of resource, got this idea, owned your
. network accesses your domain controlled, got all your passwords, signed my certificates
. and received them shortly
THERE IS NO ANY HARDWARE OR SOFTWARE IN THIS WORLD EXISTS WHICH COULD STOP MY HEAVY
. ATTACKS
MY BRAIN OR MY SKILLS OR MY WILL OR MY EXPERTISE
That's all ok! EVerything I do is out of imagination of people in world
I know you'll see this message when it is too late, sorry for that
I know it's not something you or any one in this world have thought about
But everything is not what you see in material world, when God wants something to happen


My signature as always: Janam Fadaye Rahbar


Rahbare azizam mesle hamishe asoode bash, ta vaghti ke man va amsale man baraye in marzo
. boom
va baraye barafrashte negah dashtane parchame velayate faghih kar mikonand
daste har doshmano mozdouri ghat khahad bood
Rahbaram, Tamame vojoodam fadaye to ke ham jani o ham janani
```

6.4 Timeline

06-Jun-2011	Possibly first exploration by the attacker(s)
17-Jun-2011	Servers in the DMZ in control of the attacker(s)
02-Jul-2011	First attempt creating a rogue certificate
10-Jul-2011	The first succeeded creation of rogue certificate (*.Google.com)
19-Jul-2011	Incident detected by DigiNotar by daily audit procedure
20-Jul-2011	Last known succeeded rogue certificate was created
22-Jul-2011	Last outbound traffic to attacker(s) IP (not confirmed)
22-Jul-2011	Start investigation by IT-security firm (not confirmed)
27-Jul-2011	Delivery of security report of IT-security firm
27-Jul-2011	First rogue *.google.com OSCP request
28-Jul-2011	First seen that rogue certificates were verified from Iran
04-Aug-2011	Start massive activity of *.google.com on OCSP responder
27-Aug-2011	First mention of *.google.com certificate in blog
29-Aug-2011	GOVCERT.NL is notified by CERT-Bund
29-Aug-2011	The *.google.com certificate is revoked
30-Aug-2011	Start investigation by Fox-IT
30-Aug-2011	Incident response sensor active
01-Sep-2011	OSCP responder based on white list

Interim Report

September 5, 2011
(rectifications)

DigiNotar Certificate Authority breach
"Operation Black Tulip"

Classification **PUBLIC**

Customer DigiNotar B.V.

Subject: Investigation DigiNotar Certificate Authority Environment

Date 105 ~~September~~ October 2011
Version 1.1~~0~~
Author J.R. Prins (CEO Fox-IT)
Business Unit Cybercrime
Pages 16~~13~~

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

1 Document Management

Version management

This version replaces all previous version of this document. Please destroy all previous copies!

Distribution list

Copy	Distribution (version)	Name/function/remarks

Review management

Review by	Function	Date	Version

Change management

Version	Date	By	Remarks	Approval
1.0	05-sep-2011	J.R. Prins		
1.0a	05-sep-2011	J.R. Prins	Minor layout changes	
1.1	10-oct-2011	J.R. Prins	Rectification of dates, minor addition of details	

Related documents

Version	Date	Description	Remarks

Table of Contents

Met opmaak: Standaard

~~1~~2 Introduction

~~1.1~~2.1 Background

The company DigiNotar B.V. provides digital certificate services; it hosts a number of Certificate Authorities (CA's). Certificates issued include default SSL certificates, Qualified Certificates and 'PKIoverheid' (Government accredited) certificates.

On the evening of Monday August 29th it became public knowledge that a rogue *.google.com certificate was presented to a number of Internet users in Iran. This false certificate had been issued by DigiNotar B.V. and was revoked[1] that same evening.

On the morning of the following Tuesday, Fox-IT was contacted and asked to investigate the breach and report its findings before the end of the week.

Fox-IT assembled a team and started the investigation immediately. The investigation team includes forensic IT experts, cybercrime investigators, malware analysts and a security expert with PKI experience. The team was headed by CEO J.R. Prins directly.

It was communicated and understood from the outset, that Fox-IT wouldn't be able to complete an in-depth investigation of the incident within this limited timeframe. This is due to the complexity of the PKI environment and the uncommon nature of the breach.

Rather, due to the urgency of this matter, Fox-IT agreed to prepare an interim report at the end of the week with its preliminary findings, which would be published.

~~1.2~~2.2 Investigation questions

The investigation predominately focused on following questions:

1. How did the perpetrators access the network?

2. What is the scope and status of the breach?
   - *Have other DigiNotar CA environments been breached?*
   - *Do we still see hacker activity on the network of DigiNotar?*
   - *Are rogue certificates actively being used by hackers?*

3. Can we discover anything about the impact of the incident?
   - *What certificates were issued without knowledge of DigiNotar?*
   - *What other (rogue) certificates might have been generated?*
   - *How many rogue connections were made using rogue certificates?*
   - *What was the nature of these connections?*

In order to address these questions we (basically) (i) implemented specialized monitoring to be able to detect, analyse and follow up on active misuse, and (ii) analysed digital traces on hard disks, and in databases and log files to investigate the origin and impact of the breach.

[1] Revoked: A certificate is irreversibly revoked if, for example, it is discovered that the certificate authority (CA) had improperly issued a certificate, or if a private-key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements such as publication of false documents, mis-representation of software behavior, or violation of any other policy specified by the CA operator or its customer. The most common reason for revocation is the user no longer being in sole possession of the private key (*e.g.*, the token containing the private key has been lost or stolen).

~~1.3~~2.3 This report

The goal of this report is to share relevant information with DigiNotar stakeholders (such as the Dutch Government and the Internet community), based on which they can make their own risk analysis. Because this is a public report, some investigation results and details cannot be included for privacy and/ or security reasons.

Since the investigation has been more of a fact finding mission thus far, we will not draw any conclusions with regards to the network-setup and the security management system. In this report we will not give any advice to improve the technical infrastructure for the long term. Our role is to investigate the incident and give a summary of our findings until now. We leave it to the reader in general and other responsible parties in the PKI- and internet community to draw conclusions, based on these findings. We make a general reservation, as our investigations are still on-going.

~~2~~3 Investigations

~~2.1~~3.1 Prior investigations

Some investigations were conducted before we started.

Fox-IT was given access to a report produced by another IT-security firm which performs the regular penetration testing and auditing for DigiNotar. The main conclusions from this report dated July 27th were:

> A number of servers were compromised. The hackers have obtained administrative rights to the outside webservers, the CA server "Relaties-CA" and also to "Public-CA". Traces of hacker activity started on June 17th and ended on July 22nd.

Furthermore, staff from DigiNotar and the parent company Vasco performed their own security investigation. E-mail communication and memos with further information were handed over to us.

This information gave us a rough overview of what happened:

- The signing of 128 rogue certificates was detected on July 19th during the daily routine security check. These certificates were revoked immediately;
- During analysis on July 20th the generation of another 129 certificates was detected. These were also revoked on July 21th;
- Various security measures on infrastructure, system monitoring and OCSP validation have been taken immediately to prevent further attacks.
- More fraudulent issued certificates were discovered during the investigation and 75 more certificates were revoked on July 27th.
- ~~On July 29th a *.google.com certificate issued was discovered that was not revoked before. This certificate was revoked on July 29th.~~
- DigiNotar found evidence on July 28th that rogue certificates were verified by internet addresses originating from Iran.
- On August 29th a *.google.com certificate issued was discovered that was not revoked before. This certificate was revoked on August 29th.

On August 30th Fox-IT was asked investigate the incident and recommend and implement new security measures. Fox-IT installed a specialized incident response network sensor to assist in the investigation. Furthermore we created images of several other servers.

~~2.2~~3.2 Monitoring

The rogue certificate found by Google was issued by the DigiNotar Public CA 2025. The serial number of the certificate was, however, not found in the CA system's records. This leads to the conclusion that it is unknown how many certificates were issued without any record present. In order to identify these unknown certificates and to prevent them from being used by victims, the OCSP responder[2] requests were monitored.

Current browsers perform an OCSP check as soon as the browser connects to an SSL protected website through the https-protocol[3]. The serial number of the certificate presented by the website a user visits is send~~d~~t to the issuing CA OCSP-responder. The OCSP-responder can only answer either with 'good', 'revoked' or 'unknown'. If a certificate serial number is presented to the OCSP-responder and no record of this serial is found, the normal OCSP-responder answer would be 'good'[4]. The OCSP-responder answer 'revoked' is only returned when the serial is revoked by the CA. In order to prevent misuse of the unknown issued serials the OCSP-responder of DigiNotar has been set to answer 'revoked' when presented any unknown certificate serial it has authority over. This was done on September 1st.

[2] The **Online Certificate Status Protocol** (**OCSP**) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
[3] Other applications using certificates can also use the OCSP verification method.
[4] According to the RFC2560

The incident response sensor immediately informs if a serial number of a known fraudulently issued certificate is being misused. Also, all unknown serial number requests can be analysed and used in the investigation. A~~n~~ large number of requests to a single serial number is suspicious and will be detected. Note that advanced methods for misusing the rogue certificates are possible by which a thorough attacker can circumvent our detection method.

The incident response sensor logged all network traffic since August 30th. Current analyses still show hacking attempts on the web server originating from Iran. During monitoring, we also saw unusual traffic after the company F-Secure announced its findings of a possible earlier breach of the website.[5] We haven't investigated this breach yet in detail. In August, DigiNotar installed a new web server. It's fair to assume these hacker traces where copied from the previous web server install.

~~2.3~~3.3 CA servers investigation

DigiNotar hosts several CA services on different servers. Earlier reports indicated two of these servers where compromised and misused by the attacker(s). It was essential to verify the status of the other CA systems and investigate if they were compromised or misused. Forensic disk images were made of all the CA servers for investigation.

Because of security implications, the details of these results are not shared in this public report. More generally, we found traces of hacker activity with administrator rights on the Qualified and PKIoverheid CA server as well as on other CA servers. On the CA systems a web page has been accessed on a server in the demilitarized zone (DMZ) that contained several hacker tools and malware. This web page was also accessible from the internet with a password making it a stepping stone for the attacker. Logs show that outside office hours on 1 and 2 July files were transferred. Furthermore, we can share that on September 3rd more rogue certificates were discovered. The list of certificates is in the Annex 5.1.

The log files on the Qualified & PKI Overheid CA server do not show traces of deleted entries. These traces are present on other CA servers, where rogue certificates were produced. During further investigation however, we encountered several serial numbers of certificates that cannot be related to trusted certificates. Two of these were found on the Qualified & PKI Overheid CA server. It might be possible that these serial numbers have been temporarily generated by the CA software without being used. Alternatively, these serials were generated as a result of a bug of the software. However, we cannot rule out the possibility that these serial numbers relate to rogue certificates. Further investigation needs to be done to confirm or contradict this. The list of serials is in the Annex 5.2; this list has been communicated with the web browser vendors.

~~2.4~~3.4 Firewall investigation

The firewall log files have not been analysed yet.

~~2.5~~3.5 Malicious software analyses

A number of malicious/hacker software tools was found. These vary from commonly used tools such as the famous Cain & Abel tool[6] to tailor made software.

Specifically developed software probably enabled the hackers to upload the generated certificates to a dropbox. Both the IP-addresses of an internal DigiNotar server and the IP-address of the dropbox were hardcoded in the software. Possibilities are being explored to investigate this server, as (parts of) the uploaded rogue certificates might be still available there.

A script was found on CA server public 2025. The script was written in a special scripting language only used to develop PKI software. The purpose of the script was to generate signatures by the CA for certificates which have been requested before. The script also contains English language which you can find in Annex 6.3~~5.3~~. In the text the hacker left his fingerprint: *Janam Fadaye Rahbar*[7]. The same text

[5] The IT-Security company F-Secure blogs about a breach of the webserver of DigiNotar in May 2009. http://www.f-secure.com/weblog/archives/00002228.html

[6] Cain&Abel is a very powerful hackers toolkit. It's capable of sniffing and breaking passwords. Most anti-virus software will detect C&A and flag i~~t~~ as malicious.

[7] Supposedly meaning: "I will sacrifice my soul for my leader"

was found in the Comodo hack in March of this year[8]. This breach also resulted in the generation of rogue certificates.

[8] http://www.wired.com/threatlevel/2011/03/comodo_hack/

~~3~~4 Provisional results

~~3.1~~4.1 *Fraudulent issued certificates*

In total 531 fraudulent certificates have been issued. We have no indication that more certificate were issued by the attacker(s). 344 Of these contain a domain name in the common name. 187 Certificates have in the common name 'Root CA'. We have reason to believe these certificates are not real CA certificates but normal end user certificates.

~~3.2~~4.2 *Compromised CAs*

The attacker(s) had acquired the domain administrator rights. Because all CA servers were members of the same Windows domain, the attacker had administrative access to all of them. Due to the limited time of the ongoing investigation we were unable to determine whether all CA servers were used by the attacker(s). Evidence was found that the following CAs *were* misused by the attacker(s):

- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- Koninklijke Notariele Beroepsorganisatie CA
- Stichting TTP Infos CA

The security of the following CAs was compromised, but no evidence of misuse was found (this list is incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Qualified CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association
- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TU Delft CA

For some of these CAs extra security measures were in place (like the CCV CA). This makes it more unlikely they were misused.

~~3.3~~4.3 Misuse

We investigated the OCSP responder log files around the time of the *.google.com incident. That incident was detected on August 27th. The first known public mention was a posting in a google forum. The user (from Iran) was warned by the Google Chrome browser that there was something wrong with the certificate. The corresponding rogue certificate was created on July 10th.

Based on the logging mentioned above from the OCSP responder, we were able to extract the following information. On August 4th the number of request rose quickly until the certificate was revoked on August 29th at 19:09. Around 300.000 unique requesting IPs to google.com have been identified. Of these IPs >99% originated from Iran, as illustrated in figure 1.[9]

Figure 1: OCSP requests for the rogue *.google.com certificate

A sample of the IP's outside of Iran showed mainly to be TOR-exit nodes, proxies and other (VPN) servers, and almost no direct subscribers.

The list of IP-addresses will be handed over to Google. Google can inform their users that during this period their e-mail might have been intercepted. Not only the e-mail itself but also a login cookie could have been intercepted. Using this cookie the hacker is able to log in directly to the Gmail mailbox of the victim and also read the stored e-mails. Besides that, he is able to log in all other services Google offers to users like stored location information from Latitude or documents in GoogleDocs. Once the hacker is able to receive his targets' e-mail he is also able to reset passwords of others services like Facebook and Twitter using the lost password button. The login cookie stays valid for a longer period. It would be wise for all users in Iran to at least logout and login but even better change passwords.

Other OSCP request logs show some activity on August the 30th with a misused *.torproject.org certificate. None of these originated from Iran. However this does not prove that rogue certificates weren't abused between the issue date and revocation date of the certificates based on the OCSP logs because some applications might not use the OCSP protocol for revocation checking.

[9] This static image shows all IP-addresses detected. On http://www.youtube.com/watch?v=wZsWoSxxwVY ~~http://www.youtube.com/watch?v=_eIbNWUyJWQ~~ you can see the interception of Google users taking place in a timeline.

~~4~~5 Discussion

~~4.1~~5.1 Skills and goal of the hackers

We found that the hackers were active for a longer period of time. They used both known hacker tools as well as software and scripts developed specifically for this task. Some of the software gives an amateurish impression, while some scripts, on the other hand, are very advanced. In at least one script, fingerprints from the hacker are left on purpose, which were also found in the Comodo breach investigation of March 2011. Parts of the log files, which would reveal more about the creation of the signatures, have been deleted.

The list of domains and the fact that 99% of the users are in Iran suggest that the objective of the hackers is to intercept private communications in Iran.

~~4.2~~5.2 Other possible rogue certificates

Using the OCSP responder requests we verify if the requested serial belongs to a known certificate. We have seen requests for unknown serials that cannot be matched against a known certificate. It's possible that these serials belong to a "rogue" certiticate or are just bogus OCSP requests, for instance done by security researchers. It's still possible other unknown[10] rogue certificates have been produced.

OCSP logging could still catch other possible rogue certificates based on the number of requests for an unknown serial, although it's difficult to match the common name with that serial if the certificate in question is not known.

~~4.3~~5.3 Trust in the PKIoverheid and Qualified environment

Although all CA-servers have been accessed by a hacker with full administrative access rights and attempts have been made to use the running PKI-software we have no proof of generated rogue Qualified or PKIoverheid certificates. The log files of these CA-Servers validate as correct and no deleted log files have been found on these CA-servers. This is in contrast to our findings on the other breached CA servers.

Investigators encountered two (2) serial numbers of certificates on the Qualified or PKIoverheid server that cannot be related to trusted certificates[11]. Based on this, we cannot rule out the possibility that these relate to rogue certificates.

~~4.4~~5.4 Current network infrastructure at DigiNotar

The successful hack implies that the current network setup and / or procedures at DigiNotar are not sufficiently secure to prevent this kind of attack.

The most critical servers contain malicious software that can normally be detected by anti-virus software. The separation of critical components was not functioning or was not in place. We have strong indications that the CA-servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the management LAN.

The network has been severely breached. All CA servers were members of one Windows domain, which made it possible to access them all using one obtained user/password combination. The password was not very strong and could easily be brute-forced.

The software installed on the public web servers was outdated and not patched.

No antivirus protection was present on the investigated servers.

An intrusion prevention system is operational. It is not clear at the moment why it didn't block some of the outside web server attacks. No secure central network logging is in place.

[10] Unknown as in, that we haven't been able to revoke them yet because we don't know their existence.
[11] OCSP requests to these serial numbers will result in a 'revoke' reply.

~~5~~6 Appendix

~~5.1~~6.1 *Fraudulent issued certificates*

The following list of Common Names in certificates are presumed to be generated by the attacker(s):

Common Name	Number of certs issued
CN=*.*.com	1
CN=*.*.org	1
CN=*.10million.org	2
CN=*.JanamFadayeRahbar.com	1
CN=*.RamzShekaneBozorg.com	1
CN=*.SahebeDonyayeDigital.com	1
CN=*.android.com	1
CN=*.aol.com	1
CN=*.azadegi.com	1
CN=*.balatarin.com	3
CN=*.comodo.com	3
CN=*.digicert.com	2
CN=*.globalsign.com	7
CN=*.google.com	26
CN=*.logmein.com	1
CN=*.microsoft.com	3
CN=*.mossad.gov.il	2
CN=*.mozilla.org	1
CN=*.skype.com	22
CN=*.startssl.com	1
CN=*.thawte.com	6
CN=*.torproject.org	14
CN=*.walla.co.il	2
CN=*.windowsupdate.com	3
CN=*.wordpress.com	14
CN=Comodo Root CA	20
CN=CyberTrust Root CA	20
CN=DigiCert Root CA	21
CN=Equifax Root CA	40
CN=GlobalSign Root CA	20
CN=Thawte Root CA	45
CN=VeriSign Root CA	21
CN=addons.mozilla.org	17
CN=azadegi.com	16
CN=friends.walla.co.il	8
CN=login.live.com	17
CN=login.yahoo.com	19
CN=my.screenname.aol.com	1
CN=secure.logmein.com	17
CN=twitter.com	19
CN=wordpress.com	12
CN=www.10million.org	8
CN=www.Equifax.com	1
CN=www.balatarin.com	16
CN=www.cia.gov	25
CN=www.cybertrust.com	1
CN=www.facebook.com	14
CN=www.globalsign.com	1
CN=www.google.com	12
CN=www.hamdami.com	1
CN=www.mossad.gov.il	5
CN=www.sis.gov.uk	10
CN=www.update.microsoft.com	4

Met opmaak: Aantal kolommen: 1

~~5.2~~6.2 *Unknown serial numbers*

Root-CA server

On the 'Root-CA' server the following serials were encountered:

```
83120A023016C9E1A59CC7D146619617
68E32B2FE117DFE89C905B1CCBE22AB7
711CE18C0423218425510EF51513B7B8
B7ABEFC8A1F844207B774C782E5385B3
6E0088D11C7E4E98CC9E0694D32A0F6B
80C990D339F177CA9FDAC258105882AB
7F73EC0A14C4BA065BECFAD69DC5A61D
```

Qualified-CA server

On the 'Qualified-CA' server the following serials were encountered:

```
C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4
```

These serials might have been issued by the following CAs:

- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven

'Taxi-CA

On the 'Taxi-CA' server the following serials were encountered:

```
25B6CA311C52F0E4F72A1BD53774B5B3
A0CF459D0D1EA9A946861A0A02783D88
71A10FA4C491D3A72D18D33E3CCF576C
FE456B099700A6C428A193FE5968C9FD
E7E2B46B8C9AA64679E03841F88CA5A0
AEC9F2324D80020B6E2B2A1103D6A4E8
CB20C25F14583AFC86465F14E621FBC1
947FF1DB66A41D809A9BC7E7344E342A
90BCA541B4DF5E77FB1349684F84A930
AB4967CE8B94FCF8DA7691922E6FD59C
BA479991C9103C005726FAB83088A8D6
363E9AAF4DAC7085F31B89B2AC49059A
8A63042B8A8FA256035773BC9417435A
963CCB2601B15C73DCA821F4BC4C7458
6B7057D5DE0170842C372821D3F17DB2
C391438C15FF31BD89544A7F68DDF3B3
7278CB2A8270A3E66A021A7CD75F1211
F401D4C50FCA9161A70ED9D91D40E684
6C396359C423417E20C54CFC6690F3FF
9916C8350225BB607857375A02B6DC72
0F48A14121370B5CF4828EF826749FBC
DB43E2CE6110750785FCBBE9A8EAE061
C641E4B7F19B63C4FF1EA6D3833FC874
D8B771F90BC01C9ED1333C23EF24CFC1
```

'Public-CA server

On the 'Public-CA' server the following serials were encountered:

```
79C03FE0C81A3022DBF8143B27E40223    8B0EABAF922D4C6E6917FCBE365DD64A    82C42F0EDC18BD751727BE5C54413EF7
FCCF53CB3D0A71494AF9664690FFCF84    4FC2D72D6427CABBE3E859453865F43B    03124C25849D9E49BC2A2FAD3E10C8A4
82BC18B1AA5D59C61D0EFDBEA7664C08    53B53BF2F74997EBEB2577D63DA692B7    EFF0DD4B4927DF64232C5D2FF280C1E4
5D4352671C39616670B2F34C173A1F63    ABB21F43553F2695031A1C85355D7F1C    9EDCB5E1FE1255A2F1D7FC52C4AFA3B1
6FA3C48173B3B289943F113A8CD9DB8C    5563605FDC2DC865E2A1C32995B5A086    3A32AAA9DFE2CA7F9E003885E316944B
CFAF9BE4E5BD0F5A75F628E45E0178C9    5DD6A72747D90C018B63F959DFE7C976    4455B43B9173CBAE4E247272EE2573D5
4ADA28D281D3D14D19FB782D64086D0C    CAB736FFE7DCB2C47ED2FF88842888E7    B95F62E86194734C9F68D4BF8B200C49
0B41ABEE6F4168D3CDE5A7D223B58BC1    9C79C9FE16727BAC407B4AA21B153A54    FE873B742B230B22AE540E840490A2F4
13548FC160BC5C9F315AE28CDB490E36    2D711C9CB79EC15445747BFE3F8BC92F    8779917563EC38B7746B8ECAFE239BE6
5D8D0D43611275982E6A5490E7F87BD7    752A2D0325A3D34D9F5198C2F5C92A6C    72CBC4824C6215B139FDE6BA10DAC6AD
C880AE4D7927E6A8FA7D456CB03E9763    39936336286F843756FC4BC296D7A8E0    8D09D4B98DE67C9E9C7C18CB72AD2418
82072FC8F8DD7E6C0ECE9B47185F0521    4A6D90618A5CA6797C768C03C860C4F8    07BC72A463D4DE33B2BE733D6FAC991D
90DB656E273476CC836778255582FA8B    0954E1AB9141ED7E8B640FE681046451    D3E2205C3B899FC99D77FE802985283F
171A8599EDE711A3315BC7D694CEBEC6    8259C3E1DB6C2C9B7FCD6A305EADEFE4    A5029D6A057D50D20ECFE0E528EDA067
E9EB8075F7FE3683B431552C2D962CB0    BC01852405D3F4E22C486002666555026    C8B2487ADFAF969E34306029AC934406
E6F9E095464F64448840A832FB3443DB    9F7DDFE3CAAD224EC6BD68B60DE78550    5F3C1BDC7A2BCD47ABAF0C8E62D9F757
C83D16E9CB29DCF35F3B351CB942FE0D    A67C22A6E1F9D87799548EBFC7D5527E    601315BB085FECF29538DA3F9B7BA1CE
39B5DD0ECC85C3F62A72391DC055F561    11661878CCE9DC337CEEBB16E30F9A3A    30170F15A240446E6B482E0A364E3CCA
DF3FD6AFBBFBC30C9AD80BF764A102DB    6BF3BEB26AFF31116200B14F4378C33B    0590B310AEFC7A3EDC03ECA2A6F6624F
327B9A443C49018D7B0A97B6EC2254B8    7A61A7778842E502E2291166C4574485    FDEB145AAC81B8CD29B8DA018E71456F
```

```
C3F9F45F19E334C8303F44288856D843    DEB427AC9F1E8A0D0237049C80DF7E7F    ED4C2EBC14B85F46A9A75F159DF8BEB3
028CF7556F8BE27026800448FA6AA527    FD8FE350325318C893AFE03F9DFC7096    CDBC0441C10DB5ABA43120E63A048425
E93B28B47C34B243EBA62E58FE2FF46F    A8031D608F65499418799817646 4DD7    DC1665266A0198728861AC99ED368928
F89F5DE575755A3B4C0DECC6EDA7C804    DDAD29B8B1215191E7EB5AAEE0219338    706BBC770C62D41DD799721ABD1868AB
5D8F8D78B0C19EF4479F744DECBD84BC    3F8A5EA1756DDF4A6B6F2645B4911486    B2205D8CBDDFE49D7C5F0F95D506718F
EAACDC2F46D4A86F39B035B793F4A94F    30DF96D87EEC8CA77A135ECCAB1AD25E    901F30DB86EEB1666F5A8CAE1C7BD08B
9D06313F21A4EDF734C324FFBCB9E2B5    7DD8E0E1906C1754E11E901927CCABBD    9A3A951BE27E0729726FD8B80060E7E1
35C54E845AE855F818504C8C189F52C7    DAC51C3D23B163601305AF99DF129689    6410577C738133297472F6C22C2BB397
E3E120935934CBD77E1DA7F00431F745    D77EC92400AE0D9FA57DEF4DD8CFA4D4    C8C06B0C6B7FE7CA66BCFE617AB6C4E6
0A6DFACFDEAE74A816031534BE90B75A    09369288E36D7AFFEE94EA81998FA316    58C18B290620E18B8C78AC1912E5DCD7
9AD82BE2FED538B10BDFBD229A8A5AEA    EEBE1885532234328919 1913F6D769EB    2F5ABFDCCAB1A2927E54283296F19FB8
C0F216CA8197AD00F0D98927EAE29E64    C00132DA154BDEE361EDEE727226D0F5    A07CB7881E35C91FD9C5D20F6102572C
DE76B17BFB1B6D6D6634C8C104A6E59F    6580BE22A0566352B9622777BFCB7164    05E2E6A4CD09EA54D665B075FE22A256
A90F1BB43E9DB5EDFC60C15FB897C593    7352C61297D6B04E874EDAD12480F78E    8BA800DDDD865B6BF3A85ADEC4C29730
8625B32398C2722D96E7B972580A0238    F658C0D52B3EEF71DDE6C284E7E1B337    07B546E8E002FC5854651BE31802F96D
D1FDE3A78C9D2E80C2303CC4E3E92A4C    E1253D04A17AB8E47F4A5916B9BF9D23    DF2AD7F766E2EEFAF0FD1FB5C6883AB4
B355E909FD55C5E9EF1A6E67E9C18203    8922A9A23BE960FFE9707A0B3F4D75BD    1C6EA2DA6ECED5C5C761BCA9CA4C5308
ADB59A303C6260DBE466F0149AB11A4A    EAE97F465015E49A14F3B23403ACFA11    A640A29E706AF38557B86619EAF45E7A
5CEBD524469A075FB6B42D06C9BF27AD    13A757022817C0514A5C142FE9BF143A    F88885670C3D55EBA52096A65310DACA
0E0886EEAA119CF14F1C54387060929A    5132F0FCB3F8DCAA501C620575D33FEE    B85E7BB83667097F15D8A3DEAAA1B198
B4F9299F05A327E60543C4CDE3277FC0    39953BF6383A00D29BEB377568E3DE7A    A5F6F149B468683318DC178F4208E237
E4B2F09505726306314DF05B734FD9D0    67887932934DFF086153CA905E7DE9EE    04841B82A9D81E44CB4F2D98CFE7C374
4DD0497CBAABBA058574A611B26151BA    DCD1072719692871126E4159D80EFDA8    A81686CEFDEFFCE82B8DBF100E1395F1
7073C6C01DEE4E158F554555F697F7D9    C6741E3D08C0FFD4617B94E654DD89F1    9952073595776A3D7A8101664A56AB96
EB72415ECD0B4AACBDEEA3734F4349BF    D0BA58BA609CC1A001F612987A822BEF    A076DA72A8C8E2137F05FE3FA59870EB
BED90D98FA3A1E0A5BD78AD54E55774D    6B339433956F1505104BB231314A153E    121378A6DE0A13DDB295106E912A4E14
3CDCD81930F91AC0B990664931E5412E    C1366C7246041A3089E1C244C5DC42E7    65A925E578098658FADA30E9FB67B5E4
763B0C2A7B83066A9D995C8C4FD9E35E    61D11B35765ECB85890D5349786D9FCA    5B8E5202EC6769F2389605D33DC245B2
720DF591261D710ADC73127C1BC4303D    44C287C1C3697367B0E6CB78A78C1DF5    EA71F746BD17D1B05450329818572F2E
C06C12DBBC7055FE40950803238EC104    DAACF72BC91FB6DA90A804933CB72E23    DD8C315D2CA61870CBCF9D56ED7474E2
62BF5A170CC779ADE7EF0090F395D5E6    2ACBA14BB6F65F7BD0A485BFCB6D023F    F346A1E62FED476F472560C6DDE0CADC
61BF9A0FF2CE9D55D86BC063839F72F4    84BE5D762F37E9018D623C8E91F4D924    CBBCB9E06F9FC92C533B2F2A5284BA22
B5D7A148CA6C1F9693A2C16ACDD66226    1A89324D6D3E6DE6726C688BFF225DDD    79DCFDA2700E06F8EAA640BA9B827810
35FBDCDF923F99B5E1C5FF4423B715B8    F5FA42A5B421705E4803DA93C4F7E099    17CF5474D5A8B4E735E69E017CEC2F37
F1EBE73557546DC8B21E0A2DE5E3A33E    A869B96BCDF1D474C0714763AA34A8C9    7034FBF641CEB257FC109A6819D19DA0
EBE7561CA573DA5DBB8EFAA250A40FD3    3EA0F90DE57187FC7E1AC45AE44D16C6    6E6D052B5ABC015C779EA3500FA11A28
6BACB6C5B74FA747A3CF375EC3095035    F7DE638B76C3958AA3413A9785A19900    FAB79682C8EAE556F11ECF6DAD7121BA
6C1950AA83F4663F1BA063B5275C25EC    3F8C9CDAACBB533AE94F47456819FA0E    0370390E48A7F26AA62188A79E612DC3
56EF1EE54D65EF7B39AF541E95BB45A9    209920C169512D3EB4A1ED7CAD17D033    59F8BDDA3F56D8026FAB6E3130F5D843
2B1EA767EC59E46364BC2DF9B1F30B97    B2F57BD01BAAF7AF01EF442910CEBBA0    C731140FAA7690918BABF17BECB7938D
3913B1E1C35BDDF02CE03C916E8AA638    C0766829AA4D2E1A5D97213A4E4A654E    8C605DFAA0EC88CDB7D12F7250C9F53A
AFA2F7E964280B36DB0D714B86256F54    FC9993EA7A4E761B6CB79ABE2BD3CDE1    68F252CD36F2798A2182F6406A31A5A2
022E35B1ACD40F040C444DF32A7B8DE6    4D556B338FAA020979A740B4C3AEE28C    BD7CB0D124DFDE784CD5B9EF288C304E
170370B60D515F164119BE54FD55E1ED    8ED896B9A622FF24559A3429E5888E0A    3D2BC95A85EF539A68DAC84542A1AE7A
CBFE437C9B62805C4353516699E44649    8CF1F45323EC5AB449451E7A9476CFDC    8CC74931E640614916 52CC169C8BAAB3
5FFA79AB76CE359089A2F729A1D44B31    D1718E9BD91257D2169C81197D508A67    4157D99E46A3E45E6130A95645410DAC
5298BCBD11B3952E3FDDC6FDD6711F5C    E4A691D60266784968DF971D6BF473AF    E34C4FC7488C4DFEF0EA475A17AF2C7B
1836289F75F74A0BA5E769561DE3E7CD    B3B64F1925F759A2E145190333D1D6D2
```

These serials might have been issued by the following CAs (list incomplete):

- Algemene Relatie Services System CA
- CCV CA
- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar PKIoverheid CA Organisatie - G2
- DigiNotar PKIoverheid CA Overheid en Bedrijven
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- DigiNotar Qualified CA
- DigiNotar Qualified CA Administrative CA
- DigiNotar Qualified CA System CA
- DigiNotar Root CA
- DigiNotar Root CA Administrative CA
- DigiNotar Root CA G2
- DigiNotar Root CA System CA
- DigiNotar Services 1024 CA
- DigiNotar Services CA
- EASEE-gas CA
- Hypotrust CA
- Koninklijke Notariele Beroepsorganisatie CA
- MinIenM Autonome Apparaten CA - G2
- MinIenM Organisatie CA - G2
- Ministerie van Justitie JEP1 CA
- Nederlandse Orde van Advocaten - Dutch Bar Association

- Orde van Advocaten SubCA Administrative CA
- Orde van Advocaten SubCA System CA
- Renault Nissan Nederland CA
- SNG CA
- Stichting TTP Infos CA
- TenneT CA 2011
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
- TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
- TU Delft CA

~~5.3~~6.3 Plain text left in script to generate signatures on rogue certificates

```
I know you are shocked of my skills, how i got access to your network
to your internal network from outside
how I got full control on your domain controller
how I got logged in into this computer
HoW I LEARNED XUDA PROGRAMMING
HOW I got this IDEA to write such XUDA code
How I was sure it's going to work?
How i bypassed your expensive firewall, routers, NetHSM, unbreakable hardware keys
How I did all xUDA programming without 1 line of resource, got this idea, owned your
. network accesses your domain controlled, got all your passwords, signed my certificates
. and received them shortly
THERE IS NO ANY HARDWARE OR SOFTWARE IN THIS WORLD EXISTS WHICH COULD STOP MY HEAVY
. ATTACKS
MY BRAIN OR MY SKILLS OR MY WILL OR MY EXPERTISE
That's all ok! EVerything I do is out of imagination of people in world
I know you'll see this message when it is too late, sorry for that
I know it's not something you or any one in this world have thought about
But everything is not what you see in material world, when God wants something to happen


My signature as always: Janam Fadaye Rahbar


Rahbare azizam mesle hamishe asoode bash, ta vaghti ke man va amsale man baraye in marzo
. boom
va baraye barafrashte negah dashtane parchame velayate faghih kar mikonand
daste har doshmano mozdouri ghat khahad bood
Rahbaram, Tamame vojoodam fadaye to ke ham jani o ham janani
```

~~5.4~~6.4 Timeline

06-Jun-2011	Possibly first exploration by the attacker(s)
17-Jun-2011	Servers in the DMZ in control of the attacker(s)
~~19-Jun-2011~~	~~Incident detected by DigiNotar by daily audit procedure~~
02-Jul-2011	First attempt creating a rogue certificate
10-Jul-2011	The first succeeded creation of rogue certificate (*.Google.com)
19-Jul-2011	Incident detected by DigiNotar by daily audit procedure
20-Jul-2011	Last known succeeded rogue certificate was created
22-Jul-2011	Last outbound traffic to attacker(s) IP (not confirmed)
22-Jul-2011	Start investigation by IT-security firm (not confirmed)
27-Jul-2011	Delivery of security report of IT-security firm
27-Jul-2011	First rogue *.google.com OSCP request
28-Jul-2011	First seen that rogue certificates were verified from Iran
04-Aug-2011	Start massive activity of *.google.com on OCSP responder
27-Aug-2011	First mention of *.google.com certificate in blog
29-Aug-2011	GOVCERT.NL is notified by CERT-Bund~~UND~~
29-Aug-2011	The *.google.com certificate is revoked
30-Aug-2011	Start investigation by Fox-IT
30-Aug-2011	Incident response sensor active
01-Sep-2011	OSCP responder based on white list

Van: [redacted] Logius [redacted]@logius.nl]
Verzonden: donderdag 8 december 2011 17:39
Aan: [redacted]
Onderwerp: concept fox-it
Bijlagen: HH-Operation Black Tulip Update (draft) 0.1-1207b[1].pdf

[redacted]

Bijgaand de huidige status van het rapport. Zou af moeten zijn op inleiding, samenvatting en evt wat toelichtingen op diensten / CA's van Diginotar na. Ik mis nog veel meer, maar ben ook nog niet direct blij met dit rapport. Ik zoek alleen nog even waar dit in zit.

[redacted]

Black Tulip

Investigation update
hack of DigiNotar

Classification	**CONFIDENTIAL**
Customer	BZK
RE:	Investigation update
Project no./Ref. no.	PR-110202_CC
Date	8 December 2011
Version	0.1
Team	Hans Hoogstraaten (Team leader) Ronald Prins (CEO and advisor) Kevin Strooy (Forensic expert) Steffen Moorrees (Forensic expert) Danny Heppener (Malware expert) Robbert Kouprie (Security Expert) 1 other Security Expert
Business Unit	Cybercrime
Pages	86

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

CONFIDENTIAL
This document is classified as confidential. Any information published in this document and its appendices is intended exclusively for the addressee(s) as listed on the document management distribution list. Only these addressee(s) and additional persons explicitly granted permissions by any of these originally authorized addressee(s) may read this document. Any use by a party other than the addressee(s) is prohibited. The information contained in this document may be confidential in nature and fall under a pledge of secrecy.

If your name is not listed on the document management page or if you have not obtained the appropriate (written) authorization to read this document from an authorized addressee, you should close this document immediately and return it to its original owner.

Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. Fox-IT cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by its contained information.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

Document Management

Version management

Project name: [project]
Customer: [customer]
Subject: [subject]
Date: [date]
Version: [version]
Status: [status]
Author(s): [author]

This version replaces all previous version of this document. Please destroy all previous copies!

Distribution list

Copy	Distribution (version)	Name/function/remarks

Review management

Review by	Function	Date	Version

Change management

Version	Date	By	Remarks	Approval

Related documents

Version	Date	Description	Remarks

Table of Contents

1 Introduction

Doel van het rapport:

- Weergeven welke efforts Fox-IT heeft gedaan.
- Overzicht van het onderzoek.
- Onderzoek kan verder worden opgepakt als dat nog nodig is.

{het rapport is geschreven vanuit het perspectief van Fox}

{investigation is limited for resources, and time. Therefore not everything is finished. Open ends are marked so someone can later follow up is needed. It also puts the results in perspective}

{gevoellige informative t.b.v. de opsporing is in bijlage opgenomen en is niet publiek beschikbaar}

{alle investigations zijn zo opgeschreven dat iemand deze kan herhalen met de bron info}

{leeswijzer}

{?wat feitjes opnemen?: aantal systemen veiliggesteld, uren, mailtjes e.d.?}

References to servers are made using the original name of server that was used by DigiNotar.

References to servers are made using the name of the server that was DigiNotar used. Additionally the function of the server is added and the IP address. Some servers have multiple IP addresses. Only the relevant IP address is noted. For example: WINSRV157 (eHerkenning HM; 10.10.20.139). A list of referenced server is in Appendix I {references to equipment} [eenmalig lijstje waarschijnlijk handiger dan telkens deze opsomming?]

All dates and time stamps are based on the Central European Time (CET; GMT+1) timezone, unless explicitly stated otherwise.

1.1 TODO's

{lijstje met TODO's voor dit rapport. Wordt uit het finale rapport verwijderd}

Vragen:

? misschien bij ieder hoofdstukje een mangament samenvatting maken? [of gewoon één management samenvatting aan het begin van het rapport?]
? Wie wil zijn naam op de cover

Marketing sausje

Laatste checks:

- Aantal aanvallers in het midden laten ("Perpetrator**(s)**") OF: overall in enkelvoud en opnemen in inleiding dat het een of meerdere kunnen zijn
- Tijd/ datum formaat standaardiseren (30-August-2011 11:12:13).
- Universele referenties naar servers (naam en evt IP als niet uniek)
- Universele referenties naar netwerken (Secure-net, e.d.)
- Afco's controle. En in de afco's lijst achterin.

Review's

- Onderzoeksteam op feiten
- directive/ MT op 'gevoellige' zaken
- AM/ marketing op profilering Fox

2 What happened?

{wat is er global gebeurd. Inhuur door DigiNotar, overname BZK, vertrouwen opgezegd, Opta, faillisement, status nu}

[Uit "Investigation approach": Initially Fox-IT started an incident response investigation at the request of DigiNotar, with the aim of establishing to what extent which systems had been compromised. As of [date] the Dutch The Dutch Ministry of the Interior and Kingdom Relations took over the role of the client in regard to the investigation. The primary aim of the investigation that ensued was to determine if the CA severs that were used to issue qualified certificates and/or certificates for PKIOverheid had been compromised. A further aim of the ensuing investigation was to support the Dutch police in their investigation into the identity and location of the attacker(s).]

2.1 Parties involved

{questions needed to be answered}

Party	Role
AIVD	Identifying potential threats for national security.
BZK	The Dutch Ministry of the Interior and Kingdom Relations.
DigiNotar	Former notarial collaboration acquired by VASCO Data Security International.
DigiNotar customers	Customers of DigiNotar that used certificates that were issued by DigiNotar.
Fox-IT	Provides solutions for the protection of state secrets, the investigation of digital crime, audits, managed security services and consultancy.
GOVCERT.NL	Cyber Security and Incident Response Team of the government.
Hoffman	Offers investigative, forensic and strategic risk management services.
Iranian people	Primary targets of the MitM-attack during which rogue certificates were used.
Internet community	Affected by the consequences of the attacks in a general sense.
KLPD	Responsible for the investigation into the attack(er)(s).
Manufacturers	Parties that operate at the highest layer of the Public Key Infrastructure.
OM	Responsible for the prosecution of the attacker(s).
OPTA	OPTA checks whether registered CSPs parties comply with Dutch law.
PWC	Performs audits of CSPs, including DigiNotar.
RSA	Provides diverse security, risk and compliance solutions.
Raad van accreditatie	Dutch Accreditation Council.

2.2 Timeline events

{tijdslijn}

2.3 Questions and answers

{welke onderzoeksvragen beantwoorden in dit rapport, en welke niet} {time caught up on the early questions. No need to answer them}
{This report is setup so the analysis can be continued with the source material}

This report is aimed to answer to the following questions:

- **What was the path of the attacker(s) through the network?**
  - What was the point of first entry?
  - What technical actions were performed?
  - Which security measures were breached?
  - What tools were used in order to perform the attack?
  - What vulnerabilities were exploited?
  - Was malware used and if so what did it consist of?
  - What are the steps that were taken before the attacker(s)'s goal was reached?
  - What systems outside of DigiNotar were used to do so?

- **What were the technically observed consequences for the population of Iran?**
  - What other activity were needed? [strekking?]

This report is *not* aimed to answer the following questions: [moet dit zo expliciet? Zie ook het aparte hoofdstuk 15 m.b.t. follow-up vragen?]

- What was stolen?
  - What information has left the digital premises?
  - Certificates:
    - Have CA certificates been created?
    - Were certificates been unjustly revoked?
  - Personal information:
    - What personal information such as personal, client and contract information was stolen?
  - Other DigiNotar services:
    - What other services DigiNotar offered were compromised or misused?
  - Intellectual property:
    - What intellectual properties, for instance source code, was stolen, adjusted or deleted?
- What was the mode of operation in detail?
  - Waar hebben de gegevens het systeem verlaten? (Artikel 139C wetboek van strafrecht (Aftappen gegevens), lid 1) (vraag vanuit KLPD)
  - Hoe hebben zij dit gedaan? (Technische ingreep, doorbreken van de beveiliging) (Artikel 138AB wetboek van strafrecht (Hacking), lid 1) (vraag vanuit KLPD)
    - Is er gebruik gemaakt van een technisch hulpmiddel? Is software een technisch hulpmiddel (antwoord van OvJ) (Artikel 139D wetboek van strafrecht (Plaatsen afluister- cq opnameapparatuur), Lid 1) (vraag vanuit KLPD)
    - Welke tools?
    - Hoeveel hacks hebben er daadwerkelijk plaatsgevonden? (Deze moeten afzonderlijk beschreven worden) (vraag vanuit KLPD)
    - Welke exploits zijn gebruikt?
    - Is er gebruik gemaakt van een computer wachtwoord waardoor toegang kon worden verkregen tot het systeem (138ab)? Artikel 139D wetboek van strafrecht (Plaatsen afluister- cq opnameapparatuur), Lid 2) (vraag vanuit KLPD)
    - Hoeveel stappen hebben ze moet nemen om tot het uiteindelijke doel te komen? (vraag vanuit KLPD)
      - Wat waren de aanvalspaden?
      - Was e-mail gebruikt?
  - Is er gebruik gemaakt van radio ontvangstapparatuur door de hacker? (Artikel 139C wetboek van strafrecht (Aftappen gegevens), lid 2) (vraag vanuit KLPD)
  - Hebben ze gebruik gemaakt van een ander geautomatiseerd werk om toegang te krijgen? (Artikel 138AB wetboek van strafrecht (Hacking), Lid 3) (vraag vanuit KLPD)
    - Welke systemen buiten DigiNotar zijn gebruikt?
- Information about the attacker(s):
  - How sophisticated was the attack?
    - What knowledge was required?
  - How many persons?
  - What are the similarities/ differences compared to other TTP attacks?
  - What were the motives?
- Status of the security
  - What security measures were active before and during the attack?
  - Did DigiNotar comply to the requirements (Besluit elektronische handtekeningen and ETSI TS 101 456)
- Has DigiNotar acted negligent or are they liable?
- What are the potential consequences of this attack?

3 Situation

3.1 Organisation

DigiNotar BV was founded as a privately-owned notarial collaboration in 1998. The customer base of DigiNotar consisted of government institutions, profit and non-profit organizations as well as individual citizens. The company provided digital certificate services as a Trusted Third Party (TTP) and hosted a number of Certificate Authorities (CAs). Certificates issued by DigiNotar included SSL certificates, Qualified Certificates and government accredited certificates. The government accredited 'PKIOverheid'-certificates were used for critical public services such as DigiD (Digital Identity), which is used for various Dutch eGovernment purposes. On January 10th of 2011 VASCO Data Security International announced its acquisition of DigiNotar BV. On September 20th of 2011 the court of Haarlem declared DigiNotar BV to be insolvent following the breach of the security of crucial segments of its internal network.

{wat troffen we aan}

3.2 Certificate issuing process

[Algemene informatie over uitgifte van certificaten]

There were four different processes in regard to the storage of private keys:

- **SSL PKCS10**
  The Public-Key Cryptography Standard (PKCS) defines a file format used to store X.509 private keys and the corresponding public key certificates. In this process the client generated a private key and sent a certificate signing request to DigiNotar. As a result, no private key entered the DigiNotar domain during this process.
- **SSL PKCS12**
  When a client requests an SSL certificate a private key is generated with the DARPI application. The DARPI application then created a signing request and sent it it to the appropriate CA system. The DARPI application uses the API of the appropriate CA to perform this task, for which a authentication certificate is used. The key and the certificate and joined together in a PKCS#12 file that is protected with a password that consisted of 10 alphanumeric characters. The P12 file was then sent to the customer. A copy of the P12 file was stored in the DARPI database. The password was sent to the PIN mailer and a PIN letter was sent to the customer.
- **Smartcard and USB token**
  PKIOverheid differentiates between three certificates. The first type of certificate is used for electronic signatures, a second type for encryption and a third for qualified signatures (non-repudiation). When electronic or qualified signatures were used the private keys were generated on the token. The CSR was then signed by the CA and placed on the token with the private keys. In the case of the encryption certificate, the private key was generated on the darpi system and not on the token itself because of key escrow [verder uitleggen]. Both the key and the certificate were protected with a password and were stored in the database as in the SSL P12 process. The PIN is sent to the customer by the PIN mailer.
- **Special cases**
  In special cases where the DARPI software was not sufficient [verder uitleggen waarom niet sufficient] the certificates were generated manually on the RSA Keon terminal. These special cases included the generation of EVSSL certificates.

The passwords of the P12 files are stored in the CAP database. The database is unencrypted. Every period of 6 weeks the passwords and P12 files are removed and archived. The archive is encrypted. The private key of this archive is stored offline in a vault. This key is can only be used when two persons enter their PIN (four eyes principle).

TODO's:
•How did the authentication work exactly?
•Is this authentication traceable? Is this the 'ID' in the xslogs of the CAs?
•Was this authentication misused by the attacker(s)?
•What was the password (policy) of the P12 SSL files?

•*What was the password (policy) of the encryption keys stored in the key escrow?*

The DARPI application is a self written application that is installed on several workstations. Those were not constantly turned on.

For every certificate request a dossier was created in CAP. Every day all the certificate dossiers were gathered in a centrale certificaten database (CCDB) and compared with a copy of the RSA Keon database ldif). This could show any fraudulent actions. This process was inoperative from xx until July the 18th. On July the 19th

https://afst-portal.test.fox.local/confluence/display/BlackTulip/Certificate+issuing+process

3.3 Other services

In addition to their certificate issuing service, DigiNotar provided several other services:

- Signing service (certified information exchange service on behalf of other companies):
  - CORUS
  - Money You
  - BNG
  - WKPB
  - NWRO
  - APG (uitvoering ABP)
  - Achmea
- Authentication service
  - BISTRO/ORDE
  - eHerkenning
  - Pass
  - HLB (accountants)
  - PKI-overheid
  - Notaries
  - BAPI
- Document proof service
  - FME
  - PWC
  - Official publications (Staatcourant c.a.)
  - TAXI
  - For Lawers
- Other
  - Parelsnoer: anonymised exchange of human test subject information for medical universities (universitair medisch centrum; UMC). Anomysation of citizen service number (Burgerservicenummer; BSN)
  - CCV: initialisatie PIN-automaten

3.4 Customers

- PKI-overheid
- Notarissen
- BAPI
- TENNET
- EASIGAS
- Notarissen/KNB
- Gerechtsdeurwaarders/SNG
- TU delft

Decos en Circle Software
(http://www.computable.nl/artikel/ict_topics/security/4141174/1276896/diginotarpartners-zoeken-naar-alternatieven.html)

3.5 Network

{Inleiding toevoegen.}
{→ main location and co-location}
{Kort iets over de fysieke beveiliging (pasjes, dubbele deuren, inner room, hand scanner) (productie ruimte)}.

The DigiNotar network had two connection to the Internet that is provided by two different ISP internet providers. Behind the router that is responsible for Internet connectivity a TippingPoint 50 Intrusion Prevention System (IPS) was present. The IPS was running a default configuration and was not effectively used by DigiNotar. The IPS was not effective as it was placed in front of the firewall and consequently gives a lot of false positives, although it was planned to be placed behind the firewall. Behind the IPS a redundant Nokia firewall appliance was running Checkpoint Firewall-1/ VPN-1 {controleer exacte naamgeving/ versie} with a separate management server. An external company managed the firewalls at DigiNotar.

The DigiNotar network was divided in 25 different internal network segments. The following list of networks was enforced as extracted from the firewall settings (as it was on 30-September-2011):

{sorteren op IP range}

Net name[1]	IP range	Description
DMZ-old-net	10.10.0.0/24	Old DMZ network
DMZ-ext-net	10.10.20.0/24	External DMZ network
DMZ-ext-closed-net	10.10.30.0/24	Closed external DMZ network
DMZ-ext-vasco-net	10.10.50.0/24	Vasco external DMZ network
DMZ-ext-vpn-net	10.10.40.0/24	VPN network
production-net	10.10.110.0/24	Secure production network
DMZ-int-net	10.10.200.0/24	Internal DMZ network
admin-net	10.10.210.0/24	Management network
acceptance-net	10.10.230.0/24	Acceptance network
test-net	10.10.240.0/24	Test network
develop-net	10.10.250.0/24	Development network
office-new-net	10.31.32.0/23	New office network
vasco-net	10.32.0.0/16	Vasco network
iscsi-net	10.200.200.0/23	Internal ISCSI network
iscsi-colo-net	10.200.202.0/23	Co-location - ISCSI DMZ network
office-net	172.17.20.0/25	Office network and temporary network
hosted1-old-net	172.17.20.128/28	Old 'hosted1' network
hosted3-old-net	172.17.20.160/28	Old 'hosted3' network
secure-net	172.18.20.0/24	Secure 'Unicert/RSA' network
DMZ-ext-colo-net	172.25.20.0/24	Co-location - external DMZ network
DMZ-int-colo-net	172.26.20.0/24	Co-location - internal DMZ network
secure-colo-net	172.27.20.0/24	Co-location - Secure network
office-colo-net	172.28.20.0/24	Co-location – office network
sync-1-net	192.168.1.0/29	First FireWall-1 synchronisation
ext-net	62.58.35.96/28	Network between the firewall and the Internet
pinewood-mgmt-net	62.58.74.128/27	Pinewood remote management

[1] Network segment name as it is used in this report.

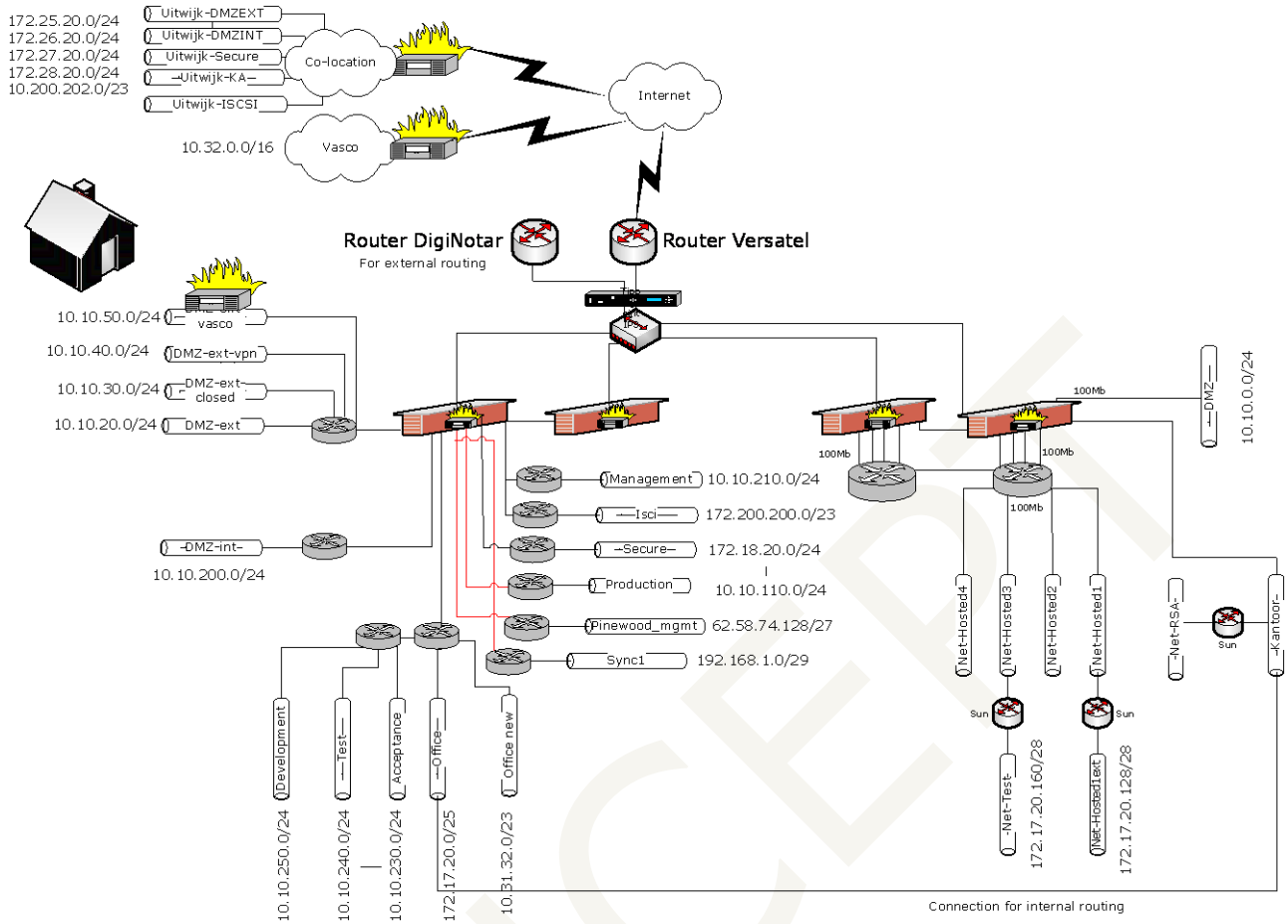


Figure 1 A rough sketch of the DigiNotar network[2]

Most of the systems in the network were machines running a Windows operating system from Microsoft.

In the secure-net network segment the systems were located that needed the most protection. Herein the servers running the CA management software, the 'production' servers and the over the network accessible hardware security module (netHSM) were located. The production workstations and servers used to initialise and personalise smartcards or other PKI tokens, issue certificates, create PIN letters etc. These production systems were connected to the back-end administration in the office-net network segment and the CA servers. The production software and systems were called CAP (Control Application), DARPI (DigiNotar Abonnementen Registratie[3] Production Interface) and BAPI (Belastingdienst[4] Advanced Program Integration).

The CA management software running on the CA servers connected over the network to the netHSMs where the private keys of the CAs are securely stored. On the main location a total of eight CA servers, including one test CA server and one root CA server were present. {dit waren er meer... nog uit te zoeken}. On the co-location seven (virtual) CA servers were located that functioned as a redundant business continuity measure[5]. In total four netHSMs were present, one of which was in the secure segment for the CAs, a second in the internal DMZ (DMZ-int) for the 'Parelsnoer' service, a third in the test environment and in co-location another netHSM was present.

[2] Based on a drawing provided by DigiNotar. The exact lay-out of the layer-2 {zo heet dat toch?} network (switches) in this sketch is not verified.
[3] Translates to "Subscription Registration".
[4] The Dutch tax collectors office.
[5] It was unclear if the systems were on cold, warm or hot standby. The servers were switched on but it was unknown if backups had to be restored and if the netHSMs were

During normal operation, a customer requests a certificate on one of the web servers in the external DMZ (DMZ-ext-net). The request is then stored by the web server on a server in the internal DMZ (DMZ-int-net). The firewall prohibited any communication initiated from the DMZ-int-net to the DMZ-ext-net[6]. The requests that had been stored were periodically collected by a service in the secure-net. The firewall prohibited any connection is initiated from the DMZ-int to the secure-net. In the CAP application the request was stored and administrative procedures such as vetting are initiated. The CAP application is a custom developed application by [x] that provides [x].

When a request was approved {"4 ogen" ingevoegd in de review}, a field in the database was marked. Subsequently, an administrative employee logged on to a workstation, which ran the custom developed application DARPI, in a separate room and processed the request. An API on the CA servers was used to communicate and control the CA service. Depending on the type of certificate process [in welk geval meer specifiek? – in review ingevoegd: "of deze is nog bij de klant zoals bij BAPI"] a private key was generated and a certificate request was sent to one of the CA servers. On the CA server an authorised employee accessed the CA server {with smartcard authentication?} and approved the requests {is dat ook zo? Moet de request ook op deze manier goedgekeurd worden of gebeurde dit automatisch?} [ingevoegd in review: "dit klopt niet. De Darpi doet de productie. Deze applicatie draait ook alleen in secure. De werknemers komen helemaal zelf niet op de CA"]. In order for the CA software to sign the certificate request, the appropriate private key stored in the netHSM need to be activated. This was done by an authorised employee who entered a smartcard into the netHSM combined with a PIN-code. For root-access multiple [smartcards en/of authorised employees] were required.

The CA operator manually created certificates for certificates requests that could not be processed by the DARPI application. In order to generate these 'special' certificates [is dit een quote van een intern gebruikte omschrijving?] the CA operator had to log into the CA application together with someone [wie?] who could provide access.

De netHSM bedient alle CA's. Er is nog een netHSM maar die is voor een specifieke klant.

Er worden van alle systemen (welke ook al weer?) req en certs verzameld en gecontroleerd of deze matchen. Er gaat een alarm af als er een mismatch is.

Er is een RSA envision log analyse door maar die doet niets.

BAPI werkstations. T.b.v. belastingdienst certs.

Er is een uitwijk locatie (cold standby).

Beheerder VPN toegang naar hun eigen werkstation via RDP.

In totaal hebben we er 4 (HSMs). De 172.18.20.254 is voor de CA's. De 10.10.200.254 voor website die een hsm nodig hebben (alleen parelsnoer op dit moment). 10.10.240.254 voor test en de 172.27.20.254 voor uitwijk.

Alle applicaties halen hier gegevens uit (settings en usernames/ww, etc) en loggen hier naar toe. We hebben ook authenticatie, maar dat is Pass (ASelect).

Er staat een Barracuda spam firewall te luisteren op extern adres 62.58.36.114:25

Mail server: 62.58.36.114.25 uit pcap.

DNS server: 87.213.114.2.53 uit pcap (20110831)

De server WINSRV101 met daarop de website www.diginotar, 10.10.20.41 (en 10.10.20.46?), is door DigiNotar uit gezet en bewaard. Deze is veiligesteld als SVO8. Er is vervolgens met nieuwe hardware een nieuwe webserver opgezet (WINSRV150 ???).

De server WINSRV119 is de docproof server (10.10.20.65?)

[6] The operation of the firewall as was explained by the administrators of DigiNotar. The firewall rules were not verified.

Uitwijk locatie
De locatie heeft een eigen internet verbinding.
Er is een eigen firewall.

Gevist uit server-spreadsheet van Diginotar en Whois:

ip_start	ip_end	netname
62.58.35.96	62.58.35.111	TELE2-CUST-DIGINOTAR-BV
62.58.36.112	62.58.36.127	VERSATEL-CUST-Diginotar-B-Vx
62.58.44.96	62.58.44.127	VERSATEL-CUST-Diginotar-B-Vx
81.58.241.160	81.58.241.175	VERSATEL-CUST-Diginotar-B-Vx
87.213.105.80	87.213.105.95	TELE2-CUST-Diginotar
87.213.114.0	87.213.114.15	VERSATEL-CUST-Diginotar-B-Vx
87.213.114.160	87.213.114.191	VERSATEL-CUST-Diginotar-B-Vx
143.177.3.40	143.177.3.47	-
143.177.11.0	143.177.11.15	-
193.173.36.32	193.173.36.47	OTS25849

Onze bevindingen n.a.v. een poortscan van de IP-adressen van Diginotar (rapportage do 15-9-2011 15:40):

- Een (schijnbaar verouderde) ProFTPd-server op 62.58.44.111 ('ftp.diginotar.nl'). ProFTPd 1.3.3b kan remote op ingebroken worden. Potentieel serieus. We kunnen testen of 'ie echt kwetsbaar is door er zelf op in te breken, maar heb met Forensics afgestemd dat ze er eerst met voorrang een image van maken.
- Een heel aantal websites/-services gevonden (79 HTTP, 67 HTTPS). Dat zou nogal grootschalig onderzoek vergen om die allemaal in detail te onderzoeken. Het grote aantal is op zich al wel opmerkelijk.
- Op http://87.213.105.92:8888/ draait een webservice van VASCO, iets met IdentiKeys
- Twee systemen geven HOST UNREACHABLE als response op bepaalde poorten, die staan wellicht uit maar nog wel open in de firewall:
  - 87.213.114.1 (poort 22, SSH)
  - 87.213.114.2 (poort 53, DNS)
- Systeem 143.177.3.42 luistert op poort 389 (LDAP), niet een protocol dat je verwacht aan het internet aan te treffen
- Voor systeem 143.177.3.45 staat poort 8777 open in de firewall (maar geeft daarop geen antwoord), dat is een bijzondere poort om open te hebben in de firewall, zou kunnen wijzen op een (inmiddels uitgeschakelde) backdoor. Maar kan ook een logische verklaring voor zijn, kunnen wij niet zien.
- Er zijn 3 VPN-servers actief (62.58.35.108, 62.58.35.109, 62.58.35.110).

Webservices vinden we op de volgende IP-adressen (zoals gezegd, het gaat om een behoorlijk aantal...):

Webservices vinden we op de volgende IP-adressen (zoals gezegd, het gaat om een behoorlijk aantal...):

IP address	Port 80 HTTP	Port 443 HTTPS	62.58.36.121	X	X	62.58.44.98	X	X
			62.58.36.122	X	X	62.58.44.99	X	X
			62.58.36.123		X	62.58.44.100		X
62.58.35.107	X	X	62.58.36.124		X	62.58.44.102	X	X
62.58.36.113	X	X	62.58.36.125	X	X	62.58.44.103	X	X
62.58.36.116	X	X	62.58.36.126	X	X	62.58.44.104	X	X
62.58.36.117	X	X	62.58.36.127	X	X	62.58.44.105	X	
62.58.36.118	X	X	62.58.44.96	X	X	62.58.44.107	X	X
62.58.36.119	X	X	62.58.44.97	X	X	62.58.44.109	X	X

62.58.44.110		X	81.58.241.173	X	X	143.177.3.41		X
62.58.44.112	X	X	81.58.241.174	X	X	143.177.3.44	X	X
62.58.44.113	X	X	81.58.241.175	X		143.177.3.45	X	
62.58.44.114	X	X	87.213.105.80	X		143.177.3.46	X	
62.58.44.118	X	X	87.213.105.81	X	X	143.177.3.47	X	X
62.58.44.119	X	X	87.213.105.82	X		143.177.11.1	X	X
62.58.44.121	X	X	87.213.105.83	X		143.177.11.2	X	
62.58.44.123	X	X	87.213.105.84	X		143.177.11.3	X	X
62.58.44.125	X	X	87.213.105.85	X		143.177.11.4	X	
62.58.44.126	X	X	87.213.105.87	X	X	143.177.11.5	X	X
62.58.44.127	X	X	87.213.105.89	X		143.177.11.6	X	X
81.58.241.160	X	X	87.213.105.90	X	X	143.177.11.7	X	X
81.58.241.161	X	X	87.213.105.91	X	X	143.177.11.8	X	X
81.58.241.162	X		87.213.105.92			143.177.11.9	X	
81.58.241.163	X	X	87.213.105.93	X		143.177.11.10	X	X
81.58.241.164	X		87.213.105.94	X	X	143.177.11.11	X	X
81.58.241.165	X	X	87.213.105.95	X	X	143.177.11.12	X	
81.58.241.167	X	X	87.213.114.3	X	X	143.177.11.14	X	X
81.58.241.168	X	X	87.213.114.4	X	X	143.177.11.15	X	X
81.58.241.171	X	X	87.213.114.5	X	X			
81.58.241.172	X	X	143.177.3.40	X	X			

IP address	DNS lookup
62.58.36.114	mailhost.diginotar.nl
62.58.36.116	mail.diginea.nl
62.58.36.118	www.diginotar.nl
62.58.36.120	authenticatie.pass.nl
62.58.36.121	belastingdienst.diginotar.nl
62.58.36.125	service.diginotar.nl
62.58.36.126	Registratie.diginotar.nl
62.58.44.107	digi01.mailwitness.net
62.58.44.108	digibackup.mailwitness.net
62.58.44.116	genghini.mailwitness.net
62.58.44.121	danka.mailwitness.net
62.58.44.122	bgg.mailwitness.net
62.58.44.123	diginotar.mailwitness.net
62.58.44.124	test.pass.nl
62.58.44.125	*.diginotar.com
	diginotar.com
	diginotar.net
143.177.3.41	mailhost1.diginotar.nl
	mail.digifactuur.nl
	mail.diginotar.com
143.177.3.42	directory.diginotar.nl
143.177.3.43	www.servicecentrum.diginotar.nl
143.177.3.45	validation.diginotar.nl
143.177.11.2	servicecenter.diginotar.nl
143.177.11.4	demonstratie.pass.nl
143.177.11.10	onlineaanvraag.diginotar.nl
143.177.11.11	www.pass.nl
193.173.36.36	ns1.diginotar.nl
193.173.36.39	mailhostuw.diginotar.nl

Source: http://www.robtex.com

`Netwerk plaatje: 10.10.20.46 (niet in lijst?)` (=de www web server)?

From the file systemroot\System32\Inetsrv\MetaBase.xml taken from WINSRV101 (main webserver; svo8) the following IP address bindings were present:

- 10.10.20.11 Notarisgombert.nl
- 10.10.20.14 Darwizard
- 10.10.20.28 evssl.diginotar.nl (nslookup: 62.58.44.108)
- 10.10.20.41 DigiNotar.nl
- 10.10.20.46 www.evssl.nl (nslookup: 62.58.44.113)
- 10.10.20.58 DigiNotar.com

- 10.10.20.61 OCSPclient
- 10.10.20.69 sha2.diginotar.nl (nslookup 62.58.44.109)
- 10.10.20.73 BapiOphalen
- 10.10.20.97 Bapiviewer

From the file systemroot\System32\Inetsrv\MetaBase.xml taken from WINSRV118 (nieuwe? DocProof; svo11) the following IP address bindings were present:
- 10.10.20.37 Docproof

From the WINSRV119 (old docproof) image from ITSec:
- WINSRV119
- IP address: 10.10.20.65
- Primary Domain Name: DNDMZEXT

From the file systemroot\System32\Inetsrv\MetaBase.xml the following IP address bindings were present:
- :80: :443: Docproof (local addresses)

From the WINSRV055 () image from ITSec:
- WINSRV055
- IP address: 172.18.20.244
- Primary Domain Name: DNPRODUCTIE

From the WINSRV056 () image from ITSec:
- WINSRV056
- IP address: 172.18.20.245
- Primary Domain Name: DNPRODUCTIE

SVO7
- WINSRV054
- IP address: 172.18.20.250
- Primary Domain Name: DNPRODUCTIE

SVO5
- Computer Account Name: WINSRV053
- IP address: 172.18.20.251
- Primary Domain Name: DNPRODUCTIE

SVO4
- Computer Account Name: WINSRV021
- IP address: 172.18.20.252
- Primary Domain Name: DNPRODUCTIE

SVO3
- Computer Account Name: WINSRV057
- IP address: 172.18.20.246
- Primary Domain Name: DNPRODUCTIE

SVO2
- Computer Account Name: WINSRV022
- IP address: 172.18.20.249
- Primary Domain Name: DNPRODUCTIE

SVO1
- Computer Account Name: WINSRV167
- IP address: 172.18.20.247
- Primary Domain Name: DNPRODUCTIE

Btw ze hebben twee load-balancers:

10.10.20.8 dnlb01

10.10.20.9 dnlb02

3.6 Actions taken

{? Misschien naar een eigen hoofdstukje?}
{welke acties zijn er uitgevoerd onder leiding van Fox?}

3.6.1 OCSP responder monitoring

[link met chapter 10?]

4 Research {approach?}

4.1 Preliminary research

{wat is er al door DigiNotar/ Vasco/ ITSec gedaan?}{wellicht in h2?}
{samenvatting van email Vasco}
{samevatting Research report ITSec}
{Samenvatting Memo en incidentlogboek DigiNotar}

ITSec had een doosje staan die PCAPjes opsloeg van het externe verkeer. Die hebben we veiliggesteld/ gekopieerd. (van welke datums waren dat?)
We hebben 6 pcaps gedateerd van: 2011-08-25 t/m 2011-08-30. Het is intern verkeer, in de 172.x.x.x range, en 10.10.x.x
Er is in 1 pcap gekeken of er OCSP verkeer in voor kwam. wat niet het geval was.

4.1.1 Emergency response monitoring

One of the first measures that was taken by Fox-IT was to place our incident monitoring service [device?] within the DigiNotar intranet. This sensor captures and monitors all traffic between the intranet and the internet. Suspicious traffic can be detected by the sensor and all traffic [of alleen suspicious traffic?] will be stored on disk if evaluation is necessary. If suspicious traffic is detected it can be escalated to [X] if necessary so that further action can be taken. Examples of actions that can be taken are the blocking of an IP-address or IP-range or changing the rules on the firewall for specific ports. In this particular case a tailored OCSP responder monitoring service was added to the emergency sensor.

4.2 Safeguard evidence

{Het process van veiligstellen. Hoe hebben we dat gedaan, waarom e.d.}
Subsequently ["forensically sound"?] disk images were made by Fox-IT of the systems that were prone to be infected. Initially this process was restricted to the servers hosting the CA software and the firewall management system that contained the firewall logs. At the request of the Dutch police, the process was extended to include the creation of images of all the computer systems within the DigiNotar intranet. [On/after ...] it was decided that a disk image would not be created of every system [reden?]. A total of [xxx] images were created of [xxx] servers and [xxx] workstations that amount to [xxx] terabyte of data.

The items [=images?] that were produced as evidence were numbered with the prefix SVO, which refers to "Stuk Van Overtuiging" [English?]. References within this report to (images of) machines that can also service as evidence will be made using the function of the server. In appendix [x] an overview is included of all the server names that were used including their corresponding SVO-number and place [function?] within the network.

Fox-IT has rolled out its own infrastructure in order to examine all systems within the DigiNotar network live in a iterative and ["forensically sound"?] way. This infrastructure aided our researchers so that they could instantly use their research results to perform further research. The investigation was limited by the fact that if a system were to be shut down or be placed under a heavy load, it would have had impacted the production environment that was still in use by DigiNotar. For this reason a large number of systems could not be shut down during the investigation, which hindered the creation of images and meant that unauthorized software could have been active after the investigation was initiated [toegevoegd n.a.v. comments Daniel].

Een alternatief is het gezamelijke gebruik van de door ons opgezette infrastructuur (Encase Enterprise). Hierdoor zouden andere partijen door middel van een centraal systeem ook kunnen zoeken op machines, of images kunnen maken. Hierbij wel een opmerking. We maken hiervoor gebruik van de bestaadne netwerkinfrastructuur van DigiNotar, en die is slechts 100Mbit. Wanneer meerdere partijen hier tegelijk onderzoek op willen doen, of images van machines over willen maken heeft dat een zeer grote impact op de netwerkinfrastructuur. Op dit moment is dat zelfs voor ons onderzoek gedeeltelijk een beperkende factor in het uitzetten van zoekvragen, en het maken van images.

[Als er geen gebruik is gemaakt van dit alternatief hoeft het denk ik ook niet in het rapport, tenzij het is om uit te leggen waarom er niet voor het alternatief is gekozen?]

Oude web server 10.10.20.41 vermelden!

4.3 Investigation approach

Initially Fox-IT started an incident response investigation at the request of DigiNotar, with the aim of establishing to what extent which systems had been compromised. As of [date] the Dutch The Dutch Ministry of the Interior and Kingdom Relations took over the role of the client in regard to the investigation. The primary aim of the investigation that ensued was to determine if the CA severs that were used to issue qualified certificates and/or certificates for PKIOverheid had been compromised. A further aim of the ensuing investigation was to support the Dutch police in their investigation into the identity and location of the attacker(s).

The main strategy to accomplish this aim was to determine the extent to which servers within the DigiNotar network had been compromised and to identify IP-addresses and other evidence that could provide more information about the attacker(s). Once the information had been obtained that the security of the CA servers used for PKIOverheid and qualified certificates had been compromised by (in all probability) foreign attacker(s), the investigative stage of the involvement of Fox-IT was concluded. This report is the culmination of the incident response investigation that was performed at the request of both DigiNotar and the Ministry of the Interior and Kingdom Relations.

4.4 Actions taken

{uitleg voor de hoofdstukken daarna}
In the next chapters individual investigations of items are reported. They are sometimes incomplete or unfinished.

5 Investigation of CA managing software

In this chapter the results of the investigation of the managing CA software is described {right word?}.

- How many certificates have been illegitimate issued? Identify the illegitimate issued certificates that have been created by the attacker(s).
- What were the serial numbers of the illegitimate issued certificates? In order to revoke the certificates the serials numbers must be known.
- What CAs are administered on what server? As is described in chapter 8 "System access, tools and files" {all?} the CA servers were compromised and the attacker had administrative access. To determine if the 'trust' of the CAs is compromised it must be known what CA was administered on what CA server.

At DigiNotar eight machines were encountered that operated as CA servers. A disk image of all these servers was created. These servers named:

- Root-CA
- Qualified-CA
- CCV-CA
- Orde-CA
- Taxi-CA
- Test-CA
- Relatie-CA
- Public-CA

The CA servers had access to the nCipher netHSMs in the Secure network segment (Secure-net) {Eerste keer in een Hoofdstuk network segment → 'net' vertaling} . The nCipher devices contain private key material in a secure way, so that the key material cannot leave the device. The private keys inside the {uitschrijven} (HSM) can only be used if a smartcard is presented to the HSM. On the main location in Beverwijk (in the Netherlands) three nCipher NetHSM500s were present. In the co-location another nCipher Nethsm500s was present [dit is eerder genoemd in "Network"].

On the CA servers software from RSA (The Security Division of EMC) was installed in order to manage certificates. More specifically RSA offers the product RSA Certificate Manger. Older versions were named RSA Keon. The CA software consists of several services. One of services provides a web interface for users and administrators. Another service logs the activity of the software into log files. The CA software also provides an application programming interface (API) that enables programmers to develop PKI applications. These applications can be developed using a scripting language called XUDA (Xcert Universal Database API) [controleren of dit de eerste keer is dat CA software wordt genoemd].

The different CA servers served different services {TODO: uitwerken}:

- Root-CA. Manages all the root CA certificates...
- Qualified-CA
- CCV-CA. [Voor de CA van CCV bestaan extra procedures en beveiligingsmaatregelen. De CA van CCV is een zogenaamde off-line CA. Standaard zijn de noodzakelijke services (programmatuur) uitgeschakeld. Het aanmaken en verspreiden van de certificaten gebeuren handmatig. Voor het opstarten van de services en het aanmaken van een nieuw certificaat zijn twee medewerkers en het gebruik van twee passen met pincode vereist. Deze passen worden na het afsluiten van het aanmaakproces verwijderd. CCV gebruikt de certificaten voor het initialiseren van pinbetaalautomaten voor de detailhandel. De certificaten zijn bij CCV geïnstalleerd op apparaten in de vestigingen van CCV, waarmee nieuwe en gereviseerde pinbetaalautomaten worden geïnitialiseerd en het dient voor het beveiligen van de informatie die wordt uitgewisseld bij het initialiseren van pinbetaalautomaten. Het gaat in totaal om enkele tientallen certificaten.]
- Orde-CA
- Taxi-CA
- Test-CA
- Relatie-CA
- Public-CA

For the purpose of the investigation, Fox-IT used a list that was provided by DigiNotar which contained all the certificates that had been issued by DigiNotar. This list (alcerts.csv) was created by exporting the CA databases and contained the following information regarding the certificates that were issued by DigiNotar:

Value	Meaning
md5	The MD5 checksum of the certificate as calculated by the CA software
CA md5	The MD5 checksum of the issuing CA certificate
Serial nr.	The serial number of the certificate
Cert dn	The distinguished name field of the certificate
Valid from & valid until	The date fields of the certificate
Revocation date	The date of revocation (if applicable)

5.1 CA software log files

5.1.1 Sources/ content

All CA servers were outfitted with software that logged relevant information for the ongoing processes. The information was stored in log files that were in the format `xslog_{yyyyMMdd}.xml`. It appears that the log files were not being rotated or removed automatically and that a new log file was created whenever the machine was rebooted or when the (log) service was restarted. Given the timeframe during which the attacker was active, only the most significant log files were examined thoroughly.

The list of the investigated database files {dit lijstje weg!}:

Name	Log files
Root-CA	{TODO}
Qualified-CA	{TODO}
CCV-CA	{TODO}
Orde-CA	{TODO}
Taxi-CA	{TODO}
Test-CA	{TODO}
Relatie-CA	{TODO}

Public-CA	`xslog_20110325.xml`
	`xslog_20110711.xml`
	`xslog_20110711_1.xml`

Within the log files the integrity of blocks of data is secured using a signature. Using CA software the integrity of the log files can be checked. The integrity of the log files of all CA installations was verified by an DigiNotar employee. Two log files from the Public-CA failed the verification by the CA software:

- `xslog_20110711_1.xml`
- `xslog_20110720.xml`

The integrity of other log files is verified by the CA software without failure. The breached {?} integrity of `xslog_20110711_1.xml` conforms with a description that was found in the incident logbook [REF]. The logbook contains log entries that show that when the console on the Public-CA machine was started 20-July-2011 it was detected that rogue certificates were being issued and that the machine was shut down. The corresponding customary entries for "`Log Server Stopped`" and "`Final Entry`" are missing from this log file.

The entries in the log files contain the following information:

- `LOG_NUMBER`: a sequential unique log entry number
- `LOG_SOURCE`: the source of the log entry (either from the Certificate management Administration, Secure Directory or Logging Server)
- `EVENT_CONDITION`: either `ATTEMPT` or `COMPLETION` of an action
- `DATE,TIME`: the date and time of the entry {nazoeken welke timezone}
- `ID`: a hexadecimal value consisting of 32 characters (29 unique IDs have been encountered - 6 of these were encountered more than 100.000 times)

- `IP_ADDR`: the IP-address associated with the action (the following internal IP-addresses were mentioned: 127.0.0.1, 172.18.20.244, 172.18.20.245, 172.18.20.247, 172.18.20.249, 172.18.20.251, 172.18.20.252 and 172.18.20.253).
- `LOG_DATA`: the structure of this field varies depending on the data that it contains. A "Certificate signing" entry has the following fields:
    - `Succeeded` or `failed`
    - `Certificate presented`: an MD5-value of 32 characters for the certificates presented to the CA with the request
    - `certDN` with distinguished name fields
    - `MD5`-value of the certificate
    - `Issuing CA MD5` – the serial number of the issuing or created certificate are not present in the log files.

5.1.2 Analysis

Relatie-CA

The analysis of the log file `xslog_20110407.xml` on the Relatie-CA server shows that the first signs of extraordinary activity and certificate signing attempts occurred on 02-July-2011 at 19:59:34. The first successful rogue certificate was created on 10-July-2011 at 13:05:10 for *.google.com. In total 85 rogue certificates are successfully created, all on 10-July-2011 between 13:05:10 and 23:35:54.

Public-CA

The analysis of the log file `xslog_20110325.xml` on the Public-CA server shows that the first signs of extraordinary activity and certificate signing attempts occurred on Sunday 03-July-2011 at 12:15:44. Between Thursday 07-July-2011 at 23:19:33 and Sunday 09-July-2011 at 12:53:16 is looks like experiments took place by the attacker outside office hours. During this time old, probably already rightfully issued certificate requests seem to have been reissued. For example "beveiligd.gemeentesudwestfryslan.nl" is issued twice with different CA keys.

On 10-July-2011 at 19:55:56 the first rogue certificate is issued (*.google.com). Between 10-July-2011 at 19:55:56 and 23:55:57 a total of 198 rogue certificates were issued. The log server was stopped at 11-July-2011 at 01:41:19. The next log file `xslog_20110711.xml` starts at 11-July-2011 at 08:18:42 leaving a gap in the logs of about 7½ hours. This next log file contains only a few entries, most of them logging failed certificate signing attempts.

The next log file (`xslog_20110711_1.xml`) starts at 11-July-2011 11:24:49 probably after a reboot of the system or (log) service. On 18-July-2011 at 16:19:27 a burst of 124 rogue certificates were created. Another burst of 124 rogue certificates were generated on 20-July-2011 at 08:56:41. After this no other rogue certificate is found in the logs of the Public-CA server.

This log file is not properly terminated. The last log entry is on 20-July-2011 at 08:57:11. The next log file (xslog_20110720.xml) starts on 20-July-2011 at 12:19:37, has no entries stops normally on 12:21:41. The next log file (xslog_20110720_1.xml) start on 20-July-2011 at 12:34:52. No obvious suspicious activity is found in this log. The final entry is on 20-July-2011 18:20:14. After that all entries in the log files seems normal activity. The servers are shutdown daily.

A total number of 446 rogue certificates is issued between 10-July-2011 at 19:55:56 and 20-July-2011 at 08:57:11 on the Public-CA server.

5.2 Databases

The CA software used databases to store application data such as certificates. Several database files were stored in the directory `{install directory}\Xudad\db\`. The main database file was named `id2entry.dbh`. The main database file contained records of the certificates that had been issued with several characteristics. During our investigation we came across another interesting database files named `serial_no.dbh` `[waarom interesting?].` This database files contained certificate serial numbers. All the database files are in the Berkeley DB format.

List of [encountered/ investigated] database files {weg??}:

Name	Database files
Root-CA	
Qualified-CA	
CCV-CA	
Orde-CA	
Taxi-CA	
Test-CA	
Relatie-CA	
Public-CA	

5.2.1 Certificates

The certificates stored in the main database file can be extracted in PEM (Privacy Enhanced Mail) format. The following methodology was used in order to do this:

- Perform a case insensitive search for the string `pem_x509::`
- Extract the trailing data block
- Decode the text from its base64 format
- Encapsulate the text with `-----BEGIN PUBLIC KEY-----` and `-----END PUBLIC KEY-----`.

When the certificates were extracted in this way, some extracted data blocks were invalid. An attempt to read them with for instance OpenSSL will consequently result in an error. A quick (not exhaustive) investigation revealed that these incomplete blocks are indeed present in the database file. Complete versions of these data blocks are also present in the database, which led us to conclusion that no certificates were missed using this method.

Additionally, some certificates were stored more than once in the database. Comparing the fingerprint of the certificates identifies the duplicates. This was done by comparing the fingerprints of the certificates. These incomplete and duplicate certificates were excluded from further analysis.

5.2.2 Private keys

The `id2entry.dbh` database files contained entries labelled `privatekey::`. After decoding the base64 data these entries showed the following asn.1 structure (example from the Root-CA):

```
0:d=0  hl=2 l= 111 cons: SEQUENCE
 2:d=1  hl=2 l=   1 prim: INTEGER    :02
 5:d=1  hl=2 l=  19 prim: IA5STRING  :XCSP nCipher Native
26:d=1  hl=2 l=   1 prim: INTEGER    :53
29:d=1  hl=2 l=  64 prim: cont [ 0 ] :30 3E 16 0E 72 73 61 2D 6B 65 6F 6E 2D 63 61 2D  0>..rsa-keon-ca-
                                      36 38 16 10 31 33 30 38 32 32 33 37 36 30 33 32  68..130822376032
                                      37 30 30 30 16 11 53 45 43 55 52 45 20 4F 50 45  7000..SECURE OPE
                                      52 41 54 49 4F 4E 53 01 01 FF 02 01 02 02 01 04  RATIONS.........
95:d=1  hl=2 l=  16 prim: cont [ 1 ] :30 0E 80 01 01 81 01 00 04 06 02 04 84 8D A7 10  0.?.............
```

The decoded asn.1 structure led us to believe that these are references to private keys stored in the netHSM. If this is true, then we can conclude that the software installed on the server could use these keys.

In the data surrounding the private key entries there was no indication of the certificate or common name linked to these keys. However, directly following the private key entries a data block labelled `publickey::` is present. For the example above we have extracted the public key and matched it with the public keys of the extracted certificates. This resulted in the CA certificate with the common name '`C=NL, O=Ministerie van Infrastructuur en Milieu, OU=Referentie CA, CN=MinIenM Autonome Apparaten CA - G2`'. By following this method we were able to determine what CA servers had access to what private keys in the netHSM with its corresponding certificate.

5.2.3 Serial numbers

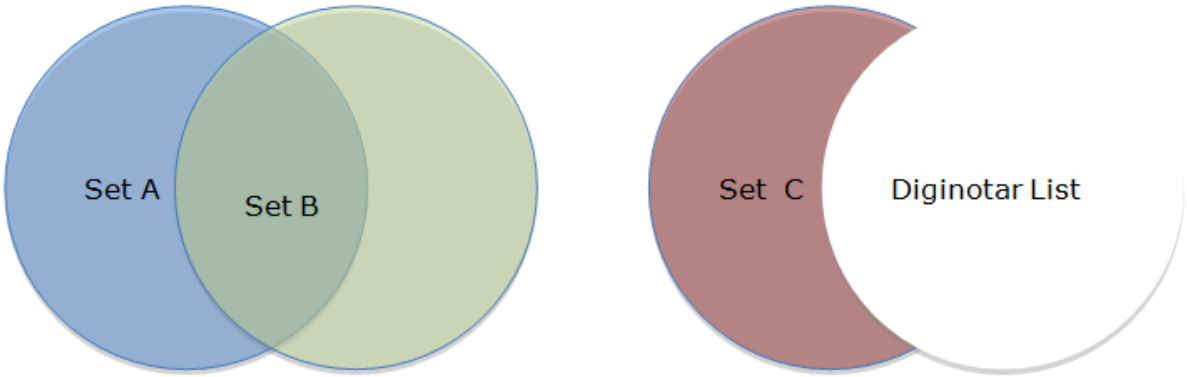
The suspicion arose that the attacker(s) may have manipulated database and log files during the attack. The reason for this suspicion is that removed database files were discovered on multiple CA servers. For

example the serial number that corresponds with the rogue wildcard certificate for the Google.com domain was only present in a `serial_no.dbh` database that had been removed.

The assumption is made that the `serial_no.dbh` database contained all serial numbers for certificates that had been issued by the CA software. To determine if serial numbers that correspond with rogue certificates were present, all `id2entry.dbh` and `serial_no.dbh` files were collected for each CA server, including all recoverable files that had previously been removed. It was investigated whether every serial number in the `serial_no.dbh` could be matched with an issued certificate.

In order to determine this, two sets of serial numbers were created. Set A included all serial numbers from all `serial_no.dbh` file. Set B includes serial numbers from all `id2entry.dbh` files. The difference between these list is determined by subtracting the set A and B. The resulting set are serials that are unknown serials. As an extra check these serials are matched against a list of issued certificates provided by DigiNotar.

{plaatje aanpassen! A=serial_no.dbh, B=id2entry.dbh, A is groter dan B, C is subset en geen intersection A^B; C = unknown}.



{naar conclusie stukje?}
For all the CA servers this method is applied. The results show unknown serial numbers by four out of the eight CA servers. A complete list of unknown serials for the CA servers can be found in appendix [...]. As a precautionary measure, all of the unknown serial numbers that remained were revoked.

CA server	Number of unknown serials
ROOT CA	7
R&A Qualified CA	2
TAXI CA	24
Public CA	203

It the time available for the investigation it could not be determined why this discrepancy existed between the databases. It could be due to software errors or as a result of aborted issuing process. However, because this was not concluded the difference in numbers remains suspicious and points more in the direction of misuse of the servers than the contrary.

5.3 Conclusion

It was not easy for DigiNotar to produce an up-to-date overview of the CAs it operates and on what servers. In order to create an overview of the CAs and their hierarchy Fox-IT had to extract relevant information from the log files and the databases.

5.3.1 CA activity {right title?}

For the purpose of this investigation, it was important to know what CAs were actively used on what servers. Since the servers generally hosted multiple CAs, the attacker(s) could gain access to all the CAs that were hosted on a specific server once access to that server was obtained.

As described, the issuing CA MD5 hash was logged when a certificate was signed. Having looked at the log entries for certificates that were successfully signed and searching for the private keys in the databases we have conclude that the following servers were used to manage the following CAs (inclusive system CAs):
{van deze tabel klopt geen HOL!!! Issuing CAmd5 uit de logs klopt niet!!!}

CA server	Common name of issuing CA	Source	
		log	db
Public-CA	DigiNotar Services 1024 CA	X	TODO
	DigiNotar Public CA 2025	X	
	DigiNotar Public CA - G2	X	
	DigiNotar Services CA	X	
	DigiNotar Extended Validation CA	X	
	DigiNotar Cyber CA	X	
Orde-CA	DigiNotar Cyber CA		X
	DigiNotar Extended Validation CA		X
	DigiNotar Private CA		X
	DigiNotar Public CA 2025		X
	DigiNotar Public CA 2025 Administrative CA	X	X
	DigiNotar Public CA 2025 System CA		X
	DigiNotar Root CA	X	????
	DigiNotar Services 1024 CA		X
	DigiNotar Services CA		X
	Nederlandse Orde van Advocaten - Dutch Bar Association	X	X
	Orde van Advocaten SubCA Administrative CA		X
	Orde van Advocaten SubCA System CA	X	X
QC-CA	Algemene Relatie Services System CA	X	????
	DigiNotar PKIoverheid CA Organisatie - G2	X	????
	DigiNotar PKIoverheid CA Overheid en Bedrijven	X	????
	DigiNotar Qualified CA	X	X
	DigiNotar Qualified CA - G2		X
	EASEE-gas CA	X	????
	Hypotrust CA	X	????
	Koninklijke Notariele Beroepsorganisatie CA	X	????
	Ministerie van Justitie JEP1 CA	X	????
	Renault Nissan Nederland CA	X	????
	SNG CA	X	????
	Stichting TTP Infos CA	X	????
	TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2	X	????
	TU Delft CA	X	????
			Nog 6
Relatie-CA	Koninklijke Notariele Beroepsorganisatie CA	X	TODO
	Algemene Relatie Services System CA	X	
	TenneT CA 2011	X	
	Hypotrust CA	X	
	EASEE-gas CA	X	
	SNG CA	X	
	TU Delft CA	X	
	Ministerie van Justitie JEP1 CA	X	
	Stichting TTP Infos CA	X	
	Renault Nissan Nederland CA	X	
Root-CA	DigiNotar Root CA	X	X

CA server	Common name of issuing CA	Source log	Source db
	DigiNotar Root CA Administrative CA	X	X
	DigiNotar Root CA G2	X	X
	DigiNotar Root CA System CA	X	X
	MinIenM Autonome Apparaten CA - G2	X	X
	MinIenM Organisatie CA - G2	X	X
	MinIenM SIMULATOR NL Autonome Apparaten CA - G2		X
	MinIenM SIMULATOR NL Organisatie CA - G2		X
	MinIenM SIMULATOR NL Root CA - G2		X
	winsvr020		X
Taxi-CA	{no log entries found}		TODO
CCV-CA	CCV Group CA Administrative CA		X
	CCV Group CA System CA		X
	Prod SSL3 Client Root CA 2010 (O=CCV Jeronimo S.A.; C=CH)		X
	Prod SSL3 Server Root CA 2010 (O=CCV Jeronimo S.A.; C=CH)		X
	Prod UpLoad Root CA 2010 (O=CCV Belgium NV; SA; C=BE)		X
	Prod UpLoad Root CA 2010 (O=CCV Deutschland GmbH; C=DE)		X
	Prod UpLoad Root CA 2010 (O=CCV Jeronimo S.A.; C=CH)		X
	Prod UpLoad Root CA 2010 (O=CCV Services B.V.)		X
	RSA CCV CA Administrative CA		X
	RSA CCV CA System CA		X
	ids CA		X
			Nog2

5.4 CA hierarchy

{TODO}

5.5 Rogue Certificates

{TODO}

5.6 Conclusion

{TODO}
{Match the serials with the found rogue certs}

6 Investigation of firewall logs

Within the DigiNotar infrastructure a central position was taken by the firewall. A CheckPoint appliance on a redundant Nokia IP390 platform with a separate management server was used for this purpose within the main infrastructure. A previously used redundant Sun firewall platform was also present in the network . At the co-location a firewall based on a Nokia appliance platform was present.

For reference a list of server names used in this chapter is included. A complete list is in Appendix I {references to equipment}.

Name	Server ID	IP	network

WINSRV007 (Bapi Database New; 172.17.20.4)
WINSRV155 (eHerkenning-AD; 10.10.20.134)
WINSRV108 (Website auth.pass.nl; 10.10.20.16)
WINSRV003 (CI - Source build server; 172.17.20.25)
WINSRV155 (eHerkenning-AD; 10.10.20.134)

6.1 Sources/ content

Fox-IT created an image of the disk of the firewall management server. In the lab a copy of the disk image was virtualised and the management station was accessed using the CheckPoint SmartConsole software. The log files were exported for further processing and examination.

The firewall management server contained all the log files from {TODO: nazoeken van welke firewalls?}. Accepted traffic connections as well as violations of firewall rules were logged, which resulted in up to 2 million log entries per day. The enormous amount of log data that was generated has great potential for tracing the attacker(s) steps, even though data mining on such a large amount of data is time intensive. The firewall is only able to connections between network segments it segregates. Traffic within a segment is not logged by the firewall.

During the investigation two kinds of log files from the firewall were examined: the traffic logs and the audit logs. The traffic logs contain the following fields:

- Timestamp
- 'Action' (accept/drop/reject/encrypt/decrypt/keyinst)
- Firewall interface name and traffic direction
- Firewall rule (name, ID and number)
- Source and destination IP and port
- Protocol
- ICMP (code and type)
- NAT (rule number, translated IP/port)
- DNS query
- VPN (scheme, method, peer gateway)
- TCP out of state, flags
- IPSec specification
- Attack info

The audit logs contains the following fields:

- Timestamp
- Object type
- Operation (log in/out, modify object, create object, et cetera)
- Administrator
- Changes (details of the operation, e.g. the changes applied to a rule)
- General information
- Subject
- Status

- Application

The timestamps of the firewall logs are based on the UTC timezone. {XXX: dit moet geverifieerd worden} [RK: "Ik dacht juist dat de timestamps 2 uur voor liepen? Kan alleen geen referentie meer vinden. Daniel heeft me dat verteld denk ik."]

6.2 Analysis

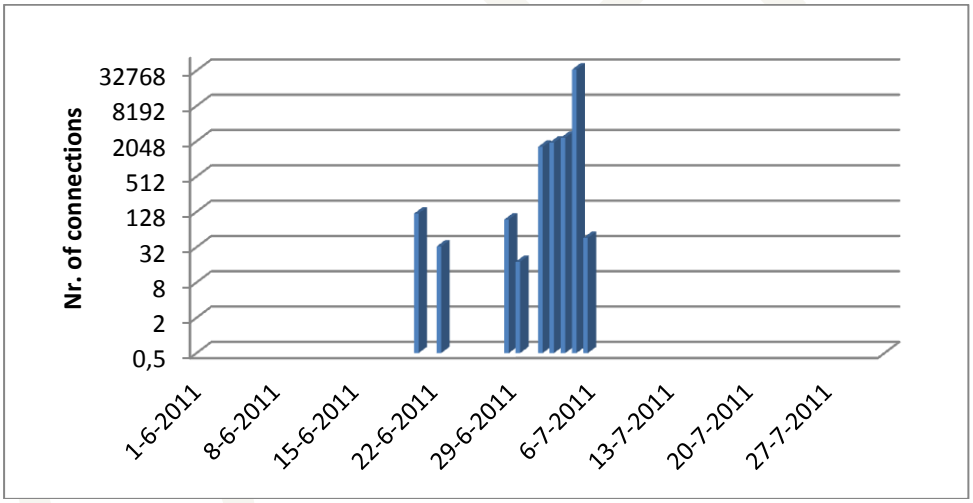
Due to time limitations the analysis of the firewall logs is not done in a very structural way.
Not all the fields in the log have been used in this investigation. Only the source and destination IP and port and the actions accept and drop have been used. The used logs are from 31-May-2011 23:51:57 up until 31-July-2011 23:51:36. The confiscated logs go further back in time.

6.2.1 Internet tunnels

In of the tools an external IP addresses used by the attacker(s) was found. It was discovered that connections from the external DMZ network to this IP address were have taken place. Based on entries in the log files, the following connections from internal systems to external systems can be identified:

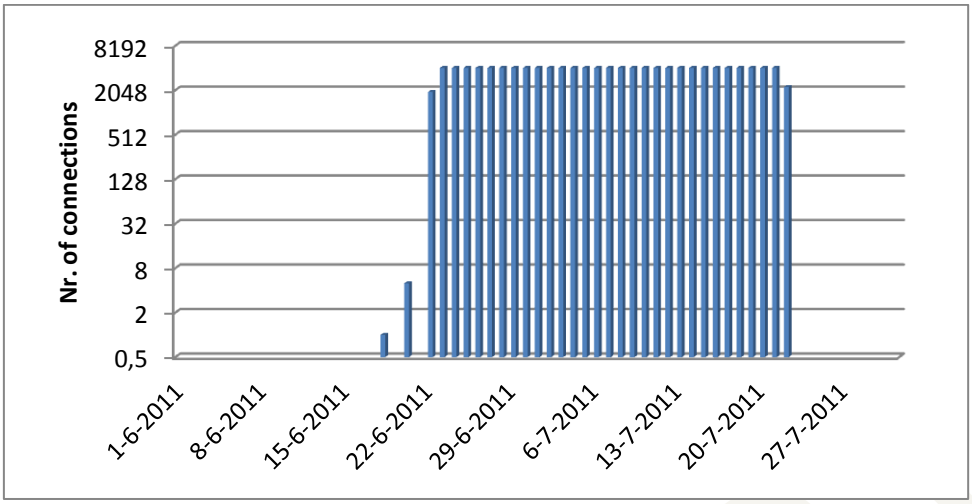
{opmaak}
{grafiekjes of tabelletjes?}

Connect-back from: WINSRV108 (Website auth.pass.nl; 10.10.20.16)
Connect-back to: AttIP1[7] port 443
Connections:

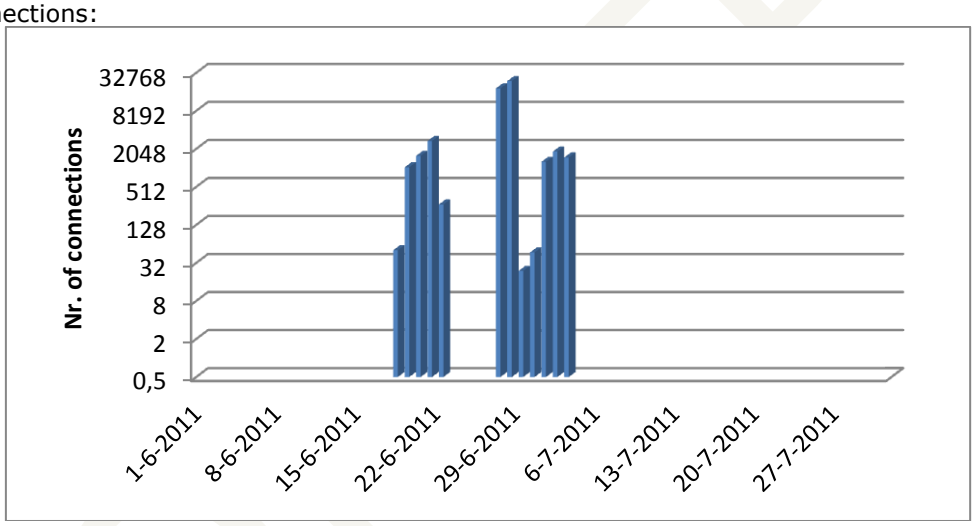


Connect-back from: WINSRV118 (DocProof 10.10.20.37)
Connect-back to: AttIP1 port 443
Connections:

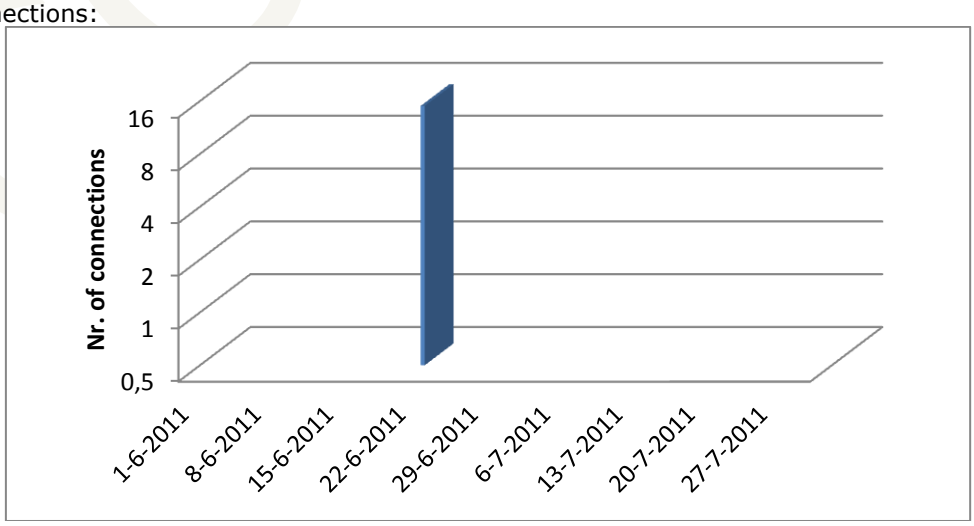
[7] The Internet IP addresses presumably used by the attacker are not included in the text. A reference ID is used and can be looked up in Appendix V-I "List of attackers IP addresses".



Connect-back from: WINSRV101 (main webserver; 10.10.20.46)
Connect-back to: AttIP1 port 443
Connections:



Connect-back from: WINSRV119 (DocProof; 10.10.20.65)
Connect-back to: AttIP1 port 443
Connections:



No connections were found originating from 10.10.20.41, 10.10.20.58, 10.10.20.134 or 10.10.20.139 to AttIP1:443.

{include a network picture: DMZ-ext –(tunnels)- internet - AttIP1}

6.2.2 Internal tunnels

A number of hacking tools were encountered and analysed, which is detailed in chapter 8.1.5. One of the functions these hacking tools performed was to create a connect-back, that is making a connect back to a system that is controlled by the attacker(s). Analysis of the traffic log files of the firewall showed connect-back connections were initiated on the following dates:

{opmaak}

File name: Troj134.exe
Connect-back from: WINSRV007 (Bapi Database New; 172.17.20.4)
Connect-back to: WINSRV155 (eHerkenning-AD; 10.10.20.134) on port 443
Connections: 172.17.20.4 → 10.10.20.134:443

Date	Nr. of connections
2011-06-30	74522
2011-07-01	124510
2011-07-02	26351
2011-07-03	49021
2011-07-04	530
2011-07-05	11

File name: Troj172.exe
Connect-back from: WINSRV007 (Bapi Database New; 172.17.20.4)
Connect-back to: WINSRV108 (Website auth.pass.nl; 10.10.20.16) on port 443
Connections: 172.17.20.4 → 10.10.20.16:443

Date	Nr. of connections
2011-06-29	1

File name: Troj25.exe
Back-connect from: WINSRV003 (CI - Source build server; 172.17.20.25)
Back-connect to: WINSRV155 (eHerkenning-AD; 10.10.20.134) on port 443
Connections: None were found {wel dropped log entries?}

Please note that although the connections in the log files explicitly show a source and destination of the connection, files and commands could have been transported in either direction once a connection had been set up between these two systems.

{include a network picture: Office net –(tunnels)- DMZ-ext}

6.2.3 Tunnels from secure-net

It would seem that the servers located in the external DMZ acted as an intermediate hop between the internal network of DigiNotar and the internet. For this the attacker used at least tunnels over port 443 to connect between servers. Additional a search has been conducted for all connections to WINSRV155 (eHerkenning-AD; 10.10.20.134) on port 443. This showed connections were made from the Public-CA server in the Secure network to this server:

{opmaak}

Connections: 172.18.20.245 → 10.10.20.134:443

Date	Nr. of connections
2011-07-04	14
2011-07-05	1

This shows that a direct connection was made between the Secure network external DMZ. No other connections were seen to WINSRV155 on port 443 from the secure network between 31-May-2011 and 01-August-2011.

Subsequently all traffic originating from the secure network to other network segments on port 443 was examined. The log files show 2970 of the in total 3062 traffic connections originating from the Secure network segment to the external DMZ. More precise this traffic came from WINSRV130 (Application server (CAP web); 172.18.20.10) and WINSRV125 (Webserver (CAP web) 172.18.20.12) to the server cluster-prodpass (Cluster production Pass; 10.10.20.18/ 62.58.44.107). The traffic between these systems existed before and after the attack and was probably regular traffic. [hoezo 'regular' traffic tussen 'secure' en 'external DMZ'?].

If this traffic is ignored, this leaves 92 traffic connections of the 3062 that need further investigation. Out of these 92 connections, 54 relate to blocked traffic that originates from WINSRV056 (Public-CA; 172.18.20.245) on 2011-07-04 between 03:25 en 04:42. The blocked traffic was intended for the following IPs:

- AttIP1:443 (Attacker IP: refer to Appendix V-I)
- 10.10.20.35:443 WINSRV108 (Website auth.pass.nl)
- 10.10.20.37:443 unknown (not in server list {maak referentie})
- 10.10.2.139:443 unknown (not in server list - presumably a typing error made by the attacker).

Due to the time of the day these attempt were made it safe to assume the attacker had access to the Public-CA server during this time.

The remaining 38 out of the 92 connections relate to accepted traffic. These log entries show that direct connections were made from the Secure network segment to the external DMZ segment:

From	To	Nr. of conn.
WINSRV131 (SQL database (CAP); 172.18.20.11)	WINSRV101 (Old main website; 10.10.20.41)	5
WINSRV055 (Relations CA; 172.18.20.244)	WINSRV101 (Old main website; 10.10.20.41)	2
WINSRV056 (Public CA; 172.18.20.245)	WINSRV155 (eherkenning AD; 10.10.20.134)	15 [8]
WINSRV056 (Public CA; 172.18.20.245)	WINSRV157 (eHerkenning HM; 10.10.20.139)	7
WINSRV056 (Public CA; 172.18.20.245)	WINSRV108 (Website auth.pass.nl; 10.10.20.40)	3
WINSRV056 (Public CA; 172.18.20.245)	WINSRV101 (Old main website; 10.10.20.41)	2
WINSRV057 (Ccv CA; 172.18.20.246)	WINSRV101 (Old main website; 10.10.20.41)	2
WINSRV053 (Taxi CA; 172.18.20.251)	WINSRV101 (Old main website; 10.10.20.41)	2

{include a network picture: Office net –(tunnels)- DMZ-ext}

6.2.4 Network scan

Traffic from the secure network with the destination port 80 was examined. The following out of the ordinary entry was found:

2011-07-01 01:16:36 - drop - [tcp] 172.18.20.230:2404 -> 172.18.20.2:80

The entry concerns traffic within the Secure network segment, but which was still logged by the firewall. The reason for this is that the destination (172.18.20.2) is the firewall itself. This is the earliest suspicious log entry from the secure network segment, which occurred on 30-June-2011 at 23:16 CET {klopt dit?} (adjusted from the firewall log timestamp). After this point in time additional suspicious connections appear in the log files from other servers in the Secure network segment.

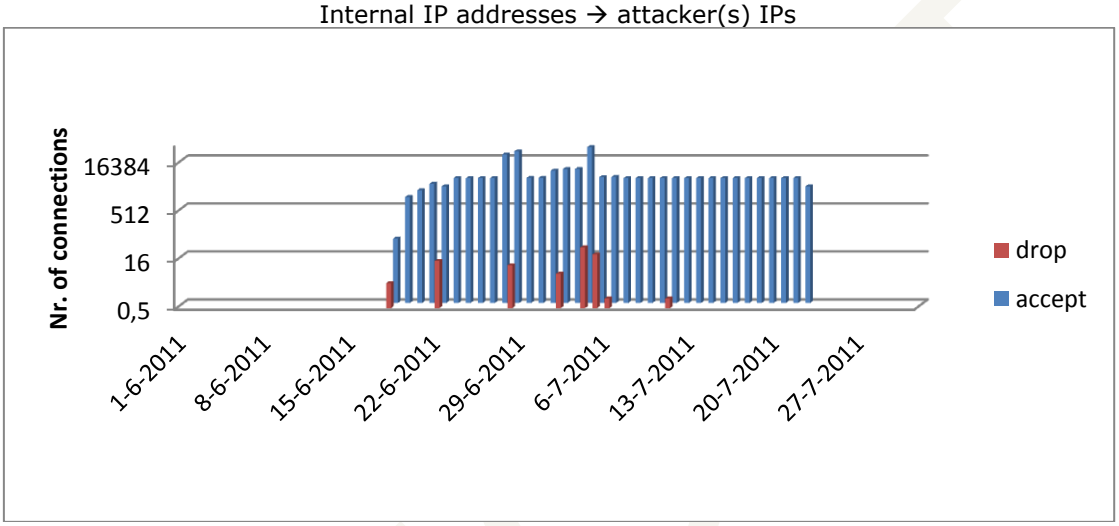
[8] As was seen in the previous analysis of connections to WINSRV155.

The data is consistent with the theory that the attacker first entered the secure segment on 172.18.20.230 and then conducted a services scan on the ports 80, 139, 443 and 445 within the subnet, which includes the firewall and thus resulted in the abovementioned log entry. {moet nog worden nagekeken?}

6.3 Connections to attackers IP

During the investigation a list of suspicious external IP addresses that was probably used by the attacker(s) was created. The complete list is included in Appendix V-I. The log entries regarding connections from internal IP addresses (10.x.x.x and 172.x.x.x) to these IP addresses in the firewall log files are visualized in the following graph:

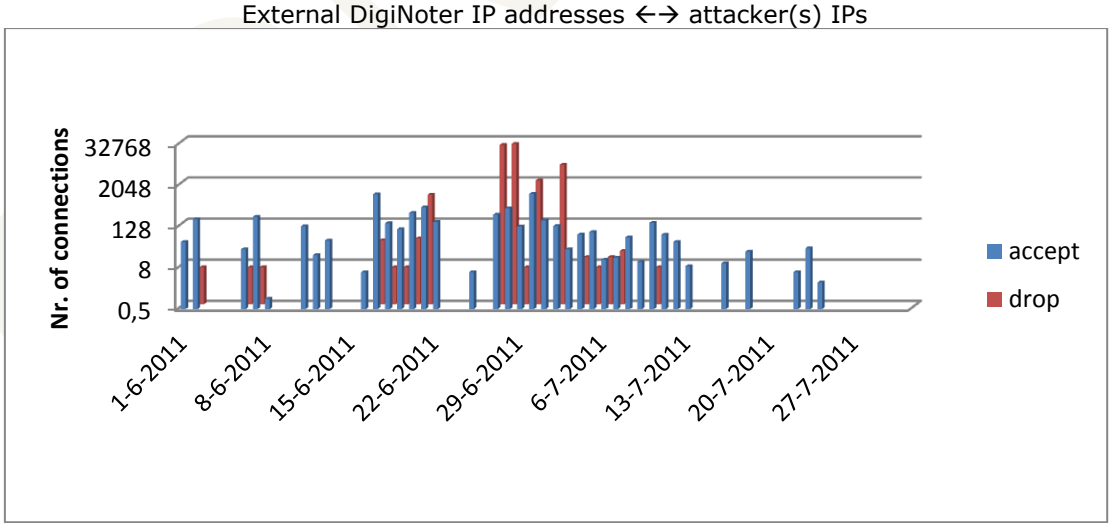
Internal IP addresses → attacker(s) IPs



This shows that on 18-June-2011 the first connections were made from internal IP addresses (10.10.20.46 and 10.10.20.37) to an IP-address that is known to have been used by the attacker(s).

The connection between the external IP addresses of DigiNotar (like 62.58.36.118) and the known attacker(s) IPs is shown the graph below.

External DigiNoter IP addresses ←→ attacker(s) IPs



This shows that from the earliest analysed firewall log entries (1-June-2011) the attacker IPs have been active on DigiNotar systems.

{toevoegen lijst van systemen die met AttIPs connective hebben gehad (heen of terug)}. Parelsnoer even expliciet noemen.}

6.3.1 Remarkable traffic

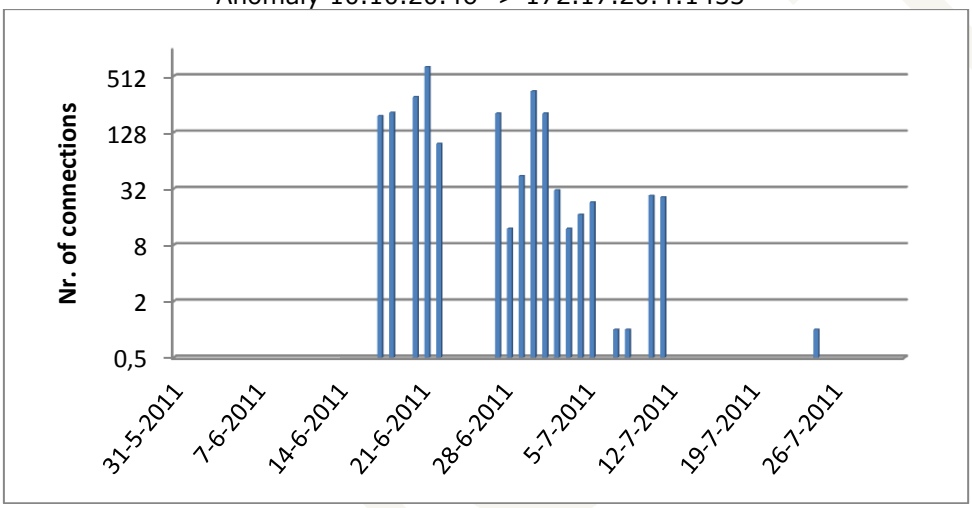
{NAZOEKEN of dit er al in staat…}{Uit de fw logs blijkt dat hij het KA-segment (172.17.20.*) is binnengekomen via de database server in dat segment.}

The firewall logs have been scanned for irregular traffic.

6.3.1.1 DMZext-net to Office-net

Normally no traffic should be initiated from the external DMZ network to the Office network. However as of 17-June-2011 11:28 accepted connections appear between WINSRV101 (main webserver; 10.10.20.46) and WINSRV007 (Bapi Database New; 172.17.20.4) port 1433 ({naam port}).

Anomaly 10.10.20.46 -> 172.17.20.4:1433[9]



This indicates the WINSRV007 was presumably attacked from WINSRV101 starting at 17-Juni-2011.

6.3.1.2 Old DMZ network

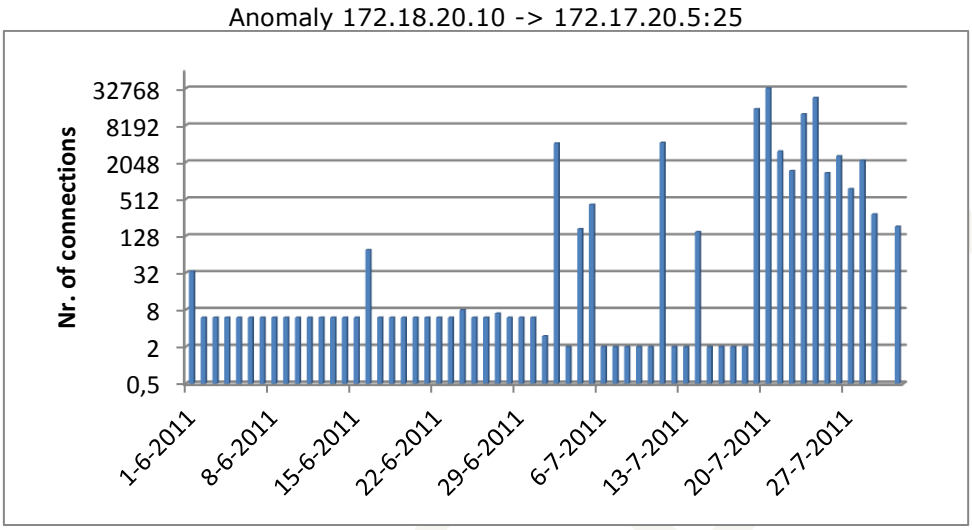
In the firewall logs scanning activity was discovered from the 10.10.20.46 in the external DMZ to 10.10.0.12 in the old DMZ:

```
2011-06-29 13:33:32 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:33:34 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:33:35 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:33:37 - accept - [tcp] 10.10.20.46:2506 -> 10.10.0.12:80
2011-06-29 13:34:03 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:34:05 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:34:06 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:34:08 - accept - [tcp] 10.10.20.46:2510 -> 10.10.0.12:443
```

[9] Note the logarithmic scale. This emphasis the occurrence instead of the number of connections.

6.3.1.3 E-mail traffic

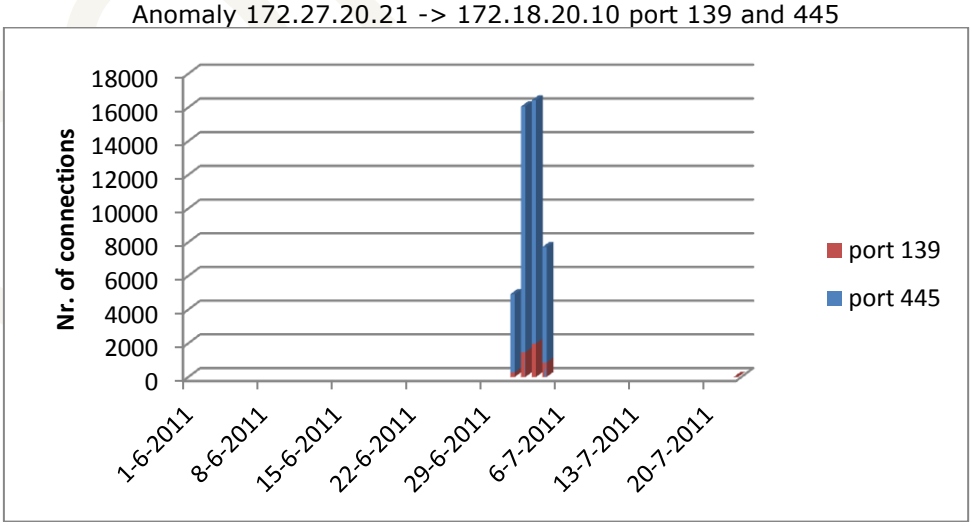
The firewall logs show unusual traffic with destination port 25 (SMTP) between WINSRV130 (Application server (CAP web); 172.18.20.10) in the Secure network segment and WINSRV126 (Exchange DigiNotar; 172.17.20.5) in the Office network segment. As port 25 is generally used for the purpose of e-mail, this indicated intensive e-mail traffic that normally does not occur in these quantities. The figure below illustrates the anomaly logarithmically:



The normal traffic on port 25 consists of six regular SMTP-connections each day at given intervals (four at 9:00 and two at 00:30) that probability originate from a scheduled task. After 30-June-2011 the regular connections at 09:00 cease to take place. Suddenly, in the night of 2-July-2011 about 4100 connections occurred. Then additional spikes of traffic occurred at 4, 5, 11 and 14-July-2011. Between 19 July until 29-July very large amounts of SMTP connections took place.

6.3.1.4 Co-location

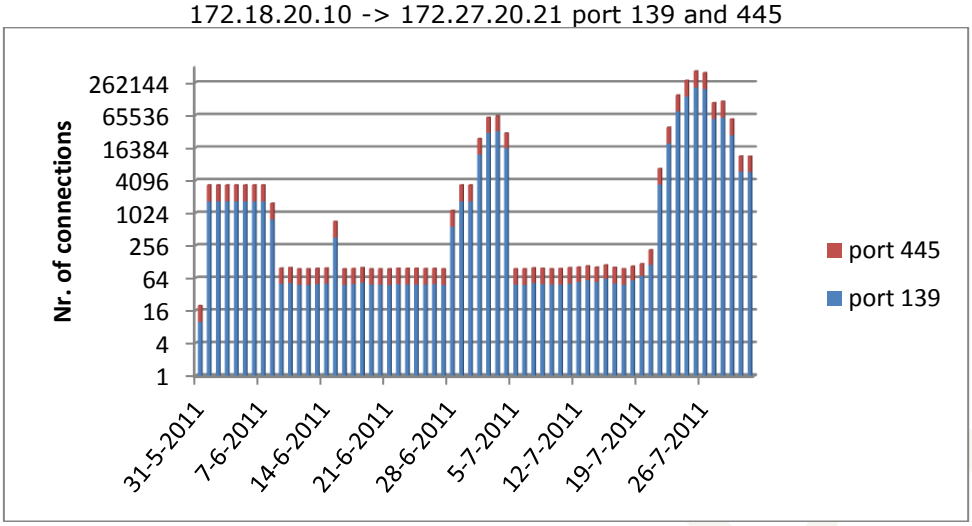
At the co-location suspicious (dropped) traffic was detected from the secure network segment and the main secure network. The traffic occurred between WINSRVUW05 (Administrator server - DNS; 172.27.20.21) and WINSRV130 (Application server (CAP web); 172.18.20.10) on ports 139 and 445.



This could indicate that the attacker(s) had access to the server WINSRVUW05 in the co-location from 1-July-2011.

The reverse connection (from the main to the co-located secure network segment) shows the following:

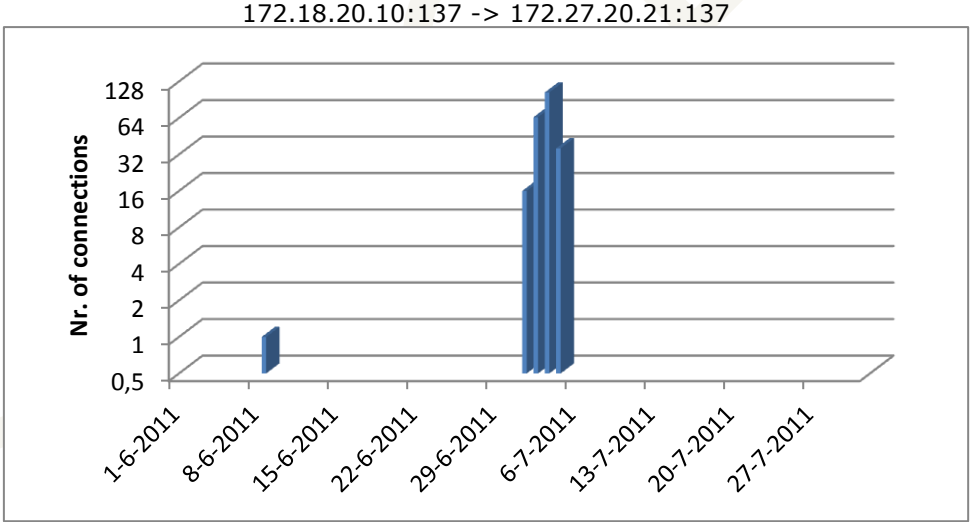
172.18.20.10 -> 172.27.20.21 port 139 and 445



This shows some regular traffic (approximately 50 packets per day) and some monthly traffic. The spikes during the first four days of July are anomalous. The traffic after 19-July is extreme when compared to the regular traffic, but could be explained by incident response activity.

Other noticeable traffic was discovered on port 137 during the first four days of July (in addition to a connection on 8-June-2011):

172.18.20.10:137 -> 172.27.20.21:137



6.4 Timeline

The following table contains a variety of noticeable log entries regarding anomalous traffic sorted by the date and time. {moet verder worden uitgezocht om er iets over te kunnen roepen...}

Attempts = all dropped connections to a specific IP and port combination
Discovery = multiple destination ports or IP addresses, dropped and accepted
{moet nog wat meer worden samengevat. Tabel kleiner maken?}
{verifiëren of bovenstaande er ook allemaal instaat!}

Time start	Time end	What	From srv	To srv	To port
2011-06-17					

Time start	Time end	What	From srv	To srv	To port
13:06:57	13:07:00	RDP attempts[10] from office net to admin net	digiws182	10.10.210.14	DRP
2011-06-28					
14:24:42	14:24:51	{139/ 445} attempts[11] from secure to colo-secure net	WINSRV053	172.27.20.21	139/445
2011-06-29					
11:56:15	11:56:24	RDP attempts from DMZ ext to Office net	WINSRV101	172.17.20.25	DRP
13:13:33	13:14:40	Network discovery from DMZ ext to Test net	WINSRV101	.35, .48	80,137
13:17:42	13:18:45	Network discovery from DMZ ext to DMZ int	WINSRV101	10.10.200.254	80,137, 443
13:20:52	13:21:05	Network discovery from DMZ ext to secure net	WINSRV101	172.18.20.254	137, 443
13:21:38	13:21:54	Network discovery from DMZ ext to Colo-Secure net	WINSRV101	172.27.20.254	137, 443
13:22:26	13:22:40	Network discovery from DMZ ext to Test net	WINSRV101	10.10.240.254	137, 443
13:26:06	13:26:23	Connection attempts from Office to Secure net	WINSRV007	172.18.20.10	80, 3389
13:26:22	13:26:35	Network discovery from DMZ ext to Secure	WINSRV101	172.18.20.10	80, 137
13:27:14	13:29:25	Connection attempts from Office to Secure net	WINSRV007	.10, .11	21, 1433, 135, 137
13:29:39	13:29:52	Network discovery from DMZ ext to Secure net	WINSRV101	172.18.20.11	137, 1433
13:29:50	13:30:03	Connection attempts from Office to Secure net	WINSRV007	172.18.20.11	80, 137
13:31:06	13:31:19	Network discovery from DMZ ext to Test net	WINSRV101	10.10.240.25	80, 137
13:33:32	13:34:08	Network discovery from DMZ ext to DMZ old	WINSRV101	10.10.0.12	80, 137, 443
13:40:40	13:40:44	Connection attempts from DMZ ext to Office	WINSRV101	172.17.20.164	137, 443
15:11:13	15:11:25	Strange?	172.17.20.8	172.18.20.230	139->4461
2011-06-30					
00:08:21	00:08:24	Some more attempts	10.10.20.134	172.17.20.4	137
00:16:34		Connect back home	10.10.20.134	AttIP2	443
00:36:46	00:41:37	Connection attempts from DMZ ext to Ofice net	WINSRV101	172.17.20.4	21, 80, 137
02:22:26	02:22:35	Failed RDP attempts	172.17.20.4	172.18.20.10	3389
02:22:56	02:23:38	Successful HTTP/HTTPS connections	172.17.20.4 172.17.20.7	172.18.20.10	80, 443
02:24:18	02:24:19	Connect back from Office db server to drop server @DMZ	172.17.20.4	10.10.20.134	443
02:25:10	02:26:59	Failed RDP/SQL attempts from the Office net	172.17.20.25 172.17.20.4	172.18.20.10 172.18.20.11	80, 137, 1433, 3389
02:28:31	02:28:40	{What's this??? Robbert?}	10.10.20.134	10.10.240.25	443
08:25:36	08:28:33	Appears a legitimate admin login	10.10.210.31	172.18.20.247	3389
10:39:59	10:40:29	Failed attempts	10.10.20.16	172.17.20.4	139, 445, 1433
13:22:05	13:22:15	conveniently FTP-ing from the DMZ (could be legal activity)	10.10.20.46	172.17.20.21	21
23:54:04	23:56:36	Unknown dropped activity	172.17.20.8:139	172.18.20.230	
2011-07-01					
01:15:30	01:15:38[12]	And again from another host	172.17.20.22:139	172.18.20.230	2400

[10] Probably not relevant for this attack.
[11] Probably not relevant for this attack since... {no traces on Taxi has been found before...?}
[12] From here on outgoing traffic exists originating from the CA network.

Time start	Time end	What	From srv	To srv	To port
2011-07-01					
01:16:15	01:17:16	Port scan on local segment.[13]	172.18.20.230	172.18.20.2	
01:17:22	01:19:49	Connect back attempts to the mgmt LAN	172.17.20.59 172.18.20.230	10.10.210.14	80, 139, 445
01:23:52	01:24:46	Possible failed psexec?	172.17.20.4:139	172.18.20.230	
18:00:56	18:02:26	Failed attempts	172.17.20.4	172.18.20.239	135, 319, 389
20:23:52	20:24:05	And again some time later	172.17.20.4	172.18.20.251	80,137
21:21:54	21:22:24	Possible failed psexec?	172.17.20.4:139	172.18.20.230	
22:52:47	23:40:45	Successful connections to DMZ drop	172.18.20.10	10.10.20.41	80
2011-07-02					
00:14:14	00:47:07	Successful connections to DMZ drop	172.18.20.10	10.10.20.41	80
01:48:42	01:48:42	And again	172.18.20.10	10.10.20.41	80
02:10:01	02:10:01	And again	172.18.20.10	10.10.20.41	80
02:10:01		First occurrence of many SMTP connections	172.18.20.10	172.17.20.5	25
02:18:36	02:18:36	Successful connections to DMZ drop	172.18.20.10	10.10.20.41	80
02:26:54	02:27:02	Strange port combinations	172.27.20.21:445	172.18.20.10:1433	
03:36:15	03:44:19	unsuccessful connections to public drop	172.18.20.247 [ICMP]	AttIP1{ref}	8/0 {???}
04:40:06	04:40:06	Successful connections to DMZ drop	172.18.20.247	10.10.20.41	80
05:37:05	05:48:56	Successful connections to DMZ drop	172.18.20.247	10.10.20.41	80
21:57:55	22:35:20	Successful connections to DMZ drop	172.18.20.247	10.10.20.41	80
{???}	{???}	VPN connection from administrator	10.10.40.32		
23:33:40	23:34:56	Admin working late?	10.10.210.32	172.18.20.11	1056,1433
23:35:57	23:35:57	Admin working late?	10.10.210.32	172.18.20.11	1433, 3389
2011-07-03					
00:14:48	00:14:48	Successful connections to DMZ drop	172.18.20.249	10.10.20.41	80
13:03:02	13:15:51	Successful connections to DMZ drop	172.18.20.245	10.10.20.41	80
16:51:36	16:54:06	Successful connections to DMZ drop	172.18.20.245	10.10.20.41	80
2011-07-04					
00:48:43	21:09:36	Successful connections to DMZ drop	172.18.20.245	10.10.20.41	80
2011-07-05					
00:15:40	00:18:26	Admin working late?	10.10.210.32	172.18.20.10	3389
15:09:35	21:09:36	Successful connections to DMZ drop at regular intervals. Automation in place?	172.18.20.245	10.10.20.41	80
2011-07-06					
15:09:36	21:09:36	Same. Automation in place?	172.18.20.245	10.10.20.41	80
2011-07-07					
15:09:36	21:09:36	Same. Automation in place?	172.18.20.245	10.10.20.41	80
22:58:18	22:58:27	Dropped ???	172.18.20.230	10.10.200.254	80
2011-07-08					
01:09:36	07:09:36	Successful connections to DMZ drop. Other interval.	172.18.20.245	10.10.20.41	80
2011-07-09					
01:09:36	07:09:36	Same.	172.18.20.245 172.18.20.10	10.10.20.41	80
10:05:32	10:06:03	Dropped ???	172.18.20.10	10.10.2.41	80

[13] Only the IP address of firewall itself is logged.

Time start	Time end	What	From srv	To srv	To port
10:06:07	23:34:59	Successful connections to DMZ drop.	172.18.20.10	10.10.2.41	80
2011-07-10					
00:00:14	00:26:24	Continued	172.18.20.10	10.10.2.41	80
01:09:36	01:09:37	Successful connections to DMZ drop.	172.18.20.245	10.10.2.41	80
01:24:36	01:24:36	Switching host	172.18.20.10	10.10.2.41	80
04:09:36	04:11:36	Successful connections to DMZ drop.	172.18.20.245 172.18.20.10	10.10.2.41	80
07:09:36	07:09:36	Same	172.18.20.245	10.10.2.41	80
10:01:04	23:57:55	Same	172.18.20.10	10.10.2.41	80
2011-07-11					
00:46:58	00:51:43	Same	172.18.20.245	10.10.2.41	80

From here on there are connections from 172.18.20.245:1385 to 10.10.20.41:80 at regular intervals at 01:09:36, 01:09:36 , 01:33:33 , 04:09:36 , 04:09:37 , 07:09:43 and 07:09:44 each day from 11-07-2011 up until 20-07-2011.

Time start	Time end	What	From srv	To srv	To port
2011-07-20					
16:46:50	16:47:30	Dropped connections. Incident response actions?	172.18.20.230	172.17.20.8	80
16:57:33	16:57:33	Successful connections to DMZ drop. Incident response actions?	172.18.20.230	172.17.20.8	80
2011-07-25					
18:50:52	19:10:08	Few days later. Successful connections to DMZ drop. Incident response actions?	172.18.20.245	10.10.20.41	80
19:10:37	19:13:05	Dropped connections to DMZ drop. Firewall adjusted.	172.18.20.245	10.10.20.41	80
2011-07-26					
09:09:14	09:09:23	Dropped connection. Incident response actions?	172.18.20.10	62.58.36.117	80
09:10:46	09:10:47	Accepted connections. Incident response actions?	172.18.20.25	62.58.36.117	80

6.5 Conclusion

{deze conclusive moet nog worden uitgebreid}
It appears [was: presumably oftewel een aanname zonder feitelijke basis?] that files and/or commands were exchanged between the external DMZ and the Office network:

From Office	To DMZ-ext	Date first	Nr. Of conn.
WINSRV007	WINSRV155	2011-06-30	
WINSRV007	WINSRV108	2011-06-29	1

Furthermore suspicious connections were made directly between servers located in the Secure network segment and the external DMZ.

From Secure	To DMZ-ext	Date first	Nr. Of conn
WINSRV131	WINSRV101		
WINSRV055	WINSRV101		
WINSRV056	WINSRV155		
WINSRV056	WINSRV157		
WINSRV056	WINSRV108		
WINSRV056	WINSRV101		
WINSRV057	WINSRV101		
WINSRV053	WINSRV101		

This leads us to believe that the attacker(s) obtained access to the following servers:

DMZ-ext network

WINSRV101 (Old main website; 10.10.20.41)
WINSRV155 (eHerkenning AD; 10.10.20.134)
WINSRV157 (eHerkenning HM; 10.10.20.139)
WINSRV108 (Website auth.pass.nl; 10.10.20.40)
WINSRV101 (Old main website; 10.10.20.41)

Office network
WINSRV007 (Bapi Database New; 172.17.20.4)

Secure network
WINSRV131 (SQL database (CAP); 172.18.20.11)
WINSRV055 (Relations CA; 172.18.20.244)
WINSRV056 (Public CA; 172.18.20.245)
WINSRV057 (Ccv CA; 172.18.20.246)
WINSRV053 (Taxi CA; 172.18.20.251)

This indicates that the attacker(s) had access to the server WINSRVUW05 in the co-location between 1-July-2011 and 4-July-2011.

7 Investigation of web server logs

7.1 Sources/ content

Around 24-July-2011 {datum klopt niet!} the main web server of DigiNotar (www.diginotar.nl) had crashed. An employee of DigiNotar found traces that the WINSRV101 running the web server was used to by an attacker to save files on the web server. A new web server was installed on new hardware leaving the attacked server intact for further investigation.

During the incident response investigation that was performed by Fox-IT on the systems WINSRV053 and WINSRV022 traces were encountered that indicated these systems had connected to the web server WINSRV101. [OF even though dat niet de bedoeling is OF naar de specifieke directory /beurs]. Other systems within the network contained cached information originating from the directory `/beurs` on WINSRV101 (identifiable with the local IP-address 10.10.20.41) as is explained in chapter 8.1.1. An exact image of the disk the web server was created and investigated.

The directory `/beurs` was located at `D:\Websites\DigiNotar.nl\DigiNotarweb01\beurs` and was available locally at `http://10.10.20.41/beurs` and publicly at `http://www.diginotar.nl/beurs` {hoe weten we dat?}. When the directory `/beurs` was examined on WINSRV101 no files were present, but the traces on WINSRV053 and WINSRV022 indicated that files had been present in this directory.

The log files of the WINSRV101 webserver were subsequently examined in order to determine which internal and external systems had made a connection to the directory `/beurs` and what files they had accessed. The log files were stored in `C:\WINDOWS\system32\LogBestands\W3SVC1062701327\` and `C:\Data\Websites\Logging\W3SVC1062701327\` and are named `EX<JJMMDD>.log`. The log files have the following format:

```
2011-07-11 00:30:48 W3SVC1062701327 10.10.20.41 GET /beurs/settings.aspx - 80 -
83.96.129.78 Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1)+Gecko/20100101+Firefox/4.0.1 200 0 0
```

In a log entry such as the one above one can distinguish when a system identifiable by its IP-address made a connection to WINSRV101 (10.10.20.41) and which operating system and browser (`Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1`) were used. Furthermore one can distinguish the request that was performed (`GET /beurs/settings.aspx`) and if the webserver's response to this request (status OK `200`).

During the incident response investigation traces were found that a number of log files had been removed. It was not studied whether these files were manually deleted or automatically rolled over, as this was not the aim of the incident response investigation.

7.2 Analysis

Since the removed log files had partially been overwritten the recovery software could not be used. Therefore, the `GREP` command {is 'carven' niet de term in F-land?} was used to probe the image of WINSRV101 for all text entries that contained the string `/beurs`, which allowed to include deleted portions of files that had not been overwritten. Based on the results of this query the following internal systems have connected to WINSRV101:

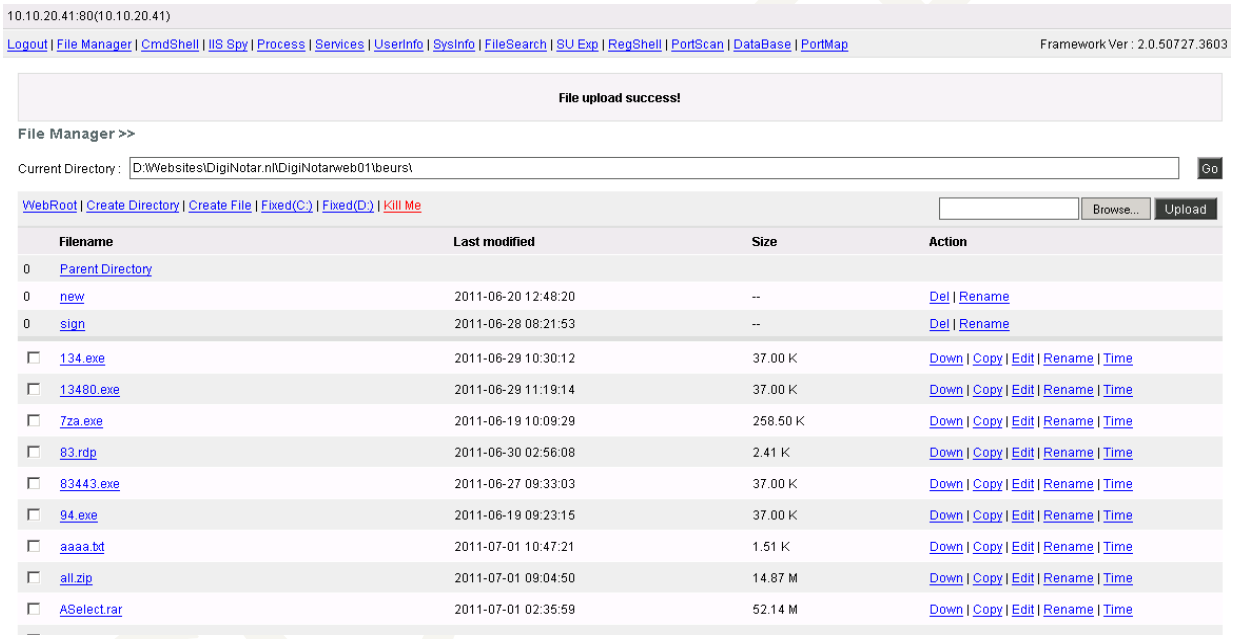
{dit moet een lijstje van WINSRVxxx worden.}

10.10.20.58		
10.10.200.20	WINSRV066	Docproof Database
172.17.20.4	WINSRV007	Bapi Database New
172.17.20.59		
172.17.20.7	DLX001	[P] Proxy (Squid)
172.17.20.8	WINSRV065	Kantoor Fileserver

172.18.20.10	WINSRV130	[P] Applicatieserver (CAP web)
172.18.20.11	WINSRV131	[P] SQL database (CAP)
172.18.20.244	WINSRV055	RSA Relatie CA
172.18.20.245	WINSRV056	RSA Public CA
172.18.20.246	WINSRV057	RSA Ccy CA
172.18.20.247	WINSRV167	RSA root CA
172.18.20.249	WINSRV022	RSA Qualified CA
172.18.20.251	WINSRV053	RSA Taxi CA

The IP-addresses of external systems that have accessed the directory /beurs are likely to have been utilize by the attacker(s) and are included in Appendix V-I. The list of IP addresses is not exhaustive, as a number of log files appear to have been overwritten. In total 25 unique external IP addresses have been found including AttIP2, AttIP3, AttIP4, AttIP6 and AttIP7 reference in other parts of this report.

Based on traces that were found on WINSRV053 and WINSRV022, one of the files that had been present in the directory `/beurs` on WINSRV101 is `settings.aspx`. Traces on other systems show that this file appears to have provided file manager functionality.



From the results of the `GREP`-command a list of files can be composed that have been present in the directory `/beurs` of the webserver WINSRV101 over time. The files Default.aspx and old_Default.aspx that were originally located in this directory were recovered in a backup that was made on 27-August-2011 and that was located at D:\Websites\BackUp\Diginotar01.old. The following list of 125 files is not exhaustive, as a number of log files appear to have been overwritten.

File name	File name	File name	File name
aaaa.txt	dar.rar	darv21.zip	darv30.zip
all.zip	dar.zip	darv22.zip	darv31.zip
asdasd.zip	darpi.zip	darv23.zip	darv33.zip
aselect.rar	darv11.zip	darv24.exe	darv34.exe
bapi.zip	darv12.zip	darv24.zip	darv34.zip
beurs.aspx	darv13.zip	darv25.zip	darv35.zip
bin.zip	darv15.zip	darv26.zip	darv36.zip
c.zip	darv16.zip	darv27.zip	darv37.zip
cachedump.exe	darv17.zip	darv28.exe	darv38.zip
certcontainer.dll	darv18.zip	darv28.zip	darv4.zip
code.zip	darv19.zip	darv29.zip	darv5.zip
csign.zip	darv20.zip	darv3.zip	darv6.zip

File name	File name	File name	File name
darv7.zip	last.zip	PwDump.exe	Troj25.exe
darv8.zip	lastdb.zip	qualifieddata.zip	twitter.zip
darv9.zip	lb.msi	Read1.exe	up.aspx
data.zip	ldap.msi	Read2.exe	USBDeview.exe
dbpub.zip	ldap.msi	Read3.exe	validate.zip
Default.aspx	md5s.txt	Repositories.zip	vcredist_x86.exe
Demonstraties/tabid/409/language/nl-NL/Default.aspx	mimi.zip	rsa_cm_68.zip	webapp.zip
	mohem.zip	rsaservice.rar	websign.rar
Depends.exe	mswinsck.ocx	saerts.zip.part1.txt	win.exe
DigiNotar_Services_CA.cer	msxml6.msi	saerts.zip.part2.txt	win2.exe
direct.exe	nc.exe	saerts.zip.part3.txt	win3.exe
direct.zip	newjob.zip	saerts.zip.part4.txt	z3.exe
direct83.exe	nfast.zip	settings	z4.exe
elm.zip	nssl.zip	Settings.aspx	z5.exe
ev-add.zip	origrsa.zip	settings.aspxdepends.exe	Zip2.exe
f1.cer	passadmin.rar	settings.zip	zip3.exe
final.zip	pki.zip	sms.msi	zipped.zip
ids.zip	PortQry.exe	SQLServer2005_SSMSEE.msi	Zipper.exe
jobdone.zip	psexec.exe	ssl.zip	
keo.zip	putty.exe	tijdstempel.pfx	

7.2.1 Nog verwerken?

In H IIS logs opnemen:

winsrv119 (docproof)
2011-06-06 13:42:52
- mogelijk eerste verkenning (iis logs)

2011-06-14 14:27:30
- mogelijk tweede verkenning (iis logs)

{winsrv Beurs dir is voorheen niet gebruikt. (tekeningenetje van een tijdslijntje invoegen?)}

8 System access, tools and files

The hard disk drives of a number of systems have been investigated for traces of the attack. Although this kind of investigation can be done on all the suspicious systems, only a few important systems were scrutinised:

SVO2	winsrv022	Qualified CA
SVO5	winsrv053	Taxi CA
DD.055	winsrv055	Relatie CA
DD.056	winsrv056	Public CA
DD.119	winsrv119	docproof
SVO1	winsrv167	Root CA
SVO75	winsvr007	bapi db new
SVO3	winsvr057	CCV CA
SVO77	winsvr065	Office file server
SVO8	winsvr101	www

During the start of the investigation it quickly became clear that the attacker(s) used a web server in the external DMZ network to tranship files back home. The browser history or temporary internet files is examined on the DigiNotar machines the attacker(s) used to connect to these web server hops.

{wat is eigenlijk een mooie naam voor die web server doorhop contructie? Zoek en vervang…}

Another investigations have been done by examining the timestamps of the files on disk. These timestamps indicate if a file was created, copied of modified. Together with the file location and file name a file can become suspicious and can cause reason to examine it further. Deleted files that could be recovered are also included in this investigation.

8.1.1 Temporary internet files

{wat is het verschil tussen temporary internet files en \Local Settings\History\History.IE5\?}
The temporary internet files of the Windows systems shows cashed web pages of the transhipment {?} web server in the external DMZ network winsrv101 (also in chapter 7). These cashed pages show directory listing of file names with files size and modification date.

The temporary internet files also show cashed files from these web server(s) {zijn het er ook meedere?}. These cashed files are a result of a downloaded file. The temporary internet files however do not show traces of files that are uploaded on the web server. The temporary internet files also show what windows user accessed the web page or downloaded the file.

By searching the (deleted or not) temporary internet files for the file `settings[*].htm` (with * being a number) and inspecting the content of this file, a systems can be identified as used by the attacker(s).

Of the investigated systems the following systems showed this cashed page:

{vervang servernamen}
bapi db new
Taxi CA
Qualified CA
Root CA
winsrv055 Relatie CA
Public CA

{welke tijdstempel is het meest relevant? Create, modify of access?}
{zelfde entries erin laten staan?}
{Timeline.xlsx, filter op 'User (Temp internet file)' != #VALUE!; Filename == Settings[*].htm. Sort op create date&time}

Hostname	Filename	User (Local settings)	Size	Created date	Created time[14]

[14] Universal Time zone.

winsvr007	Settings[1].htm	Administrator	3097	1-Jul-2011	14:33:59
winsvr007	Settings[1].htm	Administrator	90587	1-Jul-2011	14:34:57
winsvr007	Settings[1].htm	Administrator	91912	1-Jul-2011	14:35:59
winsvr007	Settings[1].htm	Administrator	93049	1-Jul-2011	14:38:44
winsvr007	Settings[2].htm	Administrator	94254	1-Jul-2011	14:42:55
winsvr007	Settings[2].htm	Administrator	95463	1-Jul-2011	14:43:30
winsvr007	Settings[2].htm	Administrator	96638	1-Jul-2011	14:43:51
winsvr007	Settings[2].htm	Administrator	97774	1-Jul-2011	14:58:11
winsrv053	Settings[1].htm	Administrator	104502	1-Jul-2011	22:14:31
winsrv053	Settings[1].htm	Administrator	105810	1-Jul-2011	22:14:49
winsrv053	Settings[1].htm	Administrator	105657	1-Jul-2011	22:26:30
winsrv053	Settings[2].htm	Administrator	107011	1-Jul-2011	22:27:44
winsrv022	settings[1].htm	Administrator.DNPRODUCTIE	102048	1-Jul-2011	23:48:43
winsrv022	settings[1].htm	Administrator.DNPRODUCTIE	102048	1-Jul-2011	23:48:43
winsrv022	settings[1].htm	Administrator.DNPRODUCTIE	109400	1-Jul-2011	23:50:05
winsrv022	settings[1].htm	Administrator.DNPRODUCTIE	109400	1-Jul-2011	23:50:05
winsrv022	settings[2].htm	Administrator.DNPRODUCTIE	110645	2-Jul-2011	0:12:30
winsrv022	settings[2].htm	Administrator.DNPRODUCTIE	110645	2-Jul-2011	0:12:30
winsrv167	Settings[1].htm	administrator.DNPRODUCTIE	3097	2-Jul-2011	2:40:06
winsrv167	Settings[1].htm	administrator.DNPRODUCTIE	3097	2-Jul-2011	2:40:06
winsrv167	Settings[1].htm	administrator.DNPRODUCTIE	111657	2-Jul-2011	2:40:13
winsrv167	Settings[1].htm	administrator.DNPRODUCTIE	111657	2-Jul-2011	2:40:13
winsrv167	Settings[1].htm	administrator.DNPRODUCTIE	112982	2-Jul-2011	2:41:00
winsrv055	SETtings[1].htm	Administrator.DNPRODUCTIE	3097	2-Jul-2011	20:35:21
winsrv055	SETtings[1].htm	Administrator.DNPRODUCTIE	100888	2-Jul-2011	20:35:30
winsrv055	SETtings[1].htm	Administrator.DNPRODUCTIE	102197	2-Jul-2011	20:36:11
winsrv022	settings[1].htm	Administrator.DNPRODUCTIE	3097	2-Jul-2011	22:14:48
winsrv022	settings[1].htm	Administrator.DNPRODUCTIE	103305	2-Jul-2011	22:15:48

The temporary internet files also showed activity on the locate CA software web service:
{ Timeline.xlsx, filter op 'User (Temp internet file)' != #VALUE!; Filename == iets met CA software. Sort op create date}
All user Administrator.DNPRODUCTIE. Sort on file created timestamp.

Hostname	Filename	Size	Created date	Created Time
winsrv022	domain-main[3].htm	4162	1-Jul-2011	23:22:03
winsrv167	domain-main[1].htm	4162	2-Jul-2011	1:01:41
winsrv167	request-cacert[1].htm	27449	2-Jul-2011	1:05:47
winsrv167	cert-search-results[1].htm	26718	2-Jul-2011	1:06:36
winsrv167	view-cert[1].htm	13557	2-Jul-2011	1:07:17
winsrv167	domain-main[1].htm	4166	2-Jul-2011	1:08:38
winsrv167	request-msie[1].htm	233043	2-Jul-2011	1:08:45
winsrv167	add-msie-request[1].htm	7332	2-Jul-2011	1:10:03
winsrv167	cert-search-results[1].htm	2309	2-Jul-2011	1:11:23

winsrv167	view-cert[1].htm	15164	2-Jul-2011	1:11:52
winsrv167	MinIenM Organisatie CA - G2[1].p7b	5239	2-Jul-2011	1:12:42
winsrv167	cert-search-results[1].htm	3711	2-Jul-2011	1:15:56
winsrv055	cert-search-script[1]	20027	2-Jul-2011	20:42:08
winsrv055	cert-search-results[5].htm	58415	2-Jul-2011	20:43:29
winsrv055	view-cert[1].htm	13654	2-Jul-2011	20:43:43
winsrv055	index[2].htm	5291	2-Jul-2011	21:20:20
winsrv055	cert-search[1].htm	11192	2-Jul-2011	21:20:30
winsrv055	cert-search-script[1].htm	19411	2-Jul-2011	21:20:30
winsrv055	cert-search-results[4].htm	340	2-Jul-2011	21:22:25
winsrv055	cert-search-results[6].htm	9966	2-Jul-2011	21:37:08
winsrv055	get-ca-list[3].htm	3071717	2-Jul-2011	21:51:22
winsrv055	get-ca-list[2].htm	3071717	2-Jul-2011	21:54:12
winsrv055	index[1].htm	2525	2-Jul-2011	21:55:49
winsrv055	get-ca-list[5].htm	332	2-Jul-2011	21:55:57

The temporary internet files also show downloaded files and other unspecified pages{?}:
{tabel nog aanpassen/ mooier maken/ kleiner maken?}
{Eerste aantal ander timestamp selecteren? B.v. modif of access?}
{Timeline.xlsx, filter op 'User (Temp internet file)' != #VALUE!; Filename != bovengenoemde. Sort op?}

Hostname	Filename	User (Temp internet file)	Size	Created date	Created Time
winsvr007	$I30	MSSQLusr	4096	10-Nov-2008	8:26:34
winsvr007	$I30	MSSQLusr	4096	10-Nov-2008	8:26:34
winsvr007	$I30	MSSQLusr	4096	10-Nov-2008	8:26:34
winsvr007	KH6BWL27	MSSQLusr	56	10-Nov-2008	8:26:34
winsvr007	S5A38DAJ	MSSQLusr	56	10-Nov-2008	8:26:34
winsvr007	W9IJGHEF	MSSQLusr	56	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	index.dat	MSSQLusr	49152	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	kir[1].txt	MSSQLusr	9	17-Jun-2011	16:15:49
winsvr007	libeay32[1].dll	MSSQLusr	1017344	17-Jun-2011	16:18:44
winsvr007	PwDump7[1].exe	MSSQLusr	77824	17-Jun-2011	16:19:21
winsvr007	PwDump[1].exe	MSSQLusr	393216	17-Jun-2011	18:56:01
winsvr007	7za[1].exe	MSSQLusr	264704	17-Jun-2011	19:33:55
winsvr007	mswinsck[1].ocx	MSSQLusr	127808	17-Jun-2011	19:41:31
winsvr007	base64[1].exe	MSSQLusr	45056	18-Jun-2011	0:34:05
winsvr007	test[1].zip	MSSQLusr	2666	18-Jun-2011	5:11:53
winsvr007	mstsc[1].exe	MSSQLusr	407552	18-Jun-2011	14:46:46

winsvr007	mstscax[1].dll	MSSQLusr	655360	18-Jun-2011	14:47:28
winsvr007	clxtshar[1].dll	MSSQLusr	69632	18-Jun-2011	14:47:51
winsvr007	tclient[1].dll	MSSQLusr	68096	18-Jun-2011	14:48:29
winsvr007	test2[1].zip	MSSQLusr	2666	18-Jun-2011	14:53:55
winsvr007	nc[1].exe	MSSQLusr	65028	20-Jun-2011	10:34:15
winsvr007	demineur[1].dll	MSSQLusr	151552	20-Jun-2011	11:14:09
winsvr007	klock[1].dll	MSSQLusr	153600	20-Jun-2011	11:14:27
winsvr007	mimikatz[1].exe	MSSQLusr	368128	20-Jun-2011	11:15:40
winsvr007	sekurlsa[1].dll	MSSQLusr	200704	20-Jun-2011	11:15:51
winsvr007	cachedump[1].exe	MSSQLusr	45056	21-Jun-2011	12:50:00
winsvr007	PwDump[1].exe	MSSQLusr	393216	21-Jun-2011	13:09:47
winsvr007	mswinsck[2].ocx	MSSQLusr	127808	21-Jun-2011	13:46:33
winsvr007	uploader[2].exe	MSSQLusr	28672	21-Jun-2011	14:18:15
winsvr007	uploader[1].exe	MSSQLusr	28672	21-Jun-2011	15:07:23
winsvr007	up3[1].exe	MSSQLusr	28672	21-Jun-2011	15:21:03
winsvr007	sfk[1].exe	MSSQLusr	1155072	21-Jun-2011	19:53:15
winsvr007	ReadF[1].exe	MSSQLusr	8192	22-Jun-2011	8:41:06
winsvr007	Read1[1].exe	MSSQLusr	9728	22-Jun-2011	10:26:02
winsvr007	Read2[1].exe	MSSQLusr	9728	22-Jun-2011	10:46:20
winsvr007	Read3[1].exe	MSSQLusr	9728	22-Jun-2011	12:17:29
winsvr007	Read4[1].exe	MSSQLusr	9728	22-Jun-2011	12:20:09
winsvr007	Read5[1].exe	MSSQLusr	10240	22-Jun-2011	12:34:28
winsvr007	PortQry[1].exe	MSSQLusr	143360	29-Jun-2011	9:44:53
winsvr007	troj172[1].exe	MSSQLusr	61440	29-Jun-2011	22:13:34
winsvr007	troj172[1].exe	MSSQLusr	61440	29-Jun-2011	22:13:34
winsvr007	troj134[1].exe	MSSQLusr	61440	29-Jun-2011	22:18:17
winsvr007	troj134[1].exe	MSSQLusr	61440	29-Jun-2011	22:18:17
winsvr007	134[1].exe	MSSQLusr	37888	29-Jun-2011	22:30:33
winsvr007	RunAs[1].exe	MSSQLusr	24576	29-Jun-2011	22:52:25
winsvr007	RDP[1].exe	MSSQLusr	553472	29-Jun-2011	23:01:49
winsvr007	13480[1].exe	MSSQLusr	37888	29-Jun-2011	23:19:32
winsvr007	Troj25[1].exe	MSSQLusr	61440	1-Jul-2011	13:45:18
winsvr007	psexec[1].exe	MSSQLusr	381816	1-Jul-2011	19:12:25
winsvr007	mimi[1].zip	MSSQLusr	477545	1-Jul-2011	22:15:25
winsrv053	mimi[1].zip	Administrator	477545	1-Jul-2011	22:15:49
winsrv022	172.18.20[1].htm	Administrator.DNPRODUCTIE	4867	1-Jul-2011	23:20:51
winsrv053	winsvr130[1].htm	Administrator.DNPRODUCTIE	476	2-Jul-2011	0:53:44
winsrv167	corner[2].gif	administrator.DNPRODUCTIE	3196	2-Jul-2011	1:00:58
winsrv167	enrollbg[4].gif	administrator.DNPRODUCTIE	558	2-Jul-2011	1:00:58
winsrv167	icontrol[1].vbs	administrator.DNPRODUCTIE	35007	2-Jul-2011	1:08:45
winsrv167	up[1]	administrator.DNPRODUCTIE	3415	2-Jul-2011	1:24:31

winsrv167	favicon[1].ico	administrator.DNPRODUCTIE	3878	2-Jul-2011	2:40:06
winsvr007	ldap[1].msi	MSSQLusr	14297088	2-Jul-2011	18:41:27
winsrv055	get[1].htm	Administrator.DNPRODUCTIE	323	2-Jul-2011	20:57:35
winsrv055	banner[1].htm	Administrator.DNPRODUCTIE	6143	2-Jul-2011	21:55:49
winsrv055	172.18.20[1].htm	Administrator.DNPRODUCTIE	5291	2-Jul-2011	21:59:01
winsrv055	172.18.20[1]	Administrator.DNPRODUCTIE	5692	2-Jul-2011	21:59:34
winsvr007	direct[1].exe	MSSQLusr	37888	3-Jul-2011	23:40:23
winsvr007	direct[1].zip	MSSQLusr	19702	4-Jul-2011	1:06:00
winsrv053	direct[1].zip	Administrator.DNPRODUCTIE	19702	4-Jul-2011	4:18:39

8.1.2 Resent files

A number of resent used files are suspicious {omdat?}:
{Deze opnieuw exporteren: Timeline.xlsx, filter op. 'User (Recent)' != #VALUE!. Sort Create date & time}

Hostname	Filename	User (Recent)	Size	Created date	Created Time
winsvr101	Nieuw - Tekstdocument.txt.lnk	Administrator	872	20-Jun-2011	2:15:43
winsvr007	pki.zip.lnk	Administrator	424	1-Jul-2011	14:58:07
winsvr007	DARPI.lnk	Administrator	941	1-Jul-2011	16:13:07
winsrv053	Desktop.ini	Administrator	150	1-Jul-2011	22:32:39
winsrv053	Recent	Administrator	152	1-Jul-2011	22:32:39
winsrv022	certs.lnk	Administrator.DNPRODUCTIE	598	1-Jul-2011	23:29:57
winsrv022	ssl.crt.lnk	Administrator.DNPRODUCTIE	720	1-Jul-2011	23:29:57
winsrv022	root.crt.lnk	Administrator.DNPRODUCTIE	725	1-Jul-2011	23:31:45
winsrv022	cas.crt.lnk	Administrator.DNPRODUCTIE	720	1-Jul-2011	23:32:06
winsrv022	a.crt.lnk	Administrator.DNPRODUCTIE	736	1-Jul-2011	23:35:35
winsrv022	qualifiedData.zip.lnk	Administrator.DNPRODUCTIE	448	2-Jul-2011	0:09:57
winsrv022	qualifiedData.zip.lnk	Administrator.DNPRODUCTIE	448	2-Jul-2011	0:09:57
winsrv167	MinIenM Organisatie CA - G2.p7b.lnk	administrator.DNPRODUCTIE	560	2-Jul-2011	1:12:54
winsrv167	httpd.conf.lnk	administrator.DNPRODUCTIE	696	2-Jul-2011	2:13:05
winsrv167	dist.lnk	administrator.DNPRODUCTIE	531	2-Jul-2011	2:27:17
winsrv167	schema.conf.lnk	administrator.DNPRODUCTIE	677	2-Jul-2011	2:27:49
winsrv167	iXudad.conf.lnk	administrator.DNPRODUCTIE	677	2-Jul-2011	2:29:19
winsrv167	xudad.oc.conf.lnk	administrator.DNPRODUCTIE	683	2-Jul-2011	2:30:43
winsrv167	origrsa.zip.lnk	administrator.DNPRODUCTIE	416	2-Jul-2011	2:40:26
winsrv167	CertiID Enterprise Certificate Authority.crt.lnk	administrator.DNPRODUCTIE	804	2-Jul-2011	2:48:45
winsrv167	muh.lnk	administrator.DNPRODUCTIE	571	2-Jul-2011	2:48:45
winsrv167	USPP-Perso Certificate ST4000 260-160-364.crt.lnk	administrator.DNPRODUCTIE	879	2-Jul-2011	2:50:20
winsrv167	certs.lnk	administrator.DNPRODUCTIE	631	2-Jul-2011	2:50:20
winsrv055	dbpub.zip.lnk	Administrator.DNPRODUCTIE	404	2-Jul-2011	20:35:41
winsrv022	m.zip.lnk	Administrator.DNPRODUCTIE	380	2-Jul-2011	22:15:28

winsrv056	Desktop.ini	ljensma[15]	150	4-Jul-2011	0:05:17

8.1.3 Other local settings files

{ Timeline.xlsx, filter op 'User (Temp internet file)' == #VALUE!; 'User (Recent)' == #VALUE!, 'User (Local settings)' != #VALUE!. Sort?}
{path inkorten!}
{History opnemen in temporary internet files?}

Host name	File name	Full path	Size	Create date	Create time
winsvr007	S-1-5-21-2196791791-1123517030-1950105499-500	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-2196791791-1123517030-1950105499-500\	256	30-Jan-2006	11:44:01
winsrv056	$I30	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\$I30	4096	20-Jul-2010	12:55:21
winsrv056	Microsoft	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\	56	20-Jul-2010	12:55:21
winsrv056	Application Data	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\ljensma\Local Settings\Application Data\	472	17-Jun-2011	14:05:22
winsvr007	Credentials	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-2196791791-1123517030-1950105499-500\Credentials	346	1-Jul-2011	14:46:46
winsrv053	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\index.dat	49152	2-Jul-2011	0:53:44
winsrv053	MSHist012011061320110620	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\	152	2-Jul-2011	0:53:44
winsrv167	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\index.dat	32768	2-Jul-2011	1:00:58
winsrv167	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070220110703\index.dat	32768	2-Jul-2011	1:00:58
winsrv167	MSHist012011061320110620	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\	152	2-Jul-2011	1:00:58
winsrv167	MSHist012011070220110703	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070220110703\	152	2-Jul-2011	1:00:58
winsrv167	Dr Watson	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\	264	2-Jul-2011	2:18:56
winsrv167	Dr Watson	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\	264	2-Jul-2011	2:18:56
winsrv167	drwtsn32.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\drwtsn32.log	203258	2-Jul-2011	2:18:56
winsrv167	drwtsn32.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\drwtsn32.log	203258	2-Jul-2011	2:18:56
winsrv167	user.dmp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\user.dmp	90852	2-Jul-2011	2:18:56
winsrv167	user.dmp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application	90852	2-Jul-2011	2:18:56

[15] Naam weghalen? Zoek en vervang met ref. (Admin1)

		Data\Microsoft\Dr Watson\user.dmp			
winsrv167	{51503BD7-A456-11E0-941C-D48564505644}.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Last Active\{51503BD7-A456-11E0-941C-D48564505644}.dat	70144	2-Jul-2011	2:52:26
winsrv055	UserImages.bmp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\Application Data\Softerra\LDAP Browser 4\UserImages.bmp	9014	2-Jul-2011	21:46:30
winsrv056	Terminal Server Client	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Terminal Server Client\	144	4-Jul-2011	4:11:29
winsrv053	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011062720110704\index.dat	32768	4-Jul-2011	4:19:23
winsrv053	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070420110705\index.dat	32768	4-Jul-2011	4:19:23
winsrv053	MSHist012011062720110704	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011062720110704\	152	4-Jul-2011	4:19:23
winsrv053	MSHist012011070420110705	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070420110705\	152	4-Jul-2011	4:19:23

8.1.4 Other files

{ Timeline.xlsx, filter op 'User (Local settings)' == #VALUE!. Sort?}
{deze moet echt kleiner...}

Hostname	Filename	Full Path	Size	Created date	Created Time
winsvr007	hosts	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\drivers\etc\hosts	792	25-Mar-2003	12:00:00
winsvr007	savrt.dat	Partition 1\NONAME [NTFS]\[root]\Program Files\Symantec AntiVirus\savrt.dat	3220	17-Jan-2005	17:15:52
winsvr007	SRTSEXCL.DAT	Partition 1\NONAME [NTFS]\[root]\Program Files\Symantec AntiVirus\SRTSEXCL.DAT	76	17-Jan-2005	17:15:52
winsvr007	default	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\default	262144	30-Jan-2006	11:11:01
winsvr007	SAM	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\SAM	262144	30-Jan-2006	11:18:17
winsvr007	SECURITY	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\SECURITY	262144	30-Jan-2006	11:18:17
winsvr007	SchedLgU.Txt	Partition 1\NONAME [NTFS]\[root]\WINDOWS\Tasks\SchedLgU.Txt	10364	30-Jan-2006	11:37:22
winsvr007	ipconfig.exe	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ipconfig.exe	63488	30-Jan-2006	12:04:22
winsvr007	$I30	Partition 1\NONAME [NTFS]\[root]\Program Files\Symantec AntiVirus\$I30	12288	28-Mar-2006	7:42:25
winsvr007	Symantec AntiVirus	Partition 1\NONAME [NTFS]\[root]\Program Files\Symantec AntiVirus\	288	28-Mar-2006	7:42:25
winsvr007	settings.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\Symantec\Common Client\settings.dat	20204	28-Mar-2006	7:42:46
winsvr007	BBConfig.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBConfig.log	3676	28-Mar-2006	7:42:49
winsvr007	BBDebug.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBDebug.log	64	28-Mar-2006	7:42:49
winsvr007	BBDetect.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBDetect.log	64	28-Mar-2006	7:42:49
winsvr007	BBNotify.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBNotify.log	64	28-Mar-2006	7:42:49
winsvr007	BBRefr.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBRefr.log	64	28-Mar-2006	7:42:49
winsvr007	BBSetCfg.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetCfg.log	64	28-Mar-2006	7:42:49
winsvr007	BBSetDev.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetDev.log	64	28-Mar-2006	7:42:49
winsvr007	BBSetLoc.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetLoc.log	2108	28-Mar-2006	7:42:49
winsvr007	BBSetUsr.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetUsr.log	64	28-Mar-2006	7:42:49
winsvr007	BBStHash.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBStHash.log	64	28-Mar-2006	7:42:49
winsvr007	BBStMSI.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBStMSI.log	7576	28-Mar-2006	7:42:49
winsvr007	BBValid.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBValid.log	64	28-Mar-2006	7:42:49
winsvr007	SPPolicy.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPPolicy.log	64	28-Mar-2006	7:42:49
winsvr007	SPStart.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPStart.log	64	28-Mar-2006	7:42:49
winsvr007	SPStop.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPStop.log	64	28-Mar-2006	7:42:49
winsvr007	finance01_Log.LDF	Partition 5\Log [NTFS]\[root]\MSSQL\Log\finance01_Log.LDF	1048576	27-Feb-2007	13:40:29

winsvr007	Applog01_Log.LDF	Partition 5\Log [NTFS]\[root]\MSSQL\Log\Applog01_Log.LDF	2359296	28-Mar-2007	11:02:45
winsvr007	Web.config	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\wschmitt\Bureaublad\WebRAOBeheer02\Web.config	7415	14-Jun-2007	6:52:21
winsvr101	web.config	Partition 3\Data [NTFS]\[root]\Websites\Bapiviewer\BapiViewer\web.config	5471	23-Nov-2009	14:25:02
winsrv056	mofcomp.log	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\wbem\Logs\mofcomp.log	14664	19-Jul-2010	12:43:54
winsvr007	wietse_log.ldf	Partition 5\Log [NTFS]\[root]\MSSQL\Log\wietse_log.ldf	3145728	8-Jun-2011	10:55:12
winsrv119	b.aspx	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\js\b.aspx	72689	17-Jun-2011	2:33:35
winsrv119	RunAs.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\RunAs.exe	24576	17-Jun-2011	5:43:32
winsvr007	06172011.Log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\06172011.Log	262	17-Jun-2011	15:46:37
winsvr007	06172011.Log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\06172011.Log	262	17-Jun-2011	15:46:37
winsvr007	archive.zip	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\archive.zip	198024801	17-Jun-2011	19:35:47
winsvr007	mswinsck.ocx	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\mswinsck.ocx	127808	17-Jun-2011	19:41:31
winsvr101	demineur.dll	Partition 3\Data [NTFS]\[orphan]\demineur.dll	151552	19-Jun-2011	23:43:00
winsvr101	klock.dll	Partition 3\Data [NTFS]\[orphan]\klock.dll	153600	19-Jun-2011	23:43:13
winsvr101	mimikatz.exe	Partition 3\Data [NTFS]\[orphan]\mimikatz.exe	368128	19-Jun-2011	23:43:40
winsvr101	sekurlsa.dll	Partition 3\Data [NTFS]\[orphan]\sekurlsa.dll	200704	19-Jun-2011	23:43:58
winsvr101	Nieuw - Tekstdocument.txt.lnk	Partition 2\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\Nieuw - Tekstdocument.txt.lnk	872	20-Jun-2011	2:15:43
winsvr007	WINSVR007_MS IIS DCOM Server.pvk	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_MS IIS DCOM Server.pvk	332	20-Jun-2011	11:17:30
winsvr007	WINSVR007_SELFSIGN_DEFAULT_CONTAINER.pvk	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_SELFSIGN_DEFAULT_CONTAINER.pvk	620	20-Jun-2011	11:17:30
winsvr007	WINSVR007_Microsoft Internet Information Server.pvk	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_Microsoft Internet Information Server.pvk	332	20-Jun-2011	11:17:30
winsvr007	WINSVR007_tmpHydraLSKeyContainer.pvk	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_tmpHydraLSKeyContainer.pvk	332	20-Jun-2011	11:17:30
winsvr007	WINSVR007_0_winsvr007.diginotar.nl.pfx	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_0_winsvr007.diginotar.nl.pfx	1737	20-Jun-2011	11:17:30
winsvr007	Documents.7z	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Documents.7z	1015873568	21-Jun-2011	12:46:54
winsvr007	bsqweyec.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\bsqweyec.dll	65536	21-Jun-2011	13:18:45
winsvr007	xjegjvhr.exe	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\xjegjvhr.exe	53760	21-Jun-2011	13:18:45
winsvr007	uploader	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\uploader\	48	21-Jun-2011	13:54:25
winsrv119	94.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\94.exe	37888	21-Jun-2011	21:20:43
winsrv119	Troj65.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\Troj65.exe	61440	22-Jun-2011	10:42:52
winsrv119	PwDump.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\PwDump.exe	393216	22-Jun-2011	12:09:07
winsrv119	cachedump.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\cachedump.exe	45056	22-Jun-2011	12:40:32
winsrv119	test.txt	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\test.txt	127	22-Jun-2011	12:40:44
winsvr007	rdp.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\rdp.exe	553472	29-Jun-2011	23:05:04
winsvr007	rdp.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\rdp.exe	553472	29-Jun-2011	23:05:04
winsvr007	Default.rdp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\Default.rdp	2458	29-Jun-2011	23:10:56
winsvr065	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	141	30-Jun-2011	8:56:18
winsvr065	sfk.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\sfk.exe\	1155072	30-Jun-2011	9:17:51
winsvr065	sfk.exe	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\sfk.exe\	1155072	30-Jun-2011	10:56:34
winsvr007	13480.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\13480.exe	37888	1-Jul-2011	13:10:17
winsvr007	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	141	1-Jul-2011	14:33:59
winsvr007	pki.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\pki.zip.lnk	424	1-Jul-2011	14:58:07
winsvr007	DARPI.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\DARPI.lnk	941	1-Jul-2011	16:13:07
winsrv053	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	139	1-Jul-2011	22:14:14
winsrv053	Crypto	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Microsoft\Crypto\	136	1-Jul-2011	22:17:28
winsrv053	MachineKeys	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Microsoft\Crypto\RSA\MachineKeys\	48	1-Jul-2011	22:17:28
winsrv053	RSA	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Microsoft\Crypto\RSA\	256	1-Jul-2011	22:17:28
winsrv053	Desktop.ini	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\Desktop.ini	150	1-Jul-2011	22:32:39
winsrv053	Recent	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\	152	1-Jul-2011	22:32:39
winsrv022	certs.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\certs.lnk	598	1-Jul-2011	23:29:57
winsrv022	ssl.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\ssl.crt.lnk	720	1-Jul-2011	23:29:57
winsrv022	root.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\root.crt.lnk	725	1-Jul-2011	23:31:45
winsrv022	cas.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\cas.crt.lnk	720	1-Jul-2011	23:32:06
winsrv022	a.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\a.crt.lnk	736	1-Jul-2011	23:35:35
winsrv022	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	141	1-Jul-2011	23:48:43
winsrv022	qualifiedData.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\qualifiedData.zip.lnk	448	2-Jul-2011	0:09:57
winsrv022	qualifiedData.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\qualifiedData.zip.lnk	448	2-Jul-2011	0:09:57
winsrv022	457718b9-fa34-41e3-8d9d-3ecf7391929c	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Microsoft\Protect\S-1-5-18\User\457718b9-fa34-41e3-8d9d-3ecf7391929c	388	2-Jul-2011	0:13:40
winsrv022	nfmodexp.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\nfmodexp.dll	742680	2-Jul-2011	0:24:03
winsrv022	nfmodexp.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\nfmodexp.dll	742680	2-Jul-2011	0:24:03
winsrv022	ncspmess.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspmess.dll	357656	2-Jul-2011	0:24:03
winsrv022	ncspmess.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspmess.dll	357656	2-Jul-2011	0:24:03

winsrv022	ncsp.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncsp.dll	1041688	2-Jul-2011	0:24:03
winsrv022	ncsp.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncsp.dll	1041688	2-Jul-2011	0:24:03
winsrv022	ncspdd.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspdd.dll	1041688	2-Jul-2011	0:24:03
winsrv022	ncspdd.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspdd.dll	1041688	2-Jul-2011	0:24:03
winsrv022	ncspsigdd.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspsigdd.dll	1033496	2-Jul-2011	0:24:03
winsrv022	ncspsigdd.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspsigdd.dll	1033496	2-Jul-2011	0:24:03
winsrv167	DNproductie.sch	Partition 1\NONAME [NTFS]\[root]\WINDOWS\SchCache\DNproductie.sch	370536	2-Jul-2011	1:03:25
winsrv167	SchCache	Partition 1\NONAME [NTFS]\[root]\WINDOWS\SchCache\	272	2-Jul-2011	1:03:25
winsrv167	9cb4f8bdfaa302f85333ef07 fa3fb192_60643e52-42b0-4d55-aea2-38a5b64b11ec	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\Crypto\RSA\S-1-5-21-4190788878-266275749-1156481715-500\9cb4f8bdfaa302f85333ef07fa3fb192_60643e52-42b0-4d55-aea2-38a5b64b11ec	2073	2-Jul-2011	1:10:02
winsrv167	40F1C4C24E802122FBC4DB 5061CADF1DDCEB33DD	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\Certificates\40F1C4C24E802122FBC4DB5061CADF1D DCEB33DD	858	2-Jul-2011	1:10:03
winsrv167	Certificates	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\Certificates\	320	2-Jul-2011	1:10:03
winsrv167	CRLs	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\CRLs\	48	2-Jul-2011	1:10:03
winsrv167	CTLs	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\CTLs\	48	2-Jul-2011	1:10:03
winsrv167	Request	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\	456	2-Jul-2011	1:10:03
winsrv167	MinIenM Organisatie CA - G2.p7b.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\MinIenM Organisatie CA - G2.p7b.lnk	560	2-Jul-2011	1:12:54
winsrv167	keysafe.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\nCipher\Log Files\keysafe.log	566	2-Jul-2011	1:28:19
winsrv167	cmdadp.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\nCipher\Log Files\cmdadp.log	388	2-Jul-2011	1:28:20
winsrv167	cmdadp-debug.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\nCipher\Log Files\cmdadp-debug.log	0	2-Jul-2011	1:28:20
winsrv167	httpd.conf.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\httpd.conf.lnk	696	2-Jul-2011	2:13:05
winsrv167	ErrorRep	Partition 1\NONAME [NTFS]\[root]\WINDOWS\PCHealth\ErrorRep\	256	2-Jul-2011	2:18:54
winsrv167	ErrorRep	Partition 1\NONAME [NTFS]\[root]\WINDOWS\PCHealth\ErrorRep\	256	2-Jul-2011	2:18:54
winsrv167	UserDumps	Partition 1\NONAME [NTFS]\[root]\WINDOWS\PCHealth\ErrorRep\UserDumps\	576	2-Jul-2011	2:18:54
winsrv167	UserDumps	Partition 1\NONAME [NTFS]\[root]\WINDOWS\PCHealth\ErrorRep\UserDumps\	576	2-Jul-2011	2:18:54
winsrv167	dist.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\dist.lnk	531	2-Jul-2011	2:27:17
winsrv167	schema.conf.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\schema.conf.lnk	677	2-Jul-2011	2:27:49
winsrv167	iXudad.conf.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\iXudad.conf.lnk	677	2-Jul-2011	2:29:19
winsrv167	xudad.oc.conf.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\xudad.oc.conf.lnk	683	2-Jul-2011	2:30:43
winsrv167	administrator@10.10.20[1]. txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	140	2-Jul-2011	2:40:06
winsrv167	administrator@10.10.20[1]. txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	140	2-Jul-2011	2:40:06
winsrv167	origrsa.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\origrsa.zip.lnk	416	2-Jul-2011	2:40:26
winsrv167	CertiID Enterprise Certificate Authority.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\CertiID Enterprise Certificate Authority.crt.lnk	804	2-Jul-2011	2:48:45
winsrv167	d$ on winsvr057	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\	256	2-Jul-2011	2:48:45
winsrv167	d$ on winsvr057	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\	256	2-Jul-2011	2:48:45
winsrv167	Desktop.ini	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\Desktop.ini	75	2-Jul-2011	2:48:45
winsrv167	Desktop.ini	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\Desktop.ini	75	2-Jul-2011	2:48:45
winsrv167	muh.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\muh.lnk	571	2-Jul-2011	2:48:45
winsrv167	target.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\target.lnk	463	2-Jul-2011	2:48:45
winsrv167	target.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\target.lnk	463	2-Jul-2011	2:48:45
winsrv167	USPP-Perso Certificate ST4000 260-160-364.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\USPP-Perso Certificate ST4000 260-160-364.crt.lnk	879	2-Jul-2011	2:50:20
winsrv167	certs.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\certs.lnk	631	2-Jul-2011	2:50:20
winsvr057	winsvr022.txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\winsvr022.txt	461	2-Jul-2011	4:56:07
winsvr057	winsvr167.txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\winsvr167.txt	272	2-Jul-2011	4:58:03
winsvr057	kcavkfsc.dll	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\kcavkfsc.dll	65536	2-Jul-2011	4:59:38
winsvr057	njnypgqa.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\njnypgqa.exe	53760	2-Jul-2011	4:59:38
winsvr057	winsvr056.txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\winsvr056.txt	458	2-Jul-2011	4:59:38

winsrv055	get.xuda	Partition 2\Data [NTFS]\[root]\Progs\rsa_cm_68\WebServer\enroll-server\ca\get.xuda	254	2-Jul-2011	16:58:51
winsrv055	dbpub.zip	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Desktop\dbpub.zip	59545925	2-Jul-2011	20:32:25
winsrv055	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\npost\Desktop\administrator@10.10.20[1].txt	141	2-Jul-2011	20:35:21
winsrv055	dbpub.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\dbpub.zip.lnk	404	2-Jul-2011	20:35:41
winsrv022	m.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\m.zip.lnk	380	2-Jul-2011	22:15:28
winsrv056	add-pkcs10-request[16].htm	Partition 5\NONAME [NTFS]\[orphan]\add-pkcs10-request[16].htm	96617	3-Jul-2011	14:17:11
winsrv056	osvchost.exe	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system\osvchost.exe	36864	3-Jul-2011	23:56:43
winsrv056	Desktop.ini	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\ljensma\Recent\Desktop.ini	150	4-Jul-2011	0:05:17
winsrv056	C8463ECBE33BC240263A0B094E46D510.mof	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\wbem\AutoRecover\C8463ECBE33BC240263A0B094E46D510.mof	2826402	4-Jul-2011	1:28:46
winsrv056	23BDE61F1F4FACE17E9B0C01F2A1FD9B.mof	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\wbem\AutoRecover\23BDE61F1F4FACE17E9B0C01F2A1FD9B.mof	36574	4-Jul-2011	1:28:46
winsrv056	Settings[2].htm	Partition 5\NONAME [NTFS]\[orphan]\Settings[2].htm	3097	4-Jul-2011	1:35:03
winsrv056	direct83[1].exe	Partition 5\NONAME [NTFS]\[orphan]\direct83[1].exe	37888	4-Jul-2011	1:35:25
winsrv056	csrsss.exe	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\csrsss.exe\	37888	4-Jul-2011	1:38:33
winsrv056	Zone.Identifier	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\csrsss.exe\Zone.Identifier	26	4-Jul-2011	1:38:33
winsrv056	139[1].exe	Partition 5\NONAME [NTFS]\[orphan]\139[1].exe	37888	4-Jul-2011	2:29:25
winsrv056	svhost.exe	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\svhost.exe\	37888	4-Jul-2011	2:31:06
winsrv056	Zone.Identifier	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\svhost.exe\Zone.Identifier	26	4-Jul-2011	2:31:06
winsrv053	svchost.exe	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system\svchost.exe\	19702	4-Jul-2011	4:19:23
winsrv053	Zone.Identifier	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system\svchost.exe\Zone.Identifier	26	4-Jul-2011	4:19:23
winsrv055	Default.rdp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\My Documents\Default.rdp	1214	4-Jul-2011	9:08:50
winsrv056	x-select-settings.xuda	Partition 2\NONAME [NTFS]\[orphan]\x-select-settings.xuda	28875	20-Jul-2011	10:11:07

8.1.5 Tools

Several suspicious tools and files were discovered during the investigation. First, they were found in the web server logs of winsrv101 that showed a list of file names that were uploaded or downloaded by the attacker(s) (refere to chapter 7). Second, in the browser history or temporary internet files on the machines the attacker(s) used to connect to these web server hops. And last, the timestamp of the files on disk indicated suspicious usage of these files.

8.1.5.1 Back connect

A few files that were examined more closely produce a network connection tunnel between two IP addresses if executed. The IP addresses are 'hard coded' in the executable. This and the fact the creation time {build time?} made us believe the files are especially created to run in the DigiNotar network. These back connect files create an encrypted {is dat ook zo?} tunnel (a VPN) between two systems making it possible to transfer files and commands {is dat ook zo?} and to execute for example remote desktop connection between on a server. Also, the tunnel made it possible for the attacker to gain access to the systems when other means were cut off. For example if new firewall settings or password change {is dat ook zo?} made it impossible to log on the internal network the created tunnel allows simple access.

These files were all extracted from the temporary internet files on winsvr007 in the Office network.

File name	IP addres 1 (from)	IP address 2 (to)
troj134.exe	172.17.20.4 winsvr007 Bapi Database New	10.10.20.134 winsvr155 eherkenning AD port 443
troj172.exe	172.17.20.4 winsvr007 Bapi Database New	10.10.20.16 winsvr108 Websites met auth.pass.nl port 443
troj25.exe	172.17.20.25 winsvr003 CI - Source build server	10.10.20.134 winsvr155 eherkenning AD Port 443
134.exe	{weten we dit nog of stond er maar een IP in?}	10.10.20.134 winsvr155 eherkenning AD Port 443
13480.exe	{weten we dit nog of stond er maar een IP in?}	10.10.20.134 winsvr155 eherkenning AD Port 443

8.1.5.2 Xuda script

On the Public-CA a deleted file x-select-settings.xuda was found. This file was probably deleted by the DigiNotar employees when the hack was discovered. This script contains XUDA-code that uses the Xcert Universal Database API in order to use the CA software {ref naar hoofdstukje xx}. In this script two lists

of 113 signing requests are included. Other investigations have shown[16] that the script was placed in the directory "WebServer\x-templates\" of the CA software on winsrvxxx (Public CA). This investigation states that this script is then run whenever the web interface of the CA software is started and consequently certificates are issued by four different CA private keys.

On the Relatie-CA the file get.xuda is encountered. This script is then assessed by the internet explorer. The cashed page shows a xuda error.

{waar moet onderstaande in het rapport terecht komen?}
The previous investigation (note12) also show that a svchost.exe found on the Public CA creates a file 'jobsdone.zip' and uploads this file to the web server 10.10.20.41 in the external DMZ using the /beurs/up.aspx script on that server. The investigation also states that the file svchost.exe creates a connection to 10.10.20.41 on port 53.

The previous investigation (note12) also investigated another file discovered on one of the CA servers. This file creates an connection to an external IP address:

File name	Connection destination
csrsss.exe[17]	AttIP1{ref} port 137

{end Waar?}

8.1.5.3 Other tools/ timeline

Some of the other encountered files were quick assessed based on their filenames:

First upload date	File name	Remark
2011-06-17_05:26:36	Settings.aspx	web up/downloader
2011-06-18_01:43:26	nc.exe	Netcat tool
2011-06-18_02:46:04	mstsc.exe	MS Terminal Services Client
2011-06-18_02:47:01	mstscax.dll	Part of Terminal Services bruteforcer?
2011-06-18_02:47:37	clxtshar.dll	Part of Terminal Services bruteforcer?
2011-06-18_02:48:03	tclient.dll	Part of Terminal Services bruteforcer?
2011-06-18_03:00:52	test2.rdp	
2011-06-19_06:48:47	datapipe.exe	Port redirector
2011-06-19_06:58:01	Redirector.exe	
2011-06-19_08:52:57	T1.exe	
2011-06-19_08:56:24	mswinsck.ocx	
2011-06-19_09:23:15	94.exe	Doorway to AttIP2?
2011-06-19_09:29:05	Troj.exe	
2011-06-19_09:35:39	PwDump.exe 384.00K	Dump password hashes tool.
2011-06-19_09:40:49	res.txt	
2011-06-19_10:09:29	7za.exe	7zip SFX?
2011-06-19_11:58:40	mimi.zip	mimikatz zip?
2011-06-20_11:13:18	demineur.dll	mimikatz - This library allows to manipulate the minesweeper
2011-06-20_11:13:59	klock.dll	mimikatz - This library allows you to switch desktops
2011-06-20_11:14:51	mimikatz.exe	mimikatz - mimikatz is a security auditing tool, its primary role is to place a library in a remote process and enable communication between the target process and mimikatz in the manner of a shell
2011-06-20_11:15:25	sekurlsa.dll	mimikatz - This library allows to manipulate the Windows authentication process
2011-06-21_01:48:50	rdpv.exe	

[16] This investigation is done by a security expert at Vasco {vasco niet noemen?} and has not been verified.
[17] Analised by security expert at Vasco

2011-06-21_09:28:54	RunAs.exe	
2011-06-21_12:28:29	up.aspx	
2011-06-21_12:49:52	cachedump.exe	Recovering Windows Password Cache Entries
2011-06-22_08:39:14	ReadF.exe	
2011-06-22_10:25:13	Read1.exe	
2011-06-22_10:46:06	read2.exe	
2011-06-22_12:17:23	read3.exe	
2011-06-22_12:19:53	read4.exe	
2011-06-22_12:34:07	read5.exe	
2011-06-27_08:41:55	TheRunAs.exe	
2011-06-27_08:49:34	Run2.exe	
2011-06-27_08:54:07	Run3.exe	
2011-06-27_09:01:41	RunAsMy.exe	
2011-06-27_09:29:48	Run5.exe	
2011-06-27_09:33:03	83443.exe	Doorway to AttIP1 port 443?
2011-06-27_09:42:12	Run6.exe	
2011-06-27_10:19:10	bb.bat	
2011-06-27_10:20:53	My3.exe	
2011-06-27_10:26:15	My7.exe	
2011-06-27_10:32:35	My8.exe	
2011-06-27_10:39:58	Mk.exe	
2011-06-27_10:55:58	Mk2.exe	
2011-06-27_12:34:50	Raexer.exe	
2011-06-27_12:36:10	ra2.exe	
2011-06-27_12:40:40	Ra3.exe	
2011-06-29_09:23:41	PortQry.exe	
2011-06-29_10:12:22	testproxy.exe	
2011-06-29_10:18:02	troj134.exe	Creates a connection between 10.10.20.134 (winsvr155/AD) and 172.17.20.4 (winsvr007/Bapi DB)
2011-06-29_10:30:12	134.exe	Creates a connection with 10.10.20.134:443
2011-06-29_11:01:15	RDP.exe	
2011-06-29_11:19:14	13480.exe	Creates a connection with 10.10.20.134:443
2011-06-30_02:56:08	83.rdp	
2011-06-30_11:56:00	PsExec.exe	Psexec tool
2011-06-30_11:57:13	PsExec.zip	psexec zipped
2011-07-01_01:43:25	troj25.exe	Creates a connection between 10.10.20.134 (winsvr155/AD) and 172.17.20.25 (winsvr003/CI source build server)
2011-07-01_02:43:30	RSAService.rar	
2011-07-01_02:58:11	pki.zip	
2011-07-01_09:31:07	ssl.zip	
2011-07-01_09:40:45	nssl.zip	
2011-07-01_10:14:49	kkeys.zip	
2011-07-01_10:47:21	aaaa.txt	
2011-07-01_11:50:05	CertContainer.dll	
2011-07-01_12:25:45	MSCOMCTL.zip	
2011-07-02_06:33:47	ldap.msi	
2011-07-02_07:59:22	zipped.zip	
2011-07-02_08:04:43	msxml6.msi	
2011-07-02_08:36:11	dbpub.zip	
2011-07-02_10:15:48	m.zip	
2011-07-02_12:18:33	putty.exe	Putty

This leads to the following assumptions:

- On 17 June the up/ downloader is in place (2011-Jun-17 02:33:35 (file date) the file b.aspx is uploaded to winsrv119 (docproof))

- On 18 juni attempts were started to bruteforce RDP
- Meanwhile some proxies/ redirectors were made
- On 30 juni psexec was uploaded. Presumably {weten we echt niet?} this was used to gain acces to the Secure network by NetBIOS connections.
- On 1 july the focus was on certificates and CA software.

8.1.5.4 Password crack

On winsrv??? (CCV CA) the tool Cain & Able (with winpcap) was installed. This tool is probably used to crack password hashes. The tool pwdump extracts the password hashes from the system. The tool Cain & Able then brute force these hashes and the passwords are revealed. On the desktop deleted files were found with output from the tool pwdump:

- winsvr022.txt
- winsvr056.txt
- winsvr167.txt

With the tool Cain probably attempts are made to capture passwords by a man-in-the-middle attack method. This because of the found deleted Kerberos tickets and NTLM challenge-responses in the files K5.LST, KRB5.LST, SMB.LST and HOSTS.LST.

{Onderstaande moet in de timeline worden opgenomen}
On the Taxi-CA the attacker(s) had logged in as local administrator. Downloaded the file mimi.zip. After that the attacker(s) logged on as domain administrator.

From winsrv119 a RDP session is started with winsrv155. Although this is not suspicious the time this occurrence (11-July-2011 0:25:32) is.

The tool cacheddump.exe is uploaded on the docproof website (Websites\Docproof\Docproof01\demo\cachedump.exe). Also on the website the file test.txt is found (Accessed 2011-Jul-25 20:17:31.000324 UTC) containing the mscache of one of the administrators. This password can easily be cracked ("MazdaRX8").

On winsrv056 many pkcs10 requests have been made with the local CA software web interface. Also many Certificate Signing Requests have been manually made with this interface.

On winsrv167 (Root CA) nCipher logs have been created. Also Dr. Watson error dump of Xuda.exe is found. {wat betekend dit ...?}

The settings.aspx provides a file manager where files can be up and downloaded. To gain access to this web page a username password combination is required. {dit moet ook ergens anders komen te staan}.

On the winsrx{xxx, bapi database new} some activity on files concerning Symantec Antivirus was done by the attacker. Possibly the antivirus software was disabled.

8.1.6 eNcipher DLLs

During the investigation on the Qualified CA server it is discovered that some of the DLL used to access the netHSM were modified. These files are located in the WINDOWS\system32 directory:

- nfmodexp.dll
- ncspmess.dll
- ncsp.dll
- ncspdd.dll
- ncspsigdd.dll

The file creation, modification and accessed times are all around 2011-Jul-02 00:24:03 UTC.

Further investigations showed that three of these files have incorrect digitally signatures indicating modification of the DLLs. The manufacturer of the eCipher netHSM (Thales {}) provided us with the hash digest of the original DLLs. These matched exactly with the hashes of the found DLL. This lead to the conclusion the DLLs were not tempered with. The time stamps could have been changed because they have been copied.

Thales confirms the Authenticode can be invalid. {deze tekst nog aanpassen} "*In relation to the invalid Authenticode signatures we have traced this issue to a dual-signing mechanism that is used with these specific files. This is a hangover from Windows 2003 Server and earlier versions of Windows, where Microsoft themselves are required to sign the nCipher/Thales CSP files as part of an earlier export control process. In this case the Microsoft signatures are applied *after* the Authenticode signature is performed by Thales. The Microsoft signatures are embedded within the DLL file and this results in a modification to the files that invalidates the Authenticode signature.*

Although standard Windows tools therefore report that the Authenticode signature is invalid, the Windows system will actually validate the embedded signatures with the CSP files prior to execution and these will verify. In the event that an attacker was to modify these files Windows would automatically refuse to execute these files. This method of signing pre-dates Authenticode and is required to maintain compatibility with earlier versions of Windows."

9 Remaining Investigation

{wellicht sommige onderwerpen naar een eigen hoofdstukje}

9.1 netHSMs

DigiNotar used nCipher netHSM 500s. The systems have limited log facility. It is recommended by the supplier to store the logs on a separate log server. However this was not configured at DigiNotar. The log stored on the netHSM are deleted every time the machine is turn off. This had already occurred when the investigation was started. Therefore no log could be retrieved.

9.2 Load balancer

{Ik heb van verschillende mensen de vraag gekregen of de load-balancer bij Diginotar logging bijhoudt. De load-balancer is een appliance van het merk Coyote. De logging wordt weggeschreven naar de syslog server. Ik heb in de syslogserver zitten te grasduinen maar hierin zit van de load-balancer geen relevante informatie. Naar wat horten en stoten hebben we het wachtwoord kunnen bemachtigen van de appliance maar ook hierin geen relevante logging.}

9.3 Other?

10 Investigation of external systems

{de systemen uit UK en RU}
{hebben we niet zo veel mee gedaan, maar wel iets!}

10.1 Server hosting AttIP2

During the investigation a tool was found that created a back connect to an external IP address AttIP2{ref} {ref H}. On 13 September 2011 an official request for assistance to the authorities in the country were the server is located was issued. A copy of this server was investigated.

On this server the web server log files showed interesting entries of GET requests from AttIP3. These log entries show a file mails.rar is downloaded several times on 2011-07-19 between 16:35:51 and 19:42:17. This file is only download by AttIP3 except on the first occurrence when it is downloaded by AttIP6.

10.2 AttIP4

The IP address encountered in the web server logs AttIP4 was banned by several CA providers due to persistent hacking attempts on web servers of CA providers.

11 Investigation conclusions

{combinative van losse onderzoeksresultaten}

11.1 Path of the attacker(s)

Files or commands were exchanged between the external DMZ and the Office network (WINSRV007; Bapi Database New; 172.17.20.4) as well as the secure network (WINSRV056; Public-CA; 172.18.20.245).

A connection was made from a number for internal systems with the webserver in the DMZ (10.10.20.41). A reconstructed list of files that have been present on the `/beurs` directory of the webserver shows suspicious activity. It is highly likely that the webserver was used by the attacker(s) to transport files from internal systems to external systems on the Internet.

An indication whether a system was compromised by the attacker(s) is if traces of suspicious activity can be found in the Temporary Internet Files of the Internet Explorer webbrowser. If the cached version of `settings[1].htm` is present in the Temporary Internet Files with the before mentioned malicious content then the system was most likely compromised by the attacker(s).

The IIS log files of the webserver were secured, but log files for a crucial period were missing. Traces of log entries related to the `/beurs` directory were found on the harddisk of the webserver. The traces led to a list of 14 unique internal and an publicly undisclosed number of external IP-addresses of systems that were most likely used by the attacker(s). The IIS logs show that a total of 125 files were transported between these systems.

In order to connect from certain internal systems to proxy systems tailored hacking tools were used. These tools created a connect-back between two IP-addresses using port 443 to get through the firewall. Traces of these connections were found in the firewall log files.

Connect-back tunnels:

IP 1	IP 2	Opm.
172.17.20.4	10.10.20.134	
172.17.20.4	10.10.20.16	
172.17.20.25	10.10.20.134	Geen connecties?
172.18.20.245	10.10.20.134	Geen malware?

Proxy/ dumpplaats

			Opm.
10.10.20.134	WINSRV155	[P] eherkenning AD (SVO51)	Moet nog onderzocht worden of dit ook zo is.
10.10.20.16	WINSRV108	[P] Websites met auth.pass.nl (SVO35 SVO36)	Moet nog onderzocht worden of dit ook zo is.
10.10.20.41	WINSRV101	Website met www.diginotar.nl (SVO8)	

Uit de firewall logs is verdacht verkeer geconstateerd tussen de netwerk segmenten "secure" en "uitwijk-secure". Dit moet nog verder onderzocht worden.

11.1.1 Originating IP addresses attacker

By examining the web server logs of {servername/ SVO8}, malware and WINSRV119(?) a number of IP addresses were encountered that the attacker(s) used. In **Error! Reference source not found.**.

11.1.2 Compromised systems

IP	Server naam	Omschrijving	SVO	Bron verdenking					
				IIS log SVO8	Firewall logs	Tools found	IE history	Trojan	Other
10.10.20.16	WINSRV108	[P] Websites met auth.pass.nl	SVO35 SVO36					X	
10.10.20.40	WINSRV108	[P] Websites met auth.pass.nl			X				
10.10.20.41	WINSRV101	Externe web server	SVO8		X				
10.10.20.58	???		?	X					
10.10.20.65?	WINSRV119	DocProof	ITSec						
10.10.20.134	WINSRV155	[P] eherkenning AD	?		X			X	
10.10.20.139	WINSRV157	[P] eherkenning HM	SVO28 SVO29 SVO31		X				
10.10.200.20	WINSRV066	Docproof Database	SVO312 SVO313 SVO314	X					
172.17.20.25	???							X	
172.17.20.4	WINSRV007	Bapi Database New	SVO75 SVO76	X					
172.17.20.59	Digiws121		nog niet	X					
172.17.20.7	dlx001	[P] Proxy (Squid)	?	X					
172.17.20.8	WINSRV065	Kantoor Fileserver	SVO100	X					
172.18.20.10	WINSRV130	[P] Applicatieserver (CAP web)	SVO317	X					
172.18.20.11	WINSRV131	[P] SQL database (CAP)	SVO321 SVO322 SVO323	X	X				
172.18.20.244	WINSRV055	RSA Relatie CA	ITSec SVO12	X	X				

172.18.20.245	WINSRV056	RSA Public CA	ITSec SVO13	X	X	X	X		CA logfiles
172.18.20.246	WINSRV057	RSA Ccv CA	SVO3	X	X				
172.18.20.247	WINSRV167	RSA root CA	SVO1	X					
172.18.20.249	WINSRV022	RSA Qualified CA	SVO2	X					
172.18.20.251	WINSRV053	RSA Taxi CA	SVO5	X	X				

11.2 Stolen by perpetrator(s)

Op de CA machines zijn log bestanden en database bestanden aangetroffen. Daaruit blijkt dat er een aantal ongebruikelijke certificaten zijn uitgegeven.

Verder zijn er op de CA machines databases aangetroffen die unieke serienummers bevatten. Een aantal van deze serienummers zijn niet te herleiden.

The attacker(s) could gain access to every system on the network and every file on stored on them. This included:

- Software and licences
- All personal information of clients of DigiNotar including clients to services like the Tax administration (Belastingdienst). For example:
  - Name, e-mail address, telephone number
  - Client certificates, revocation codes
- Company data like contracts and e-mail

12 Aftermath

On the 29-August-2011 Google published a notice that a rogue wildcard certificate for the Google.com domain, which was generated on the 10-July-2011, was being abused to perform SSL man-in-the-middle (MITM) attacks. The MITM-attacks were primarily targeted at users that were located in Iran.

http://pastebin.com/ff7Yg663 (rogue *.google.com cert)
http://googleonlinesecurity.blogspot.com/2011/08/update-on-attempted-man-in-middle.html (google notice)
{X: Wat is de onderzoeksvraag? Ik zie het doel van mijn conclusies niet terug. Er zijn dingen weggelaten en met name zaken scherper gesteld. Waarom?}

12.1 Investigation of OCSP responder logs

The Online Certificate Status Protocol (OCSP) is used to obtain the revocation status of certificates without the need for Certificate Revocation Lists (CRLs). Using this protocol clients can verify the status of certificates with specialized servers called OCSP responders. When an OCSP responder receives a valid request it will respond with the certificate status good, revoked or unknown. If RFC 2560 is implemented to the letter, the status good merely implies that the certificate has not been revoked, but does not necessarily mean that the certificate was issued or that the time of response is within the timeframe during which the certificate is valid.

12.2 Sources/ content

Given the context where rogue certificates were being used in an attack, Fox-IT recommended that the OCSP responder would operate on the basis of a whitelist instead, so that the status unknown would be returned when the validity of an unrecognized certificate was checked. A customized sensor from Fox-IT was subsequently placed in front of the DigiNotar firewall that logs all PCAP and flow data, which also included Snort in combination with a custom policy and a custom sniffing service for logging OCSP requests. A number of custom scripts were written, in order to check the OCSP logs against all valid certificates, in order to check if OCSP requests persisted for known rogue certificates and to gain insight into the question what domain names were associated with rogue certificates [is dan niet al gegeven door de lijst? Zo niet: waar ligt de toegevoegde waarde t.o.v. de lijst?].

The OCSP database at DigiNotar contained logs of the OCSP requests between 01-May-2011 at 00:00 and 30-August-2011 at 01:56. The OCSP database consisted of 27.102.901 rows and contains the following fields:

Name	Meaning	Value
Id	Keyfield (uniek)	~59M-81M
IP	Internet protocol address	1.9.132.2-223.255.231.29
Status	Result of the validity check	GOOD,REVOKED,UNKNOWN
DateTime	Date and time of the request	~10-May-2011 – 30-August-2011
CA id	Identification of the CA	-,5,7,8,11,12,13,14,15,19,20,22
Serial	Identification of the certificate	~3K hexadecimal numbers that generally have 34 digits.

The OCSP database was subsequently enriched with GeoIP information:

Name	Meaning	Value
ASN	Identification of the peering provider	Numerical value between 0-393238
ASN name	Name of the peering provider	Name of a peering provider
Country code	Code for the country of origin	~200 2-digit country codes
Country name	Name of the country of origin	Name of the country of origin

The OCSP database was additionally enriched with information from SVO 1:

Name	Meaning	Value
Is_Forged	Indication if the cerficiate in question is fake	True, false

Rogue certificates were generated for the following domain names:

Domain names	Rogue certificates	Category
..com	1	**General**
..org	1	**General**
*.10million.org	2	**Unknown**
*.android.com	1	**Telecommunication**
*.aol.com	1	**Telecommunication**
*.azadegi.com	2	**Communication**
*.balatarin.com	3	**Communication**
*.comodo.com	3	**Security**
*.digicert.com	2	**Security**
*.globalsign.com	7	**Security**
*.google.com	26	**Communication**
*.JanamFadayeRahbar.com	1	**Comment**
*.logmein.com	1	**Security**
*.microsoft.com	3	**General**
*.mossad.gov.il	2	**Political**
*.mozilla.org	1	**General**
*.RamzShekaneBozorg.com	1	**Comment**
*.SahebeDonyayeDigital.com	1	**Comment**
*.skype.com	22	**Communication**
*.startssl.com	1	**Security**
*.thawte.com	6	**Security**
*.torproject.org	14	**Security**
*.walla.co.il	2	**Communication**
*.windowsupdate.com	3	**Security**
*.wordpress.com	14	**Communication**
addons.mozilla.org	17	**General**
azadegi.com	16	**Unknown**
Comodo Root CA	20	**Security**
CyberTrust Root CA	20	**Security**
DigiCert Root CA	21	**Security**
Equifax Root CA	40	**Security**
friends.walla.co.il	8	**Communication**
GlobalSign Root CA	20	**Security**
login.live.com	17	**Communication**
login.yahoo.com	19	**Communication**
my.screenname.aol.com	1	**Communication**
secure.logmein.com	17	**Security**
Thawte Root CA	45	**Security**
twitter.com	18	**Communication**
VeriSign Root CA	21	**Security**
wordpress.com	12	**Communication**
www.10million.org	8	**Unknown**
www.balatarin.com	16	**Communication**
www.cia.gov	25	**Security**
www.cybertrust.com	1	**Security**
www.Equifax.com	1	**Security**
www.facebook.com	14	**Communication**
www.globalsign.com	1	**Security**
www.google.com	12	**General**
www.hamdami.com	1	**Political**
www.mossad.gov.il	5	**Political**
www.sis.gov.uk	10	**Security**
www.update.microsoft.com	4	**Security**

12.2.1 Analysis

The list of OCSP requests can provide some insight into the way that rogue certificates were being used for MitM-attacks. Two rogue certificates are notable in this regard:

Yahoo certificate	
Serial	3612f911f611984191fc310e74645d16
CA	Koninklijke Notariele Beroepsorganisatie CA
CN	login.yahoo.com
Validity	10-July-2011 18:22:26 to 27-July-2011 12:01:41
Period of use	10-July-2011 20:12:11 to 29-July-2011 11:52:40
Total usage	8 requests 2 unique IP-addresses 0 status GOOD responses

Six OCSP requests were made for the rogue login.yahoo.com certificate around 20:00 on 10-July-2011 from the IP-address [77.104.076.097] that resulted in the status response 'unknown'. Another OCSP request was made on 11-July-2011 at 00:22 from the IP-address [77.104.076.097] that resulted in the status response 'unknown'. On 29-July-2011 at 11:52 the rogue certificate was verified by the IP-address [10.010.210.029], which resulted in the status response 'revoked'.

Google certificate	
Serial	05e2e6a4cd09ea54d665b075fe22a256
CA	DigiNotar Public CA 2025
CN	*.google.com
Validity	10-July-2011 21:06:30 to 29-August-2011 16:58:47
Period of use	30-July-2011 09:11:47 to 30-August-2011 01:56:05 (= end of log)
Total usage	665.974 requests 301.565 unique IP-addresses 654.313 status GOOD responses (298.140 unique)

A total number of 665.974 OCSP requests were made for the rogue wildcard certificate for the Google.com domain between 30-July-2011 at 09:11 and 29-August-2011 at 19:09 from 301.565 unique IP-addresses. Out of the total number of 665.974 OCSP requests, 654.313 requests from 298.140 unique IP-addresses resulted in the status response 'GOOD' between 30-July-2011 at 19:11 and 29-August-2011 at 19:09. Between 29-August-2011 at 19:09 and 30-August-2011 01:56 a further 11.661 OCSP requests resulted in the status 'revoked'.

A number of more specific findings can be reported in regard to the usage of the rogue wildcard Google certificate:

1) The number of affected IP-addresses grows exponentially between 04-August-2011 and 30-August-2011 (Table **1**).
2) The number of OCSP requests grows from an average 8.890 requests per hour to 10.599 requests per hour during the period in which the rogue wildcard certificate for Google.com was used (corresponding to 5.625 and 6.663 unique IP-addresses per hour respectively).
3) Both the OCSP requests for valid and rogue certificates occur in waves as shown in Table **2**, Table **3** and Table **4**.
4) Peaks in OCSP requests occur at the end of the month:
   a) On 28-July-2011 at 15:50 requests peak at 2.847 requests for valid certificates (Table **3**).
   b) On 29-August-2011 at 17:54 requests peak at 1.053 requests for rogue certificates (Table **2**).
   c) On 29-August-2011 at 20:53 requests peak at 3.492 requests for valid certificates (Table **4**).

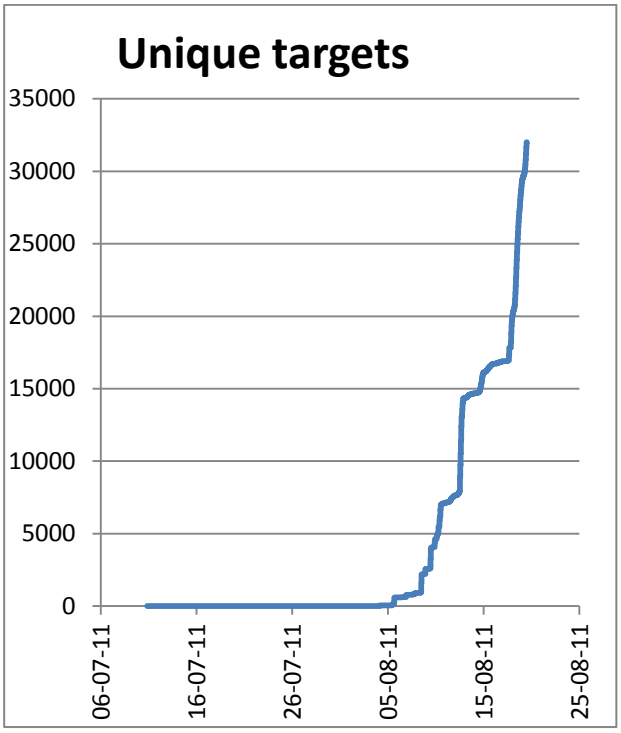


Table 1 Unique targets

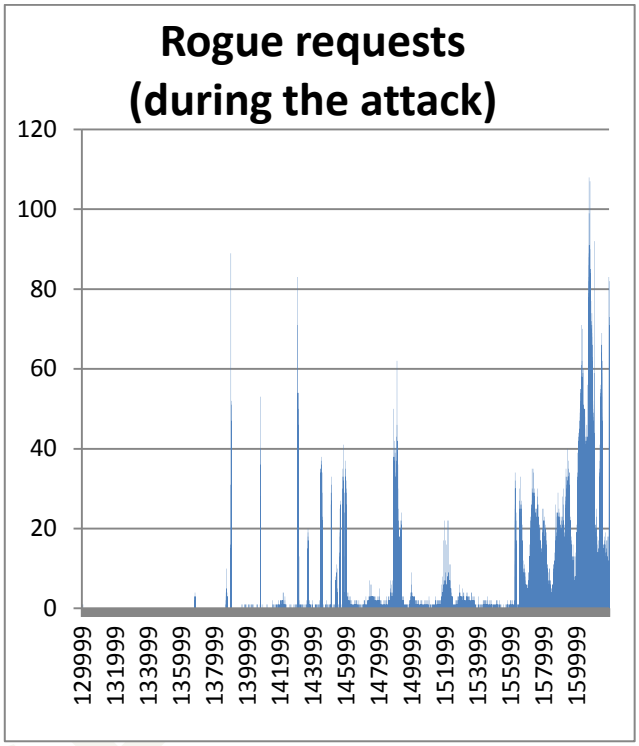


Table 2 Rogue requests (during the MitM-attack)

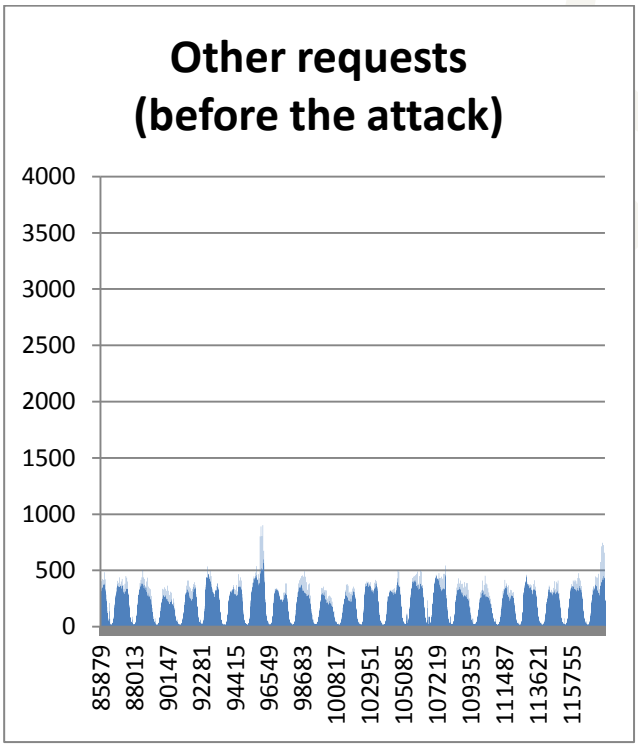


Table 3 Other requests (before the MitM-attack)

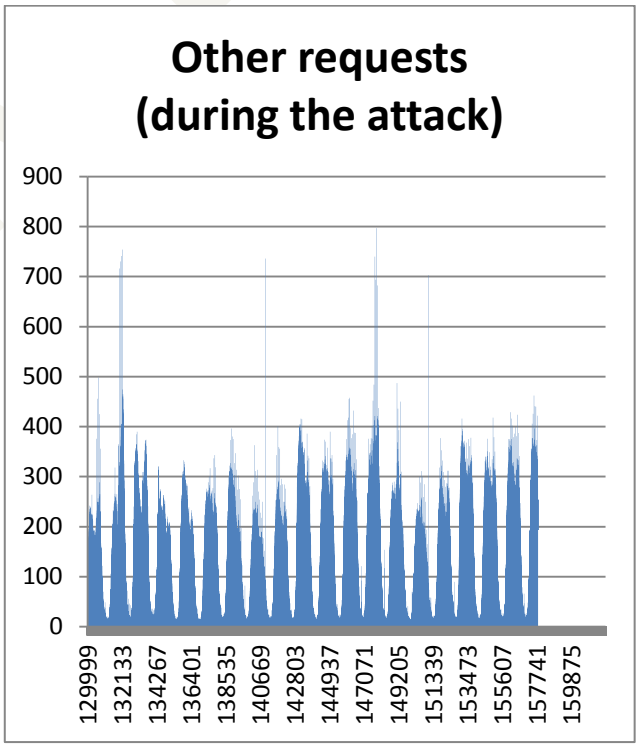


Table 4 Other requests (during the MitM-attack)

5) No regular intervals during which there are no requests for the rogue wildcard certificate for Google.com ('silence' or 'blackout') were observed. As the number of requests for the rogue wildcard certificate increases, the number of blackouts decreases.
   a) Seemingly irregular intervals of more than 15 minutes can be distinguished during which less than 5 OCSP requests per minute occur.
   b) There are no intervals of more than 10 minutes during which 0 requests per minute occur after 19-August-2011.
6) 95% of the OCSP requests for the rogue wildcard certificate for Google.com originate in Iran (634.665 out of 665.974 OCSP requests).
7) The status of different certificates is validated by users from Iran before and during the MitM-attack (29 unique certificates before the attack, 28 unique certificates during the attack and a total of 44 unique certificates).
8) 60% of the OCSP requests for rogue certificates and the majority of the requests from unique IP-addresses originate from 4 Iranian ISPs (**Figure 7** & Figure **10**).
9) Iranian ASNs from which OCSP requests were received before the MitM-attack are not excluded from the attack (**Figure 10**).
10) While a small number of ASNs are responsible for the majority of all OCSP requests, a broad spread of OCSP requests can be identified over the remaining Iranian ASNs (**Figure 11**).
11) Before 10-July-2011 928 OCSP requests for valid DigiNotar certificates from Iran occur. In total 1.780 OCSP requests from Iran occur for valid DigiNotar certificates between 01-May-2011 and 30-August-2011.
12) The amount of certificates issued by DigiNotar for which OCSP requests occur is weakly correlated with the number of requesters (**Figure 12** and **Figure 13**).

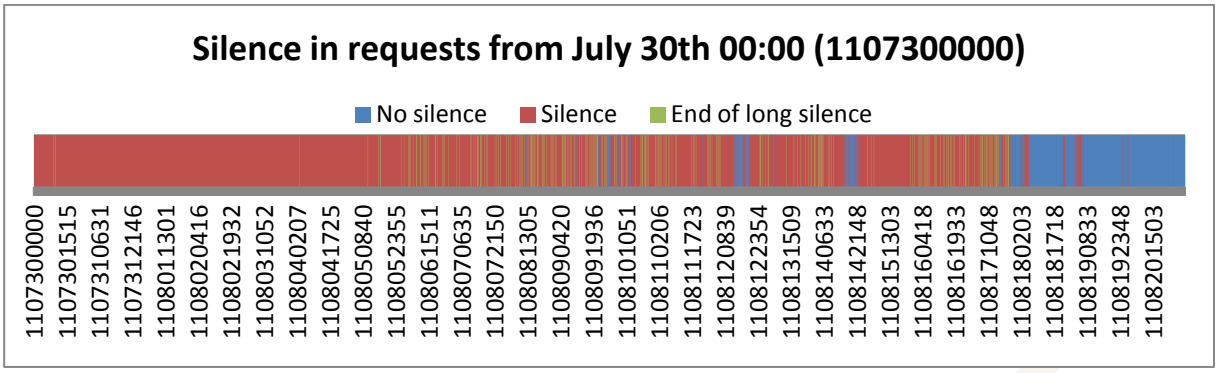


Table 5 Silence in requests for rogue certificates

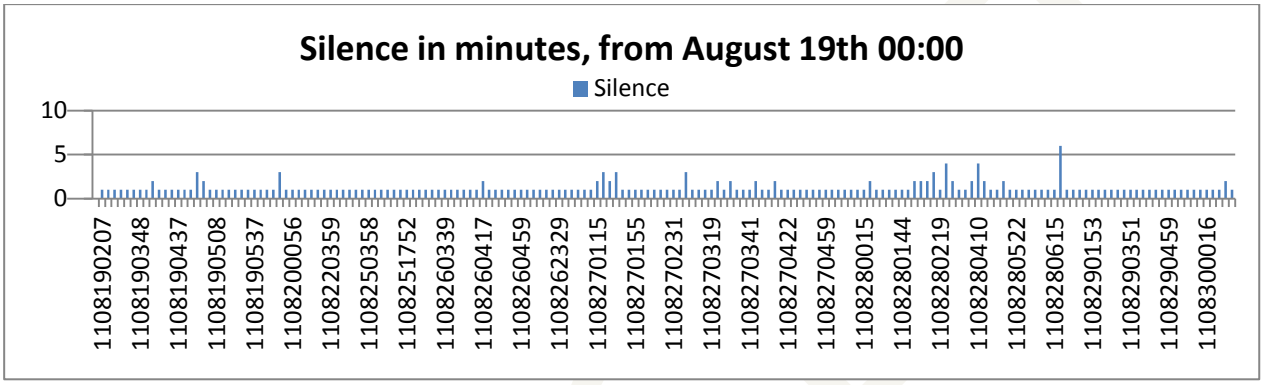


Table 6 Silence in requests for rogue certificates (zoom 1x)

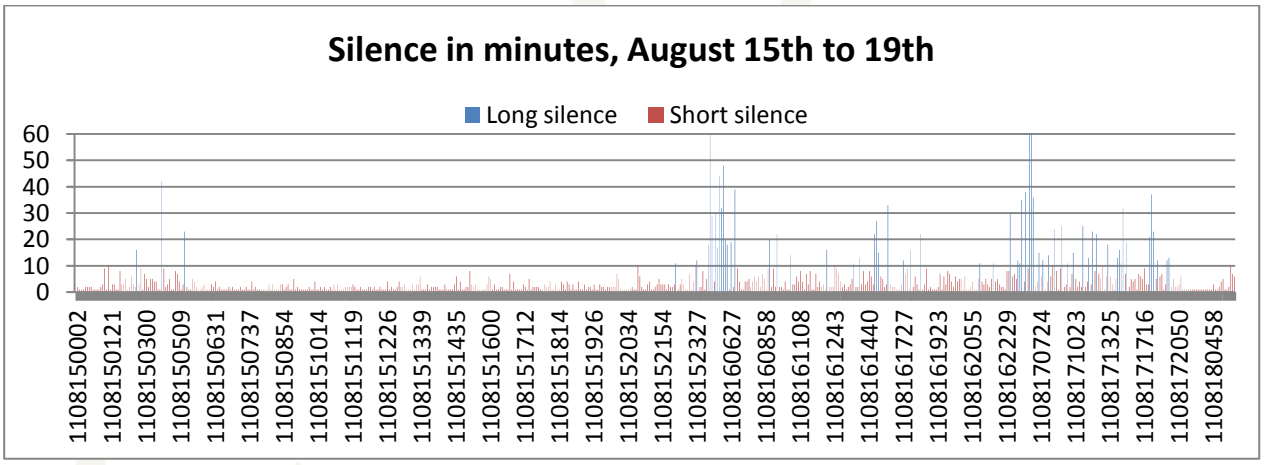


Table 7 Silence in requests for rogue certificates (zoom 2x)

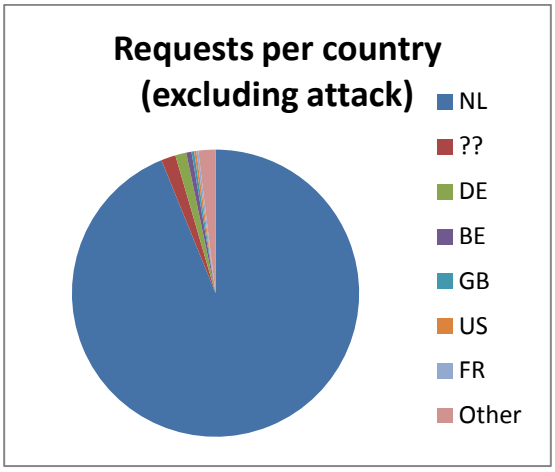


Figure 1 Requests per country

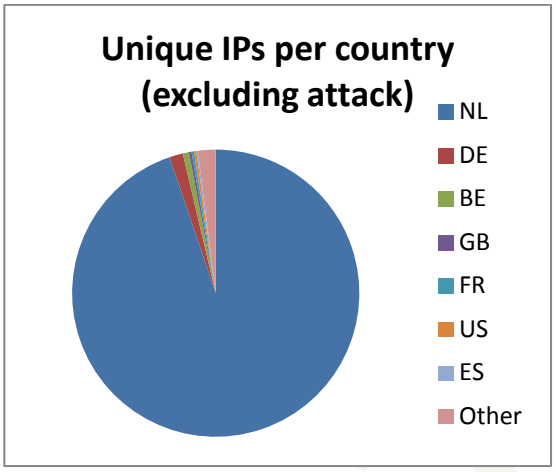


Figure 2 Unique IPs per country

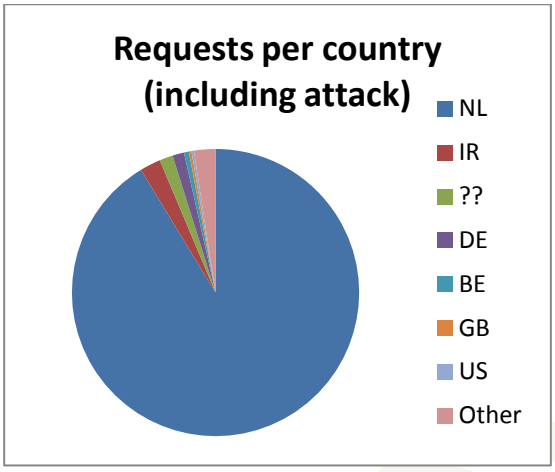


Figure 3 Requests per country

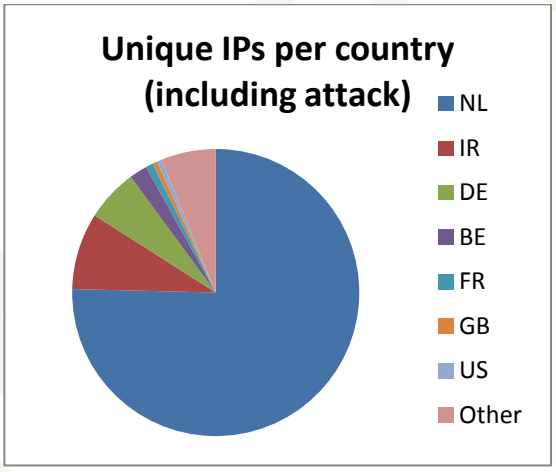


Figure 4 Unique IPs per country

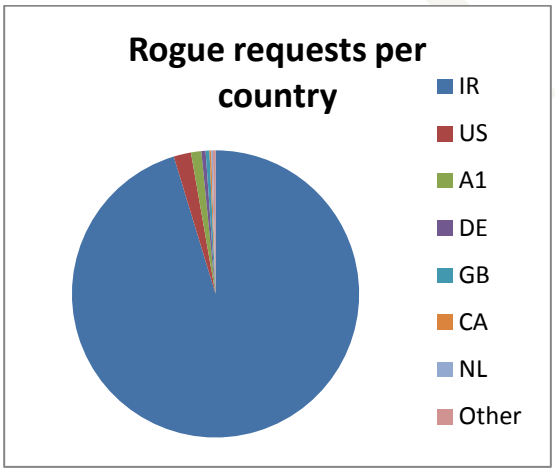


Figure 5 Rogue requests per country

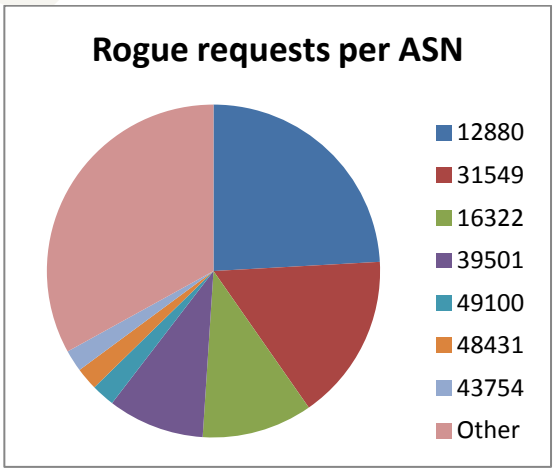


Figure 6 Rogue requests per ASN

	bt_asn	bt_value	bt_rogue_count
▶	12880	Information Technology Company (ITC)	160633
	31549	Aria Rasana Tadbir	107761
	16322	PARSONLINE Autonomous System	71520
	39501	Neda Gostar Saba Data Transfer Company Private Joint	62492
	49100	Pishgaman Tose Ertebatat	15110
	48431	Bozorg Net-e Aria	14562
	43754	AsiaTech Inc.	13998

Figure 7 Rogue requests per ASN top 7

	bt_asn	bt_value	bt_ip_ucount
▶	12880	Information Technology Company (ITC)	64251
	31549	Aria Rasana Tadbir	63589
	16322	PARSONLINE Autonomous System	37784
	39501	Neda Gostar Saba Data Transfer Company Private Joint	31624
	43754	AsiaTech Inc.	7431
	49100	Pishgaman Tose Ertebatat	7203
	48431	Bozorg Net-e Aria	6802

Figure 8 Unique requests per Iranian ASN top 7

	bt_asn	bt_value	bt_serial_ucount
▶	12880	Information Technology Company (ITC)	17
	51852	Private Layer INC	17
	31549	Aria Rasana Tadbir	15
	42337	Respina Networks & Beyond PJSC	13
	44244	Iran Cell Service and Communication Company	12
	28753	Leaseweb Germany GmbH (previously netdirekt e. K.)	11
	39501	Neda Gostar Saba Data Transfer Company Private Joint	9

Figure 9 Certificate usage per Iranian ASN top 7

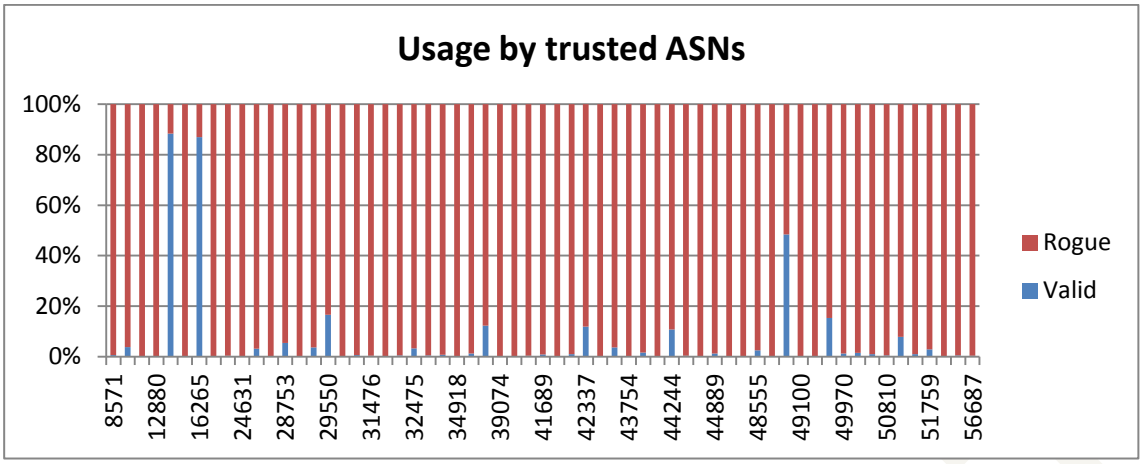


Figure 10 Iranian ASNs with requests before the attack (61)

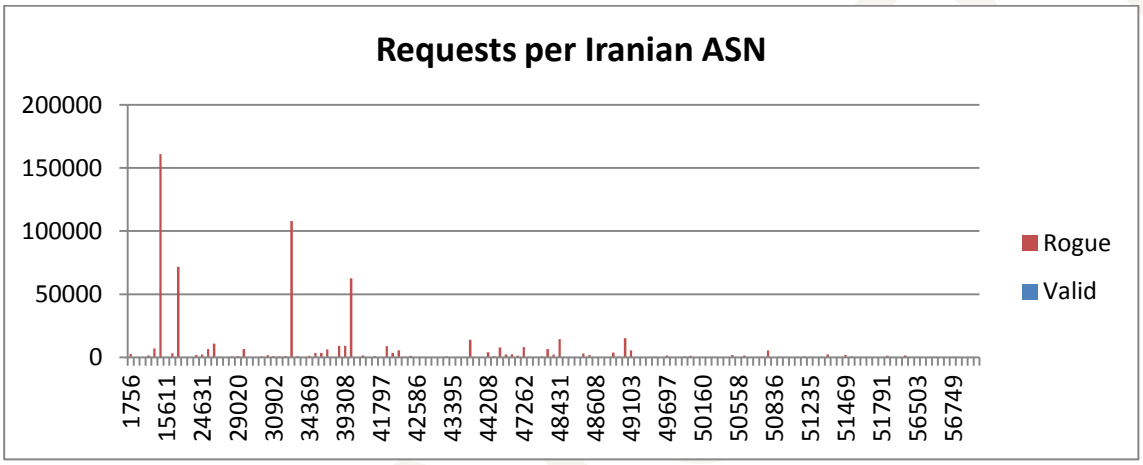


Figure 11 Requests per Iranian ASN (143)

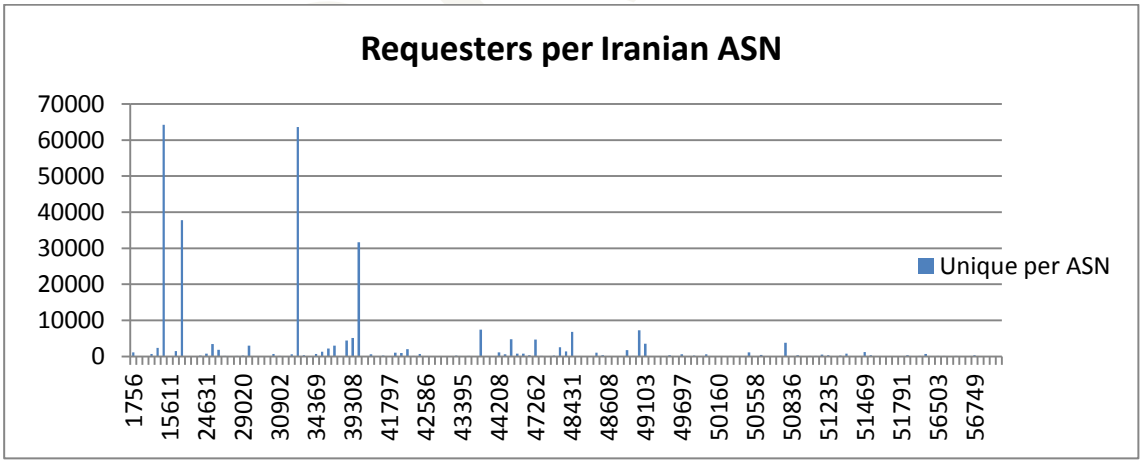


Figure 12 Requesters (unique IP-addresses performing OCSPS requests) per Iranian ASN

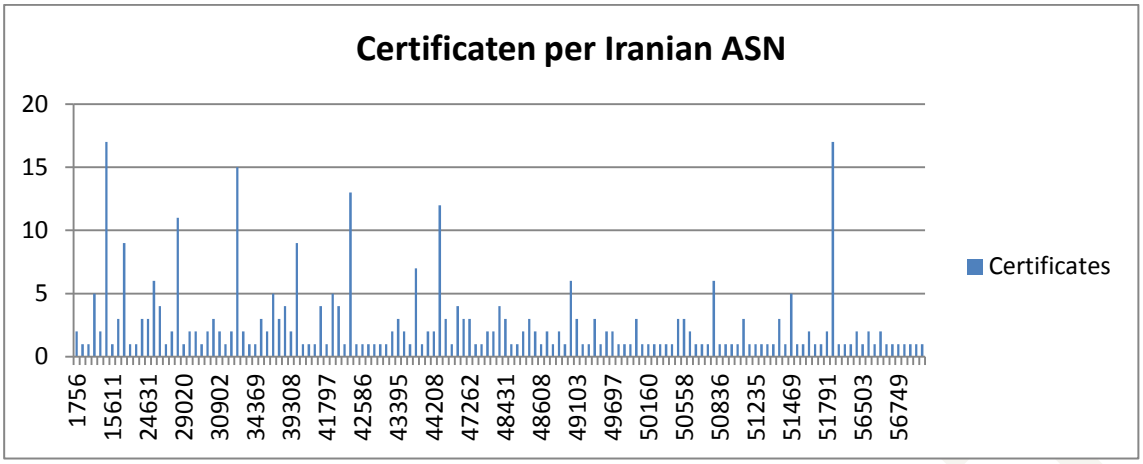


Figure 13 Certificate usage per Iranian ASN

12.2.2 Conclusion

The greatest common divisor in the MitM-attack is that a diverse group of primarily Iranian users were targeted using one rogue wildcard certificate for the Google.com domain. This conclusion is supported by the fact that the overwhelming majority of users (95%) are located in Iran based on the GeoIP information for the corresponding IP-addresses. The attack gained momentum exponentially after 04-August-2011 and had a very broad reach which affected 143 Iranian ASNs and approximately 300 hundred thousand unique IP-addresses. The number of unique IP-addresses is a conservative approximation for the amount of users that were affected, as a number of ASNs masquerade multiple users behind one unique IP-address.

The type of websites for which rogue certificates were generated consists mostly of security-related certificates (such as root CA-certificates) as well as certificates for websites used for communication. Taken together these two categories represent two-thirds of the total number of rogue certificates.

The OCSP requests occur in waves (Table **3** and Table **4**) with a peak at the end of the month (Table **2**). No regular 'blackouts' were observed. Regular blackouts would be expected if the MitM-attack relied on the repetition of botnet-instructions to perform cache-poisening (Table **6** and Table **7**). The broad spread of OCSP requests for rogue certificates from the various Iranian ASNs can be explained in terms of either the attacker(s)'s inability to narrow the scope of the systems that were targeted during the attack or the desire to target the maximum amount of systems.

The findings are consistent with a tree-like infrastructure and imply that a major peering point was consistently rerouted in order to perpetrate a large-scale MitM-attack. This could support the conclusion that in order to perform such a large-scale MitM-attack on a major peering point for an extensive period without regular blackouts the attackers must have operated from a privileged position within the Iranian infrastructure.

12.3 Academic/ closet

DNS cache poisoning?
Private keys?

13 Perpetrator(s)

{? Opnemen of niet?}
Pastebins
Xuda script

The history of the OCSP requests show that the fraudulent *.google.com certificate was massively used between {xxx} and {yyy}. However prior to these requests 3 requests have been done originating from AttIP7 {ref} on 2011-07-30 between 09:11:47 and 09:51:19. This was probably a test run.

14 Lessons learned

{what have we learned from this incident?}
{Tot op zekere hoogte deden hun best. Uitgangspunt onderzoek en rapport is helpen!}

{je kunt natuurlijk nooit een volledig veilge system maken...}

{Informatie over basis beveilging, security management system}

An unusual modus operandi was used in the attack on DigiNotar. The attacker(s) appear(s) to have had the intention to abuse the private key of a trusted CA in order to spy on a large number of Iranian users using rogue certificates. The attack resulted in an erosion of public trust in the existing Public Key Infrastructure and the role of Trusted Third Parties therein, which is central to their operation, whether this was intended or not. If the ensuing erosion of trust in PKI was indeed intended, the threat could be compared to terrorism, where the goal is to induce fear in the general public. This modus operandi is unusual when compared to what's more generally encountered, that is that of a criminal organization, where the aim is to make money and attacks are performed covertly.

The threat of cyber terrorism is typically left unaddressed in security a risk assessments that are performed when for instance CAs are audited. The assessment that the threat of cyber terrorism is merely hypothetical for all but the most critical targets is rapidly being overtaken by the reality that a much broader scope of targets face this threat. Given the impact that a breach in the security of one CA has on PKI as a whole and the Internet in general, ensuring the security of every CA is paramount to the trust in PKI and its role in providing security for a diverse range of activities on the Internet. While the approach to protecting potential targets from this type of attack does not differ significantly from other threats, the range of scenarios that need to be taken into account is rapidly expanding.

{That these attacks can, have and will happen gives new insight to you and your customers security.}

14.1 Trusted third parties

{Trust is the most important business asset of TTP and needs to be protected.
TTP might consider asking help from national security agencies.}

14.2 Intermediate users

{Bedrijven, overheden e.d.}

14.3 End users

Average users will have very limited capabilities to protect themselves properly against attacks such as those against Trusted Third Parties in the Public Key Infrastructure. The MitM-attack on users that was perpetrated in the aftermath of the hack of DigiNotar was only detected by Google when users of the Google Chrome browser reported abnormal behaviour when using Google services for which a rogue Google wildcard certificate had been issued. Because of the limited ability for users to protect themselves from attacks that abuse PKI, they need to be able to trust the security of all parties that make up the PKI in order for the system as a whole to operate.

More generally users and businesses can protect themselves against a wide range of security threats. The first step to a more secure environment is normally to obtain an overview of all machines that operate within a given network and the (business) processes and procedures that are applicable. While this may sound like an insurmountable task within large organizations, a small group of specialists within these organizations can combine their expertise to produce an overview of the attack surface. Specialists that commonly possess this type of knowledge are system and network administrators, application managers, security officers and business representatives.

Once an overview of the attack surface has been obtained [...]

The next thing to do is think of as many scenarios as possible the adversary can do to achieve his goal. Think like the attacker. And since you have a lot of inside knowledge, the attacker probably has not, it would not be hard to come up with effective scenario's.

Because you can limit yourself to one type of adversary or threat at the time you can eliminate a lot of scenario's. For example a terrorist from Iran will probably not use someone from inside your organisation. This eliminates your staff from wilfully harm your company (for this threat agent that is...). However mistakes or deceit of your staff is something you should take into account. On the other hand, if you consider the chance that someone of your staff will be bribed by a terrorist you should take that into account (like segregation of duties and authorities, internal monitoring and audit).

Next, this group of people must estimate the chance the scenario's can or will take place. What must the adversary do to run through the scenario? Don't discount the unknown event (the black swan) and your lack of technical knowledge. You don't have to know exact how to hack a server but you must acknowledge that it is possible. Therefore your scenario's must include partially successful scenario's. Do not only create scenario's visualising the attacker being outside trying to get in. Also include scenario's like "if the attacker owns this server, how easy is it then to proceed", and "if the attacker could slip through this procedure (for ex. vetting) what additional barriers have we in place?", and most useful "what can an attacker do when he has a particular username/ password or token?'.

Next step is to come up with solutions. This will require some (security) technical knowledge.}

{Meldplicht datalekken?}

15 Potential follow-up investigation

The investigation that was performed by Fox-IT focussed on the questions [...], [...] and [...]. The information that was uncovered during this investigation can be used as the basis for further research in regard to several additional questions.

General questions:

- What security measures were in place before and during the attack?
  - How was the firewall configured?
  - How was the segmentation set up? (network/domain) [er staat iets over segmentation die werd afgedwongen door de firewall in het rapport?]
  - What was the strength of the passwords that were used?
  - To what extent had patches been applied to systems in the network?
  - Were anti-malware and anti-virus measures in place? [NB: volgens Daniel was er anti-virus aanwezig]
  - Were Intrusion Detection and/or Prevention Systeem (IDS/ IPS) used? [in de tekst staat dat er een IPS voor de firewall stond]
  - Which special/specific security measures were in place?
- What measures were taken in response to the attack?

Chapter 3.5 Network:

- The described normal operation of the network segments and firewall is based on interviews with the administrators. The exact firewall rules have not been examined to confirm this.
- It is not investigated what private keys were stored in the netHSM in the co-location and how the synchronisation between the netHSMs took place.
- The CA servers, HSM, firewall and other equipment in the co-location is not investigated.
- The exact layer-2 network layout.

Chapter 5 - Investigation of CA :

- It could be investigated whether the attacker(s) used the option in the CA software to perform a complete backup of [...].
- It could be investigated whether the `RSACM-v6.7CustomizableSerialNumbers-WIN32` extension provides functionality which could have aided the attacker(s) in issuing rogue certificates.
- [{zie reference: RSA Keon Ready Implementation Guide For PKI 3rd Party Applications}. About "Unattended Startup". No investigations have been done if this was done and/or attempts were made by the perpetrator(s) to change these settings]
- The CA web servers log (`enrol-cipher.log`) of the Public-CA server contain interesting outside office hours entries.
- Investigation is needed on the log files of CCV-CA, Nova-CA, QC-CA, Root-CA and Taxi-CA.

Chapter 5.1.1 - Sources/ content:

- The RSA software could be scrutinized to determine if it can detect if log files have been removed from a system.
- It could be investigated if the CA servers contain remains of deleted log files.

Chapter 5.2.1 – Certificates:

- Further investigation could be performed to explain the appearance of the duplicate certificates that were found in the database files. This might provide an answer to the question if certificates with identical fingerprint could be issued or have been issued by the attacker.

Chapter 5.2.2 - Private keys:

- The private key `id2entry.dbh` database entries could be linked to the specific netHSMs. This could answer the question which CA server users which netHSM.
- All public keys corresponding with the private keys entries in the `id2entry.dbh` could be matched with the certificates extracted from the databases. This answers the question what CA server had access to what CA private key.

Chapter 12.2.2 – Conclusion:

- The OCSP data could be used to examine the limited set of IPs outside of Iran that were targeted in the MitM-attack in regard to determine if they can all be identified as TOR-exit nodes and VPN providers.
- If additional data from Google could be obtained it would be possible to determine if login data that could have been obtained during the MitM-attack was abused in practice.
- Data regarding OCSP requests for valid certificates from other CAs could be used to determine if round robin was used and thus capabilities of the attackers and the infrastructure that was used.
- Zooming in on the targets and the underlying infrastructure in Iran could reveal information about the identity and aim of the MitM-attacker(s).
- {er is al contact geweest met google met verzoek om info...}

Er is geen onderzoek gedaan om expliciet aan te tonen welke zwakheden zijn misbruikt in de webservers DotNetNuke. Om dat te doen moet extra onderzoek worden verricht:

- welke versie draaide (exe's onderzoeken)
- welke kwetsbaarheden had deze versie
- Zoek naar sporen in de log of deze kwetsbaarheden zijn misbruikt.

The system event logs (applications logs) of most of the servers were exported and retained. This was done in august 2011. These logs have not been examined.

Chapter 6 Investigation of firewall logs:
- The integrity of the firewall logs is not investigated.

Er is niet volledig onderzocht of er resten van verwijderde bestanden aanwezig zijn op de CA servers; niet naar deleted files gekeken en niet naar resten van log entries in slack of andere disk space (zgn. d.m.v. carven).

Back-up tapes

PABX logs

CRL requests.

Netflow
→ niets mee gedaan.

Onderzoek TODO:
private key velden controleren asn.1 of ref allemaal naar hsm verwijzen.

Syslogserver????? (10.10.210.35 dlx131 [T] Syslog server)

externe IP's, en naar welke interne (DMZ) IP's werwijzen ze?

Onderzoekenswaardig:
- hoe connect ie naar de db?
- Had ie al sa credentials?
- Is mssqlusr de user waaronder de sql service draaide?
- Welke rechten had deze user in windows (local admin?)?

e-mail logs
Hebben we logs van deze Exchange server?

Nee niet direct logs.

Ben lang bezig geweest om de tapes te krijgen zodat we daar iets mee konden, want vanaf de 1e dag dat ik er was wist ik al, dat zga alle segmenten zonder enige vorm van checks op een reguliere manier mail naar buiten kunnen sturen. Dat zit in het hele proces en de opbouw van de omgeving. Alles gaat via een exchange server, en voor sommige systemen dacht ik via een smtp connector die er nog tussenhangt (of hing)

Smtp logging staat niet aan op de exchange server, Net als andere logging is er veel afwezig.

Message tracking van berichten uit die tijd is er niet, of lukte niet, omdat het mail is die niet in de EDB database terecht gekomen is, maar direct naar buiten gepusht is.

Heel misschien nog korte duur info uit de backups van die systemen.... (als we ooit die tapes krijgen)

➔ toch is er misschien nog wel kans dat er wat boeiends in de error logs staat. Die zijn er meestal wel. Kan me voorstellen dat je als hacker wel een paar errors op de mailserver triggert als je aan het proberen bent je zipje naar buiten te sturen.

A netHSM was present in the internal DMZ hosting the keys for the service 'Parelsnoer' provided by DigiNotar. The servers used for this Parelsnoer service were not investigated. Therefore we have no indication if the keys in this netHSM were misused by an attacker or even if the servers were compromised. A quick scan has been done on the firewall log to check if any of the servers involved in the Parelsnoer process had any connection to the known IP addresses {ref naar chapter: TODO nog te maken}. Also the CA server running the CA management software winvm012 was quickly assessed for traces {ref. toevoegen. TODO nog uitwerken}.

15.1 Nog uitgevoerd onderzoek

Connectives naar de hsm's:

```
grep "10\.10\.200\.254" all_log > ../../tijdelijk/10.10.200.254_all_logs
grep "172\.18\.20\.254" all_log > ../../tijdelijk/172.18.20.254_all_logs
grep "10\.10\.240\.254" all_log > ../../tijdelijk/10.10.240.254_all_logs
```

10.10.200.254_all_logs
Als we de icmp eruit halen worden er maar een paar connecties gedaan. Opvallen zijn de connecties vanaf op 4 juli de hsm naar andere systemen. Port scan? Geownde hsm?
Port 9004 is normaal?

Further investigations on these servers can give a more definite answer if these were misused.

16 References

RSA Keon Ready Implementation Guide For PKI 3rd Party Applications,
http://www.rsa.com/rsasecured/guides/keonca_pdfs/nCipher_netHSM_KCA651.pdf

incident logbook

Appendix I {references to equipment}

{lijst van list van SVOs waarnaar wordt gerefereerd in het rapport}

Name[18]	Server Id[19]	SVO number(s)	IP address(es)	Network segment	Remarks
CA servers					
Root-CA	WINSRV167	SVO1	172.18.20.247	secure-net	
Qualified-CA	WINSRV022	SVO2	172.18.20.249	secure-net	
CCV-CA	WINSRV057	SVO3	172.18.20.246	secure-net	
Nova-CA	WINSRV021	SVO4	172.18.20.252	secure-net	Also called 'Orde-CA'.
Taxi-CA	WINSRV053	SVO5	172.18.20.251	secure-net	
Test-CA	WINSRV054	SVO7	172.18.20.250	secure-net	
Relatie-CA	WINSRV055	SVO12 DD.055	172.18.20.244	secure-net	
Public-CA	WINSRV056	SVO13 DD.056	172.18.20.245	secure-net	
DNTest-CA	WINVM012	SVO149	10.10.240.39	test-net	
DNAcceptance-CA	winvm032	SVO114	10.10.230.39	acceptance-net	
Public-CA-Colo	winsvruw07		172.27.20.19	secure-colo-net	
QC-CA-Colo	winsvruw08		172.27.20.20	secure-colo-net	
Relatie-CA-Colo	winsvruw09		172.27.20.17	secure-colo-net	
Root-CA-Colo	winsvruw10		172.27.20.15	secure-colo-net	
Nova-CA-Colo	winsvruw11		172.27.20.16	secure-colo-net	Also called 'Orde-CA'.
CCV-CA-Colo	winsvruw18		172.27.20.23	secure-colo-net	
Taxi-CA-Colo	winsvruw19		172.27.20.26	secure-colo-net	
netHSMs					
netHSM-CAs	dnhsm01		172.18.20.254	secure-net	
netHSM-web	dnhsm02		10.10.200.254	DMZ-int-net	
netHSM-test	dnhsm04		10.10.240.254	test-net	Also called "Stichting continuïteit hsm"
netHSM-CAs-Colo	dnhsmuw01		172.27.20.254	secure-colo-net	

WINSRV007 (Bapi Database New; 172.17.20.4)
WINSRV155 (eHerkenning-AD; 10.10.20.134)
WINSRV108 (Website auth.pass.nl; 10.10.20.16)
WINSRV003 (CI - Source build server; 172.17.20.25)
WINSRV155 (eHerkenning-AD; 10.10.20.134)

[18] Server name as it is used in this report.
[19] Server Id as it is used by DigiNotar

Appendix Complete list of equipment (Confidential?)

{complete lijst van SVO’s

Appendix II {terminology}

Term	Meaning
ASN	Autonomous System Number Identification of a registered network operator, usually an ISP.
ASN.1	
CA	Certificate Authority, an issuer of certificates.
Certificate	A digital file used amongst others to authenticate a website and to encrypt networktraffic. The validity of a certificate is generally verified with the issuer (CA)
CSR	
CSP	
Darpi	
ISP	Internet Service Provider.
MiTM	Man-in-the-Middle. In this type of attack an attacker places himself between two partiesin order to spy on the traffic between them
PIN mailer	
OCSP	Online Cretificate Status Protocol, a protocol that is used to obtain the revocation statusof certificates as described in RFC2560.
(net)HSM	(Over the network accessible) hardware security module
PKI	
SVO	

CAP (Control Application), DARPI (DigiNotar Abonnementen Registratie Production Interface) and BAPI (Belastingdienst Advanced Program Integration).

Appendix III References and tools used

python
Microsoft Excel
FTK imager
ASN1.Editor (www.lipingshare.com/Asn1Editor)
RapidMiner
OpenSSL

Appendix IV Unknown serial numbers

Root-CA server

On the 'Root-CA' server the following serial numbers were encountered:

```
83120A023016C9E1A59CC7D146619617
68E32B2FE117DFE89C905B1CCBE22AB7
711CE18C0423218425510EF51513B7B8
B7ABEFC8A1F844207B774C782E5385B3
6E0088D11C7E4E98CC9E0694D32A0F6B
80C990D339F177CA9FDAC258105882AB
7F73EC0A14C4BA065BECFAD69DC5A61D
```

Qualified-CA server

On the 'Qualified-CA' server the following serial numbers were encountered:

```
C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4
```

Taxi-CA

On the 'Taxi-CA' server the following serial numbers were encountered:

```
25B6CA311C52F0E4F72A1BD53774B5B3
A0CF459D0D1EA9A946861A0A02783D88
71A10FA4C491D3A72D18D33E3CCF576C
FE456B099700A6C428A193FE5968C9FD
E7E2B46B8C9AA64679E03841F88CA5A0
AEC9F2324D80020B6E2B2A1103D6A4E8
CB20C25F14583AFC86465F14E621FBC1
947FF1DB66A41D809A9BC7E7344E342A
90BCA541B4DF5E77FB1349684F84A930
AB4967CE8B94FCF8DA7691922E6FD59C
BA479991C9103C005726FAB83088A8D6
363E9AAF4DAC7085F31B89B2AC49059A
8A63042B8A8FA256035773BC9417435A
963CCB2601B15C73DCA821F4BC4C7458
6B7057D5DE0170842C372821D3F17DB2
C391438C15FF31BD89544A7F68DDF3B3
7278CB2A8270A3E66A021A7CD75F1211
F401D4C50FCA9161A70ED9D91D40E684
6C396359C423417E20C54CFC6690F3FF
9916C8350225BB607857375A02B6DC72
0F48A14121370B5CF4828EF826749FBC
DB43E2CE6110750785FCBBE9A8EAE061
C641E4B7F19B63C4FF1EA6D3833FC874
D8B771F90BC01C9ED1333C23EF24CFC1
```

'Public-CA server

On the 'Public-CA' server the following serial numbers were encountered:

```
79C03FE0C81A3022DBF8143B27E40223
FCCF53CB3D0A71494AF9664690FFCF84
82BC18B1AA5D59C61D0EFDBEA7664C08
5D4352671C39616670B2F34C173A1F63
6FA3C48173B3B289943F113A8CD9DB8C
CFAF9BE4E5BD0F5A75F628E45E0178C9
4ADA28D281D3D14D19FB782D64086D0C
0B41ABEE6F4168D3CDE5A7D223B58BC1
13548FC160BC5C9F315AE28CDB490E36
5D8D0D436112759826A5490E7F87BD7
C880AE4D7927E6A8FA7D456CB03E9763
82072FC8F8DD7E6C0ECE9B47185F0521
90DB656E2734476CC836778255582FA8B
171A8599EDE711A3315BC7D694CEBEC6
E9EB8075F7FE3683B431552C2D962CB0
E6F9E095464F64448840A832FB3443DB
C83D16E9CB29DCF35F3B351CB942FE0D
39B5DD0ECC85C3F62A72391DC055F561
DF3FD6AFBBFBC30C9AD80BF764A102DB
327B9A443C49018D7B0A97B6EC2254B8
8B0EABAF922D4C6E6917FCBE365DD64A
4FC2D72D6427CABBE3E859453865F43B
53B53BF2F74997EBEB2577D63DA692B7
ABB21F43553F2695031A1C85355D7F1C
5563605FDC2DC865E2A1C32995B5A086
5DD6A72747D90C018B63F959DFE7C976
CAB736FFE7DCB2C47ED2FF88842888E7
9C79C9FE16727BAC407B4AA21B153A54
2D711C9CB79EC15445747BFE3F8BC92F
752A2D0325A3D34D9F5198C2F5C92A6C
BC01852405D3F4E22C48600266655026
9F7DDFE3CAAD224EC6BD68B60DE78550
A67C22A6E1F9D87799548EBFC7D5527E
11661878CCE9DC337CEEBB16E30F9A3A
6BF3BEB26AFF31116200B14F4378C33B
7A61A7778842E502E2291166C4574485
82C42F0EDC18BD751727BE5C54413EF7
03124C25849D9E49BC2A2FAD3E10C8A4
EFF0DD4B4927DF64232C5D2FF280C1E4
9EDCB5E1FE1255A2F1D7FC52C4AFA3B1
3A32AAA9DFE2CA7F9E003885E316944B
4455B43B9173CBAE4E247272EE2573D5
B95F62E86194734C9F68D4BF8B200C49
FE873B742B230B22AE540E840490A2F4
8779917563EC38B7746B8ECAFE239BE6
72CBC4824C6215B139FDE6BA10DAC6AD
8D09D4B98DE67C9E9C7C18CB72AD2418
07BC72A463D4DE33B2BE733D6FAC991D
D3E2205C3B899FC99D77FE802985283F
A5029D6A057D50D20ECFE0E528EDA067
C8B2487ADFAF969E34306029AC934406
5F3C1BDC7A2BCD47ABAF0C8E62D9F757
601315BB085FECF29538DA3F9B7BA1CE
30170F15A240446E6B482E0A364E3CCA
0590B310AEFC7A3EDC03ECA2A6F6624F
FDEB145AAC81B8CD29B8DA018E71456F
C3F9F45F19E334C8303F44288856D843
028CF7556F8BE27026800448FA6AA527
E93B28B47C34B243EBA62E58FE2FF46F
F89F5DE575755A3B4C0DECC6EDA7C804
E3E120935934CBD77E1DA7F00431F745
0A6DFACFDEAE74A816031534BE90B75A
9AD82BE2FED538B10BDFBD229A8A5AEA
C0F216CA8197AD00F0D98927EAE29E64
DE76B17BFB1B6D6D6634C8C104A6E59F
A90F1BB43E9DB5EDFC60C15FB897C593
8625B32398C2722D96E7B972580A0238
D1FDE3A78C9D2E80C2303CC4E3E92A4C
B355E909FD55C5E9EF1A6E67E9C18203
ADB59A303C6260DBE466F0149AB11A4A
5CEBD524469A075FB6B42D06C9BF27AD
0E0886EEAA119CF14F1C54387060929A
B4F9299F05A327E60543C4CDE3277FC0
E4B2F09505726306314DF05B734FD9D0
4DD0497CBAABBA058574A611B26151BA
7073C6C01DEE4E158F554555F697F7D9
EB72415ECD0B4AACBDEEA3734F4349BF
BED90D98FA3A1E0A5BD78AD54E55774D
3CDCD81930F91AC0B990664931E5412E
763B0C2A7B83066A9D995C8C4FD9E35E
720DF591261D710ADC73127C1BC4303D
C06C12DBBC7055FE40950803238EC104
62BF5A170CC779ADE7EF0090F395D5E6
61BF9A0FF2CE9D55D86BC063839F72F4
B5D7A148CA6C1F9693A2C16ACDD66226
35FBDCDF923F99B5E1C5FF4423B715B8
F1EBE73557546DC8B21E0A2DE5E3A33E
EBE7561CA573DA5DBB8EFAA250A40FD3
6BACB6C5B74FA747A3CF375EC3095035
6C1950AA83F4663F1BA063B5275C25EC
```

```
39936336286F843756FC4BC296D7A8E0  5D8F8D78B0C19EF4479F744DECBD84BC  56EF1EE54D65EF7B39AF541E95BB45A9
4A6D90618A5CA6797C768C03C860C4F8  EAACDC2F46D4A86F39B035B793F4A94F  2B1EA767EC59E46364BC2DF9B1F30B97
0954E1AB9141ED7E8B640FE681046451  9D06313F21A4EDF734C324FFBCB9E2B5  3913B1E1C35BDDF02CE03C916E8AA638
8259C3E1DB6C2C9B7FCD6A305EADEFE4  35C54E845AE855F818504C8C189F52C7  AFA2F7E964280B36DB0D714B86256F54

022E35B1ACD40F040C444DF32A7B8DE6  D0BA58BA609CC1A001F612987A822BEF  9A3A951BE27E0729726FD8B80060E7E1
170370B60D515F164119BE54FD55E1ED  6B339433956F1505104BB231314A153E  6410577C738133297472F6C22C2BB397
CBFE437C9B62805C4353516699E44649  C1366C7246041A3089E1C244C5DC42E7  C8C06B0C6B7FE7CA66BCFE617AB6C4E6
5FFA79AB76CE359089A2F729A1D44B31  61D11B35765ECB85890D5349786D9FCA  58C18B290620E18B8C78AC1912E5DCD7
5298BCBD11B3952E3FDDC6FDD6711F5C  44C287C1C3697367B0E6CB78A78C1DF5  2F5ABFDCCAB1A2927E54283296F19FB8
1836289F75F74A0BA5E769561DE3E7CD  DAACF72BC91FB6DA90A804933CB72E23  A07CB7881E35C91FD9C5D20F6102572C
DEB427AC9F1E8A0D0237049C80DF7E7F  2ACBA14BB6F65F7BD0A485BFCB6D023F  05E2E6A4CD09EA54D665B075FE22A256
FD8FE350325318C893AFE03F9DFC7096  84BE5D762F37E9018D623C8E91F4D924  8BA800DDDD865B6BF3A85ADEC4C29730
A8031D608F65499418799817646 74DD7  1A89324D6D3E6DE6726C688BFF225DDD  07B546E8E002FC5854651BE31802F96D
DDAD29B8B1215191E7EB5AAEE0219338  F5FA42A5B421705E4803DA93C4F7E099  DF2AD7F766E2EEFAF0FD1FB5C6883AB4
3F8A5EA1756DDF4A6B6F2645B4911486  A869B96BCDF1D474C0714763AA34A8C9  1C6EA2DA6ECED5C5C761BCA9CA4C5308
30DF96D87EEC8CA77A135ECCAB1AD25E  3EA0F90DE57187FC7E1AC45AE44D16C6  A640A29E706AF38557B86619EAF45E7A
7DD8E0E1906C1754E11E901927CCABBD  F7DE638B76C3958AA3413A9785A19900  F88885670C3D55EBA52096A65310DACA
DAC51C3D23B163601305AF99DF129689  3F8C9CDAACBB533AE94F47456819FA0E  B85E7BB83667097F15D8A3DEAAA1B198
D77EC92400AE0D9FA57DEF4DD8CFA4D4  209920C169512D3EB4A1ED7CAD17D033  A5F6F149B468683318DC178F4208E237
09369288E36D7AFFEE94EA81998FA316  B2F57BD01BAAF7AF01EF442910CEBBA0  04841B82A9D81E44CB4F2D98CFE7C374
EEBE1885532234328919 1913F6D769EB  C0766829AA4D2E1A5D97213A4E4A654E  A81686CEFDEFFCE82B8DBF100E1395F1
C00132DA154BDEE361EDEE727226D0F5  FC9993EA7A4E761B6CB79ABE2BD3CDE1  9952073595776A3D7A8101664A56AB96
6580BE22A0566352B9622777BFCB7164  4D556B338FAA020979A740B4C3AEE28C  A076DA72A8C8E2137F05FE3FA59870EB
7352C61297D6B04E874EDAD12480F78E  8ED896B9A622FF24559A3429E5888E0A  121378A6DE0A13DDB295106E912A4E14
F658C0D52B3EEF71DDE6C284E7E1B337  8CF1F45323EC5AB449451E7A9476CFDC  65A925E578098658FADA30E9FB67B5E4
E1253D04A17AB8E47F4A5916B9BF9D23  D1718E9BD91257D2169C81197D508A67  5B8E5202EC6769F2389605D33DC245B2
8922A9A23BE960FFE9707A0B3F4D75BD  E4A691D60266784968DF971D6BF473AF  EA71F746BD17D1B05450329818572F2E
EAE97F465015E49A14F3B23403ACFA11  B3B64F1925F759A2E145190333D1D6D2  DD8C315D2CA61870CBCF9D56ED7474E2
13A757022817C0514A5C142FE9BF143A  ED4C2EBC14B85F46A9A75F159DF8BEB3  F346A1E62FED476F472560C6DDE0CADC
5132F0FCB3F8DCAA501C620575D33FEE  CDBC0441C10DB5ABA43120E63A048425  CBBCB9E06F9FC92C533B2F2A5284BA22
39953BF6383A00D29BEB377568E3DE7A  DC1665266A0198728861AC99ED368928  79DCFDA2700E06F8EAA640BA9B827810
67887932934DFF086153CA905E7DE9EE  706BBC770C62D41DD799721ABD1868AB  17CF5474D5A8B4E735E69E017CEC2F37
DCD1072719692871126E4159D80EFDA8  B2205D8CBDDFE49D7C5F0F95D506718F  7034FBF641CEB257FC109A6819D19DA0
C6741E3D08C0FFD4617B94E654DD89F1  901F30DB86EEB1666F5A8CAE1C7BD08B  6E6D052B5ABC015C779EA3500FA11A28
8CC74931E64061491652CC169C8BAAB3  C731140FAA7690918BABF17BECB7938D  0370390E48A7F26AA62188A79E612DC3
4157D99E46A3E45E6130A95645410DAC  8C605DFAA0EC88CDB7D12F7250C9F53A
E34C4FC7488C4DFEF0EA475A17AF2C7B  68F252CD36F2798A2182F6406A31A5A2
59F8BDDA3F56D8026FAB6E3130F5D843  BD7CB0D124DFDE784CD5B9EF288C304E
FAB79682C8EAE556F11ECF6DAD7121BA  3D2BC95A85EF539A68DAC84542A1AE7A
```

Appendix V (Confidential)

The information in this appendix must be kept confidential due to the ongoing investigation.

Appendix V-I List of attackers IP addresses

Reference	IP address	Source	Remark
	109.131.139.148	IIS logs winsrv101	
	184.73.172.213	IIS logs winsrv101	
	188.34.57.139	IIS logs winsrv101	
	202.60.66.32	IIS logs winsrv101	
	204.12.8.116	IIS logs winsrv101	
	207.232.7.167	IIS logs winsrv101	
	209.190.184.207	IIS logs winsrv101	
	213.229.81.34	IIS logs winsrv101	
	217.122.166.160	IIS logs winsrv101	
	217.169.64.30	IIS logs winsrv101	
	50.17.249.10	IIS logs winsrv101	
	50.57.92.77	IIS logs winsrv101	
	62.75.181.81	IIS logs winsrv101	
	66.249.66.23	IIS logs winsrv101	
AttIP5	67.202.50.234	WINSRV119	Not in the IIS logs of winsrv101
	74.220.215.87	IIS logs winsrv101	
	77.104.76.200	IIS logs winsrv101	
	77.104.76.95	IIS logs winsrv101	
AttIP7	77.104.76.96	IIS logs winsrv101	OCSP request test run. Resolved to an ADSL user in Iran.
AttIP3	77.104.76.97	IIS logs winsrv101	
	77.104.76.98	IIS logs winsrv101	
	80.101.202.176	IIS logs winsrv101	
	81.164.210.31	IIS logs winsrv101	
	81.242.49.214	IIS logs winsrv101	
AttIP1	83.170.68.10	Malware WINSRV119	csrsss.exe Not in the IISlog of {SVO8}? Resolves to warfit.com
AttIP6	83.220.51.66	IIS logs winsrv101	
AttIP4	85.17.182.207	IIS logs winsrv101	
	88.80.216.130	IIS logs winsrv101	
AttIP2	94.236.23.234	Malware WINSRV119	Niet in de IISlog van SVO8?

Van: [redacted] - Logius[redacted]@logius.nl]
Verzonden: maandag 19 december 2011 10:41
Aan: [redacted]
Onderwerp: RE: laatste versie van het Fox-rapport
Bijlagen: HH-Operation Black Tulip Update (draft) 0.1-1215a.pdf

[redacted] / [redacted]

De voortgang bij Fox is langzaam maar gestaag.

Bijgaand de laatste versie van het rapport. Begin deze week wil men nu (eindelijk) de versie hebben die we kunnen uitzetten voor commentaar. Daar mist dan hooguit inleiding, samenvatting e.d. in.

Feiten en bevindignen zouden dan volledig moeten zijn.

Laten we het er morgen even over hebben hoe met het rapport om te gaan. Deze versie dus niet verder verspreiden.

[redacted]

FOX-IT
EXPERTS IN IT SECURITY

Black Tulip

Investigation update
hack of DigiNotar

Classification	**CONFIDENTIAL**
Customer	BZK
RE:	Investigation update
Project no./Ref. no.	PR-110202_CC
Date	15 December 2011
Version	0.1
Team	Hans Hoogstraaten (Team leader) Ronald Prins (CEO and advisor) Kevin Strooy (Forensic expert) Steffen Moorrees (Forensic expert) Danny Heppener (Malware expert) Robbert Kouprie (Security Expert) 1 other Security Expert
Business Unit	Cybercrime
Pages	101

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

CONFIDENTIAL
This document is classified as confidential. Any information published in this document and its appendices is intended exclusively for the addressee(s) as listed on the document management distribution list. Only these addressee(s) and additional persons explicitly granted permissions by any of these originally authorized addressee(s) may read this document. Any use by a party other than the addressee(s) is prohibited. The information contained in this document may be confidential in nature and fall under a pledge of secrecy.

If your name is not listed on the document management page or if you have not obtained the appropriate (written) authorization to read this document from an authorized addressee, you should close this document immediately and return it to its original owner.

Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. Fox-IT cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by its contained information.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

Document Management

Version management

Project name: [project]
Customer: [customer]
Subject: [subject]
Date: [date]
Version: [version]
Status: [status]
Author(s): [author]

This version replaces all previous version of this document. Please destroy all previous copies!

Distribution list

Copy	Distribution (version)	Name/function/remarks

Review management

Review by	Function	Date	Version

Change management

Version	Date	By	Remarks	Approval

Related documents

Version	Date	Description	Remarks

Table of Contents

TO-DO

{lijstje met TODO's voor dit rapport. Wordt uit het finale rapport verwijderd}

Vragen:

? misschien bij ieder hoofdstukje een mangament samenvatting maken? [of gewoon één management samenvatting aan het begin van het rapport?]

? Wie wil zijn naam op de cover

Marketing sausje

Laatste checks:

- Aantal aanvallers in het midden laten ("Perpetrator**(s)**") OF: overall in enkelvoud en opnemen in inleiding dat het een of meerdere kunnen zijn
- Tijd/ datum formaat standaardiseren (30-Aug-2011 11:12:13).
- Universele referenties naar servers (naam en evt IP als niet uniek)
- Universele referenties naar netwerken (Secure-net, e.d.)
- Afco's controle. En in de afco's lijst achterin.
- Zoek en vervang winsrv met winsvr (winsvr werd gebruikt door diginotar!)

Review's

- Onderzoeksteam op feiten
- directive/ MT op 'gevoellige' zaken
- AM/ marketing op profilering Fox

1 Introduction

1.1 Background

The Certificate Authority (CA) DigiNotar B.V. provided digital certificate services, including SSL certificates, qualified certificates and the government accredited PKIOverheid certificates. During the months June and July of 2011 the security of the company was breached and rogue certificates were generated. One of these certificates, a rogue wildcard Google certificate, was abused on a large scale in August of 2011 to target primarily Iranian Internet users. At the end of August the attack became public knowledge and set in motion a chain of events that eventually ended in the revocation of the certificates that had been issued by DigiNotar and ultimately the bankruptcy of the company.

This report is the outcome of the time boxed investigation that was performed by Fox-IT into the breach of DigiNotar's internal network. The initial incident response investigation was performed at the request of DigiNotar and continued at the request of the Ministry of the Interior and Kingdom Relations of The Netherlands. The aim of the investigation was to answer specific questions, such as to what extent DigiNotar's network had been breached and what information could be uncovered in regard to rogue certificates that had been generated and the identity and location of the attacker.

This non-exhaustive report provides an overview of the relevant results of the investigation and contains information about the internal network of DigiNotar and the traces that were left by the attacker(s). Detailed information that was uncovered in regard to the identity and/or location of the attacker has been excluded from the public version of the report and will be included as a confidential appendix only for the proper authorities.

The findings will be reported in such a way that they can be repeated by third parties if they have access to the source material. References to servers are made using the original name of server that was used by DigiNotar, a comprehensive list of the referenced servers including their IP-address(es) and function can be found in appendix [X]. All dates and time stamps are based on the Central European Time (CET; GMT+1) timezone, unless explicitly stated otherwise. Questions that fall outside of the scope of the investigation and consequently this report may be answered after further research. Potential follow-up questions for further research are included in chapter 14.

{het rapport is geschreven vanuit het perspectief van Fox}

{alle investigations zijn zo opgeschreven dat iemand deze kan herhalen met de bron info}

{leeswijzer}

{?wat feitjes opnemen?: aantal systemen veiliggesteld, uren, mailtjes e.d.?}

{link met comodo hacker toevoegen?}

1.2 Events leading up to the report

In June of 2011, (an) attacker(s) gained authorized access to the internal network of the DigiNotar. Several weeks after the attacker(s) first gained access to the webserver on the perimeter of the internal network, the attacker(s) had made his/their way into the Secure network segment. On 10-Jul-2011 the attacker(s) successfully created rogue certificates for large numbers of websites. The attack was detected by DigiNotar during a routine security check on 19-Jul-2011. In the last two weeks of July 2011 large numbers of certificates were revoked and an investigation was performed by [X]. Based on the information that was available at that time, DigiNotar was under the impression that it had managed to control the damage of the hack.

During the month of August of 2011 a man-in-the-middle (MitM) attack was performed on users in Iran using a wildcard Google certificate, which became public knowledge on 28-Jul-2011. Fox-IT was asked to start an incident response investigation by DigiNotar on 30-Aug-2011, with the aim of establishing to what extent which their systems had been compromised. Fox-IT assembled a team and started the investigation immediately. The investigation team included forensic IT experts, cybercrime investigators, malware analysts and a security expert with PKI experience. Due to the urgency of the matter, the

nature of the investigation was that of incident response and would be followed up by an interim report with preliminary findings for DigiNotar stakeholders.

As of early September the Dutch Ministry of the Interior and Kingdom Relations took over the role of the client in regard to the investigation. The primary aim of the ensuing investigation was to determine if and to what extent the CA severs that were used to issue qualified certificates and/or certificates for PKIOverheid had been compromised. A further aim of the ensuing investigation was to support the Dutch police in their investigation into the identity and location of the attacker(s). This report is the result of the investigation that continued at the request of the Ministry of Interior and Kingdom Relations.

1.3 Parties involved

Party	Role
AIVD	Identifying potential threats for national security.
BZK	The Dutch Ministry of the Interior and Kingdom Relations.
DigiNotar	Former notarial collaboration acquired by VASCO Data Security International.
DigiNotar customers	Customers of DigiNotar that used certificates that were issued by DigiNotar.
Fox-IT	Provides solutions for the protection of state secrets, the investigation of digital crime, audits, managed security services and consultancy.
GOVCERT.NL	Cyber Security and Incident Response Team of the government.
Hoffman	Offers investigative, forensic and strategic risk management services.
Iranian people	Primary targets of the MitM-attack during which rogue certificates were used.
Internet community	Affected by the consequences of the attacks in a general sense.
KLPD	Responsible for the investigation into the attack(er)(s).
Manufacturers	Parties that operate at the highest layer of the Public Key Infrastructure.
OM	Responsible for the prosecution of the attacker(s).
OPTA	OPTA is an independent administrative body that checks whether registered CSPs parties comply with Dutch law.
PWC	Performs audits of CSPs, including DigiNotar.
RSA	Provides diverse security, risk and compliance solutions.
Raad van accreditatie	Dutch Accreditation Council.

1.4 Timeline of events

Date	Description
01-Jun-2011	The first day of the analyzed firewall log entries shows that an IP-address that will later be used by the attacker(s) is active on external IP-addresses of DigiNotar.
18-Jun-2011	The first unauthorized connections occur from internal IP-addresses in the DigiNotar network to an external IP-address related to the attacker(s).
30- June-2011	The firewall log files show the first signs of extraordinary activity in the Secure network segment.
02- July-2011	The CA server log files show the first signs of extraordinary activity and certificate signing requests on Relatie-CA.
10-Jul-2011	The first successful creation of a rogue certificate (for *.google.com) on Relatie-CA. Subsequently another 85 rogue certificates are created on Relatie-CA. Another 198 rogue certificates are created on Public-CA.
19-Jul-2011	The signing of 128 [5.1.2: 124] rogue certificates was detected by DigiNotar during their daily routine security check. The rogue certificates that were discovered were revoked immediately.
20-Jul-2011	During analysis the generation of another 129 [5.1.2: 124 – of kwamen de gegenereerde en gedetecteerde certs op 20-07 niet overeen?] rogue certificates was detected. This is the last known date of the creation of rogue certificates.
21-Jul-2011	The certificates that were detected on 20-Jul-2011 were revoked.
	Various security measures were taken in regard to infrastructure, system monitoring and OCSP validation to prevent further attacks.
27-Jul-2011	An additional 75 rogue certificates that were discovered during analysis were revoked.

Date	Description
27-Jul-2011	Another IT-security firm which performed the regular penetrating testing and auditing for DigiNotar reported that unauthorized administrative access had been obtained to the outside webservers, the CA server Relaties-CA as well as Public-CA.
27-Jul-2011	First OCSP request at DigiNotar for a rogue wildcard Google certificate.
28-Jul-2011	DigiNotar found evidence that rogue certificates were being verified by IP-addresses originating from Iran.
04-Aug-2011	The beginning of massive activity on the OCSP responder for a rogue *.google.com certificate.
28-Aug-2011	On the Google support forums an customer of the Iranian ISP ParsOnline posts details about a certificate warning that was presented to him by Google Chrome for a rogue *.google.com certificate (http://www.google.co.uk/support/forum/p/gmail/thread?tid=2da6158b094b225a&hl=en).
29-Aug-2011	Google receives multiple reports in regard to an attempted SSL MitM-attack and articles about a rogue *.google.com certificate appear on the blogs of amongst others Mozilla, Google and Microsoft. On the same day the rogue *.google.com certificate was revoked, which had not been discovered by DigiNotar before. Additionally, GOVCERT.NL was notified by Cert-Bund.
30-Aug-2011	Fox-IT is asked by DigiNotar to initiate an investigation into the attack on DigiNotar and places a incident response sensor in the network of DigiNotar. DigiNotar publicly reacts on the breach in its security and states that only the "Public 2025 Root" (Public-CA) was compromised.
01-Sep-2011	Fox-IT places a customized OCSP responder that is based on a whitelist.
02-Sep-2011	The preliminary investigation by Fox-T indicates that the integrity of PKIOverheid had been breached. DigiNotar and GOVCERT.NL are informed of the details of this finding.
03-Sep-2011	The Dutch government publicly revokes the trust it had placed in DigiNotar and its certificates. Following this announcement, most manufacturers also revoke their trust in DigiNotar, if they had not done so already.
05-Sep-2011	Fox-IT publishes its interim report on the breach of the DigiNotar Certificate Authority. DigiNotar reports the hack to the police.
14-Sep-2011	OPTA ends the registration of DigiNotar B.V. as a certificate authority for qualified signatures on the basis of the Dutch Telecommunicatiewet (law on telecommunication).
19-Sep-2011	DigiNotar B.V. filed a bankruptcy petition under Article 4 of the Dutch Bankruptcy Act.
20-Sep-2011	The Court of Haarlem declares DigiNotar B.V. to be bankrupt.
28-Sep-2011	Qualified and PKIOverheid certificates were revoked by DigiNotar.
01-Nov-2011	All remaining active public certificates were revoked (BAPI and two DigiNotar Private CAs were excluded).

1.5 Questions and answers

This report is aimed to answer to the following questions:

- What systems and corresponding CAs were compromised by the attacker(s)?
  - What was the point of first entry?
  - What technical actions were performed?
  - Which security measures were breached?
  - What tools were used in order to perform the attack?
  - Was malware used and if so what did it consist of?
  - What are the steps that were taken before the attacker(s)'s goal was reached?
  - What systems outside of DigiNotar were used to do so?
- What were the technically observed consequences for the population of Iran?

This report is *not* aimed to answer the following questions:

- Was information was stolen and if so what did it consist of?
- What was the mode of operation of the attacker(s) in detail?
- Were sufficient security measures in place and did DigiNotar comply with its legal requirements?
- Was DigiNotar civilly liable for the hack or its actions following the hack?
- Were legally relevant elements of certain criminal offenses perpetrated by the attacker(s)?
- Can the attacker(s) be traced on the basis of the information that was uncovered?

1.6 Structure of the report

2 Situation

2.1 Organisation

DigiNotar BV was founded as a privately-owned notarial collaboration in 1998. The customer base of DigiNotar consisted of government institutions, profit and non-profit organizations as well as individual citizens. The company provided digital certificate services as a Trusted Third Party (TTP) and hosted a number of Certificate Authorities (CAs). Certificates issued by DigiNotar included SSL certificates, Qualified Certificates and government accredited certificates. The government accredited 'PKIOverheid'-certificates were used for critical public services such as DigiD (Digital Identity), which is used for various Dutch eGovernment purposes. On January 10th of 2011 VASCO Data Security International announced its acquisition of DigiNotar BV. On September 20th of 2011 the court of Haarlem declared DigiNotar BV to be insolvent following the breach of the security of crucial segments of its internal network.

{wat troffen we aan}

2.2 Certificate issuing process

[Algemene informatie over uitgifte van certificaten]

There were four different processes in regard to the storage of private keys:

- **SSL PKCS10**
  The Public-Key Cryptography Standard (PKCS) defines a file format used to store X.509 private keys and the corresponding public key certificates. In this process the client generated a private key and sent a certificate signing request to DigiNotar. As a result, no private key entered the DigiNotar domain during this process.
- **SSL PKCS12**
  When a client requests an SSL certificate a private key is generated with the DARPI application. The DARPI application then created a signing request and sent it it to the appropriate CA system. The DARPI application uses the API of the appropriate CA to perform this task, for which a authentication certificate is used. The key and the certificate and joined together in a PKCS#12 file that is protected with a password that consisted of 10 alphanumeric characters. The P12 file was then sent to the customer. A copy of the P12 file was stored in the DARPI database. The password was sent to the PIN mailer and a PIN letter was sent to the customer.
- **Smartcard and USB token**
  PKIOverheid differentiates between three certificates. The first type of certificate is used for electronic signatures, a second type for encryption and a third for qualified signatures (non-repudiation). When electronic or qualified signatures were used the private keys were generated on the token. The CSR was then signed by the CA and placed on the token with the private keys. In the case of the encryption certificate, the private key was generated on the darpi system and not on the token itself because of key escrow [verder uitleggen]. Both the key and the certificate were protected with a password and were stored in the database as in the SSL P12 process. The PIN is sent to the customer by the PIN mailer.
- **Special cases**
  In special cases where the DARPI software was not sufficient [verder uitleggen waarom niet sufficient] the certificates were generated manually on the RSA Keon terminal. These special cases included the generation of EVSSL certificates.

The passwords of the P12 files are stored in the CAP database. The database is unencrypted. Every period of 6 weeks the passwords and P12 files are removed and archived. The archive is encrypted. The private key of this archive is stored offline in a vault. This key is can only be used when two persons enter their PIN (four eyes principle).

The DARPI application is a self written application that is installed on several workstations. Those were not constantly turned on.

For every certificate request a dossier was created in CAP. Every day all the certificate dossiers were gathered in a centrale certificaten database (CCDB) and compared with a copy of the RSA Keon database ldif). This could show any fraudulent actions. This process was inoperative from xx until July the 18th. On July the 19th

Er worden van alle systemen (welke ook al weer?) req en certs verzameld en gecontroleerd of deze matchen. Er gaat een alarm af als er een mismatch is.

Er is een RSA envision log analyse door maar die doet niets.

TODO's:
•How did the authentication work exactly?
•Is this authentication traceable? Is this the 'ID' in the xslogs of the CAs?
•Was this authentication misused by the attacker(s)?
•What was the password (policy) of the P12 SSL files?
•What was the password (policy) of the encryption keys stored in the key escrow?

2.3 Other services

In addition to their certificate issuing service, DigiNotar provided several other services:

- Signing service (certified information exchange service on behalf of other companies):
  - CORUS
  - Money You
  - BNG
  - WKPB
  - NWRO
  - APG (uitvoering ABP)
  - Achmea
- Authentication service
  - BISTRO/ORDE
  - eHerkenning
  - Pass
  - HLB (accountants)
  - PKI-overheid
  - Notaries
  - BAPI
- Document proof service
  - FME
  - PWC
  - Official publications (Staatcourant c.a.)
  - TAXI
  - For Lawers
- Other
  - Parelsnoer: anonymised exchange of human test subject information for medical universities (universitair medisch centrum; UMC). Anomysation of citizen service number (Burgerservicenummer; BSN)
  - CCV: initialisatie PIN-automaten

2.4 Customers

- PKI-overheid
- Notarissen
- BAPI
- TENNET
- EASIGAS
- Notarissen/KNB

- Gerechtsdeurwaarders/SNG
- TU delft

Decos en Circle Software
(http://www.computable.nl/artikel/ict_topics/security/4141174/1276896/diginotarpartners-zoeken-naar-alternatieven.html)

2.5 Network

{Inleiding toevoegen.}
{→ main location and co-location}
{Kort iets over de fysieke beveiliging (pasjes, dubbele deuren, inner room, hand scanner) (productie ruimte)}.

The DigiNotar network had two connections to the Internet that were provided by two different Internet Service Providers. Behind the router that is responsible for Internet connectivity a TippingPoint 50 Intrusion Prevention System (IPS) was present. The IPS was running a default configuration and was not effectively used, as it was placed in front of the firewall and consequently gives a lot of false positives, although it was planned to be placed behind the firewall. Behind the IPS a load balancer routed the traffic to a redundant Nokia firewall appliance, which was running Checkpoint Firewall-1/ VPN-1 {controleer exacte naamgeving/ versie} with a separate management server. An external company managed the firewalls at DigiNotar.

The DigiNotar network was divided in 25 different internal network segments. The following list of networks was enforced as extracted from the firewall settings (exported on 30-Sep-2011):

{sorteren op IP range}

Net name[1]	IP range	Description
DMZ-old-net	10.10.0.0/24	Old DMZ network
DMZ-ext-net	10.10.20.0/24	External DMZ network
DMZ-ext-closed-net	10.10.30.0/24	Closed external DMZ network
DMZ-ext-vasco-net	10.10.50.0/24	Vasco external DMZ network
DMZ-ext-vpn-net	10.10.40.0/24	VPN network
production-net	10.10.110.0/24	Secure production network
DMZ-int-net	10.10.200.0/24	Internal DMZ network
admin-net	10.10.210.0/24	Management network
acceptance-net	10.10.230.0/24	Acceptance network
test-net	10.10.240.0/24	Test network
develop-net	10.10.250.0/24	Development network
office-new-net	10.31.32.0/23	New office network
vasco-net	10.32.0.0/16	Vasco network
iscsi-net	10.200.200.0/23	Internal ISCSI network
iscsi-colo-net	10.200.202.0/23	Co-location - ISCSI DMZ network
office-net	172.17.20.0/25	Office network and temporary network
hosted1-old-net	172.17.20.128/28	Old 'hosted1' network
hosted3-old-net	172.17.20.160/28	Old 'hosted3' network
secure-net	172.18.20.0/24	Secure 'Unicert/RSA' network
DMZ-ext-colo-net	172.25.20.0/24	Co-location - external DMZ network
DMZ-int-colo-net	172.26.20.0/24	Co-location - internal DMZ network
secure-colo-net	172.27.20.0/24	Co-location - Secure network
office-colo-net	172.28.20.0/24	Co-location – office network
sync-1-net	192.168.1.0/29	First FireWall-1 synchronisation
ext-net	62.58.35.96/28	Network between the firewall and the Internet
pinewood-mgmt-net	62.58.74.128/27	Pinewood remote management

[1] Network segment name as it is used in this report.

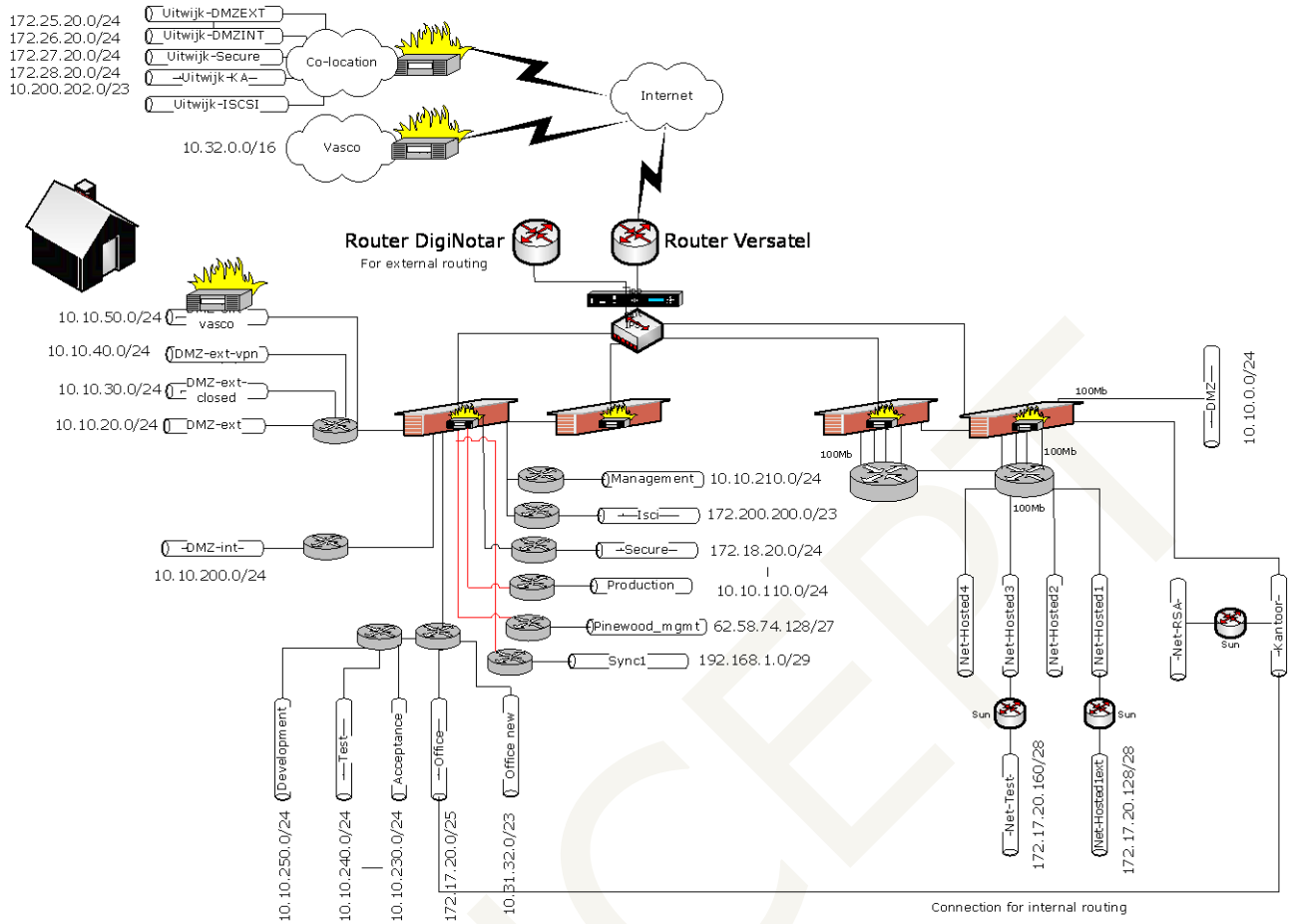


Figure 1 A rough sketch of the DigiNotar network[2]

{Plaatje: firewall in de uitwijk erbij zetten. Huisje weghalen. VPNs toevoegen.}

Most of the systems in the network were machines running a Windows operating system from Microsoft.

In the secure-net network segment the systems were located that needed the most protection. More specifically, in this network segment the servers were located that ran the CA management software, as well as the 'production' servers and a hardware security module that was accessible over the network (netHSM). The production workstations and servers were used, amongst others, to initialise and personalise smartcards or other PKI tokens, issue certificates and create PIN letters. These production systems [servers/workstations?] were connected to the back-end administration in the office-net network segment and the CA servers. The production applications were called CAP (Control Application), DARPI (DigiNotar Abonnementen Registratie[3] Production Interface) and BAPI (Belastingdienst[4] Advanced Program Integration) and were all custom developed.

The CA management software that ran on the CA servers connected over the network to the netHSMs, where the private keys of the CAs were securely stored. On the main location at least eight CA servers were present, including one test CA server and one root CA server. On the co-location seven redundant (virtual) CA servers were located for the purpose of business continuity[5]. In total DigiNotar used four netHSMs, one of which was in the secure segment for the CAs, a second in the internal DMZ (DMZ-int) for the 'Parelsnoer' service, a third in the test environment and the fourth netHSM was located in co-located secure network segment.

[2] Based on a drawing provided by DigiNotar. The exact lay-out of the layer-2 {zo heet dat toch?} network (switches) in this sketch is not verified.
[3] Which translates to "Subscription Registration".
[4] The Dutch tax and customs administration.
[5] The systems were on 'warm' standby; the servers were switched on, however it was unknown if backups had to be restored and if the netHSMs were functional.

[laatste twee alinea's mogelijk na de "during normal operation" alinea → d.w.z. "during normal operation" als opening en de netwerkschets na de schets van de normale procedure & fysieke beveiliging]

During normal operation, a customer requested a certificate on one of the web servers in the external DMZ (DMZ-ext-net). The request was then stored by the web server on a server in the internal DMZ (DMZ-int-net). The firewall prohibited any communication initiated from the DMZ-int-net to the DMZ-ext-net[6]. These request were periodically collected by a service in the secure-net. The firewall prohibited that any connection was initiated from the DMZ-int to the secure-net. In the CAP administrative application the request was stored and administrative procedures such as vetting were initiated.

When a request was approved using the four-eyes principle, a field in the database was marked. Subsequently, an administrative employee logged on to a workstation running a DARPI client, in a separate room and processed the request. Depending on the procedure a private key was generated (or not) and a certificate request was sent to one of the CA servers. The CA software automatically signed the request and returned the certificate.

In order for the CA software to automatically sign the certificate request, the appropriate private key which was stored in the netHSM needed to be activated. This was done by an authorised employee (CA operator) who entered a smartcard into the netHSM combined with a PIN-code. To activate the Root-CA private key multiple authorised employees with smartcards were required.

The CA operator manually created certificates for certificate requests that could not be processed by the DARPI application. In order to generate these certificates the CA operator had to log into the CA application together with someone else who could provide physical access.

The main servers of DigiNotar, including the CA and netHSMs, were located in a physically highly secured room. This room could be entered if authorised personnel showed their hand to a biometric hand recognition device and entered the correct PIN. This inner room was protected by a outer room with a set of doors opening depending on each other creating a sluice. These doors had to be opened with an electronic door card. To gain access to this room from a public accessible room another electronic door token had to be used twice, while passing through two different security zones.

2.6 Internet services {andere naam voor dit hoofdstukje?}

DigiNotar used the following internet IP address ranges[7]:

IP start	IP end	netname
62.58.35.96	62.58.35.111	TELE2-CUST-DIGINOTAR-BV
62.58.36.112	62.58.36.127	VERSATEL-CUST-Diginotar-B-Vx
62.58.44.96	62.58.44.127	VERSATEL-CUST-Diginotar-B-Vx
81.58.241.160	81.58.241.175	VERSATEL-CUST-Diginotar-B-Vx
87.213.105.80	87.213.105.95	TELE2-CUST-Diginotar
87.213.114.0	87.213.114.15	VERSATEL-CUST-Diginotar-B-Vx
87.213.114.160	87.213.114.191	VERSATEL-CUST-Diginotar-B-Vx
143.177.3.40	143.177.3.47	-
143.177.11.0	143.177.11.15	-
193.173.36.32	193.173.36.47	OTS25849

During a vulnerability scan performed by Fox-IT on 14-Sep-2011 a long list of web services presented itself to the internet.

[6] The operation of the firewall as was explained by the administrators of DigiNotar. The firewall rules were not verified.
[7] This list might not be complete.

IP address	Port 80 HTTP	Port 443 HTTPS
62.58.35.107	X	X
62.58.36.113	X	X
62.58.36.116	X	X
62.58.36.117	X	X
62.58.36.118	X	X
62.58.36.119	X	X
62.58.36.121	X	X
62.58.36.122	X	X
62.58.36.123		X
62.58.36.124		X
62.58.36.125	X	X
62.58.36.126	X	X
62.58.36.127	X	X
62.58.44.96	X	X
62.58.44.97	X	X
62.58.44.98	X	X
62.58.44.99	X	X
62.58.44.100		X
62.58.44.102	X	X
62.58.44.103	X	X
62.58.44.104	X	X
62.58.44.105	X	
62.58.44.107	X	X
62.58.44.109	X	X
62.58.44.110		X
62.58.44.112	X	X
62.58.44.113	X	X
62.58.44.114	X	X
62.58.44.118	X	X

IP address	Port 80 HTTP	Port 443 HTTPS
62.58.44.119	X	X
62.58.44.121	X	X
62.58.44.123	X	X
62.58.44.125	X	X
62.58.44.126	X	X
62.58.44.127	X	X
81.58.241.160	X	X
81.58.241.161	X	X
81.58.241.162	X	
81.58.241.163	X	X
81.58.241.164	X	
81.58.241.165	X	X
81.58.241.167	X	X
81.58.241.168	X	X
81.58.241.171	X	X
81.58.241.172	X	X
81.58.241.173	X	X
81.58.241.174	X	X
81.58.241.175	X	
87.213.105.80	X	
87.213.105.81	X	X
87.213.105.82	X	
87.213.105.83	X	
87.213.105.84	X	
87.213.105.85	X	
87.213.105.87	X	X
87.213.105.89	X	
87.213.105.90	X	X
87.213.105.91	X	X

IP address	Port 80 HTTP	Port 443 HTTPS
87.213.105.92		
87.213.105.93	X	
87.213.105.94	X	X
87.213.105.95	X	X
87.213.114.3	X	X
87.213.114.4	X	X
87.213.114.5	X	X
143.177.3.40	X	X
143.177.3.41		X
143.177.3.44	X	X
143.177.3.45	X	
143.177.3.46	X	
143.177.3.47	X	X
143.177.11.1	X	X
143.177.11.2	X	
143.177.11.3	X	X
143.177.11.4	X	
143.177.11.5	X	X
143.177.11.6	X	X
143.177.11.7	X	X
143.177.11.8	X	X
143.177.11.9	X	
143.177.11.10	X	X
143.177.11.11	X	X
143.177.11.12	X	
143.177.11.14	X	X
143.177.11.15	X	X

A DNS query of the IP addresses used showed the following entries[8]:

IP address	DNS lookup
62.58.36.114	mailhost.diginotar.nl
62.58.36.116	mail.diginea.nl
62.58.36.118	www.diginotar.nl
62.58.36.120	authenticatie.pass.nl
62.58.36.121	belastingdienst.diginotar.nl
62.58.36.125	service.diginotar.nl
62.58.36.126	Registratie.diginotar.nl
62.58.44.107	digi01.mailwitness.net
62.58.44.108	digibackup.mailwitness.net evssl.diginotar.nl
62.58.44.109	sha2.diginotar.nl
62.58.44.111	ftp.diginotar.nl
62.58.44.113	www.evssl.nl
62.58.44.116	genghini.mailwitness.net
62.58.44.121	danka.mailwitness.net
62.58.44.122	bgg.mailwitness.net
62.58.44.123	diginotar.mailwitness.net
62.58.44.124	test.pass.nl
62.58.44.125	*.diginotar.com diginotar.com diginotar.net
143.177.3.41	mailhost1.diginotar.nl

[8] This list is not complete.

	mail.digifactuur.nl mail.diginotar.com
143.177.3.42	directory.diginotar.nl
143.177.3.43	www.servicecentrum.diginotar.nl
143.177.3.45	validation.diginotar.nl
143.177.11.2	servicecenter.diginotar.nl
143.177.11.4	demonstratie.pass.nl
143.177.11.10	onlineaanvraag.diginotar.nl
143.177.11.11	www.pass.nl
193.173.36.36	ns1.diginotar.nl
193.173.36.39	mailhostuw.diginotar.nl

The vulnerability scan showed some other service presenting itself to the internet:

- An FTP server on 62.58.44.111 (ftp.diginotar.nl)
- A web service on 87.213.105.92 port 8888
- 3 VPN servers on 62.58.35.108, 62.58.35.109 and 62.58.35.110
- A Mail server on 62.58.36.114
- A DNS server on 87.213.114.2

2.6.1 Web servers

From some of the web servers present in the external DMZ-ext-net the internal IP addresses were extracted from the web servers configuration:

Server ID	Internal IP	Site name
WINSRV101		
	10.10.20.11	Notarisgombert.nl
	10.10.20.14	Darwizard
	10.10.20.28	evssl.diginotar.nl
	10.10.20.41	DigiNotar.nl
	10.10.20.46	www.evssl.nl
	10.10.20.58	DigiNotar.com
	10.10.20.61	OCSPclient
	10.10.20.69	sha2.diginotar.nl
	10.10.20.73	BapiOphalen
	10.10.20.97	Bapiviewer
WINSRV118		
	10.10.20.37	Docproof
WINSRV119		
	10.10.20.65	Docproof
WINSRV108		
	10.10.20.16	PassWeb - PASS15
	10.10.20.40	NTP
	10.10.20.35	TIM_tim.diginotar.nl
WINSRV109		
	10.10.20.98	SS_Provincie-Utrecht.signing.diginotar.nl
	10.10.20.129	SS_Gelderland.signing.diginotar.nl
	10.10.20.42	TimeStampServer
	10.10.20.92	SoapSigning
	10.10.20.84	SS_Lelystad.Signing.diginotar.nl
	10.10.20.85	SS_Waterschapdedommel.signing.diginotar.nl
	10.10.20.86	SS_Signing.diginotar.nl
	10.10.20.137	DigiDownload
	10.10.20.87	SS_Teylingen.signing.diginotar.nl
	10.10.20.88	SS_PZH.signing.diginotar.nl
	10.10.20.89	SS_sintanthonis.signing.diginotar.nl
	10.10.20.130	SS_Leeuwarden.Signing.diginotar.nl
	10.10.20.90	SS_PNB.signing.diginotar.nl

	10.10.20.91	SS_Leiderdorp.Signing.diginotar.nl
	10.10.20.99	SS_Drenthe.Signing.diginotar.nl
	10.10.20.93	SS_Overijssel.Signing.diginotar.nl
WINVM045[9]		
	10.10.20.172	evssl.diginotar.nl
	10.10.20.164	BapiViewer
	10.10.20.165	DarWizard
	10.10.20.182	bct.csp.minienm.nl
	10.10.20.173	www.diginotar.com
	10.10.20.167	OCSPClient
	10.10.20.174	service.diginotar.nl
	10.10.20.169	BapiOphalenCert
	10.10.20.183	test.bct.csp.minienm.nl
	10.10.20.175	www.evssl.nl
	10.10.20.158	www.diginotar.nl www.diginotar.com diginotar.com diginotar.nl www.evssl.nl evssl.diginotar.nl
	10.10.20.184	test.csp.minienm.nl
	10.10.20.181	csp.minienm.nl
	10.10.20.176	sha2.diginotar.nl

2.7 Actions taken

{? Misschien naar een eigen hoofdstukje?}
{welke acties zijn er uitgevoerd door DigiNotar (onder leiding/ advies) van Fox?}
{white list OCSP, OSCP monitoring, opnieuw inrichten van OSCP responder, virus scanner installeren, e.d….}

2.7.1 OCSP responder monitoring

[link met chapter 10?]

[9] WINSRV101 has been replaced by WINVM045. First firewall entries of 10.10.20.158 from WINVM045 appear on 18-Jul-2011.

3 Research {approach?}

3.1 Preliminary research

{wat is er al door DigiNotar/ Vasco/ ITSec gedaan?}{wellicht in h2?}
{samenvatting van email Vasco}
{samevatting Research report ITSec}
{Samenvatting Memo en incidentlogboek DigiNotar}

ITSec had een doosje staan die PCAPjes opsloeg van het externe verkeer. Die hebben we veiliggesteld/ gekopieerd. (van welke datums waren dat?)
We hebben 6 pcaps gedateerd van: 2011-08-25 t/m 2011-08-30. Het is intern verkeer, in de 172.x.x.x range, en 10.10.x.x
Er is in 1 pcap gekeken of er OCSP verkeer in voor kwam. wat niet het geval was.

3.1.1 Emergency response monitoring

One of the first measures that was taken by Fox-IT was to place our incident monitoring service [device?] within the DigiNotar intranet. This sensor captures and monitors all traffic between the intranet and the internet. Suspicious traffic can be detected by the sensor and all traffic [of alleen suspicious traffic?] will be stored on disk if evaluation is necessary. If suspicious traffic is detected it can be escalated to [X] if necessary so that further action can be taken. Examples of actions that can be taken are the blocking of an IP-address or IP-range or changing the rules on the firewall for specific ports. In this particular case a tailored OCSP responder monitoring service was added to the emergency sensor.

3.2 Safeguard evidence

{Het process van veiligstellen. Hoe hebben we dat gedaan, waarom e.d.}
Subsequently ["forensically sound"?] disk images were made by Fox-IT of the systems that were prone to be infected. Initially this process was restricted to the servers hosting the CA software and the firewall management system that contained the firewall logs. At the request of the Dutch police, the process was extended to include the creation of images of all the computer systems within the DigiNotar intranet. [On/after ...] it was decided that a disk image would not be created of every system [reden?]. A total of [xxx] images were created of [xxx] servers and [xxx] workstations that amount to [xxx] terabyte of data.

The items [=images?] that were produced as evidence were numbered with the prefix SVO, which refers to "Stuk Van Overtuiging" [English?]. References within this report to (images of) machines that can also service as evidence will be made using the function of the server. In appendix [x] an overview is included of all the server names that were used including their corresponding SVO-number and place [function?] within the network.

Fox-IT has rolled out its own infrastructure in order to examine all systems within the DigiNotar network live in a iterative and ["forensically sound"?] way. This infrastructure aided our researchers so that they could instantly use their research results to perform further research. The investigation was limited by the fact that if a system were to be shut down or be placed under a heavy load, it would have had impacted the production environment that was still in use by DigiNotar. For this reason a large number of systems could not be shut down during the investigation, which hindered the creation of images and meant that unauthorized software could have been active after the investigation was initiated [toegevoegd n.a.v. comments Daniel].

Een alternatief is het gezamelijke gebruik van de door ons opgezette infrastructuur (Encase Enterprise). Hierdoor zouden andere partijen door middel van een centraal systeem ook kunnen zoeken op machines, of images kunnen maken. Hierbij wel een opmerking. We maken hiervoor gebruik van de bestaadne netwerkinfrastructuur van DigiNotar, en die is slechts 100Mbit. Wanneer meerdere partijen hier tegelijk onderzoek op willen doen, of images van machines over willen maken heeft dat een zeer grote impact op de netwerkinfrastructuur. Op dit moment is dat zelfs voor ons onderzoek gedeeltelijk een beperkende factor in het uitzetten van zoekvragen, en het maken van images.

[Als er geen gebruik is gemaakt van dit alternatief hoeft het denk ik ook niet in het rapport, tenzij het is om uit te leggen waarom er niet voor het alternatief is gekozen?]

Oude web server 10.10.20.41 vermelden!

3.3 Investigation approach

Initially Fox-IT started an incident response investigation at the request of DigiNotar, with the aim of establishing to what extent which systems had been compromised. As of [date] the Dutch The Dutch Ministry of the Interior and Kingdom Relations took over the role of the client in regard to the investigation. The primary aim of the investigation that ensued was to determine if the CA severs that were used to issue qualified certificates and/or certificates for PKIOverheid had been compromised. A further aim of the ensuing investigation was to support the Dutch police in their investigation into the identity and location of the attacker(s).

The main strategy to accomplish this aim was to determine the extent to which servers within the DigiNotar network had been compromised and to identify IP-addresses and other evidence that could provide more information about the attacker(s). Once the information had been obtained that the security of the CA servers used for PKIOverheid and qualified certificates had been compromised by (in all probability) foreign attacker(s), the investigative stage of the involvement of Fox-IT was concluded. This report is the culmination of the incident response investigation that was performed at the request of both DigiNotar and the Ministry of the Interior and Kingdom Relations.

3.4 Actions taken

{uitleg voor de hoofdstukken daarna}
In the next chapters individual investigations of items are reported. They are sometimes incomplete or unfinished.

4 Investigation of CA managing software

4.1 conclusion

On 19-July-2011 the staff of DigiNotar realised something had gone wrong. After verifying the issued certificates with the administration some issued certificates lacked any records in the back office. Normally this verification is done daily by some automated process. This however failed to work for some time and was restored on the 19th. The staff of DigiNotar examined the CA managing applications and found fraudulently issued certificates. Their serial numbers were revoked immediately {ref to all certs.xls}. An incident response team was formed and further investigations were done. More rogue certificates were found and revoked on 21-July and on 27-July {ref to all certs.xls}. DigiNotar was convinced the hack was under control and the damage was repaired.

Later around 27-August-2011 however, another rogue certificate was found by users using the Google.com web site[10]. This certificate was not revoked before. A search though the management software did not reveal this serial number. In order to revoke the found misused *.google.com certificate a certificate was created with its serial number and then was revoked on 29-august-2011 16:58:47 {What timezone?}.

After a thorough search Fox-IT found that the number of issued rogue certificates in the log files exceeded the number of rogue certificates in the CA management application. This lead to the conclusion the CA software was manipulated and records were deleted. The log files record the distinguished name of the certificate but not its serial number. To revoke a certificate the serial number is essential. The revocation was therefore changed and based on the known valid certificates (whitelist method) at the advice of Fox-IT{ref H OCSP?}. As a result of further investigation on the database files a list of serial numbers was found that had no relation with any known issued certificates.

The situation existed where CA management software was clearly manipulated and no exact list of rogue certificates serial numbers could be produced. Therefore the only other measure that could be taken was to revoke the issuing CA certificates. That lead to the next investigation question: what CA should (or should not) be revoked? It was clear that the issuers of the found rogue certificates should be revoked since evidence was found that these CAs were misused. The untraceable serial numbers on some of the CA server raised suspicion against the CAs that were managed on that machine. Other investigations show that the operating systems of all CA servers were compromised and used by the attacker {even nalopen om zeker te weten! Ref naar Hxxx}. Additionally some CAs were continuously operational meaning that the private key in the netHSM was always usable for automated issuing of CRLs and certificates {TODO: lijstje maken van deze keys}.
No contraindicate was found that private CA keys were not or could not have been misused. The only additional barrier that existed for misuse by the attacker activation of the private CA keys. These CA keys are activated with a smartcard on the netHSM. If, for example an offline record was kept when these smartcards were present or removed a contraindication could be given that CA were not misused.

The overall conclusion is that all CA keys present at DigiNotar could have been misused and should not be trusted anymore.

The impact of this varies for each usage and should be assessed individually, however all DigiNotar certificates should be revoked and removed from any trust list. Additionally we advice to explicitly distrust any certificate managed or issued by DigiNotar unless a risk analysis convinces you otherwise. If in some use cases additional risk analysis shows no risk is run or the risk is accepted, pursue a system where the trust list is ignored whenever possible.

It was not easy for DigiNotar to produce an up-to-date overview of the CAs it operates and on what servers. In order to create an overview of the CAs and their hierarchy Fox-IT had to extract relevant information from the log files and the databases. This information helps users assess if they are using DigiNotar certificates.

[10] http://www.google.co.uk/support/forum/p/gmail/thread?tid=2da6158b094b225a&hl=en and the certificate on http://pastebin.com/ff7Yg663.

4.2 Introduction

In this chapter the results of the investigation of the managing CA software is described.

- How many certificates have been illegitimate issued? Identify the illegitimate issued certificates that have been created by the attacker(s).
- What were the serial numbers of the illegitimate issued certificates? In order to revoke the certificates the serials numbers must be known.
- What CAs are administered on what server? As is described in chapter 7 "System access, tools and files" {all?} the CA servers were compromised and the attacker had administrative access. To determine if the 'trust' of the CAs is compromised it must be known what CA was administered on what CA server.

Eight machines were investigated that operated as CA servers[11]:

- CCV-CA. [Voor de CA van CCV bestaan extra procedures en beveiligingsmaatregelen. De CA van CCV is een zogenaamde off-line CA. Standaard zijn de noodzakelijke services (programmatuur) uitgeschakeld. Het aanmaken en verspreiden van de certificaten gebeuren handmatig. Voor het opstarten van de services en het aanmaken van een nieuw certificaat zijn twee medewerkers en het gebruik van twee passen met pincode vereist. Deze passen worden na het afsluiten van het aanmaakproces verwijderd. CCV gebruikt de certificaten voor het initialiseren van pinbetaalautomaten voor de detailhandel. De certificaten zijn bij CCV geïnstalleerd op apparaten in de vestigingen van CCV, waarmee nieuwe en gereviseerde pinbetaalautomaten worden geïnitialiseerd en het dient voor het beveiligen van de informatie die wordt uitgewisseld bij het initialiseren van pinbetaalautomaten. Het gaat in totaal om enkele tientallen certificaten.]
- Nova-CA. Also called Orde-CA.
- Public-CA
- Qualified-CA.
- Relatie-CA
- Root-CA. Manages all the root CA certificates...
- Taxi-CA
- Test-CA

The CA servers had access to the nCipher netHSM {uitschrijven?} in the secure network segment (secure-net). The netHSM devices contain private key material in a secure way, so that the key material cannot leave the device. The private keys can only be used if a smartcard is presented to the HSM.

On the CA servers software from RSA (The Security Division of EMC) was installed in order to manage certificates. More specifically RSA offers the product RSA Certificate Manger (RSA CM)[12]. The CA software consists of several services. One of services provides a web interface for users and administrators. Another service logs the activity of the software into log files. The CA software also provides an application programming interface (API) that enables programmers to develop PKI applications. These applications can be developed using a scripting language called XUDA (Xcert Universal Database API) [controleren of dit de eerste keer is dat CA software wordt genoemd].

For the purpose of the investigation, Fox-IT used a list that was provided by DigiNotar which contained all the certificates that had been issued by DigiNotar. This list [alcerts.csv]{maak een ref in de ref lijst} was created by exporting the CA databases and contained the following information regarding the certificates that were issued by DigiNotar:

Value	Meaning
md5	The MD5 checksum of the certificate as calculated by the CA software
CA md5	The MD5 checksum of the issuing CA certificate
Serial nr.	The serial number of the certificate
Cert dn	The distinguished name field of the certificate
Valid from & valid until	The date fields of the certificate
Revocation date	The date of revocation (if applicable)

[11] Other systems found running CA managing software are WINVM012 and winvm032. No exhaustive search has been made to identify all the systems running CA software.
[12] Older versions of this software were named RSA Keon.

4.3 CA software log files

4.3.1 Sources/ content

All CA servers were outfitted with software that logged relevant information for the ongoing processes. The information was stored in log files that were in the format `xslog_{yyyyMMdd}.xml`. It appears that the log files were not being rotated or removed automatically and that a new log file was created whenever the machine was rebooted or when the (log) service was restarted. Given the timeframe during which the attacker was active, only the most significant log files were examined thoroughly.

The list of the investigated log files:

Name	Log files
CCV-CA	xslog_20110616.xml
Nova-CA	xslog_20110401.xml
Public-CA	xslog_20110325.xml xslog_20110711.xml xslog_20110711_1.xml
Qualified-CA	xslog_20110224.xml xslog_20110702.xml xslog_20110704.xml xslog_20110723.xml
Relatie-CA	xslog_20110407.xml
Root-CA	xslog_20110616.xml
Taxi-CA	xslog_20110517.xml xslog_20110711.xml
Test-CA	xslog_20110224.xml

Within the log files the integrity of blocks of data is secured using a signature. Using CA software the integrity of the log files can be checked. The integrity of the log files of all CA installations was verified by an DigiNotar employee. Two log files from the Public-CA failed the verification by the CA software:

- `xslog_20110711_1.xml`
- `xslog_20110720.xml`

The integrity of other log files is verified by the CA software without failure. The breached {?} integrity of `xslog_20110711_1.xml` conforms with a description that was found in the incident logbook [REF]. The logbook contains log entries that show that when the console on the Public-CA machine was started 20-Jul-2011 it was detected that rogue certificates were being issued and that the machine was shut down. The corresponding customary entries for "`Log Server Stopped`" and "`Final Entry`" are missing from this log file.

The entries in the log files contain the following information:

- `LOG_NUMBER`: a sequential unique log entry number
- `LOG_SOURCE`: the source of the log entry (either from the Certificate management Administration, Secure Directory or Logging Server)
- `EVENT_CONDITION`: either `ATTEMPT` or `COMPLETION` of an action
- `DATE,TIME`: the date and time of the entry {nazoeken welke timezone}
- `ID`: a hexadecimal value consisting of 32 characters (29 unique IDs have been encountered - 6 of these were encountered more than 100.000 times)
- `IP_ADDR`: the IP-address associated with the action (the following internal IP-addresses were mentioned: 127.0.0.1, 172.18.20.244, 172.18.20.245, 172.18.20.247, 172.18.20.249, 172.18.20.251, 172.18.20.252 and 172.18.20.253).
- `LOG_DATA`: the structure of this field varies depending on the data that it contains. A "Certificate signing" entry has the following fields:
  - `Succeeded` or `failed`
  - `Certificate presented`: an MD5-value of 32 characters for the certificates presented to the CA with the request
  - `certDN` with distinguished name fields
  - `MD5`-value of the certificate

- `Issuing CA MD5` – the serial number of the issuing or created certificate are not present in the log files.

4.3.2 Analysis

Qualified-CA
The log files of the qualified-CA have been briefly examined. The two succeeding log files `xslog_20110224.xml` and `xslog_20110702.xml` show the log server has been turned off on 2-July-2001 at 02:13:40 and turned back on again on 10:12:43. The log entries show automated CRL generation, automated back-up procedures. Several certificates have been issued what looks like ordinary certificates. No strange or remarkable log entries have been found.

Root-CA, Nova-CA and Test-CA
A brief examination of the log files show a regular automated CRL generation process and very few successful issued certificates. No strange or remarkable log entries have been found.

CCV-CA
The logs of the CCV-CA show no activity between 17-Juni-2011 and 22-July-2011.

Taxi-CA
The logs of the Taxi-CA show no activity between 16-Juni-2011 and 11-July-2011. No strange or remarkable log entries have been found.

Relatie-CA
The analysis of the log file `xslog_20110407.xml` on the Relatie-CA server shows that the first signs of extraordinary activity and certificate signing attempts occurred on 02-Jul-2011 at 19:59:34. The first successful rogue certificate was created on 10-Jul-2011 at 13:05:10 for *.google.com. In total 85 [alleen Relatie-CA?] rogue certificates are successfully created, all on 10-Jul-2011 between 13:05:10 and 23:35:54.

Public-CA
The analysis of the log file `xslog_20110325.xml` on the Public-CA server shows that the first signs of extraordinary activity and certificate signing attempts occurred on Sunday 03-Jul-2011 at 12:15:44. Between Thursday 07-Jul-2011 at 23:19:33 and Sunday 09-Jul-2011 at 12:53:16 is looks like experiments took place by the attacker outside office hours. During this time old certificate requests seem to have been reissued. For example "beveiligd.gemeentesudwestfryslan.nl" is issued twice with different CA keys.

On 10-Jul-2011 at 19:55:56 the first rogue certificate is issued (*.google.com). Between 10-Jul-2011 at 19:55:56 and 23:55:57 a total of 198 [alleen Public-CA?] rogue certificates were issued. The log server was stopped at 11-Jul-2011 at 01:41:19. The next log file `xslog_20110711.xml` starts at 11-Jul-2011 at 08:18:42 leaving a gap in the logs of about 7½ hours. This next log file contains only a few entries, most of them logging failed certificate signing attempts.

The next log file (`xslog_20110711_1.xml`) starts at 11-Jul-2011 11:24:49 probably after a reboot of the system or (log) service. On 18-Jul-2011 at 16:19:27 a burst of 124 rogue certificates were created. Another burst of 124 rogue certificates were generated on 20-Jul-2011 at 08:56:41. After this no other rogue certificate is found in the logs of the Public-CA server.

This log file is not properly terminated. The last log entry is on 20-Jul-2011 at 08:57:11. The next log file (xslog_20110720.xml) starts on 20-Jul-2011 at 12:19:37, has no entries and stops normally on 12:21:41. The next log file (xslog_20110720_1.xml) starts on 20-Jul-2011 at 12:34:52. No obvious suspicious activity is found in this log. The final entry is on 20-Jul-2011 18:20:14. After that all entries in the log files appear to relate to normal activity. The servers were shutdown daily.

A total number of 446 rogue certificates is issued between 10-Jul-2011 at 19:55:56 and 20-Jul-2011 at 08:57:11 on the Public-CA server.

4.4 Databases

The CA software used databases to store application data such as certificates. Several database files were stored in the directory `{install directory}\Xudad\db\`. The main database file was named `id2entry.dbh`. The main database file contained records of the certificates that had been issued with several characteristics. All the found `id2entry.dbh` database files were examined including any deleted ones.

During our investigation we came across database files named `serial_no.dbh`. These databases aroused our interests because the contained serial numbers. These database files contained certificate serial numbers. All the database files are in the Berkeley DB format.

4.4.1 Certificates

The certificates stored in the main database file have been extracted and converted into PEM (Privacy Enhanced Mail) format. The following methodology was used in order to do this:

- Perform a case insensitive search for the string `pem_x509::` in the `id2entry.dbh` files
- Extract the trailing data block
- Decode the text from its base64 format
- Encapsulate the text with `-----BEGIN PUBLIC KEY-----` and `-----END PUBLIC KEY-----`.

When the certificates were extracted in this way, some extracted data blocks were invalid. An attempt to read them with for instance OpenSSL will consequently result in an error. A quick (not exhaustive) investigation revealed that these incomplete blocks are indeed present in the database file and a complete version of these data blocks are also present in the database. This led us to conclusion that no certificates were missed using this method.

Additionally, some certificates were stored more than once in the database. Comparing the fingerprint of the certificates identified the duplicates. The incomplete and duplicate certificates were excluded from further analysis.

The following certificates were found:
{uitleggen; inclusief voor local gebruik.} {nazoeken hoe CA=TRUE attribute precies heet}
{deze tabellen kloppen niet!!!!}

	Root-CA	Qualified-CA	CCV-CA	Nova-CA
Total number of certificates	79	23621	63	78868
- **Unique subject name**	45	22483	33	75596
- **Different issuers**	10	13	12	15
- **CA=TRUE**	29	7	22	8
- **Self signed**	5	4	10	7

	Public-CA	Taxi-CA	Test-CA	Relatie-CA
Total number of certificates	46163	1357	3111	11671
- **Unique subject name**	44192	604	2088	11168
- **Different issuers**	17	20	32	work
- **CA=TRUE**	22	15	42	12
- **Self signed**	8	6	11	6

Details of these certificates are in Appendix II Certificate.

4.4.2 Private keys

The `id2entry.dbh` database files contained entries labelled `privatekey::`. After decoding the base64 data these entries showed the following asn.1 structure (example from the Root-CA):

```
 0:d=0  hl=2 l= 111 cons: SEQUENCE
 2:d=1  hl=2 l=   1 prim: INTEGER    :02
 5:d=1  hl=2 l=  19 prim: IA5STRING  :XCSP nCipher Native
26:d=1  hl=2 l=   1 prim: INTEGER    :53
29:d=1  hl=2 l=  64 prim: cont [ 0 ] :30 3E 16 0E 72 73 61 2D 6B 65 6F 6E 2D 63 61 2D  0>..rsa-keon-ca-
                                      36 38 16 10 31 33 30 38 32 32 33 37 36 30 33 32  68..130822376032
                                      37 30 30 30 16 11 53 45 43 55 52 45 20 4F 50 45  7000..SECURE OPE
                                      52 41 54 49 4F 4E 53 01 01 FF 02 01 02 02 01 04  RATIONS.........
```

```
95:d=1  hl=2 l=  16 prim: cont [ 1 ] :30 0E 80 01 01 81 01 00 04 06 02 04 84 8D A7 10  0.?.............
```

The decoded asn.1 structure led us to believe that these are references to private keys stored in the netHSM. If we assume this is the case, then we can conclude that the software installed on the server could use these keys.

In the data surrounding the private key entries there was no indication of the certificate or common name linked to these keys. However, directly following the private key entries a data block labelled `publickey::` is present. For the example above we have extracted the public key and matched it with the public keys of the extracted certificates. This resulted in the CA certificate with the common name '`CN=MinIenM Autonome Apparaten CA - G2`'. By following this method we were able to determine what CA servers had access to what private keys in the netHSM with its corresponding certificate.

In the list below some distinguished names (DN) can occur more than once. This is because different keys have been used for the same DN. This happens for example if a certificate is expired. Also note that for some keys no matching certificate was found.

{Deze moet nog worden na gekeken!!!}

Root-CA keys
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2

{Deze moet nog worden na gekeken!!!}

Qualified-CA keys
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl

{Deze moet nog worden na gekeken!!!}

CCV-CA keys
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=RSA CCV CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=RSA CCV CA System CA
/CN=ids CA
/CN=ids CA
No Certificate found
No Certificate found

{Deze moet nog worden na gekeken!!!}

Nova-CA keys
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl

/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association

{Deze moet nog worden na gekeken!!!}

Taxi-CA keys
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA
/CN=ids CA
No certificate found
No certificate found
No certificate found
No certificate found

{Deze moet nog worden na gekeken!!!}

Test-CA keys
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIOverheid CA Overheid en bedrijven
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL

/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/OU=TEST/CN=TEST Key Recovery CA
No certificate found
No certificate found
No certificate found
No certificate found

{Deze klopt}

Relatie-CA keys
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011
No certificate found

{deze klopt}

Public-CA keys
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA

When searching through the keys something interesting was discovered. Some keys that were found on the Root-CA system were also found on the Public-CA machine:
{moet ook nog weer nagekeken worden!!!}

Key fingerprint	DN
2611...	/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA
3092...	/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
9227...	/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
0c2c...	/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
3017...	/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
4ca3...	/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
5f31...	/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2
7f35...	/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2

This might indicate that private keys stored in the netHSM were available to the management software on both the Root-CA machine and to the Public-CA machine. Note the private key of the DigiNotar root CA is in this list.

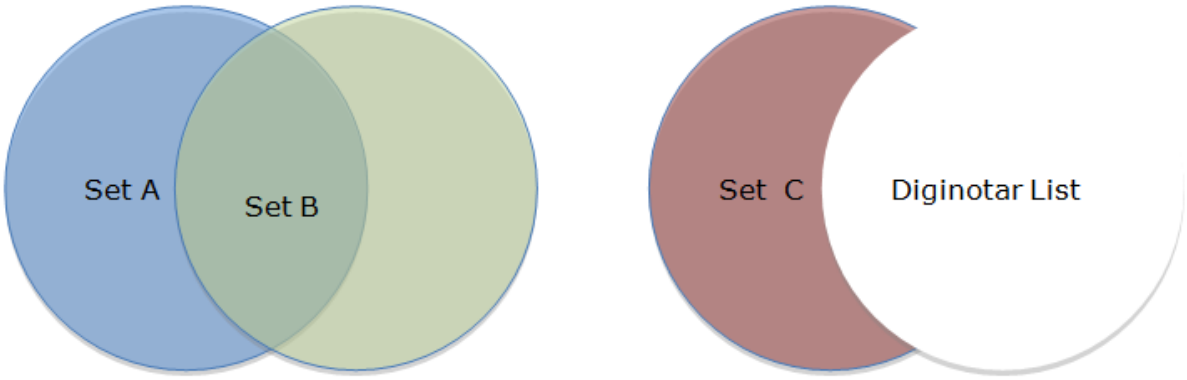
4.4.3 Serial numbers

The suspicion arose that the attacker(s) may have manipulated database and log files during the attack. The reason for this suspicion is that removed database files were discovered on multiple CA servers. For example the serial number that corresponds with the rogue wildcard certificate for the Google.com domain was only present in a `serial_no.dbh` database that had been removed.

The assumption is made that the `serial_no.dbh` database contained all serial numbers for certificates that had been issued by the CA software. To determine if serial numbers that correspond with rogue certificates were present, all `id2entry.dbh` and `serial_no.dbh` files were collected for each CA server, including all recoverable files that had previously been removed. It was investigated whether every serial number in the `serial_no.dbh` could be matched with an issued certificate.

In order to determine this, two sets of serial numbers were created. Set A included all serial numbers from all `serial_no.dbh` file. Set B includes serial numbers from all `id2entry.dbh` files. The difference between these list is determined by subtracting the set A and B. The resulting set are serials that are unknown serials. As an extra check these serials are matched against a list of issued certificates provided by DigiNotar.

{plaatje aanpassen! A=serial_no.dbh, B=id2entry.dbh, A is groter dan B, C is subset en geen intersection A^B; C = unknown}.



{naar conclusie stukje?}
For all the CA servers this method is applied. The results show unknown serial numbers by four out of the eight CA servers. A complete list of unknown serials for the CA servers can be found in appendix [...]. As a precautionary measure, all of the unknown serial numbers that remained were revoked.

CA server	Number of unknown serials
ROOT CA	7
R&A Qualified CA	2
TAXI CA	24
Public CA	203

It the time available for the investigation it could not be determined why this discrepancy existed between the databases. It could be due to software errors or as a result of aborted issuing process. However, because this was not concluded the difference in numbers remains suspicious and points more in the direction of misuse of the servers than the contrary.

4.5 Conclusion

It was not easy for DigiNotar to produce an up-to-date overview of the CAs it operates and on what servers. In order to create an overview of the CAs and their hierarchy Fox-IT had to extract relevant information from the log files and the databases.

4.5.1 CA activity {right title?}

For the purpose of this investigation, it was important to know what CAs were actively used on what servers. Since the servers generally hosted multiple CAs, the attacker(s) could gain access to all the CAs that were hosted on a specific server once access to that server was obtained.

As described, the issuing CA MD5 hash was logged when a certificate was signed. Having looked at the log entries for certificates that were successfully signed and searching for the private keys in the

databases we have conclude that the following servers were used to manage the following CAs (inclusive system CAs):
{van deze tabel klopt geen HOL!!! Issuing CAmd5 uit de logs klopt niet!!!}

CA server	Common name of issuing CA	Source	
		log	db
Public-CA	DigiNotar Services 1024 CA	X	TODO
	DigiNotar Public CA 2025	X	
	DigiNotar Public CA - G2	X	
	DigiNotar Services CA	X	
	DigiNotar Extended Validation CA	X	
	DigiNotar Cyber CA	X	
Orde-CA	DigiNotar Cyber CA		X
	DigiNotar Extended Validation CA		X
	DigiNotar Private CA		X
	DigiNotar Public CA 2025		X
	DigiNotar Public CA 2025 Administrative CA	X	X
	DigiNotar Public CA 2025 System CA		X
	DigiNotar Root CA	X	????
	DigiNotar Services 1024 CA		X
	DigiNotar Services CA		X
	Nederlandse Orde van Advocaten - Dutch Bar Association	X	X
	Orde van Advocaten SubCA Administrative CA		X
	Orde van Advocaten SubCA System CA	X	X
QC-CA	Algemene Relatie Services System CA	X	????
	DigiNotar PKIoverheid CA Organisatie - G2	X	????
	DigiNotar PKIoverheid CA Overheid en Bedrijven	X	????
	DigiNotar Qualified CA	X	X
	DigiNotar Qualified CA - G2		X
	EASEE-gas CA	X	????
	Hypotrust CA	X	????
	Koninklijke Notariele Beroepsorganisatie CA	X	????
	Ministerie van Justitie JEP1 CA	X	????
	Renault Nissan Nederland CA	X	????
	SNG CA	X	????
	Stichting TTP Infos CA	X	????
	TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2	X	????
	TU Delft CA	X	????
			Nog 6
Relatie-CA	Koninklijke Notariele Beroepsorganisatie CA	X	TODO
	Algemene Relatie Services System CA	X	
	TenneT CA 2011	X	
	Hypotrust CA	X	
	EASEE-gas CA	X	
	SNG CA	X	
	TU Delft CA	X	
	Ministerie van Justitie JEP1 CA	X	
	Stichting TTP Infos CA	X	
	Renault Nissan Nederland CA	X	
Root-CA	DigiNotar Root CA	X	X
	DigiNotar Root CA Administrative CA	X	X
	DigiNotar Root CA G2	X	X
	DigiNotar Root CA System CA	X	X

CA server	Common name of issuing CA	Source log	Source db
	MinIenM Autonome Apparaten CA - G2	X	X
	MinIenM Organisatie CA - G2	X	X
	MinIenM SIMULATOR NL Autonome Apparaten CA - G2		X
	MinIenM SIMULATOR NL Organisatie CA - G2		X
	MinIenM SIMULATOR NL Root CA - G2		X
	winsvr020		X
Taxi-CA	{no log entries found}		TODO
CCV-CA	CCV Group CA Administrative CA		X
	CCV Group CA System CA		X
	Prod SSL3 Client Root CA 2010 (O=CCV Jeronimo S.A.; C=CH)		X
	Prod SSL3 Server Root CA 2010 (O=CCV Jeronimo S.A.; C=CH)		X
	Prod UpLoad Root CA 2010 (O=CCV Belgium NV; SA; C=BE)		X
	Prod UpLoad Root CA 2010 (O=CCV Deutschland GmbH; C=DE)		X
	Prod UpLoad Root CA 2010 (O=CCV Jeronimo S.A.; C=CH)		X
	Prod UpLoad Root CA 2010 (O=CCV Services B.V.)		X
	RSA CCV CA Administrative CA		X
	RSA CCV CA System CA		X
	ids CA		X
			Nog2

4.6 Rogue Certificates

Based on the investigation of the log files and the databases a total number of 531 rogue certificates were found. These were identified as rogue because of the blatant distinguished name of the certificate. Certificates that were issued during the time the attacker was active on the CA servers are also suspected as fraudulent. Further investigation can determine this. For now they are discarded if the distinguished name of the certificate resembled valid certificates.

The number of rogue certificates grouped by issuer:

Issuer	Total	Unknown serial[13]	Cert.[14]	CA server
DigiNotar Cyber CA	108	1	107	
DigiNotar Extended Validation CA	98	14	84	
DigiNotar Public CA - G2	56	0	56	
DigiNotar Public CA 2025	184	183	1[15]	
Koninklijke Notariele Beroepsorganisatie CA	76	0		
Stichting TTP Infos CA	18	0		

{dit moet ook nog ergens worden opgenomen}{in dit hoofdstuk}
{
Zo te zien zijn alle IIS logs van de diginotar.nl server verwijderd voor 11 juli 2011… maar heeft ie daarna nog sporen achtergelaten. Ik zie nu zo snel 3 ip's:
67.202.50.234
77.104.76.97
85.17.182.207

Die 67 heeft net een andere useragent, das wel gek… doet ook maar 1 of 2 requests….
Nu het interesssante:

[13] Traces of these certificates were found in the logs and not in the databases.
[14] The certificate is found in the database.
[15] Certificate found by a Google.com user.

ex110711.log:2011-07-11 00:31:42 W3SVC1062701327 10.10.20.41 POST /Settings.aspx - 80 - 85.17.182.207 Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1)+Gecko/20100101+Firefox/4.0.1 200 0 0
ex110724.log:2011-07-24 13:16:48 W3SVC1062701327 10.10.20.41 GET /settings.aspx - 80 - 77.104.76.97 Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 200 0 0
ex110724.log:2011-07-24 13:16:53 W3SVC1062701327 10.10.20.41 POST /settings.aspx - 80 - 85.17.182.207 Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 200 0 0

mijn vermoeden:
11 juli, gewoon via proxy, nog met FF4
Tussentijd geüpgrade naar FF5
24 juli, vergeten proxy aan te zetten voor eerste request, daarna gelijk proxy aan….

77.104.76.97 is het IP-adres dat voor Yahoo cert een OCSP request deed…
}

5 Investigation of firewall logs

Within the DigiNotar infrastructure a central position was taken by the firewall. A CheckPoint appliance on a redundant Nokia IP390 platform with a separate management server was used for this purpose within the main infrastructure. A previously used redundant Sun firewall platform was also present in the network . At the co-location a firewall based on a Nokia appliance platform was present.

For reference a list of server names used in this chapter is included. A complete list is in Appendix I {references to equipment}.

Name	Server ID	IP	network

WINSRV007 (Bapi Database New; 172.17.20.4)
WINSRV155 (eHerkenning-AD; 10.10.20.134)
WINSRV108 (Website auth.pass.nl; 10.10.20.16)
WINSRV003 (CI - Source build server; 172.17.20.25)
WINSRV155 (eHerkenning-AD; 10.10.20.134)

5.1 Sources/ content

Fox-IT created an image of the disk of the firewall management server. In the lab a copy of the disk image was virtualised and the management station was accessed using the CheckPoint SmartConsole software. The log files were exported for further processing and examination.

The firewall management server contained all the log files from {TODO: nazoeken van welke firewalls?}. Accepted traffic connections as well as violations of firewall rules were logged, which resulted in up to 2 million log entries per day. The enormous amount of log data that was generated has great potential for tracing the attacker(s) steps, even though data mining on such a large amount of data is time intensive. The firewall is only able to connections between network segments it segregates. Traffic within a segment is not logged by the firewall.

During the investigation two kinds of log files from the firewall were examined: the traffic logs and the audit logs. The traffic logs contain the following fields:

- Timestamp
- 'Action' (accept/drop/reject/encrypt/decrypt/keyinst)
- Firewall interface name and traffic direction
- Firewall rule (name, ID and number)
- Source and destination IP and port
- Protocol
- ICMP (code and type)
- NAT (rule number, translated IP/port)
- DNS query
- VPN (scheme, method, peer gateway)
- TCP out of state, flags
- IPSec specification
- Attack info

The audit logs contains the following fields:

- Timestamp
- Object type
- Operation (log in/out, modify object, create object, et cetera)
- Administrator
- Changes (details of the operation, e.g. the changes applied to a rule)
- General information
- Subject
- Status

- Application

The timestamps of the firewall logs are based on the UTC timezone. {XXX: dit moet geverifieerd worden} [RK: "Ik dacht juist dat de timestamps 2 uur voor liepen? Kan alleen geen referentie meer vinden. Daniel heeft me dat verteld denk ik."] [DN: "Heb het niet op het systeem geverifieerd ofzo, ik zag gewoon dat de tijden van de webserverlogs 2 uur afweken van die van de firewall logs… dus welke goed zijn… dunno"]

5.2 Analysis

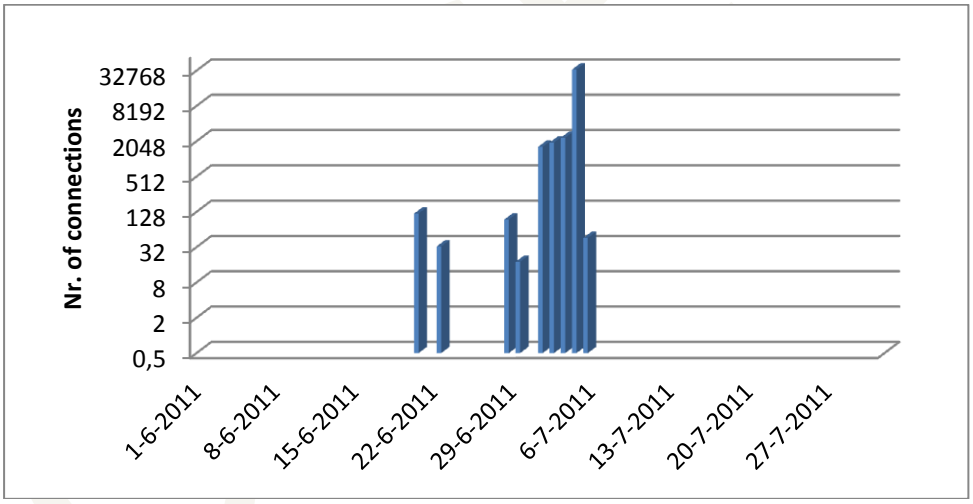
Due to time limitations the analysis of the firewall logs is not done in a very structural way.
Not all the fields in the log have been used in this investigation. Only the source and destination IP and port and the actions accept and drop have been used. The used logs are from 31-May-2011 23:51:57 up until 31-Jul-2011 23:51:36. The confiscated logs go further back in time.

5.2.1 Internet tunnels

In some of the tools an external IP addresses used by the attacker(s) was found. It was discovered that connections from the external DMZ network to this IP address were have taken place. Based on entries in the log files, the following connections from internal systems to external systems can be identified:

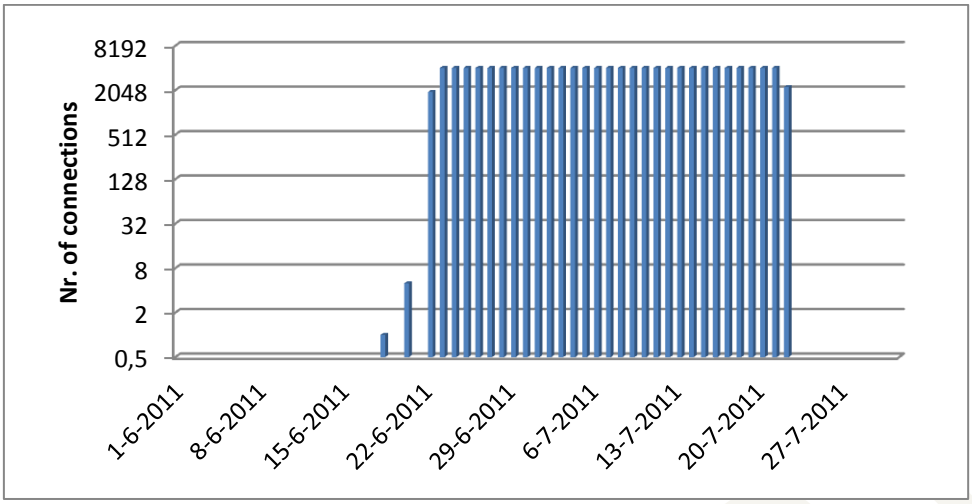
{opmaak}
{grafiekjes of tabelletjes?}

Connect-back from: WINSRV108 (Website auth.pass.nl; 10.10.20.16)
Connect-back to: AttIP1[16] port 443
Connections:

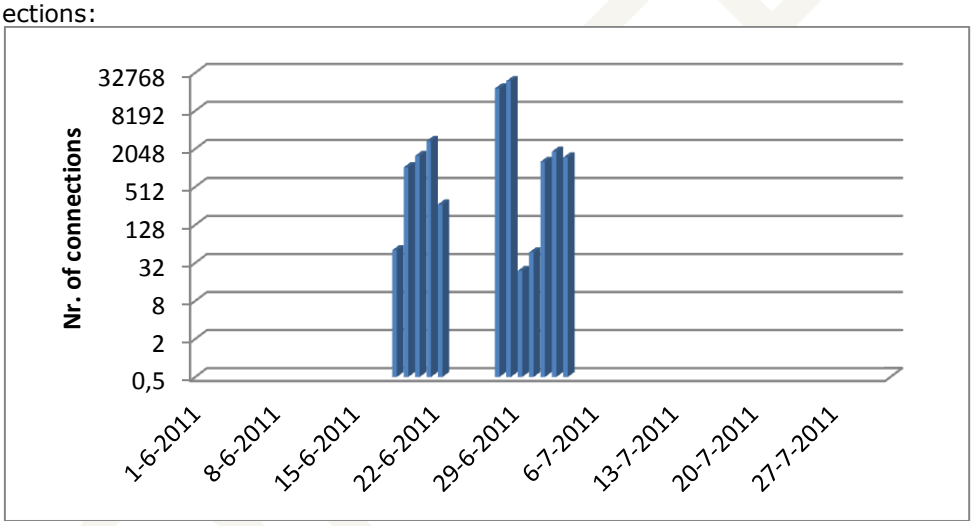


Connect-back from: WINSRV118 (DocProof 10.10.20.37)
Connect-back to: AttIP1 port 443
Connections:

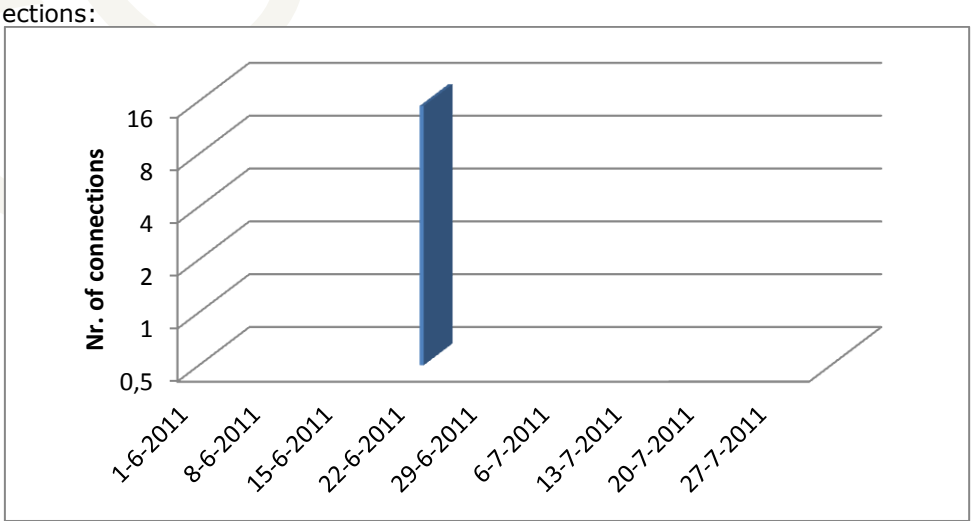
[16] The Internet IP addresses presumably used by the attacker are not included in the text. A reference ID is used and can be looked up in Appendix V-I "List of attackers IP addresses".



Connect-back from: WINSRV101 (main webserver; 10.10.20.46)
Connect-back to: AttIP1 port 443
Connections:



Connect-back from: WINSRV119 (DocProof; 10.10.20.65)
Connect-back to: AttIP1 port 443
Connections:



No connections were found originating from 10.10.20.41, 10.10.20.58, 10.10.20.134 or 10.10.20.139 to AttIP1:443.

{include a network picture: DMZ-ext –(tunnels)- internet - AttIP1}

5.2.2 Internal tunnels

A number of hacking tools were encountered and analysed, which is detailed in chapter 7.1.5. Some tools created a connect-back, that is making a connect back to a system that is controlled by the attacker(s). Analysis of the traffic log files of the firewall showed connect-back connections were initiated on the following dates:

{opmaak}

File name: Troj134.exe
Connect from: WINSRV007 (Bapi Database New; 172.17.20.4)
Connect to: WINSRV155 (eHerkenning-AD; 10.10.20.134) on port 443
Connections: 172.17.20.4 → 10.10.20.134:443

Date	Nr. of connections
2011-06-30	74522
2011-07-01	124510
2011-07-02	26351
2011-07-03	49021
2011-07-04	530
2011-07-05	11

File name: Troj172.exe
Connect from: WINSRV007 (Bapi Database New; 172.17.20.4)
Connect to: WINSRV108 (Website auth.pass.nl; 10.10.20.16) on port 443
Connections: 172.17.20.4 → 10.10.20.16:443

Date	Nr. of connections
2011-06-29	1

File name: Troj25.exe
Connect from: WINSRV003 (CI - Source build server; 172.17.20.25)
Connect to: WINSRV155 (eHerkenning-AD; 10.10.20.134) on port 443
Connections: None were found {wel dropped log entries?}

Please note that although the connections in the log files explicitly show a source and destination of the connection, files and commands could have been transported in either direction once a connection had been set up between these two systems.

{include a network picture: Office net –(tunnels)- DMZ-ext}

5.2.3 Tunnels from secure-net

It would seem that the servers located in the external DMZ acted as an intermediate hop between the internal network of DigiNotar and the internet. For this the attacker used at least tunnels over port 443 to connect between servers. Additional a search has been conducted for all connections to WINSRV155 (eHerkenning-AD; 10.10.20.134) on port 443. This showed connections were made from the Public-CA server in the Secure network to this server:

{opmaak}

Connections: 172.18.20.245 → 10.10.20.134:443

Date	Nr. of connections
2011-07-04	14
2011-07-05	1

This shows that a direct connection was made between the Secure network external DMZ. No other connections were seen to WINSRV155 on port 443 from the secure network between 31-May-2011 and 01-Aug-2011.

Subsequently all traffic originating from the secure network to other network segments on port 443 was examined. The log files show 2970 of the in total 3062 traffic connections originating from the Secure network segment to the external DMZ. More precise this traffic came from WINSRV130 (Application server (CAP web); 172.18.20.10) and WINSRV125 (Webserver (CAP web) 172.18.20.12) to the server cluster-prodpass (Cluster production Pass; 10.10.20.18/ 62.58.44.107). The traffic between these systems existed before and after the attack and was probably regular traffic. [hoezo 'regular' traffic tussen 'secure' en 'external DMZ'?].

If this traffic is ignored, this leaves 92 traffic connections of the 3062 that need further investigation. Out of these 92 connections, 54 relate to blocked traffic that originates from WINSRV056 (Public-CA; 172.18.20.245) on 2011-07-04 between 03:25 en 04:42. The blocked traffic was intended for the following IPs:

- AttIP1:443 (Attacker IP: refer to Appendix V-I)
- 10.10.20.35:443 WINSRV108 (Website auth.pass.nl)
- 10.10.20.37:443 unknown (not in server list {maak referentie})
- 10.10.2.139:443 unknown (not in server list - presumably a typing error made by the attacker).

Due to the time of the day these attempt were made it safe to assume the attacker had access to the Public-CA server during this time.

The remaining 38 out of the 92 connections relate to accepted traffic. These log entries show that direct connections were made from the Secure network segment to the external DMZ segment:

From	To	Nr. of conn.
WINSRV131 (SQL database (CAP); 172.18.20.11)	WINSRV101 (Old main website; 10.10.20.41)	5
WINSRV055 (Relations CA; 172.18.20.244)	WINSRV101 (Old main website; 10.10.20.41)	2
WINSRV056 (Public CA; 172.18.20.245)	WINSRV155 (eherkenning AD; 10.10.20.134)	15 [17]
WINSRV056 (Public CA; 172.18.20.245)	WINSRV157 (eHerkenning HM; 10.10.20.139)	7
WINSRV056 (Public CA; 172.18.20.245)	WINSRV108 (Website auth.pass.nl; 10.10.20.40)	3
WINSRV056 (Public CA; 172.18.20.245)	WINSRV101 (Old main website; 10.10.20.41)	2
WINSRV057 (Ccv CA; 172.18.20.246)	WINSRV101 (Old main website; 10.10.20.41)	2
WINSRV053 (Taxi CA; 172.18.20.251)	WINSRV101 (Old main website; 10.10.20.41)	2

{include a network picture: Office net –(tunnels)- DMZ-ext}

5.2.4 Network scan

Traffic from the secure network with the destination port 80 was examined. The following out of the ordinary entry was found:

2011-07-01 01:16:36 - drop - [tcp] 172.18.20.230:2404 -> 172.18.20.2:80

The entry concerns traffic within the Secure network segment, but which was still logged by the firewall. The reason for this is that the destination (172.18.20.2) is the firewall itself. This is the earliest suspicious log entry from the secure network segment, which occurred on 30-Jun-2011 at 23:16 CET {klopt dit?} (adjusted from the firewall log timestamp). After this point in time additional suspicious connections appear in the log files from other servers in the Secure network segment.

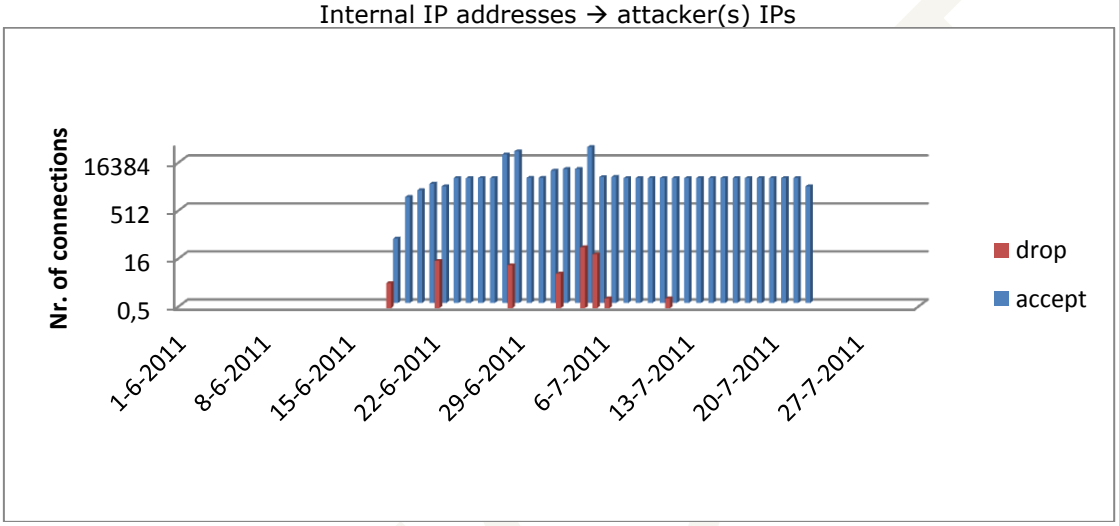
[17] As was seen in the previous analysis of connections to WINSRV155.

The data is consistent with the theory that the attacker first entered the secure segment on 172.18.20.230 and then conducted a services scan on the ports 80, 139, 443 and 445 within the subnet, which includes the firewall and thus resulted in the abovementioned log entry. {moet nog worden nagekeken?}

5.3 Connections to attackers IP

During the investigation a list of suspicious external IP addresses that was probably used by the attacker(s) was created. The complete list is included in Appendix V-I. The log entries regarding connections from internal IP addresses (10.x.x.x and 172.x.x.x) to these IP addresses in the firewall log files are visualized in the following graph:

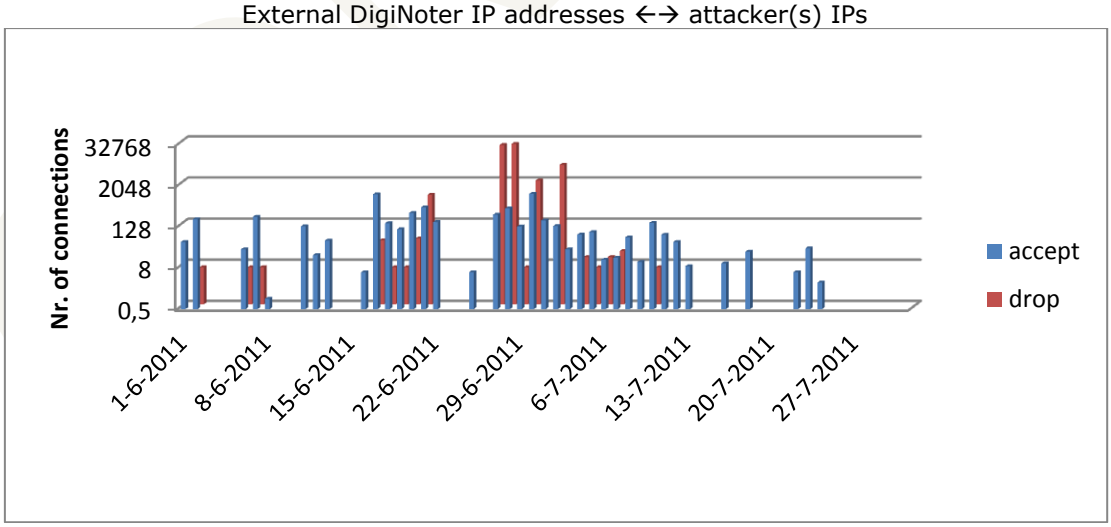
Internal IP addresses → attacker(s) IPs



This shows that on 18-Jun-2011 the first connections were made from internal IP addresses (10.10.20.46 and 10.10.20.37) to an IP-address that is known to have been used by the attacker(s).

The connection between the external IP addresses of DigiNotar (like 62.58.36.118) and the known attacker(s) IPs is shown the graph below.

External DigiNoter IP addresses ←→ attacker(s) IPs



This shows that from the earliest analysed firewall log entries (1-Jun-2011) the attacker IPs has accessed or probed DigiNotar systems or web sites. Without further analysis it is impossible to conclude that attack was started on or before 1-June. This traffic could also be normal web server traffic or hacking attempts from other attackers from the same IP addresses.

{toevoegen lijst van systemen die met AttIPs connective hebben gehad (heen of terug)}. Parelsnoer even expliciet noemen.}
{IP adrres dat al bekend was zat hier ook bij -> comodo hack}

5.3.1 Remarkable traffic

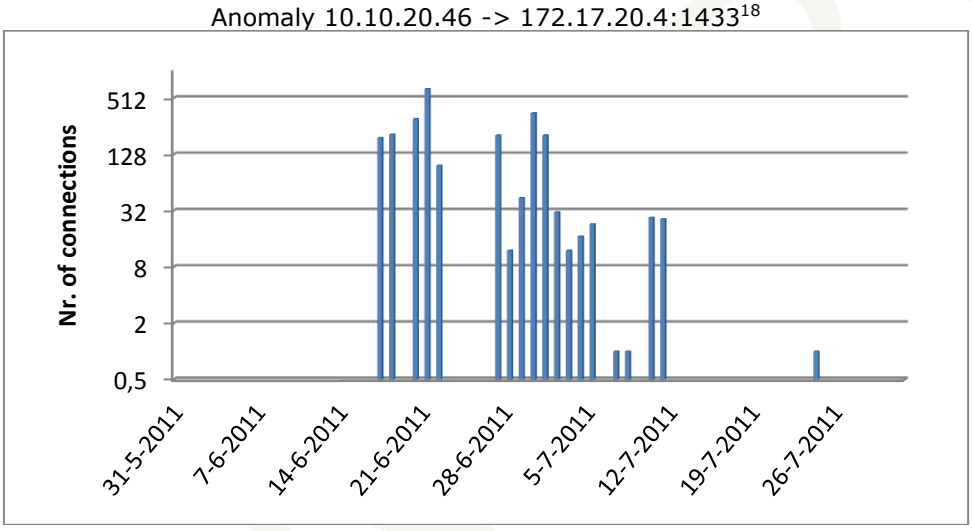
{NAZOEKEN of dit er al in staat…}{Uit de fw logs blijkt dat hij het KA-segment (172.17.20.*) is binnengekomen via de database server in dat segment.}

The firewall logs have been scanned for irregular traffic.

5.3.1.1 DMZext-net to Office-net

Normally no traffic should be initiated from the external DMZ network to the Office network. However as of 17-Jun-2011 11:28 accepted connections appear between WINSRV101 (main webserver; 10.10.20.46) and WINSRV007 (Bapi Database New; 172.17.20.4) port 1433 ({naam port}).

Anomaly 10.10.20.46 -> 172.17.20.4:1433[18]



This indicates the WINSRV007 was presumably attacked from WINSRV101 starting at 17-Juni-2011.

5.3.1.2 Old DMZ network

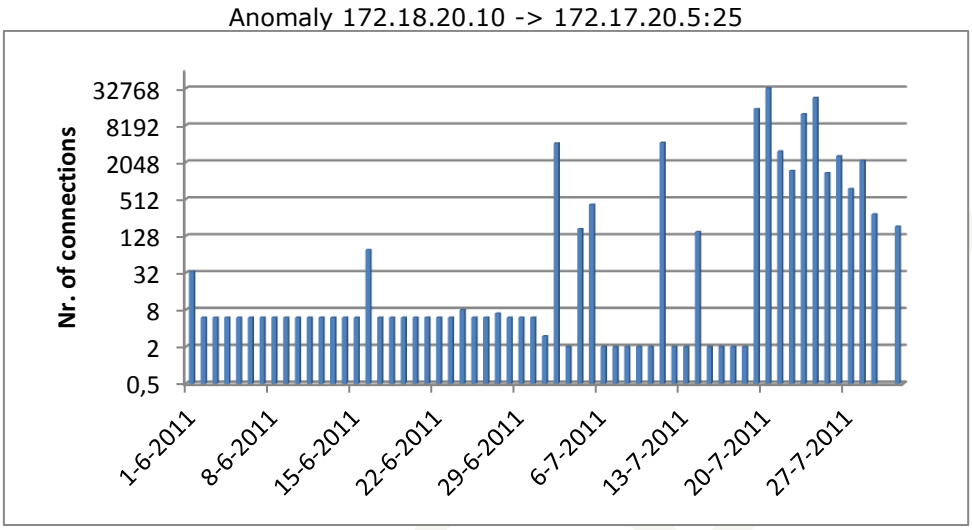
In the firewall logs scanning activity was discovered from the 10.10.20.46 in the external DMZ to 10.10.0.12 in the old DMZ:

```
2011-06-29 13:33:32 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:33:34 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:33:35 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:33:37 - accept - [tcp] 10.10.20.46:2506 -> 10.10.0.12:80
2011-06-29 13:34:03 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:34:05 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:34:06 - drop - [udp] 10.10.20.46:137 -> 10.10.0.12:137
2011-06-29 13:34:08 - accept - [tcp] 10.10.20.46:2510 -> 10.10.0.12:443
```

[18] Note the logarithmic scale. This emphasis the occurrence instead of the number of connections.

5.3.1.3 E-mail traffic

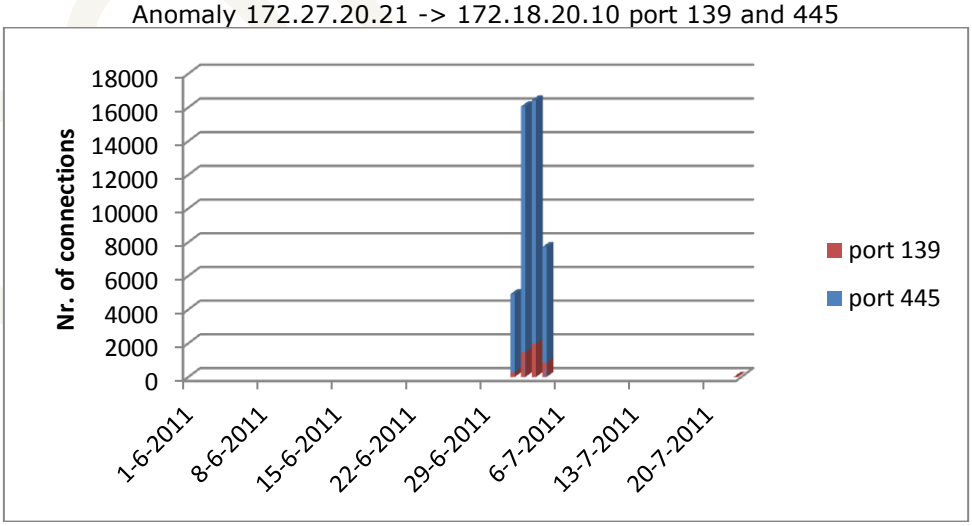
The firewall logs show unusual traffic with destination port 25 (SMTP) between WINSRV130 (Application server (CAP web); 172.18.20.10) in the Secure network segment and WINSRV126 (Exchange DigiNotar; 172.17.20.5) in the Office network segment. As port 25 is generally used for the purpose of e-mail, this indicated intensive e-mail traffic that normally does not occur in these quantities. The figure below illustrates the anomaly logarithmically:



The normal traffic on port 25 consists of six regular SMTP-connections each day at given intervals (four at 9:00 and two at 00:30) that probability originate from a scheduled task. After 30-Jun-2011 the regular connections at 09:00 cease to take place. Suddenly, in the night of 2-Jul-2011 about 4100 connections occurred. Then additional spikes of traffic occurred at 4, 5, 11 and 14-Jul-2011. Between 19 July until 29-July very large amounts of SMTP connections took place.

5.3.1.4 Co-location

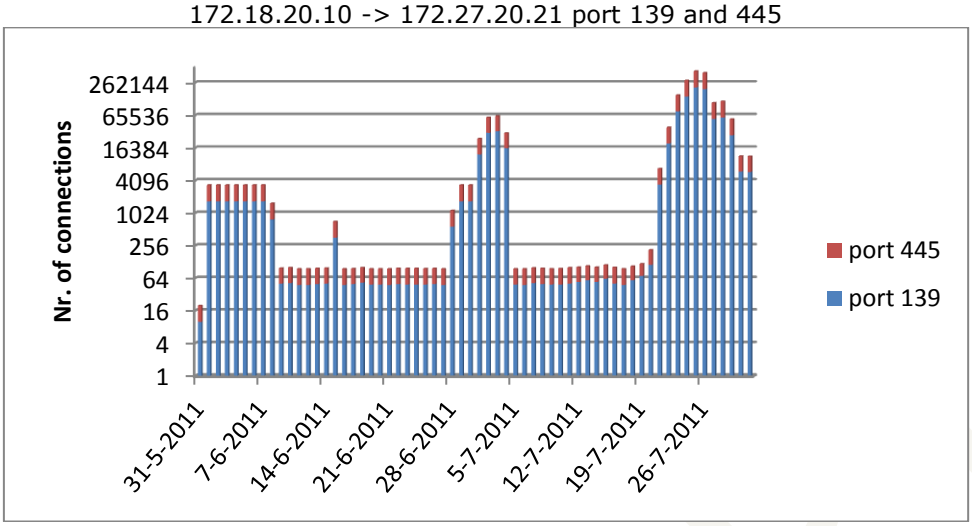
At the co-location suspicious (dropped) traffic was detected from the secure network segment and the main secure network. The traffic occurred between WINSRVUW05 (Administrator server - DNS; 172.27.20.21) and WINSRV130 (Application server (CAP web); 172.18.20.10) on ports 139 and 445.



This could indicate that the attacker(s) had access to the server WINSRVUW05 in the co-location from 1-Jul-2011.

The reverse connection (from the main to the co-located secure network segment) shows the following:

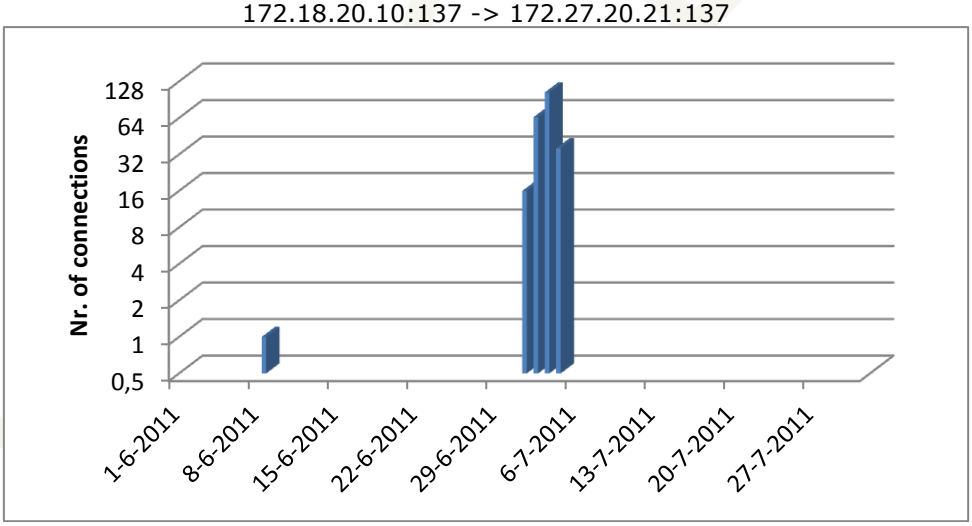
172.18.20.10 -> 172.27.20.21 port 139 and 445



This shows some regular traffic (approximately 50 packets per day) and some monthly traffic. The spikes during the first four days of July are anomalous. The traffic after 19-July is extreme when compared to the regular traffic, but could be explained by incident response activity.

Other noticeable traffic was discovered on port 137 during the first four days of July (in addition to a connection on 8-Jun-2011):

172.18.20.10:137 -> 172.27.20.21:137



5.4 Timeline

The following table contains a variety of noticeable log entries regarding anomalous traffic sorted by the date and time. {moet verder worden uitgezocht om er iets over te kunnen roepen...}

Attempts = all dropped connections to a specific IP and port combination
Discovery = multiple destination ports or IP addresses, dropped and accepted
{moet nog wat meer worden samengevat. Tabel kleiner maken?}
{verifiëren of bovenstaande er ook allemaal instaat!}

Time start	Time end	What	From srv	To srv	To port
2011-06-17					

Time start	Time end	What	From srv	To srv	To port
13:06:57	13:07:00	RDP attempts[19] from office net to admin net	digiws182	10.10.210.14	DRP
2011-06-28					
14:24:42	14:24:51	{139/ 445} attempts[20] from secure to colo-secure net	WINSRV053	172.27.20.21	139/445
2011-06-29					
11:56:15	11:56:24	RDP attempts from DMZ ext to Office net	WINSRV101	172.17.20.25	DRP
13:13:33	13:14:40	Network discovery from DMZ ext to Test net	WINSRV101	.35, .48	80,137
13:17:42	13:18:45	Network discovery from DMZ ext to DMZ int	WINSRV101	10.10.200.254	80,137, 443
13:20:52	13:21:05	Network discovery from DMZ ext to secure net	WINSRV101	172.18.20.254	137, 443
13:21:38	13:21:54	Network discovery from DMZ ext to Colo-Secure net	WINSRV101	172.27.20.254	137, 443
13:22:26	13:22:40	Network discovery from DMZ ext to Test net	WINSRV101	10.10.240.254	137, 443
13:26:06	13:26:23	Connection attempts from Office to Secure net	WINSRV007	172.18.20.10	80, 3389
13:26:22	13:26:35	Network discovery from DMZ ext to Secure	WINSRV101	172.18.20.10	80, 137
13:27:14	13:29:25	Connection attempts from Office to Secure net	WINSRV007	.10, .11	21, 1433, 135, 137
13:29:39	13:29:52	Network discovery from DMZ ext to Secure net	WINSRV101	172.18.20.11	137, 1433
13:29:50	13:30:03	Connection attempts from Office to Secure net	WINSRV007	172.18.20.11	80, 137
13:31:06	13:31:19	Network discovery from DMZ ext to Test net	WINSRV101	10.10.240.25	80, 137
13:33:32	13:34:08	Network discovery from DMZ ext to DMZ old	WINSRV101	10.10.0.12	80, 137, 443
13:40:40	13:40:44	Connection attempts from DMZ ext to Office	WINSRV101	172.17.20.164	137, 443
15:11:13	15:11:25	Strange?	172.17.20.8	172.18.20.230	139->4461
2011-06-30					
00:08:21	00:08:24	Some more attempts	10.10.20.134	172.17.20.4	137
00:16:34		Connect back home	10.10.20.134	AttIP2	443
00:36:46	00:41:37	Connection attempts from DMZ ext to Ofice net	WINSRV101	172.17.20.4	21, 80, 137
02:22:26	02:22:35	Failed RDP attempts	172.17.20.4	172.18.20.10	3389
02:22:56	02:23:38	Successful HTTP/HTTPS connections	172.17.20.4 172.17.20.7	172.18.20.10	80, 443
02:24:18	02:24:19	Connect back from Office db server to drop server @DMZ	172.17.20.4	10.10.20.134	443
02:25:10	02:26:59	Failed RDP/SQL attempts from the Office net	172.17.20.25 172.17.20.4	172.18.20.10 172.18.20.11	80, 137, 1433, 3389
02:28:31	02:28:40	{What's this??? Robbert?}	10.10.20.134	10.10.240.25	443
08:25:36	08:28:33	Appears a legitimate admin login	10.10.210.31	172.18.20.247	3389
10:39:59	10:40:29	Failed attempts	10.10.20.16	172.17.20.4	139, 445, 1433
13:22:05	13:22:15	conveniently FTP-ing from the DMZ (could be legal activity)	10.10.20.46	172.17.20.21	21
23:54:04	23:56:36	Unknown dropped activity	172.17.20.8:139	172.18.20.230	
2011-07-01					
01:15:30	01:15:38[21]	And again from another host	172.17.20.22:139	172.18.20.230	2400

[19] Probably not relevant for this attack.
[20] Probably not relevant for this attack since... {no traces on Taxi has been found before...?}
[21] From here on outgoing traffic exists originating from the CA network.

Time start	Time end	What	From srv	To srv	To port
2011-07-01					
01:16:15	01:17:16	Port scan on local segment.[22]	172.18.20.230	172.18.20.2	
01:17:22	01:19:49	Connect back attempts to the mgmt LAN	172.17.20.59 172.18.20.230	10.10.210.14	80, 139, 445
01:23:52	01:24:46	Possible failed psexec?	172.17.20.4:139	172.18.20.230	
18:00:56	18:02:26	Failed attempts	172.17.20.4	172.18.20.239	135, 319, 389
20:23:52	20:24:05	And again some time later	172.17.20.4	172.18.20.251	80,137
21:21:54	21:22:24	Possible failed psexec?	172.17.20.4:139	172.18.20.230	
22:52:47	23:40:45	Successful connections to DMZ drop	172.18.20.10	10.10.20.41	80
2011-07-02					
00:14:14	00:47:07	Successful connections to DMZ drop	172.18.20.10	10.10.20.41	80
01:48:42	01:48:42	And again	172.18.20.10	10.10.20.41	80
02:10:01	02:10:01	And again	172.18.20.10	10.10.20.41	80
02:10:01		First occurrence of many SMTP connections	172.18.20.10	172.17.20.5	25
02:18:36	02:18:36	Successful connections to DMZ drop	172.18.20.10	10.10.20.41	80
02:26:54	02:27:02	Strange port combinations	172.27.20.21:445	172.18.20.10:1433	
03:36:15	03:44:19	unsuccessful connections to public drop	172.18.20.247 [ICMP]	AttIP1{ref}	8/0 {???}
04:40:06	04:40:06	Successful connections to DMZ drop	172.18.20.247	10.10.20.41	80
05:37:05	05:48:56	Successful connections to DMZ drop	172.18.20.247	10.10.20.41	80
21:57:55	22:35:20	Successful connections to DMZ drop	172.18.20.247	10.10.20.41	80
{???}	{???}	VPN connection from administrator	10.10.40.32		
23:33:40	23:34:56	Admin working late?	10.10.210.32	172.18.20.11	1056,1433
23:35:57	23:35:57	Admin working late?	10.10.210.32	172.18.20.11	1433, 3389
2011-07-03					
00:14:48	00:14:48	Successful connections to DMZ drop	172.18.20.249	10.10.20.41	80
13:03:02	13:15:51	Successful connections to DMZ drop	172.18.20.245	10.10.20.41	80
16:51:36	16:54:06	Successful connections to DMZ drop	172.18.20.245	10.10.20.41	80
2011-07-04					
00:48:43	21:09:36	Successful connections to DMZ drop	172.18.20.245	10.10.20.41	80
2011-07-05					
00:15:40	00:18:26	Admin working late?	10.10.210.32	172.18.20.10	3389
15:09:35	21:09:36	Successful connections to DMZ drop at regular intervals. Automation in place?	172.18.20.245	10.10.20.41	80
2011-07-06					
15:09:36	21:09:36	Same. Automation in place?	172.18.20.245	10.10.20.41	80
2011-07-07					
15:09:36	21:09:36	Same. Automation in place?	172.18.20.245	10.10.20.41	80
22:58:18	22:58:27	Dropped ???	172.18.20.230	10.10.200.254	80
2011-07-08					
01:09:36	07:09:36	Successful connections to DMZ drop. Other interval.	172.18.20.245	10.10.20.41	80
2011-07-09					
01:09:36	07:09:36	Same.	172.18.20.245 172.18.20.10	10.10.20.41	80
10:05:32	10:06:03	Dropped ???	172.18.20.10	10.10.2.41	80

[22] Only the IP address of firewall itself is logged.

Time start	Time end	What	From srv	To srv	To port
10:06:07	23:34:59	Successful connections to DMZ drop.	172.18.20.10	10.10.2.41	80
2011-07-10					
00:00:14	00:26:24	Continued	172.18.20.10	10.10.2.41	80
01:09:36	01:09:37	Successful connections to DMZ drop.	172.18.20.245	10.10.2.41	80
01:24:36	01:24:36	Switching host	172.18.20.10	10.10.2.41	80
04:09:36	04:11:36	Successful connections to DMZ drop.	172.18.20.245 172.18.20.10	10.10.2.41	80
07:09:36	07:09:36	Same	172.18.20.245	10.10.2.41	80
10:01:04	23:57:55	Same	172.18.20.10	10.10.2.41	80
2011-07-11					
00:46:58	00:51:43	Same	172.18.20.245	10.10.2.41	80

From here on there are connections from 172.18.20.245:1385 to 10.10.20.41:80 at regular intervals at 01:09:36, 01:09:36 , 01:33:33 , 04:09:36 , 04:09:37 , 07:09:43 and 07:09:44 each day from 11-07-2011 up until 20-07-2011.

Time start	Time end	What	From srv	To srv	To port
2011-07-20					
16:46:50	16:47:30	Dropped connections. Incident response actions?	172.18.20.230	172.17.20.8	80
16:57:33	16:57:33	Successful connections to DMZ drop. Incident response actions?	172.18.20.230	172.17.20.8	80
2011-07-25					
18:50:52	19:10:08	Few days later. Successful connections to DMZ drop. Incident response actions?	172.18.20.245	10.10.20.41	80
19:10:37	19:13:05	Dropped connections to DMZ drop. Firewall adjusted.	172.18.20.245	10.10.20.41	80
2011-07-26					
09:09:14	09:09:23	Dropped connection. Incident response actions?	172.18.20.10	62.58.36.117	80
09:10:46	09:10:47	Accepted connections. Incident response actions?	172.18.20.25	62.58.36.117	80

5.5 Conclusion

{deze conclusive moet nog worden uitgebreid}
{dit stuk moet nog sterk gereviseerd worden}
It appears [was: presumably oftewel een aanname zonder feitelijke basis?] that files and/or commands were exchanged between the external DMZ and the Office network:

From Office	To DMZ-ext	Date first	Nr. Of conn.
WINSRV007	WINSRV155	2011-06-30	
WINSRV007	WINSRV108	2011-06-29	1

Furthermore suspicious connections were made directly between servers located in the Secure network segment and the external DMZ.

From Secure	To DMZ-ext	Date first	Nr. Of conn
WINSRV131	WINSRV101		
WINSRV055	WINSRV101		
WINSRV056	WINSRV155		
WINSRV056	WINSRV157		
WINSRV056	WINSRV108		
WINSRV056	WINSRV101		
WINSRV057	WINSRV101		
WINSRV053	WINSRV101		

This leads us to believe that the attacker(s) obtained access to the following servers:

DMZ-ext network
WINSRV101 (Old main website; 10.10.20.41)
WINSRV155 (eHerkenning AD; 10.10.20.134)
WINSRV157 (eHerkenning HM; 10.10.20.139)
WINSRV108 (Website auth.pass.nl; 10.10.20.40)
WINSRV101 (Old main website; 10.10.20.41)

Office network
WINSRV007 (Bapi Database New; 172.17.20.4)

Secure network
WINSRV131 (SQL database (CAP); 172.18.20.11)
WINSRV055 (Relations CA; 172.18.20.244)
WINSRV056 (Public CA; 172.18.20.245)
WINSRV057 (Ccv CA; 172.18.20.246)
WINSRV053 (Taxi CA; 172.18.20.251)

This indicates that the attacker(s) had access to the server WINSRVUW05 in the co-location between 1-Jul-2011 and 4-Jul-2011.

6 Investigation of web server logs

6.1 Sources/ content

Around 24-Jul-2011 {datum klopt niet!} the main web server of DigiNotar (www.diginotar.nl) had crashed. An employee of DigiNotar found traces that the WINSRV101 running the web server was used to by an attacker to save files on the web server. A new web server was installed on new hardware leaving the attacked server intact for further investigation.

During the incident response investigation that was performed by Fox-IT on the systems WINSRV053 and WINSRV022 traces were encountered that indicated these systems had connected to the web server WINSRV101. [OF even though dat niet de bedoeling is OF naar de specifieke directory /beurs]. Other systems within the network contained cached information originating from the directory `/beurs` on WINSRV101 (identifiable with the local IP-address 10.10.20.41) as is explained in chapter **Error! Reference source not found.**. An exact image of the disk the web server was created and investigated.

The directory `/beurs` was located at `D:\Websites\DigiNotar.nl\DigiNotarweb01\beurs` and was available locally at `http://10.10.20.41/beurs` and publicly at `http://www.diginotar.nl/beurs` {hoe weten we dat?}. When the directory `/beurs` was examined on WINSRV101 no files were present, but the traces on WINSRV053 and WINSRV022 indicated that files had been present in this directory.

The log files of the WINSRV101 webserver were subsequently examined in order to determine which internal and external systems had made a connection to the directory `/beurs` and what files they had accessed. The log files were stored in `C:\WINDOWS\system32\LogBestands\W3SVC1062701327\` and `C:\Data\Websites\Logging\W3SVC1062701327\` and are named `EX<JJMMDD>.log`. The log files have the following format:

```
2011-07-11 00:30:48 W3SVC1062701327 10.10.20.41 GET /beurs/settings.aspx - 80 -
83.96.129.78 Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1)+Gecko/20100101+Firefox/4.0.1 200 0 0
```

In a log entry such as the one above one can distinguish when a system identifiable by its IP-address made a connection to WINSRV101 (10.10.20.41) and which operating system and browser (`Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1`) were used. Furthermore one can distinguish the request that was performed (`GET /beurs/settings.aspx`) and if the webserver's response to this request (status OK `200`).

During the incident response investigation traces were found that a number of log files had been removed. It was not studied whether these files were manually deleted or automatically rolled over, as this was not the aim of the incident response investigation. [DN: Het was heel duidelijk dat de files verwijderd waren volgens mij… ik meen me te herinneren dat het precies de access logs van de hackperiode was… de error logs waren er namelijk nog wel.]

[hebben we ook nog IIS logs van docserver onderzocht?]

6.2 Analysis

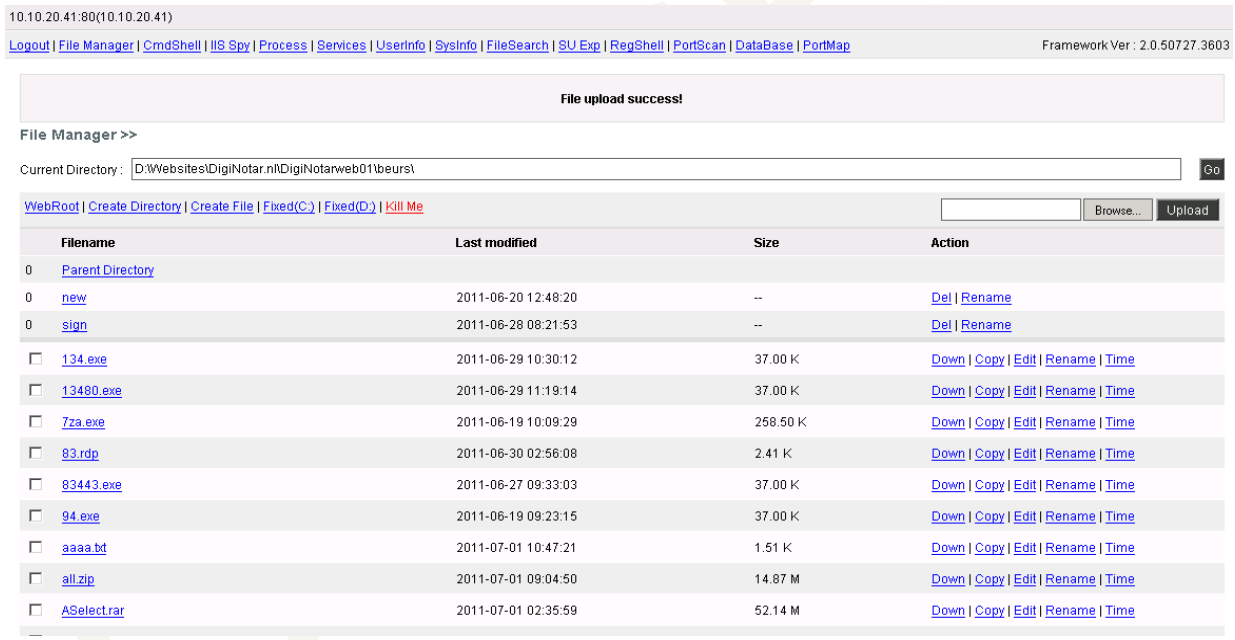
Since the removed log files had partially been overwritten the recovery software could not be used. Therefore, the `GREP` command {is 'carven' niet de term in F-land?} was used to probe the image of WINSRV101 for all text entries that contained the string `/beurs`, which allowed to include deleted portions of files that had not been overwritten. Based on the results of this query the following internal systems have connected to WINSRV101:

10.10.20.58		
10.10.200.20	WINSRV066	Docproof Database
172.17.20.4	WINSRV007	Bapi Database New

172.17.20.59		
172.17.20.7	DLX001	[P] Proxy (Squid)
172.17.20.8	WINSRV065	Kantoor Fileserver
172.18.20.10	WINSRV130	[P] Applicatieserver (CAP web)
172.18.20.11	WINSRV131	[P] SQL database (CAP)
172.18.20.244	WINSRV055	RSA Relatie CA
172.18.20.245	WINSRV056	RSA Public CA
172.18.20.246	WINSRV057	RSA Ccy CA
172.18.20.247	WINSRV167	RSA root CA
172.18.20.249	WINSRV022	RSA Qualified CA
172.18.20.251	WINSRV053	RSA Taxi CA

The IP-addresses of external systems that have accessed the directory /beurs are likely to have been utilize by the attacker(s) and are included in Appendix V-I. The list of IP addresses is not exhaustive, as a number of log files appear to have been overwritten. In total 25 unique external IP addresses have been found including AttIP2, AttIP3, AttIP4, AttIP6 and AttIP7 reference in other parts of this report.

Based on traces that were found on WINSRV053 and WINSRV022, one of the files that had been present in the directory `/beurs` on WINSRV101 is `settings.aspx`. Traces on other systems show that this file appears to have provided file manager functionality.



From the results of the `GREP`-command a list of files can be composed that have been present in the directory `/beurs` of the webserver WINSRV101 over time. The files Default.aspx and old_Default.aspx that were originally located in this directory were recovered in a backup that was made on 27-Aug-2011 and that was located at D:\Websites\BackUp\Diginotar01.old. The following list of 125 files is not exhaustive, as a number of log files appear to have been overwritten.

File name	File name	File name	File name
aaaa.txt	c.zip	darpi.zip	darv18.zip
all.zip	cachedump.exe	darv11.zip	darv19.zip
asdasd.zip	certcontainer.dll	darv12.zip	darv20.zip
aselect.rar	code.zip	darv13.zip	darv21.zip
bapi.zip	csign.zip	darv15.zip	darv22.zip
beurs.aspx	dar.rar	darv16.zip	darv23.zip
bin.zip	dar.zip	darv17.zip	darv24.exe

File name
darv24.zip
darv25.zip
darv26.zip
darv27.zip
darv28.exe
darv28.zip
darv29.zip
darv3.zip
darv30.zip
darv31.zip
darv33.zip
darv34.exe
darv34.zip
darv35.zip
darv36.zip
darv37.zip
darv38.zip
darv4.zip
darv5.zip
darv6.zip
darv7.zip
darv8.zip
darv9.zip
data.zip
dbpub.zip
Default.aspx

File name
Demonstraties/tabid/409/language/nl-NL/Default.aspx
Depends.exe
DigiNotar_Services_CA.cer
direct.exe
direct.zip
direct83.exe
elm.zip
ev-add.zip
f1.cer
final.zip
ids.zip
jobdone.zip
keo.zip
last.zip
lastdb.zip
lb.msi
ldap.msi
ldap.msi
md5s.txt
mimi.zip
mohem.zip
mswinsck.ocx
msxml6.msi
nc.exe
newjob.zip

File name
nfast.zip
nssl.zip
origrsa.zip
passadmin.rar
pki.zip
PortQry.exe
psexec.exe
putty.exe
PwDump.exe
qualifieddata.zip
Read1.exe
Read2.exe
Read3.exe
Repositories.zip
rsa_cm_68.zip
rsaservice.rar
saerts.zip.part1.txt
saerts.zip.part2.txt
saerts.zip.part3.txt
saerts.zip.part4.txt
settings
Settings.aspx
settings.aspxdepends.exe
settings.zip
sms.msi
SQLServer2005_SSMSEE.msi

File name
ssl.zip
tijdstempel.pfx
Troj25.exe
twitter.zip
up.aspx
USBDeview.exe
validate.zip
vcredist_x86.exe
webapp.zip
websign.rar
win.exe
win2.exe
win3.exe
z3.exe
z4.exe
z5.exe
Zip2.exe
zip3.exe
zipped.zip
Zipper.exe

6.2.1 Nog verwerken?

In H IIS logs opnemen:

winsrv119 (docproof)
2011-06-06 13:42:52
- mogelijk eerste verkenning (iis logs)

2011-06-14 14:27:30
- mogelijk tweede verkenning (iis logs)

{winsrv Beurs dir is voorheen niet gebruikt. (tekeningenetje van een tijdslijntje invoegen?)}

7 System access, tools and files

{dit hoofdstuk moet nog sterk gereviseerd worden; samenvatting maken van tabellen en tabellen naar bijlage}
The hard disk drives of a number of systems have been investigated for traces of the attack. Although this kind of investigation can be done on all the suspicious systems, only a few important systems were scrutinised:

- winsrv022 Qualified-CA
- winsrv053 Taxi-CA
- winsrv055 Relatie-CA
- winsrv056 Public-CA
- winsrv119 docproof
- winsrv167 Root-CA
- winsvr007 BAPI-db
- winsvr057 CCV-CA
- winsvr065 Office-fileserver
- winsvr101 Diginotar.nl-server

During the start of the investigation it quickly became clear that the attacker(s) used a web server in the external DMZ network as a steppingstone to transfer files. The browser history or temporary internet files is examined on the DigiNotar machines the attacker(s) used to connect to these web server file exchange location.

{ Zoek en vervang…: 'steppingstone' of 'file exchange location'}

To identify suspicious files the timestamps of the files on disk were examining. These timestamps indicate when a file is created, copied or modified. Together with the file location and file name a file can become suspicious and can cause reason to examine it further. Deleted files that could be recovered are also included in this investigation.

7.1.1 Temporary internet files

The temporary internet files of the Windows systems shows cached web pages of the file exchange location in the external DMZ network on winsrv101 (also in chapter 6). These cached pages show directory listing of file names with files size and modification date.

Besides cached html pages the temporary internet files also show cached files from the steppingstone web servers. These cached files are a result of a downloaded file. Files that are uploaded to the steppingstone can also be identified by the upload notification in the cached html pages. The temporary internet files also show what windows user accessed the web page or downloaded the file.

By searching the (deleted or not) temporary internet files for the file `settings[*].htm` (with * being a number) and inspecting the content of this file, a system can be identified as used by the attacker(s).

Of the investigated systems the following systems showed this cached page and therefore were used by the attacker:

Server	File name	User	Size	Create date	Create time[23]
BAPI-db	Settings[1].htm	Administrator	3097	1-Jul-2011	14:33:59
BAPI-db	Settings[1].htm	Administrator	90587	1-Jul-2011	14:34:57
BAPI-db	Settings[1].htm	Administrator	91912	1-Jul-2011	14:35:59
BAPI-db	Settings[1].htm	Administrator	93049	1-Jul-2011	14:38:44
BAPI-db	Settings[2].htm	Administrator	94254	1-Jul-2011	14:42:55
BAPI-db	Settings[2].htm	Administrator	95463	1-Jul-2011	14:43:30
BAPI-db	Settings[2].htm	Administrator	96638	1-Jul-2011	14:43:51
BAPI-db	Settings[2].htm	Administrator	97774	1-Jul-2011	14:58:11
Taxi-CA	Settings[1].htm	Administrator	104502	1-Jul-2011	22:14:31

[23] Universal Time zone.

Taxi-CA	Settings[1].htm	Administrator	105810	1-Jul-2011	22:14:49
Taxi-CA	Settings[1].htm	Administrator	105657	1-Jul-2011	22:26:30
Taxi-CA	Settings[2].htm	Administrator	107011	1-Jul-2011	22:27:44
Qualified-CA	settings[1].htm	Administrator.DNPRODUCTIE	102048	1-Jul-2011	23:48:43
Qualified-CA	settings[1].htm	Administrator.DNPRODUCTIE	102048	1-Jul-2011	23:48:43
Qualified-CA	settings[1].htm	Administrator.DNPRODUCTIE	109400	1-Jul-2011	23:50:05
Qualified-CA	settings[1].htm	Administrator.DNPRODUCTIE	109400	1-Jul-2011	23:50:05
Qualified-CA	settings[2].htm	Administrator.DNPRODUCTIE	110645	2-Jul-2011	0:12:30
Qualified-CA	settings[2].htm	Administrator.DNPRODUCTIE	110645	2-Jul-2011	0:12:30
Root-CA	Settings[1].htm	administrator.DNPRODUCTIE	3097	2-Jul-2011	2:40:06
Root-CA	Settings[1].htm	administrator.DNPRODUCTIE	3097	2-Jul-2011	2:40:06
Root-CA	Settings[1].htm	administrator.DNPRODUCTIE	111657	2-Jul-2011	2:40:13
Root-CA	Settings[1].htm	administrator.DNPRODUCTIE	111657	2-Jul-2011	2:40:13
Root-CA	Settings[1].htm	administrator.DNPRODUCTIE	112982	2-Jul-2011	2:41:00
Relatie-CA	SETtings[1].htm	Administrator.DNPRODUCTIE	3097	2-Jul-2011	20:35:21
Relatie-CA	SETtings[1].htm	Administrator.DNPRODUCTIE	100888	2-Jul-2011	20:35:30
Relatie-CA	SETtings[1].htm	Administrator.DNPRODUCTIE	102197	2-Jul-2011	20:36:11
Qualified-CA	settings[1].htm	Administrator.DNPRODUCTIE	3097	2-Jul-2011	22:14:48
Qualified-CA	settings[1].htm	Administrator.DNPRODUCTIE	103305	2-Jul-2011	22:15:48

The temporary internet files also showed activity on the locale CA software web service (all by the user Administrator.DNPRODUCTIE):

Server	File name	Size	Create date	Create Time
winsrv022	domain-main[3].htm	4162	1-Jul-2011	23:22:03
winsrv167	domain-main[1].htm	4162	2-Jul-2011	1:01:41
winsrv167	request-cacert[1].htm	27449	2-Jul-2011	1:05:47
winsrv167	cert-search-results[1].htm	26718	2-Jul-2011	1:06:36
winsrv167	view-cert[1].htm	13557	2-Jul-2011	1:07:17
winsrv167	domain-main[1].htm	4166	2-Jul-2011	1:08:38
winsrv167	request-msie[1].htm	233043	2-Jul-2011	1:08:45
winsrv167	add-msie-request[1].htm	7332	2-Jul-2011	1:10:03
winsrv167	cert-search-results[1].htm	2309	2-Jul-2011	1:11:23
winsrv167	view-cert[1].htm	15164	2-Jul-2011	1:11:52
winsrv167	MinIenM Organisatie CA - G2[1].p7b	5239	2-Jul-2011	1:12:42
winsrv167	cert-search-results[1].htm	3711	2-Jul-2011	1:15:56
winsrv055	cert-search-script[1]	20027	2-Jul-2011	20:42:08
winsrv055	cert-search-results[5].htm	58415	2-Jul-2011	20:43:29
winsrv055	view-cert[1].htm	13654	2-Jul-2011	20:43:43
winsrv055	index[2].htm	5291	2-Jul-2011	21:20:20
winsrv055	cert-search[1].htm	11192	2-Jul-2011	21:20:30
winsrv055	cert-search-script[1].htm	19411	2-Jul-2011	21:20:30
winsrv055	cert-search-results[4].htm	340	2-Jul-2011	21:22:25
winsrv055	cert-search-results[6].htm	9966	2-Jul-2011	21:37:08
winsrv055	get-ca-list[3].htm	3071717	2-Jul-2011	21:51:22
winsrv055	get-ca-list[2].htm	3071717	2-Jul-2011	21:54:12
winsrv055	index[1].htm	2525	2-Jul-2011	21:55:49
winsrv055	get-ca-list[5].htm	332	2-Jul-2011	21:55:57

The temporary internet files also show downloaded files and other unspecified pages:

Server	File name	User	Size	Create Date	Create time
winsvr007	$I30	MSSQLusr	4096	10-Nov-2008	8:26:34
winsvr007	$I30	MSSQLusr	4096	10-Nov-2008	8:26:34
winsvr007	$I30	MSSQLusr	4096	10-Nov-2008	8:26:34
winsvr007	KH6BWL27	MSSQLusr	56	10-Nov-2008	8:26:34
winsvr007	S5A38DAJ	MSSQLusr	56	10-Nov-2008	8:26:34
winsvr007	W9IJGHEF	MSSQLusr	56	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34

winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	index.dat	MSSQLusr	49152	10-Nov-2008	8:26:34
winsvr007	desktop.ini	MSSQLusr	67	10-Nov-2008	8:26:34
winsvr007	kir[1].txt	MSSQLusr	9	17-Jun-2011	16:15:49
winsvr007	libeay32[1].dll	MSSQLusr	1017344	17-Jun-2011	16:18:44
winsvr007	PwDump7[1].exe	MSSQLusr	77824	17-Jun-2011	16:19:21
winsvr007	PwDump[1].exe	MSSQLusr	393216	17-Jun-2011	18:56:01
winsvr007	7za[1].exe	MSSQLusr	264704	17-Jun-2011	19:33:55
winsvr007	mswinsck[1].ocx	MSSQLusr	127808	17-Jun-2011	19:41:31
winsvr007	base64[1].exe	MSSQLusr	45056	18-Jun-2011	0:34:05
winsvr007	test[1].zip	MSSQLusr	2666	18-Jun-2011	5:11:53
winsvr007	mstsc[1].exe	MSSQLusr	407552	18-Jun-2011	14:46:46
winsvr007	mstscax[1].dll	MSSQLusr	655360	18-Jun-2011	14:47:28
winsvr007	clxtshar[1].dll	MSSQLusr	69632	18-Jun-2011	14:47:51
winsvr007	tclient[1].dll	MSSQLusr	68096	18-Jun-2011	14:48:29
winsvr007	test2[1].zip	MSSQLusr	2666	18-Jun-2011	14:53:55
winsvr007	nc[1].exe	MSSQLusr	65028	20-Jun-2011	10:34:15
winsvr007	demineur[1].dll	MSSQLusr	151552	20-Jun-2011	11:14:09
winsvr007	klock[1].dll	MSSQLusr	153600	20-Jun-2011	11:14:27
winsvr007	mimikatz[1].exe	MSSQLusr	368128	20-Jun-2011	11:15:40
winsvr007	sekurlsa[1].dll	MSSQLusr	200704	20-Jun-2011	11:15:51
winsvr007	cachedump[1].exe	MSSQLusr	45056	21-Jun-2011	12:50:00
winsvr007	PwDump[1].exe	MSSQLusr	393216	21-Jun-2011	13:09:47
winsvr007	mswinsck[2].ocx	MSSQLusr	127808	21-Jun-2011	13:46:33
winsvr007	uploader[2].exe	MSSQLusr	28672	21-Jun-2011	14:18:15
winsvr007	uploader[1].exe	MSSQLusr	28672	21-Jun-2011	15:07:23
winsvr007	up3[1].exe	MSSQLusr	28672	21-Jun-2011	15:21:03
winsvr007	sfk[1].exe	MSSQLusr	1155072	21-Jun-2011	19:53:15
winsvr007	ReadF[1].exe	MSSQLusr	8192	22-Jun-2011	8:41:06
winsvr007	Read1[1].exe	MSSQLusr	9728	22-Jun-2011	10:26:02
winsvr007	Read2[1].exe	MSSQLusr	9728	22-Jun-2011	10:46:20
winsvr007	Read3[1].exe	MSSQLusr	9728	22-Jun-2011	12:17:29
winsvr007	Read4[1].exe	MSSQLusr	9728	22-Jun-2011	12:20:09
winsvr007	Read5[1].exe	MSSQLusr	10240	22-Jun-2011	12:34:28
winsvr007	PortQry[1].exe	MSSQLusr	143360	29-Jun-2011	9:44:53
winsvr007	troj172[1].exe	MSSQLusr	61440	29-Jun-2011	22:13:34
winsvr007	troj172[1].exe	MSSQLusr	61440	29-Jun-2011	22:13:34
winsvr007	troj134[1].exe	MSSQLusr	61440	29-Jun-2011	22:18:17
winsvr007	troj134[1].exe	MSSQLusr	61440	29-Jun-2011	22:18:17
winsvr007	134[1].exe	MSSQLusr	37888	29-Jun-2011	22:30:33
winsvr007	RunAs[1].exe	MSSQLusr	24576	29-Jun-2011	22:52:25
winsvr007	RDP[1].exe	MSSQLusr	553472	29-Jun-2011	23:01:49
winsvr007	13480[1].exe	MSSQLusr	37888	29-Jun-2011	23:19:32
winsvr007	Troj25[1].exe	MSSQLusr	61440	1-Jul-2011	13:45:18
winsvr007	psexec[1].exe	MSSQLusr	381816	1-Jul-2011	19:12:25
winsvr007	mimi[1].zip	MSSQLusr	477545	1-Jul-2011	22:15:25
winsrv053	mimi[1].zip	Administrator	477545	1-Jul-2011	22:15:49
winsrv022	172.18.20[1].htm	Administrator.DNPRODUCTIE	4867	1-Jul-2011	23:20:51
winsrv053	winsvr130[1].htm	Administrator.DNPRODUCTIE	476	2-Jul-2011	0:53:44
winsrv167	corner[2].gif	administrator.DNPRODUCTIE	3196	2-Jul-2011	1:00:58
winsrv167	enrollbg[4].gif	administrator.DNPRODUCTIE	558	2-Jul-2011	1:00:58
winsrv167	icontrol[1].vbs	administrator.DNPRODUCTIE	35007	2-Jul-2011	1:08:45
winsrv167	up[1]	administrator.DNPRODUCTIE	3415	2-Jul-2011	1:24:31
winsrv167	favicon[1].ico	administrator.DNPRODUCTIE	3878	2-Jul-2011	2:40:06
winsvr007	ldap[1].msi	MSSQLusr	14297088	2-Jul-2011	18:41:27
winsrv055	get[1].htm	Administrator.DNPRODUCTIE	323	2-Jul-2011	20:57:35
winsrv055	banner[1].htm	Administrator.DNPRODUCTIE	6143	2-Jul-2011	21:55:49
winsrv055	172.18.20[1].htm	Administrator.DNPRODUCTIE	5291	2-Jul-2011	21:59:01
winsrv055	172.18.20[1]	Administrator.DNPRODUCTIE	5692	2-Jul-2011	21:59:34
winsvr007	direct[1].exe	MSSQLusr	37888	3-Jul-2011	23:40:23
winsvr007	direct[1].zip	MSSQLusr	19702	4-Jul-2011	1:06:00

winsrv053	direct[1].zip	Administrator.DNPRODUCTIE	19702	4-Jul-2011	4:18:39

7.1.2 Recent files

A number of recent used files were marked as suspicious because of the after office hours activity or activity by users normally not active. These recent files indicate these files were opened or accessed.

Server	File name	User	Size	Create date	Create time
winsvr101	Nieuw - Tekstdocument.txt.lnk	Administrator	872	20-Jun-2011	2:15:43
winsvr007	pki.zip.lnk	Administrator	424	1-Jul-2011	14:58:07
winsvr007	DARPI.lnk	Administrator	941	1-Jul-2011	16:13:07
winsrv053	Desktop.ini	Administrator	150	1-Jul-2011	22:32:39
winsrv053	Recent	Administrator	152	1-Jul-2011	22:32:39
winsrv022	certs.lnk	Administrator.DNPRODUCTIE	598	1-Jul-2011	23:29:57
winsrv022	ssl.crt.lnk	Administrator.DNPRODUCTIE	720	1-Jul-2011	23:29:57
winsrv022	root.crt.lnk	Administrator.DNPRODUCTIE	725	1-Jul-2011	23:31:45
winsrv022	cas.crt.lnk	Administrator.DNPRODUCTIE	720	1-Jul-2011	23:32:06
winsrv022	a.crt.lnk	Administrator.DNPRODUCTIE	736	1-Jul-2011	23:35:35
winsrv022	qualifiedData.zip.lnk	Administrator.DNPRODUCTIE	448	2-Jul-2011	0:09:57
winsrv022	qualifiedData.zip.lnk	Administrator.DNPRODUCTIE	448	2-Jul-2011	0:09:57
winsrv167	MinIenM Organisatie CA - G2.p7b.lnk	administrator.DNPRODUCTIE	560	2-Jul-2011	1:12:54
winsrv167	httpd.conf.lnk	administrator.DNPRODUCTIE	696	2-Jul-2011	2:13:05
winsrv167	dist.lnk	administrator.DNPRODUCTIE	531	2-Jul-2011	2:27:17
winsrv167	schema.conf.lnk	administrator.DNPRODUCTIE	677	2-Jul-2011	2:27:49
winsrv167	iXudad.conf.lnk	administrator.DNPRODUCTIE	677	2-Jul-2011	2:29:19
winsrv167	xudad.oc.conf.lnk	administrator.DNPRODUCTIE	683	2-Jul-2011	2:30:43
winsrv167	origrsa.zip.lnk	administrator.DNPRODUCTIE	416	2-Jul-2011	2:40:26
winsrv167	CertiID Enterprise Certificate Authority.crt.lnk	administrator.DNPRODUCTIE	804	2-Jul-2011	2:48:45
winsrv167	muh.lnk	administrator.DNPRODUCTIE	571	2-Jul-2011	2:48:45
winsrv167	USPP-Perso Certificate ST4000 260-160-364.crt.lnk	administrator.DNPRODUCTIE	879	2-Jul-2011	2:50:20
winsrv167	certs.lnk	administrator.DNPRODUCTIE	631	2-Jul-2011	2:50:20
winsrv055	dbpub.zip.lnk	Administrator.DNPRODUCTIE	404	2-Jul-2011	20:35:41
winsrv022	m.zip.lnk	Administrator.DNPRODUCTIE	380	2-Jul-2011	22:15:28
winsrv056	Desktop.ini	Admin1[24]	150	4-Jul-2011	0:05:17

7.1.3 Other local settings files

A great number of other files were found in the local settings of the Windows user. These files could relate to activity by the attacker.

{admin names vervangen!}

Server	File name	Full path	Size	Create date	Create time
winsvr007	S-1-5-21-2196791791-1123517030-1950105499-500	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-2196791791-1123517030-1950105499-500\	256	30-Jan-2006	11:44:01
winsrv056	$I30	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\$I30	4096	20-Jul-2010	12:55:21
winsrv056	Microsoft	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\	56	20-Jul-2010	12:55:21

[24] The real username is replaced by a pseudonym to protect the privacy of the personnel of DigiNotar. The real usernames are in the confidential Appendix V-II.

winsrv056	Application Data	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\ljensma\Local Settings\Application Data\	472	17-Jun-2011	14:05:22
winsvr007	Credentials	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-2196791791-1123517030-1950105499-500\Credentials	346	1-Jul-2011	14:46:46
winsrv053	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\index.dat	49152	2-Jul-2011	0:53:44
winsrv053	MSHist012011061320110620	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\	152	2-Jul-2011	0:53:44
winsrv167	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\index.dat	32768	2-Jul-2011	1:00:58
winsrv167	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070220110703\index.dat	32768	2-Jul-2011	1:00:58
winsrv167	MSHist012011061320110620	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\	152	2-Jul-2011	1:00:58
winsrv167	MSHist012011070220110703	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070220110703\	152	2-Jul-2011	1:00:58
winsrv167	Dr Watson	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\	264	2-Jul-2011	2:18:56
winsrv167	Dr Watson	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\	264	2-Jul-2011	2:18:56
winsrv167	drwtsn32.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\drwtsn32.log	203258	2-Jul-2011	2:18:56
winsrv167	drwtsn32.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\drwtsn32.log	203258	2-Jul-2011	2:18:56
winsrv167	user.dmp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\user.dmp	90852	2-Jul-2011	2:18:56
winsrv167	user.dmp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\user.dmp	90852	2-Jul-2011	2:18:56
winsrv167	{51503BD7-A456-11E0-941C-D48564505644}.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Last Active\{51503BD7-A456-11E0-941C-D48564505644}.dat	70144	2-Jul-2011	2:52:26
winsrv055	UserImages.bmp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\Application Data\Softerra\LDAP Browser 4\UserImages.bmp	9014	2-Jul-2011	21:46:30
winsrv056	Terminal Server Client	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Terminal Server Client\	144	4-Jul-2011	4:11:29
winsrv053	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011062720110704\index.dat	32768	4-Jul-2011	4:19:23
winsrv053	index.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070420110705\index.dat	32768	4-Jul-2011	4:19:23
winsrv053	MSHist012011062720110	Partition 1\NONAME [NTFS]\[root]\Documents and	152	4-Jul-2011	4:19:23

	704	Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011062720110704\			
winsrv053	MSHist012011070420110705	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070420110705\	152	4-Jul-2011	4:19:23

7.1.4 Other files

A great number of other files were found on the examined servers. These files could relate to activity by the attacker. This list is in Appendix V Suspicious files.

7.1.5 Tools

Several suspicious tools and files were discovered during the investigation. First, they were found in the web server logs of winsrv101 that showed a list of file names that were uploaded or downloaded by the attacker(s) (refere to chapter 6). Second, in the browser history or temporary internet files on the machines the attacker(s) used to connect to these web server hops. And last, the timestamp of the files on disk indicated suspicious usage of these files.

7.1.5.1 Back connect

A few files that were examined more closely produce a network connection tunnel between two IP addresses if executed. The IP addresses are 'hard coded' in the executable. This and the fact the creation time {build time?} made us believe the files are especially created to run in the DigiNotar network. These back connect files create an encrypted {is dat ook zo?} tunnel (a VPN) between two systems making it possible to transfer files and commands {is dat ook zo?} and to execute for example remote desktop connection between on a server. Also, the tunnel made it possible for the attacker to gain access to the systems when other means were cut off. For example if new firewall settings or password change {is dat ook zo?} made it impossible to log on the internal network the created tunnel allows simple access.

These files were all extracted from the temporary internet files on winsvr007 in the Office network.

File name	IP addres 1 (from)	IP address 2 (to)
troj134.exe	172.17.20.4 winsvr007 Bapi Database New	10.10.20.134 winsvr155 eherkenning AD port 443
troj172.exe	172.17.20.4 winsvr007 Bapi Database New	10.10.20.16 winsvr108 Websites met auth.pass.nl port 443
troj25.exe	172.17.20.25 winsvr003 CI - Source build server	10.10.20.134 winsvr155 eherkenning AD Port 443
134.exe	{weten we dit nog of stond er maar een IP in?}	10.10.20.134 winsvr155 eherkenning AD Port 443
13480.exe	{weten we dit nog of stond er maar een IP in?}	10.10.20.134 winsvr155 eherkenning AD Port 443

7.1.5.2 Xuda script

On the Public-CA a deleted file x-select-settings.xuda was found. This script contains XUDA-code that uses the Xcert Universal Database API in order to use the CA software {ref naar hoofdstukje xx}. In this script two lists of 113 signing requests are included. Other investigations have shown[25] that the script was placed in the directory "WebServer\x-templates\" of the CA software on Public-CA server. This investigation states that this script is then run whenever the web interface of the CA software is started and consequently certificates are issued by four different CA private keys.

{hacker bericht toevoegen}

Investigations on the CA management software as described in chapter **Error! Reference source not found. Error! Reference source not found.** shows more than 113 or 226 rogue certificates have been

[25] This investigation is done by a security expert at Vasco {vasco niet noemen! "Intern onderzoek"} and has not been verified.

issued. It could not be determined whether or not by using xuda scripts the rogue certificates were created or this was the only way.

On the Relatie-CA the file get.xuda is encountered. This script is accessed by the local internet explorer on Relatie-CA. The cached page shows a xuda error.

{waar moet onderstaande in het rapport terecht komen?}
The previous investigation (note12) also show that a svchost.exe found on the Public CA creates a file 'jobsdone.zip' and uploads this file to the web server 10.10.20.41 in the external DMZ using the /beurs/up.aspx script on that server. The investigation also states that the file svchost.exe creates a connection to 10.10.20.41 on port 53.

The previous investigation (note12) also investigated another file discovered on one of the CA servers. This file creates an connection to an external IP address:

File name	Connection destination
csrsss.exe[26]	AttIP1{ref} port 137

{end Waar?}

7.1.5.3 Other tools/ timeline

Some of the other encountered files were quick assessed based on their filenames:

First upload date	File name	Remark
2011-06-17_05:26:36	Settings.aspx	web up/downloader
2011-06-18_01:43:26	nc.exe	Netcat tool
2011-06-18_02:46:04	mstsc.exe	MS Terminal Services Client
2011-06-18_02:47:01	mstscax.dll	Part of Terminal Services bruteforcer?
2011-06-18_02:47:37	clxtshar.dll	Part of Terminal Services bruteforcer?
2011-06-18_02:48:03	tclient.dll	Part of Terminal Services bruteforcer?
2011-06-18_03:00:52	test2.rdp	
2011-06-19_06:48:47	datapipe.exe	Port redirector
2011-06-19_06:58:01	Redirector.exe	
2011-06-19_08:52:57	T1.exe	
2011-06-19_08:56:24	mswinsck.ocx	
2011-06-19_09:23:15	94.exe	Doorway to AttIP2?
2011-06-19_09:29:05	Troj.exe	
2011-06-19_09:35:39	PwDump.exe 384.00K	Dump password hashes tool.
2011-06-19_09:40:49	res.txt	
2011-06-19_10:09:29	7za.exe	7zip SFX?
2011-06-19_11:58:40	mimi.zip	mimikatz zip?
2011-06-20_11:13:18	demineur.dll	mimikatz - This library allows to manipulate the minesweeper
2011-06-20_11:13:59	klock.dll	mimikatz - This library allows you to switch desktops
2011-06-20_11:14:51	mimikatz.exe	mimikatz - mimikatz is a security auditing tool, its primary role is to place a library in a remote process and enable communication between the target process and mimikatz in the manner of a shell
2011-06-20_11:15:25	sekurlsa.dll	mimikatz - This library allows to manipulate the Windows authentication process
2011-06-21_01:48:50	rdpv.exe	
2011-06-21_09:28:54	RunAs.exe	
2011-06-21_12:28:29	up.aspx	
2011-06-21_12:49:52	cachedump.exe	Recovering Windows Password Cache Entries
2011-06-22_08:39:14	ReadF.exe	

[26] Analysed internally by DigiNotar

2011-06-22_10:25:13	Read1.exe	
2011-06-22_10:46:06	read2.exe	
2011-06-22_12:17:23	read3.exe	
2011-06-22_12:19:53	read4.exe	
2011-06-22_12:34:07	read5.exe	
2011-06-27_08:41:55	TheRunAs.exe	
2011-06-27_08:49:34	Run2.exe	
2011-06-27_08:54:07	Run3.exe	
2011-06-27_09:01:41	RunAsMy.exe	
2011-06-27_09:29:48	Run5.exe	
2011-06-27_09:33:03	83443.exe	Doorway to AttIP1 port 443?
2011-06-27_09:42:12	Run6.exe	
2011-06-27_10:19:10	bb.bat	
2011-06-27_10:20:53	My3.exe	
2011-06-27_10:26:15	My7.exe	
2011-06-27_10:32:35	My8.exe	
2011-06-27_10:39:58	Mk.exe	
2011-06-27_10:55:58	Mk2.exe	
2011-06-27_12:34:50	Raexer.exe	
2011-06-27_12:36:10	ra2.exe	
2011-06-27_12:40:40	Ra3.exe	
2011-06-29_09:23:41	PortQry.exe	
2011-06-29_10:12:22	testproxy.exe	
2011-06-29_10:18:02	troj134.exe	Creates a connection between 10.10.20.134 (winsvr155/AD) and 172.17.20.4 (winsvr007/Bapi DB)
2011-06-29_10:30:12	134.exe	Creates a connection with 10.10.20.134:443
2011-06-29_11:01:15	RDP.exe	
2011-06-29_11:19:14	13480.exe	Creates a connection with 10.10.20.134:443
2011-06-30_02:56:08	83.rdp	
2011-06-30_11:56:00	PsExec.exe	Psexec tool
2011-06-30_11:57:13	PsExec.zip	psexec zipped
2011-07-01_01:43:25	troj25.exe	Creates a connection between 10.10.20.134 (winsvr155/AD) and 172.17.20.25 (winsvr003/CI source build server)
2011-07-01_02:43:30	RSAService.rar	
2011-07-01_02:58:11	pki.zip	
2011-07-01_09:31:07	ssl.zip	
2011-07-01_09:40:45	nssl.zip	
2011-07-01_10:14:49	kkeys.zip	
2011-07-01_10:47:21	aaaa.txt	
2011-07-01_11:50:05	CertContainer.dll	
2011-07-01_12:25:45	MSCOMCTL.zip	
2011-07-02_06:33:47	ldap.msi	
2011-07-02_07:59:22	zipped.zip	
2011-07-02_08:04:43	msxml6.msi	
2011-07-02_08:36:11	dbpub.zip	
2011-07-02_10:15:48	m.zip	
2011-07-02_12:18:33	putty.exe	Putty

This leads to the following assumptions:

- On 17 June the up/ downloader is in place (2011-Jun-17 02:33:35 (file date) the file b.aspx is uploaded to winsrv119 (docproof))
- On 18 juni attempts were started to bruteforce RDP
- Meanwhile some proxies/ redirectors were made
- On 30 juni psexec was uploaded.
- On 1 july the focus was on certificates and CA software.

7.1.5.4 Password crack

On winsrv??? (CCV CA) the tool Cain & Able (with winpcap) was installed. This tool is probably used to crack password hashes. The tool pwdump extracts the password hashes from the system. The tool Cain & Able then brute force these hashes and the passwords are revealed. On the desktop deleted files were found with output from the tool pwdump:

- winsvr022.txt
- winsvr056.txt
- winsvr167.txt

With the tool Cain probably attempts are made to capture passwords by a man-in-the-middle attack method. This because of the found deleted Kerberos tickets and NTLM challenge-responses in the files K5.LST, KRB5.LST, SMB.LST and HOSTS.LST.

{Onderstaande moet in de timeline worden opgenomen}
On the Taxi-CA the attacker(s) had logged in as local administrator. Downloaded the file mimi.zip. After that the attacker(s) logged on as domain administrator.

From winsrv119 a RDP session is started with winsrv155. Although this is not suspicious the time this occurrence (11-Jul-2011 0:25:32) is.

The tool cacheddump.exe is uploaded on the docproof website (Websites\Docproof\Docproof01\demo\cachedump.exe). Also on the website the file test.txt is found (Accessed 2011-Jul-25 20:17:31.000324 UTC) containing the mscache of one of the administrators. This password can easily be cracked ("MazdaRX8").

On winsrv056 many pkcs10 requests have been made with the local CA software web interface. Also many Certificate Signing Requests have been manually made with this interface.

On Root-CA server nCipher logs have been created. Also Dr. Watson error dump of Xuda.exe is found meaning xuda.exe has crashed.

The settings.aspx script provides, among other things, a file manager where files can be up and downloaded. To gain access to this web page a username password combination is required. {dit moet ook ergens anders komen te staan}.

On the winsrx{xxx, bapi database new} some activity on files concerning Symantec Antivirus was done by the attacker. Possibly the antivirus software was disabled.

7.1.6 nCipher DLLs

During the investigation on the Qualified CA server it is discovered that possibly some of the DLL used to access the netHSM were modified. These files are located in the WINDOWS\system32 directory:

- nfmodexp.dll
- ncspmess.dll
- ncsp.dll
- ncspdd.dll
- ncspsigdd.dll

The file creation, modification and accessed times for these files are all around 2011-Jul-02 00:24:03 UTC.

Further investigations showed that three of these files have incorrect digitally signatures indicating modification of the DLLs. The manufacturer of the nCipher netHSM (Thales {nog invullen}) provided us with the hash digest of the original DLLs. These matched exactly with the hashes of the found DLL.

This lead to the conclusion the DLLs were not tempered with. The time stamps could have been changed because they have been copied. It might however be possible the DLL were modified and later the original copied back explaining the creation date.

{dit weg?: Thales confirms the Authenticode can be invalid. {deze tekst nog aanpassen} "*In relation to the invalid Authenticode signatures we have traced this issue to a dual-signing mechanism that is used with these specific files. This is a hangover from Windows 2003 Server and earlier versions of Windows, where Microsoft themselves are required to sign the nCipher/Thales CSP files as part of an earlier export control process. In this case the Microsoft signatures are applied *after* the Authenticode signature is performed by Thales. The Microsoft signatures are embedded within the DLL file and this results in a modification to the files that invalidates the Authenticode signature.*

Although standard Windows tools therefore report that the Authenticode signature is invalid, the Windows system will actually validate the embedded signatures with the CSP files prior to execution and these will verify. In the event that an attacker was to modify these files Windows would automatically refuse to execute these files. This method of signing pre-dates Authenticode and is required to maintain compatibility with earlier versions of Windows."}

8 Remaining Investigation

{wellicht sommige onderwerpen naar een eigen hoofdstukje}

8.1 netHSMs

DigiNotar used nCipher netHSM 500s. The systems have limited log facility. It is recommended by the supplier to store the logs on a separate log server. However this was not configured at DigiNotar. The log stored on the netHSM are deleted every time the machine is turn off. This had already occurred when the investigation was started. Therefore no log could be retrieved.

8.2 Load balancer

{Ik heb van verschillende mensen de vraag gekregen of de load-balancer bij Diginotar logging bijhoudt. De load-balancer is een appliance van het merk Coyote. De logging wordt weggeschreven naar de syslog server. Ik heb in de syslogserver zitten te grasduinen maar hierin zit van de load-balancer geen relevante informatie. Naar wat horten en stoten hebben we het wachtwoord kunnen bemachtigen van de appliance maar ook hierin geen relevante logging.}

8.3 Other?

9 Investigation of external systems

{de systemen uit UK en RU}
{hebben we niet zo veel mee gedaan, maar wel iets!}

9.1 Server hosting AttIP2

During the investigation a tool was found that created a back connect to an external IP address AttIP2{ref} {ref H}. On 13 September 2011 an official request for assistance to the authorities in the country were the server is located was issued. A copy of this server was investigated.

On this server the web server log files showed interesting entries of GET requests from AttIP3. These log entries show a file mails.rar is downloaded several times on 2011-07-19 between 16:35:51 and 19:42:17. This file is only download by AttIP3 except on the first occurrence when it is downloaded by AttIP6.

9.2 AttIP4

The IP address encountered in the web server logs AttIP4 was banned by several CA providers due to persistent hacking attempts on web servers of CA providers.

10 Investigation conclusions

{combinative van losse onderzoeksresultaten}
{dit stuk moet nog sterk gereviseerd worden}

10.1 Path of the attacker(s)

{dit is allemaal oud...}

Files or commands were exchanged between the external DMZ and the Office network (WINSRV007; Bapi Database New; 172.17.20.4) as well as the secure network (WINSRV056; Public-CA; 172.18.20.245).

A connection was made from a number for internal systems with the webserver in the DMZ (10.10.20.41). A reconstructed list of files that have been present on the `/beurs` directory of the webserver shows suspicious activity. It is highly likely that the webserver was used by the attacker(s) to transport files from internal systems to external systems on the Internet.

An indication whether a system was compromised by the attacker(s) is if traces of suspicious activity can be found in the Temporary Internet Files of the Internet Explorer webbrowser. If the cached version of `settings[1].htm` is present in the Temporary Internet Files with the before mentioned malicious content then the system was most likely compromised by the attacker(s).

The IIS log files of the webserver were secured, but log files for a crucial period were missing. Traces of log entries related to the `/beurs` directory were found on the harddisk of the webserver. The traces led to a list of 14 unique internal and an publicly undisclosed number of external IP-addresses of systems that were most likely used by the attacker(s). The IIS logs show that a total of 125 files were transported between these systems.

In order to connect from certain internal systems to proxy systems tailored hacking tools were used. These tools created a connect-back between two IP-addresses using port 443 to get through the firewall. Traces of these connections were found in the firewall log files.

Connect-back tunnels:

IP 1	IP 2	Opm.
172.17.20.4	10.10.20.134	
172.17.20.4	10.10.20.16	
172.17.20.25	10.10.20.134	Geen connecties?
172.18.20.245	10.10.20.134	Geen malware?

Proxy/ dumpplaats

			Opm.
10.10.20.134	WINSRV155	[P] eherkenning AD (SVO51)	Moet nog onderzocht worden of dit ook zo is.
10.10.20.16	WINSRV108	[P] Websites met auth.pass.nl (SVO35 SVO36)	Moet nog onderzocht worden of dit ook zo is.
10.10.20.41	WINSRV101	Website met www.diginotar.nl (SVO8)	

Uit de firewall logs is verdacht verkeer geconstateerd tussen de netwerk segmenten "secure" en "uitwijk-secure". Dit moet nog verder onderzocht worden.

10.1.1 Originating IP addresses attacker

By examining the web server logs of {servername/ SVO8}, malware and WINSRV119(?) a number of IP addresses were encountered that the attacker(s) used. In **Error! Reference source not found.**.

10.1.2 Compromised systems

IP	Server naam	Omschrijving	SVO	Bron verdenking					
				IIS log SVO8	Firewall logs	Tools found	IE history	Trojan	Other
10.10.20.16	WINSRV108	[P] Websites met auth.pass.nl	SVO35 SVO36					X	
10.10.20.40	WINSRV108	[P] Websites met auth.pass.nl			X				
10.10.20.41	WINSRV101	Externe web server	SVO8		X				
10.10.20.58	???		?	X					
10.10.20.65?	WINSRV119	DocProof	ITSec						
10.10.20.134	WINSRV155	[P] eherkenning AD	?		X			X	
10.10.20.139	WINSRV157	[P] eherkenning HM	SVO28 SVO29 SVO31		X				
10.10.200.20	WINSRV066	Docproof Database	SVO312 SVO313 SVO314	X					
172.17.20.25	???							X	
172.17.20.4	WINSRV007	Bapi Database New	SVO75 SVO76	X					
172.17.20.59	Digiws121		nog niet	X					
172.17.20.7	dlx001	[P] Proxy (Squid)	?	X					
172.17.20.8	WINSRV065	Kantoor Fileserver	SVO100	X					
172.18.20.10	WINSRV130	[P] Applicatieserver (CAP web)	SVO317	X					
172.18.20.11	WINSRV131	[P] SQL database (CAP)	SVO321 SVO322 SVO323	X	X				

172.18.20.244	WINSRV055	RSA Relatie CA	ITSec SVO12	X	X				
172.18.20.245	WINSRV056	RSA Public CA	ITSec SVO13	X	X	X	X		CA logfiles
172.18.20.246	WINSRV057	RSA Ccv CA	SVO3	X	X				
172.18.20.247	WINSRV167	RSA root CA	SVO1	X					
172.18.20.249	WINSRV022	RSA Qualified CA	SVO2	X					
172.18.20.251	WINSRV053	RSA Taxi CA	SVO5	X	X				

10.2 Stolen by perpetrator(s)

Op de CA machines zijn log bestanden en database bestanden aangetroffen. Daaruit blijkt dat er een aantal ongebruikelijke certificaten zijn uitgegeven.

Verder zijn er op de CA machines databases aangetroffen die unieke serienummers bevatten. Een aantal van deze serienummers zijn niet te herleiden.

The attacker(s) could gain access to every system on the network and every file on stored on them. This included:

- Software and licences
- All personal information of clients of DigiNotar including clients to services like the tax administration (Belastingdienst). For example:
  - Name, e-mail address, telephone number
  - Client certificates, revocation codes
- Company data like contracts and e-mail

11 Aftermath

On the 29-Aug-2011 Google published a notice that a rogue wildcard certificate for the Google.com domain, which was generated on the 10-Jul-2011, was being abused to perform SSL man-in-the-middle (MITM) attacks. The MITM-attacks were primarily targeted at users that were located in Iran.

http://pastebin.com/ff7Yg663 (rogue *.google.com cert)
http://googleonlinesecurity.blogspot.com/2011/08/update-on-attempted-man-in-middle.html (google notice)
{X: Wat is de onderzoeksvraag? Ik zie het doel van mijn conclusies niet terug. Er zijn dingen weggelaten en met name zaken scherper gesteld. Waarom?}

11.1 Investigation of OCSP responder logs

The Online Certificate Status Protocol (OCSP) is used to obtain the revocation status of certificates without the need for Certificate Revocation Lists (CRLs). Using this protocol clients can verify the status of certificates with specialized servers called OCSP responders. When an OCSP responder receives a valid request it will respond with the certificate status good, revoked or unknown. If RFC 2560 is implemented to the letter, the status good merely implies that the certificate has not been revoked, but does not necessarily mean that the certificate was issued or that the time of response is within the timeframe during which the certificate is valid.

11.2 Sources/ content

Given the context where rogue certificates were being used in an attack, Fox-IT recommended that the OCSP responder would operate on the basis of a whitelist instead, so that the status unknown would be returned when the validity of an unrecognized certificate was checked. A customized sensor from Fox-IT was subsequently placed in front of the DigiNotar firewall that logs all PCAP and flow data, which also included Snort in combination with a custom policy and a custom sniffing service for logging OCSP requests. A number of custom scripts were written, in order to check the OCSP logs against all valid certificates, in order to check if OCSP requests persisted for known rogue certificates and to gain insight into the question what domain names were associated with rogue certificates [is dan niet al gegeven door de lijst? Zo niet: waar ligt de toegevoegde waarde t.o.v. de lijst?].

The OCSP database at DigiNotar contained logs of the OCSP requests between 01-May-2011 at 00:00 and 30-Aug-2011 at 01:56. The OCSP database consisted of 27.102.901 rows and contains the following fields:

Name	Meaning	Value
Id	Keyfield (uniek)	~59M-81M
IP	Internet protocol address	1.9.132.2-223.255.231.29
Status	Result of the validity check	GOOD,REVOKED,UNKNOWN
DateTime	Date and time of the request	~10-May-2011 – 30-Aug-2011
CA id	Identification of the CA	-,5,7,8,11,12,13,14,15,19,20,22
Serial	Identification of the certificate	~3K hexadecimal numbers that generally have 34 digits.

The OCSP database was subsequently enriched with GeoIP information:

Name	Meaning	Value
ASN	Identification of the peering provider	Numerical value between 0-393238
ASN name	Name of the peering provider	Name of a peering provider
Country code	Code for the country of origin	~200 2-digit country codes
Country name	Name of the country of origin	Name of the country of origin

The OCSP database was additionally enriched with information from SVO 1:

Name	Meaning	Value
Is_Forged	Indication if the cerficiate in question is fake	True, false

Rogue certificates were generated for the following domain names:

Domain names	Rogue certificates	Category
..com	1	**General**
..org	1	**General**
*.10million.org	2	**Unknown**
*.android.com	1	**Telecommunication**
*.aol.com	1	**Telecommunication**
*.azadegi.com	2	**Communication**
*.balatarin.com	3	**Communication**
*.comodo.com	3	**Security**
*.digicert.com	2	**Security**
*.globalsign.com	7	**Security**
*.google.com	26	**Communication**
*.JanamFadayeRahbar.com	1	**Comment**
*.logmein.com	1	**Security**
*.microsoft.com	3	**General**
*.mossad.gov.il	2	**Political**
*.mozilla.org	1	**General**
*.RamzShekaneBozorg.com	1	**Comment**
*.SahebeDonyayeDigital.com	1	**Comment**
*.skype.com	22	**Communication**
*.startssl.com	1	**Security**
*.thawte.com	6	**Security**
*.torproject.org	14	**Security**
*.walla.co.il	2	**Communication**
*.windowsupdate.com	3	**Security**
*.wordpress.com	14	**Communication**
addons.mozilla.org	17	**General**
azadegi.com	16	**Unknown**
Comodo Root CA	20	**Security**
CyberTrust Root CA	20	**Security**
DigiCert Root CA	21	**Security**
Equifax Root CA	40	**Security**
friends.walla.co.il	8	**Communication**
GlobalSign Root CA	20	**Security**
login.live.com	17	**Communication**
login.yahoo.com	19	**Communication**
my.screenname.aol.com	1	**Communication**
secure.logmein.com	17	**Security**
Thawte Root CA	45	**Security**
twitter.com	18	**Communication**
VeriSign Root CA	21	**Security**
wordpress.com	12	**Communication**
www.10million.org	8	**Unknown**
www.balatarin.com	16	**Communication**
www.cia.gov	25	**Security**
www.cybertrust.com	1	**Security**
www.Equifax.com	1	**Security**
www.facebook.com	14	**Communication**
www.globalsign.com	1	**Security**
www.google.com	12	**General**
www.hamdami.com	1	**Political**
www.mossad.gov.il	5	**Political**
www.sis.gov.uk	10	**Security**
www.update.microsoft.com	4	**Security**

11.2.1 Analysis

The list of OCSP requests can provide some insight into the way that rogue certificates were being used for MitM-attacks. Two rogue certificates are notable in this regard:

Yahoo certificate	
Serial	3612f911f611984191fc310e74645d16
CA	Koninklijke Notariele Beroepsorganisatie CA
CN	login.yahoo.com
Validity	10-Jul-2011 18:22:26 to 27-Jul-2011 12:01:41
Period of use	10-Jul-2011 20:12:11 to 29-Jul-2011 11:52:40
Total usage	8 requests 2 unique IP-addresses 0 status GOOD responses

Six OCSP requests were made for the rogue login.yahoo.com certificate around 20:00 on 10-Jul-2011 from the IP-address [77.104.076.097] that resulted in the status response 'unknown'. Another OCSP request was made on 11-Jul-2011 at 00:22 from the IP-address [77.104.076.097] that resulted in the status response 'unknown'. On 29-Jul-2011 at 11:52 the rogue certificate was verified by the IP-address [10.010.210.029], which resulted in the status response 'revoked'.

Google certificate	
Serial	05e2e6a4cd09ea54d665b075fe22a256
CA	DigiNotar Public CA 2025
CN	*.google.com
Validity	10-Jul-2011 21:06:30 to 29-Aug-2011 16:58:47
Period of use	30-Jul-2011 09:11:47 to 30-Aug-2011 01:56:05 (= end of log)
Total usage	665.974 requests 301.565 unique IP-addresses 654.313 status GOOD responses (298.140 unique)

A total number of 665.974 OCSP requests were made for the rogue wildcard certificate for the Google.com domain between 30-Jul-2011 at 09:11 and 29-Aug-2011 at 19:09 from 301.565 unique IP-addresses. Out of the total number of 665.974 OCSP requests, 654.313 requests from 298.140 unique IP-addresses resulted in the status response 'GOOD' between 30-Jul-2011 at 19:11 and 29-Aug-2011 at 19:09. Between 29-Aug-2011 at 19:09 and 30-Aug-2011 01:56 a further 11.661 OCSP requests resulted in the status 'revoked'.

A number of more specific findings can be reported in regard to the usage of the rogue wildcard Google certificate:

1) The number of affected IP-addresses grows exponentially between 04-Aug-2011 and 30-Aug-2011 (**Table 1**).
2) The number of OCSP requests grows from an average 8.890 requests per hour to 10.599 requests per hour during the period in which the rogue wildcard certificate for Google.com was used (corresponding to 5.625 and 6.663 unique IP-addresses per hour respectively).
3) Both the OCSP requests for valid and rogue certificates occur in waves as shown in **Table 2**, **Table 3** and **Table 4**.
4) Peaks in OCSP requests occur at the end of the month:
   a) On 28-Jul-2011 at 15:50 requests peak at 2.847 requests for valid certificates (**Table 3**).
   b) On 29-Aug-2011 at 17:54 requests peak at 1.053 requests for rogue certificates (**Table 2**).
   c) On 29-Aug-2011 at 20:53 requests peak at 3.492 requests for valid certificates (**Table 4**).

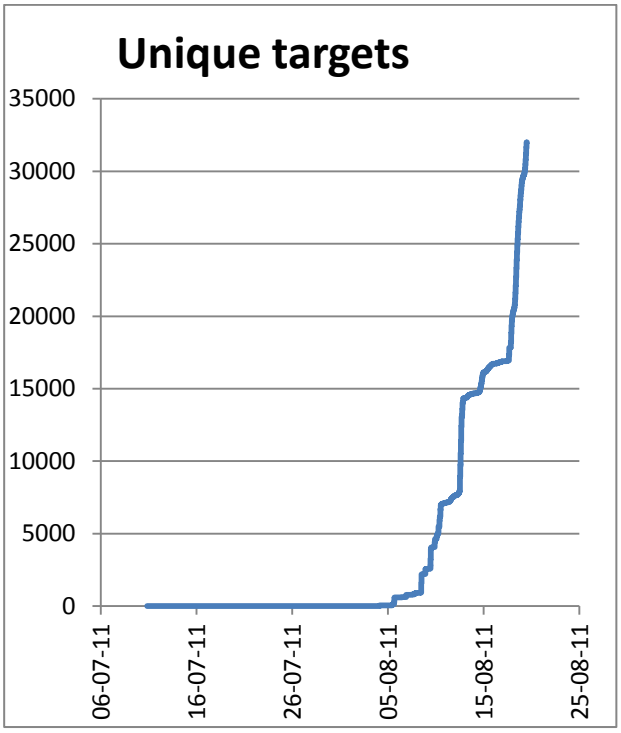


Table 1 Unique targets

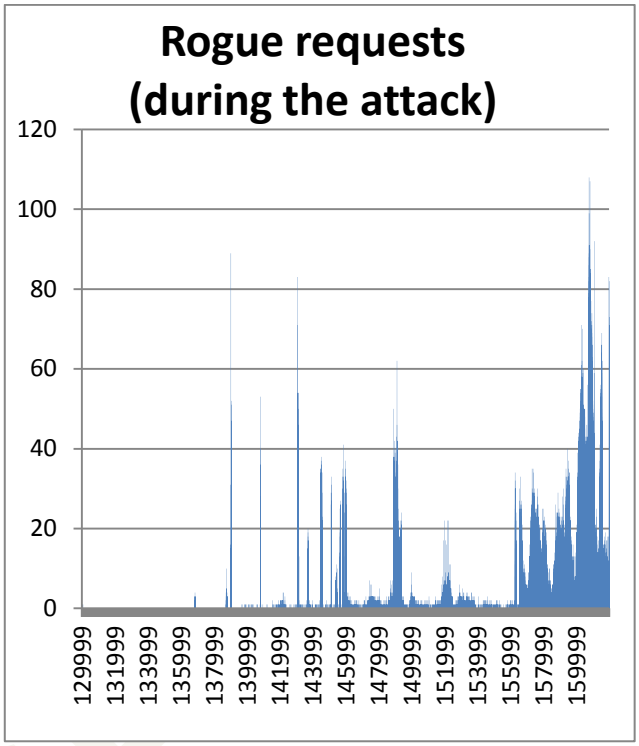


Table 2 Rogue requests (during the MitM-attack)

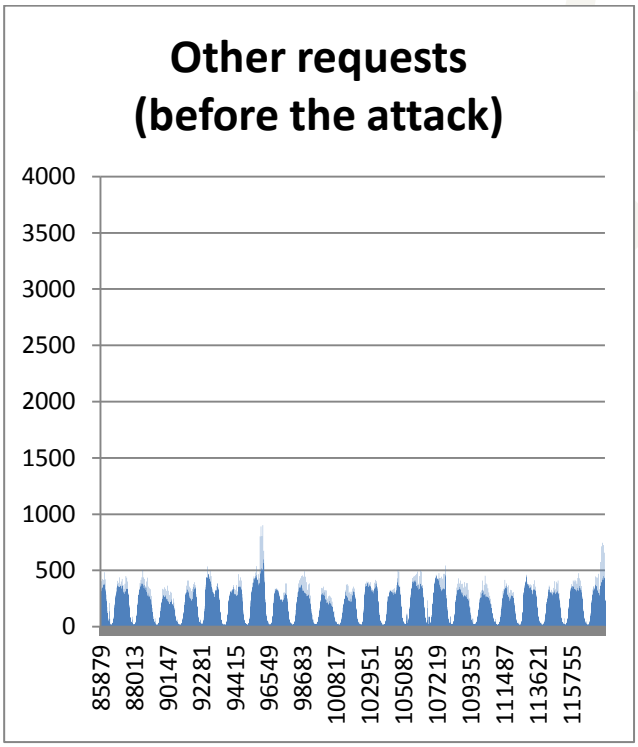


Table 3 Other requests (before the MitM-attack)

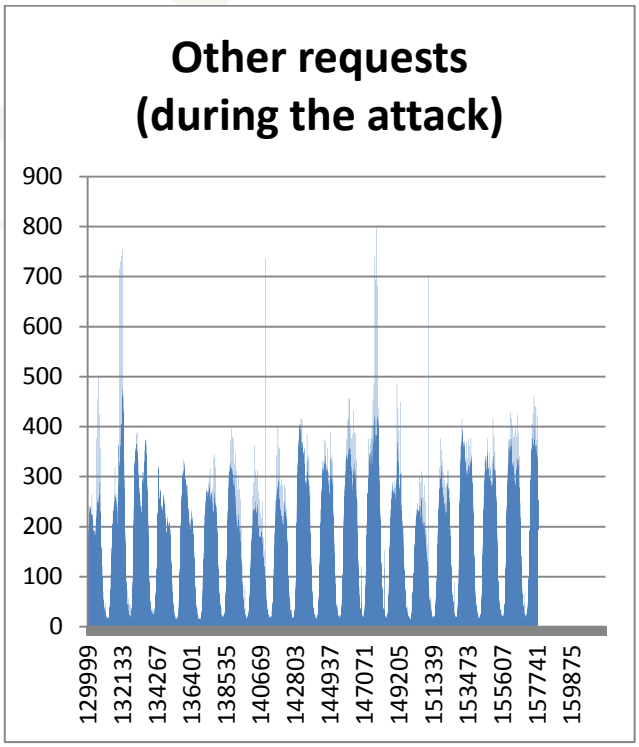


Table 4 Other requests (during the MitM-attack)

5) No regular intervals during which there are no requests for the rogue wildcard certificate for Google.com ('silence' or 'blackout') were observed. As the number of requests for the rogue wildcard certificate increases, the number of blackouts decreases.
   a) Seemingly irregular intervals of more than 15 minutes can be distinguished during which less than 5 OCSP requests per minute occur.
   b) There are no intervals of more than 10 minutes during which 0 requests per minute occur after 19-Aug-2011.
6) 95% of the OCSP requests for the rogue wildcard certificate for Google.com originate in Iran (634.665 out of 665.974 OCSP requests).
7) The status of different certificates is validated by users from Iran before and during the MitM-attack (29 unique certificates before the attack, 28 unique certificates during the attack and a total of 44 unique certificates).
8) 60% of the OCSP requests for rogue certificates and the majority of the requests from unique IP-addresses originate from 4 Iranian ISPs (**Figure 7** & **Figure 10**).
9) Iranian ASNs from which OCSP requests were received before the MitM-attack are not excluded from the attack (**Figure 10**).
10) While a small number of ASNs are responsible for the majority of all OCSP requests, a broad spread of OCSP requests can be identified over the remaining Iranian ASNs (**Figure 11**).
11) Before 10-Jul-2011 928 OCSP requests for valid DigiNotar certificates from Iran occur. In total 1.780 OCSP requests from Iran occur for valid DigiNotar certificates between 01-May-2011 and 30-Aug-2011.
12) The amount of certificates issued by DigiNotar for which OCSP requests occur is weakly correlated with the number of requesters (**Figure 12** and **Figure 13**).

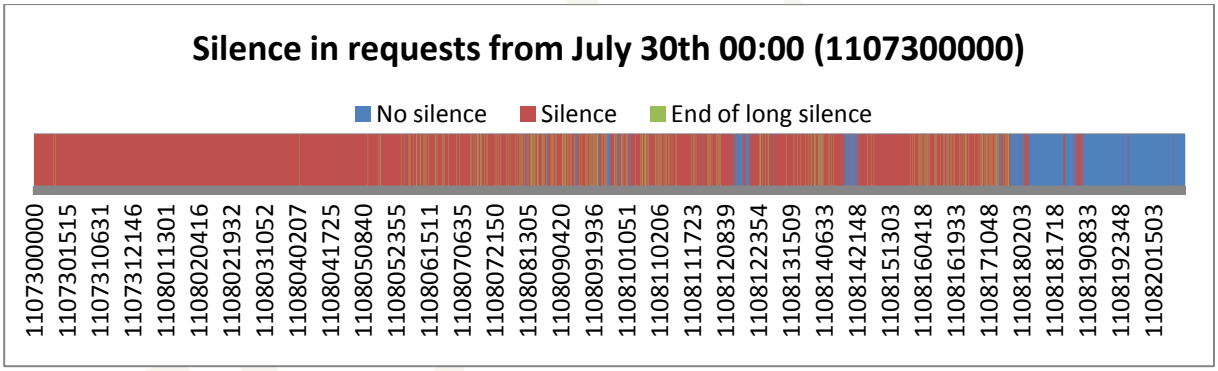


Table 5 Silence in requests for rogue certificates

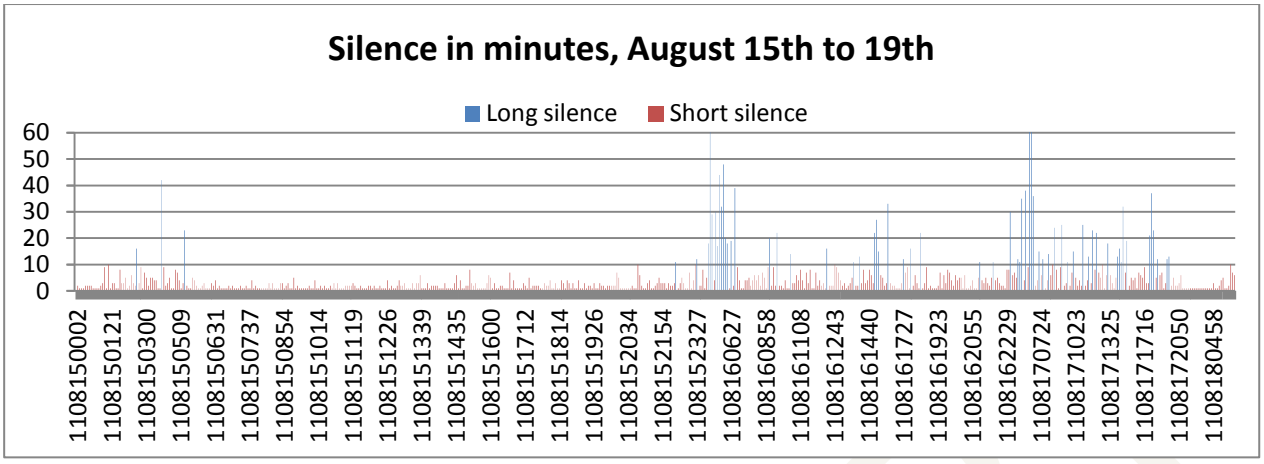


Table 6 Silence in requests for rogue certificates (zoom 2x)

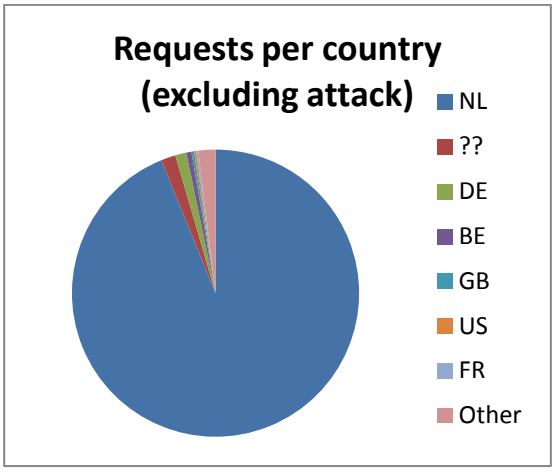


Figure 1 Requests per country

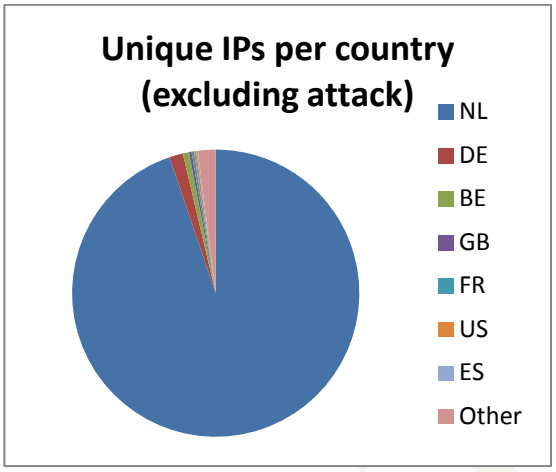


Figure 2 Unique IPs per country

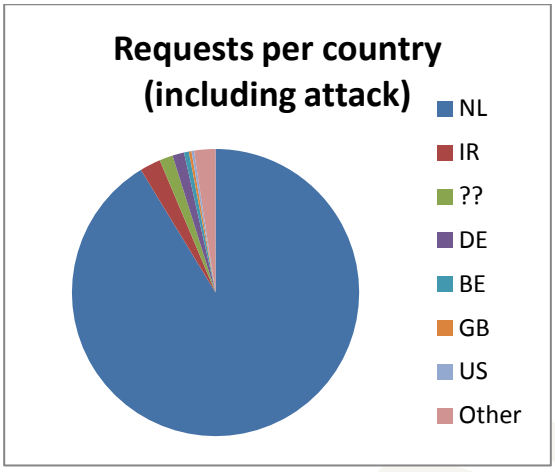


Figure 3 Requests per country

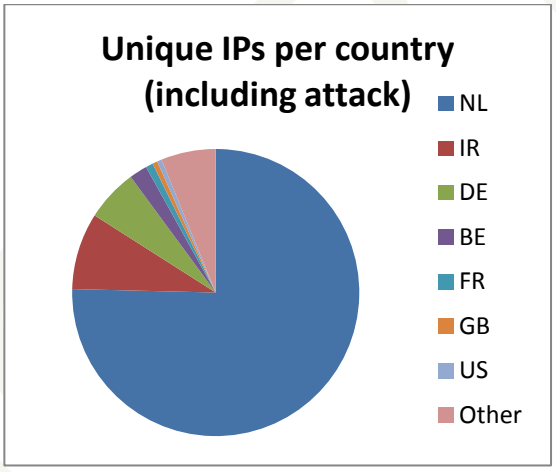


Figure 4 Unique IPs per country

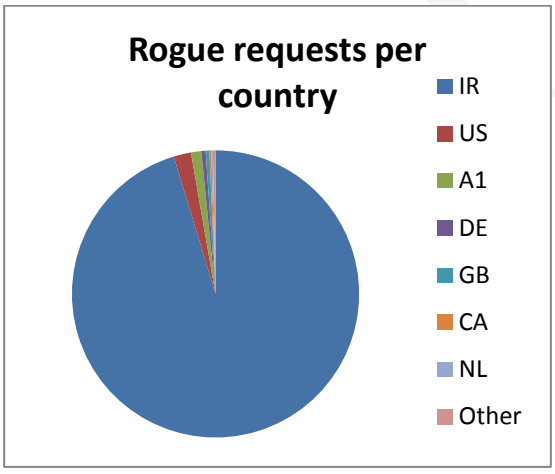


Figure 5 Rogue requests per country

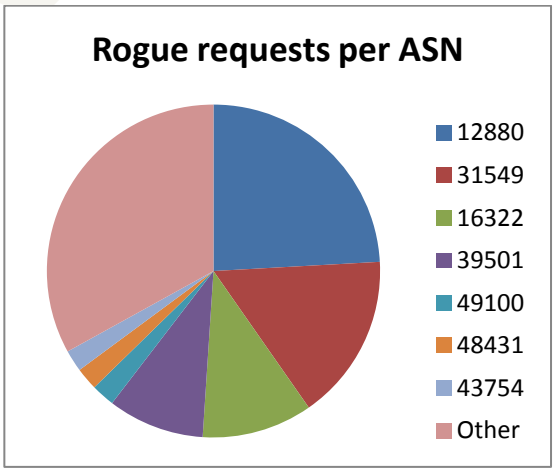


Figure 6 Rogue requests per ASN

	bt_asn	bt_value	bt_rogue_count
▶	12880	Information Technology Company (ITC)	160633
	31549	Aria Rasana Tadbir	107761
	16322	PARSONLINE Autonomous System	71520
	39501	Neda Gostar Saba Data Transfer Company Private Joint	62492
	49100	Pishgaman Tose Ertebatat	15110
	48431	Bozorg Net-e Aria	14562
	43754	AsiaTech Inc.	13998

Figure 7 Rogue requests per ASN top 7

	bt_asn	bt_value	bt_ip_ucount
▶	12880	Information Technology Company (ITC)	64251
	31549	Aria Rasana Tadbir	63589
	16322	PARSONLINE Autonomous System	37784
	39501	Neda Gostar Saba Data Transfer Company Private Joint	31624
	43754	AsiaTech Inc.	7431
	49100	Pishgaman Tose Ertebatat	7203
	48431	Bozorg Net-e Aria	6802

Figure 8 Unique requests per Iranian ASN top 7

	bt_asn	bt_value	bt_serial_ucount
▶	12880	Information Technology Company (ITC)	17
	51852	Private Layer INC	17
	31549	Aria Rasana Tadbir	15
	42337	Respina Networks & Beyond PJSC	13
	44244	Iran Cell Service and Communication Company	12
	28753	Leaseweb Germany GmbH (previously netdirekt e. K.)	11
	39501	Neda Gostar Saba Data Transfer Company Private Joint	9

Figure 9 Certificate usage per Iranian ASN top 7

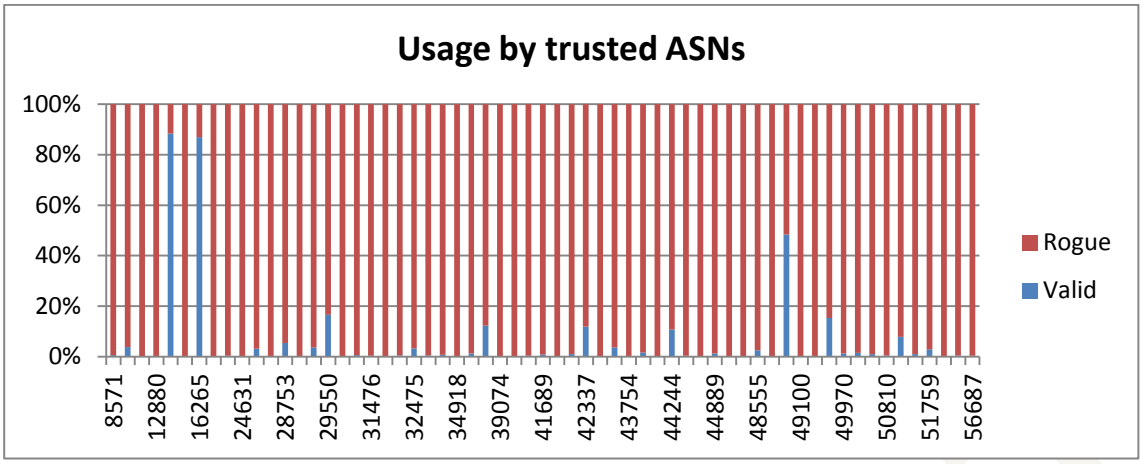


Figure 10 Iranian ASNs with requests before the attack (61)

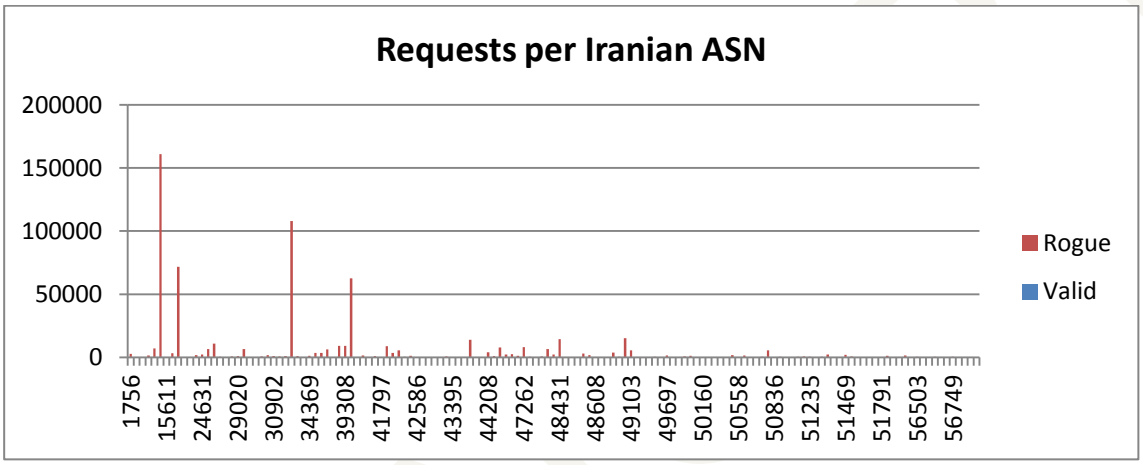


Figure 11 Requests per Iranian ASN (143)

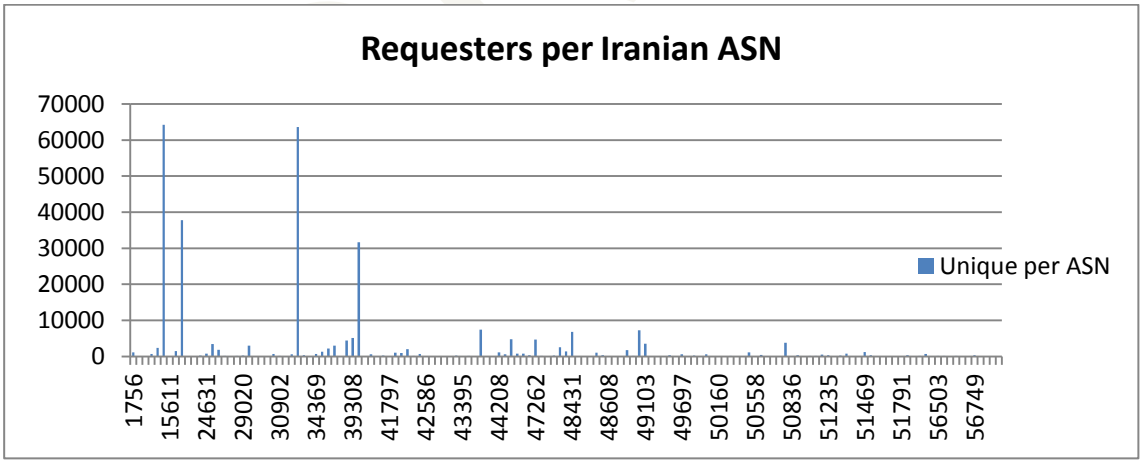


Figure 12 Requesters (unique IP-addresses performing OCSPS requests) per Iranian ASN

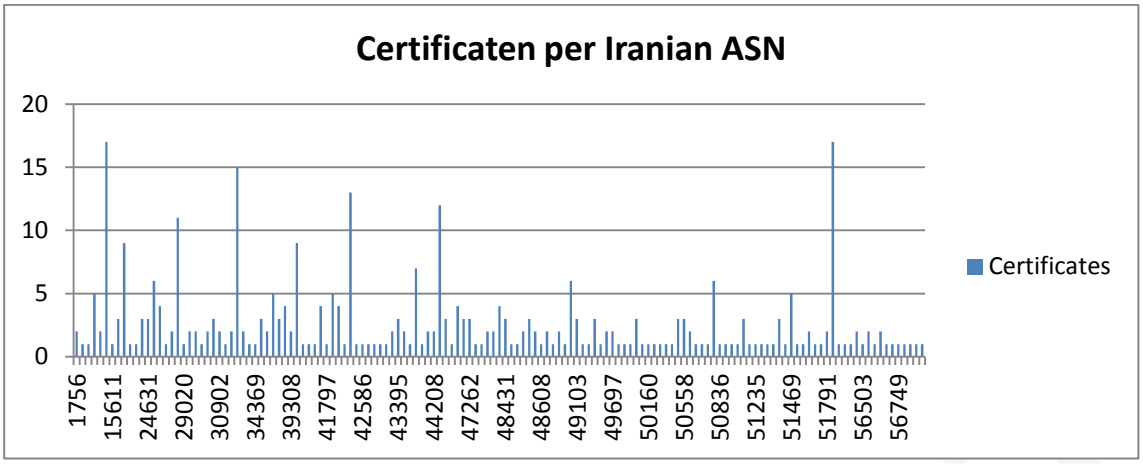


Figure 13 Certificate usage per Iranian ASN

11.2.2 Conclusion

{dit stuk moet nog sterk gereviseerd worden}
The greatest common divisor in the MitM-attack is that a diverse group of primarily Iranian users were targeted using one rogue wildcard certificate for the Google.com domain. This conclusion is supported by the fact that a large majority of users (95%) are located in Iran based on the GeoIP information for the corresponding IP-addresses. The attack gained momentum exponentially after 04-Aug-2011 and had a broad reach which affected 143 Iranian ASNs and approximately 300 hundred thousand unique IP-addresses. The number of unique IP-addresses can be regarded as a conservative approximation for the amount of users that were affected, as a number of ASNs seemingly masquerade multiple users behind one unique IP-address.

Rogue certificates were mostly generated for websites that are related to security (such as root CA-certificates) as well as websites that are used for social or communication purposes. Taken together these two categories represent two-thirds of the total number of rogue certificates.

The OCSP requests occur in waves (**Table 3** and **Table 4**) with a peak at the end of the month (**Table 2**). No regular 'blackouts' were observed. Regular blackouts would be expected if the MitM-attack relied on the repetition of botnet-instructions to perform cache-poisening (**Error! Reference source not found.** and **Table 6**). The broad spread of OCSP requests for rogue certificates from the various Iranian ASNs can be explained in terms of either the attacker(s)'s inability to narrow the scope of the systems that were targeted during the attack or the desire to target the maximum amount of systems.

The findings are consistent with a tree-like infrastructure and imply that a major peering point was consistently rerouted in order to perpetrate a large-scale MitM-attack. This could support the conclusion that in order to perform such a large-scale MitM-attack on a major peering point for an extensive period without regular blackouts the attackers must have operated from a privileged position within the Iranian infrastructure.

11.3 Academic/ closet

{based speculation...} {niet openemen?}
DNS cache poisoning?
Private keys?

12 Perpetrator(s)

{? Opnemen of niet?}{→ niet opnemen! Is al verwerkt in andere teksten}
Pastebins
Xuda script

The history of the OCSP requests show that the fraudulent *.google.com certificate was massively used between {xxx} and {yyy}. However prior to these requests 3 requests have been done originating from AttIP7 {ref} on 2011-07-30 between 09:11:47 and 09:51:19. This was probably a test run.

13 Lessons learned

{dit stuk moet nog sterk gereviseerd worden}
{what have we learned from this incident?}
{Tot op zekere hoogte deden hun best. Uitgangspunt onderzoek en rapport is helpen!}

{je kunt natuurlijk nooit een volledig veilge system maken...}

{Informatie over basis beveilging, security management system}

An unusual modus operandi was used in the attack on DigiNotar. The attacker(s) appear(s) to have had the intention to abuse the private key of a trusted CA in order to spy on a large number of Iranian users using rogue certificates. The attack resulted in an erosion of public trust in the existing Public Key Infrastructure and the role of Trusted Third Parties therein, which is central to their operation, whether this was intended or not. If the ensuing erosion of trust in PKI was indeed intended, the threat could be compared to terrorism, where the goal is to induce fear in the general public. This modus operandi is unusual when compared to what's more generally encountered, that is that of a criminal organization, where the aim is to make money and attacks are performed covertly.

The threat of cyber terrorism is typically left unaddressed in security a risk assessments that are performed when for instance CAs are audited. The assessment that the threat of cyber terrorism is merely hypothetical for all but the most critical targets is rapidly being overtaken by the reality that a much broader scope of targets face this threat. Given the impact that a breach in the security of one CA has on PKI as a whole and the Internet in general, ensuring the security of every CA is paramount to the trust in PKI and its role in providing security for a diverse range of activities on the Internet. While the approach to protecting potential targets from this type of attack does not differ significantly from other threats, the range of scenarios that need to be taken into account is rapidly expanding.

{That these attacks can, have and will happen gives new insight to you and your customers security.}

13.1 Trusted third parties

{Trust is the most important business asset of TTP and needs to be protected.
TTP might consider asking help from national security agencies.}

13.2 Intermediate users

{Bedrijven, overheden e.d.}

The attack that targeted DigiNotar and the subsequent MitM-attack show the importance of proper incident reporting procedures. The European Network and Information Security Agency (Enisa) recently underlined in their recent report on the Black Tulip operation that companies who provide important digital services for a society, such as CAs, should pro-actively detect and investigate incidents and quickly inform the relevant parties. The relevant parties include the users that are involved, as well as corporate customers and government authorities.

The legislative proposal in regard to an obligation for security incident reporting that is currently pending in The Netherlands, as well as its European source, is targeted at specific parties (telecommunication providers) when the breach affected the security of personal data. The attack on DigiNotar and the subsequent MitM-attack on users however show that a breach in the security of other parties within the information society, that does not have any direct effect on personal data, can nonetheless have far reaching consequences for the general public.

European Commissioner Neelie Kroes indicated on behalf of the European Commission that possible amendments to the currently applicable legal framework will be considered in the course of 2012 during a revision of the Directive 1999/93/EC. On the short term the consideration will apparently be limited to the question if a standard on common minimal supervision on CAs will increase the efficiency of supervision. A more comprehensive European Internet Security Strategy is being developed by the European Commission.

13.3 End users

Average users will have very limited capabilities to protect themselves properly against attacks such as those against Trusted Third Parties in the Public Key Infrastructure. The MitM-attack on users that was perpetrated in the aftermath of the hack of DigiNotar was only detected by Google when users of the Google Chrome browser reported abnormal behaviour when using Google services for which a rogue Google wildcard certificate had been issued. Because of the limited ability for users to protect themselves from attacks that abuse PKI, they need to be able to trust the security of all parties that make up the PKI in order for the system as a whole to operate.

More generally users and businesses can protect themselves against a wide range of security threats. The first step to a more secure environment is normally to obtain an overview of all machines that operate within a given network and the (business) processes and procedures that are applicable. While this may sound like an insurmountable task within large organizations, a small group of specialists within these organizations can combine their expertise to produce an overview of the attack surface. Specialists that commonly possess this type of knowledge are system and network administrators, application managers, security officers and business representatives.

Once an overview of the attack surface has been obtained [...]

The next thing to do is think of as many scenarios as possible the adversary can do to achieve his goal. Think like the attacker. And since you have a lot of inside knowledge, the attacker probably has not, it would not be hard to come up with effective scenario's.

Because you can limit yourself to one type of adversary or threat at the time you can eliminate a lot of scenario's. For example a terrorist from Iran will probably not use someone from inside your organisation. This eliminates your staff from wilfully harm your company (for this threat agent that is...). However mistakes or deceit of your staff is something you should take into account. On the other hand, if you consider the chance that someone of your staff will be bribed by a terrorist you should take that into account (like segregation of duties and authorities, internal monitoring and audit).

Next, this group of people must estimate the chance the scenario's can or will take place. What must the adversary do to run through the scenario? Don't discount the unknown event (the black swan) and your lack of technical knowledge. You don't have to know exact how to hack a server but you must acknowledge that it is possible. Therefore your scenario's must include partially successful scenario's. Do not only create scenario's visualising the attacker being outside trying to get in. Also include scenario's like "if the attacker owns this server, how easy is it then to proceed", and "if the attacker could slip through this procedure (for ex. vetting) what additional barriers have we in place?", and most useful "what can an attacker do when he has a particular username/ password or token?'.

Next step is to come up with solutions. This will require some (security) technical knowledge.}

{Meldplicht datalekken?}
IP addres van de aanvaller was al bekend via Comodo en CA-b forum {nazoeken!}

14 Potential follow-up investigation

The investigation that was performed by Fox-IT focussed on the questions [...], [...] and [...]. The information that was uncovered during this investigation can be used as the basis for further research in regard to several additional questions.

General questions:

- What security measures were in place before and during the attack?
  - How was the firewall configured?
  - How was the segmentation set up? (network/domain) [er staat iets over segmentation die werd afgedwongen door de firewall in het rapport?]
  - What was the strength of the passwords that were used?
  - To what extent had patches been applied to systems in the network?
  - Were anti-malware and anti-virus measures in place? [NB: volgens Daniel was er anti-virus aanwezig]
  - Were Intrusion Detection and/or Prevention Systeem (IDS/ IPS) used? [in de tekst staat dat er een IPS voor de firewall stond]
  - Which special/specific security measures were in place?
- What measures were taken in response to the attack?

Chapter 2.5 Network:

- The described normal operation of the network segments and firewall is based on interviews with the administrators. The exact firewall rules have not been examined to confirm this.
- It is not investigated what private keys were stored in the netHSM in the co-location and how the synchronisation between the netHSMs took place.
- The CA servers, HSM, firewall and other equipment in the co-location is not investigated.
- The exact layer-2 network layout.

Chapter 4 - Investigation of CA :

- It could be investigated whether the attacker(s) used the option in the CA software to perform a complete backup of [...].
- It could be investigated whether the `RSACM-v6.7CustomizableSerialNumbers-WIN32` extension provides functionality which could have aided the attacker(s) in issuing rogue certificates.
- [{zie reference: RSA Keon Ready Implementation Guide For PKI 3rd Party Applications}. About "Unattended Startup". No investigations have been done if this was done and/or attempts were made by the perpetrator(s) to change these settings]
- The CA web servers log (`enrol-cipher.log`) of the Public-CA server contain interesting outside office hours entries.
- Investigation is needed on the log files of CCV-CA, Nova-CA, QC-CA, Root-CA and Taxi-CA.

Chapter 5.1.1 - Sources/ content:

- The RSA software could be scrutinized to determine if it can detect if log files have been removed from a system.
- It could be investigated if the CA servers contain remains of deleted log files.

Chapter 5.2.1 – Certificates:

- Further investigation could be performed to explain the appearance of the duplicate certificates that were found in the database files. This might provide an answer to the question if certificates with identical fingerprint could be issued or have been issued by the attacker.

Chapter 5.2.2 - Private keys:

- The private key `id2entry.dbh` database entries could be linked to the specific netHSMs. This could answer the question which CA server users which netHSM.
- All public keys corresponding with the private keys entries in the `id2entry.dbh` could be matched with the certificates extracted from the databases. This answers the question what CA server had access to what CA private key.

Chapter 12.2.2 – Conclusion:

- The OCSP data could be used to examine the limited set of IPs outside of Iran that were targeted in the MitM-attack in regard to determine if they can all be identified as TOR-exit nodes and VPN providers.
- If additional data from Google could be obtained it would be possible to determine if login data that could have been obtained during the MitM-attack was abused in practice.
- Data regarding OCSP requests for valid certificates from other CAs could be used to determine if round robin was used and thus capabilities of the attackers and the infrastructure that was used.
- Zooming in on the targets and the underlying infrastructure in Iran could reveal information about the identity and aim of the MitM-attacker(s).
- {er is al contact geweest met google met verzoek om info...}

Er is geen onderzoek gedaan om expliciet aan te tonen welke zwakheden zijn misbruikt in de webservers DotNetNuke. Om dat te doen moet extra onderzoek worden verricht:

- welke versie draaide (exe's onderzoeken)
- welke kwetsbaarheden had deze versie
- Zoek naar sporen in de log of deze kwetsbaarheden zijn misbruikt.

The system event logs (applications logs) of most of the servers were exported and retained. This was done in august 2011. These logs have not been examined.

14.1 Chapter 4.6 Rogue Certificates

Based on the investigation of the log files and the databases a total number of 531 rogue certificates were found. These were identified as rogue because of the blatant distinguished name of the certificate. Certificates that were issued during the time the attacker was active on the CA servers are also suspected as fraudulent. Further investigation can determine this. For now they are discarded if the distinguished name of the certificate resembled valid certificates.

The number of rogue certificates grouped by issuer:

Issuer	Total	Unknown serial	Cert.	CA server
DigiNotar Cyber CA	108	1	107	
DigiNotar Extended Validation CA	98	14	84	
DigiNotar Public CA - G2	56	0	56	
DigiNotar Public CA 2025	184	183	1	
Koninklijke Notariele Beroepsorganisatie CA	76	0		
Stichting TTP Infos CA	18	0		

{dit moet ook nog ergens worden opgenomen}{in dit hoofdstuk}
{
Zo te zien zijn alle IIS logs van de diginotar.nl server verwijderd voor 11 juli 2011… maar heeft ie daarna nog sporen achtergelaten. Ik zie nu zo snel 3 ip's:
67.202.50.234
77.104.76.97
85.17.182.207

Die 67 heeft net een andere useragent, das wel gek… doet ook maar 1 of 2 requests….
Nu het interesssante:

ex110711.log:2011-07-11 00:31:42 W3SVC1062701327 10.10.20.41 POST /Settings.aspx - 80 - 85.17.182.207 Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1)+Gecko/20100101+Firefox/4.0.1 200 0 0
ex110724.log:2011-07-24 13:16:48 W3SVC1062701327 10.10.20.41 GET /settings.aspx - 80 - 77.104.76.97 Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 200 0 0
ex110724.log:2011-07-24 13:16:53 W3SVC1062701327 10.10.20.41 POST /settings.aspx - 80 - 85.17.182.207 Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 200 0 0

mijn vermoeden:
11 juli, gewoon via proxy, nog met FF4

Tussentijd geüpgrade naar FF5
24 juli, vergeten proxy aan te zetten voor eerste request, daarna gelijk proxy aan….

77.104.76.97 is het IP-adres dat voor Yahoo cert een OCSP request deed…
}
Investigation of firewall logs:

- The integrity of the firewall logs is not investigated.

Er is niet volledig onderzocht of er resten van verwijderde bestanden aanwezig zijn op de CA servers; niet naar deleted files gekeken en niet naar resten van log entries in slack of andere disk space (zgn. d.m.v. carven).

Back-up tapes

PABX logs

CRL requests.

Netflow
→ niets mee gedaan.

Onderzoek TODO:
private key velden controleren asn.1 of ref allemaal naar hsm verwijzen.

Syslogserver????? (10.10.210.35 dlx131 [T] Syslog server)

externe IP's, en naar welke interne (DMZ) IP's werwijzen ze?

Onderzoekenswaardig:
- hoe connect ie naar de db?
- Had ie al sa credentials?
- Is mssqlusr de user waaronder de sql service draaide?
- Welke rechten had deze user in windows (local admin?)?

e-mail logs
Hebben we logs van deze Exchange server?

Nee niet direct logs.

Ben lang bezig geweest om de tapes te krijgen zodat we daar iets mee konden, want vanaf de 1e dag dat ik er was wist ik al, dat zga alle segmenten zonder enige vorm van checks op een reguliere manier mail naar buiten kunnen sturen. Dat zit in het hele proces en de opbouw van de omgeving. Alles gaat via een exchange server, en voor sommige systemen dacht ik via een smtp connector die er nog tussenhangt (of hing)

Smtp logging staat niet aan op de exchange server, Net als andere logging is er veel afwezig.

Message tracking van berichten uit die tijd is er niet, of lukte niet, omdat het mail is die niet in de EDB database terecht gekomen is, maar direct naar buiten gepusht is.

Heel misschien nog korte duur info uit de backups van die systemen.... (als we ooit die tapes krijgen)

➔ toch is er misschien nog wel kans dat er wat boeiends in de error logs staat. Die zijn er meestal wel. Kan me voorstellen dat je als hacker wel een paar errors op de mailserver triggert als je aan het proberen bent je zipje naar buiten te sturen.

A netHSM was present in the internal DMZ hosting the keys for the service 'Parelsnoer' provided by DigiNotar. The servers used for this Parelsnoer service were not investigated. Therefore we have no indication if the keys in this netHSM were misused by an attacker or even if the servers were compromised. A quick scan has been done on the firewall log to check if any of the servers involved in

the Parelsnoer process had any connection to the known IP addresses {ref naar chapter: TODO nog te maken}. Also the CA server running the CA management software winvm012 was quickly assessed for traces {ref. toevoegen. TODO nog uitwerken}.

Welke servers draaide er nog meer RSA Keon software?

- ⇨ Andere stepping stones
- ⇨ web server doc proof system.

14.2 Nog uitgevoerd onderzoek

Connectives naar de hsm's:

```
grep "10\.10\.200\.254" all_log > ../../tijdelijk/10.10.200.254_all_logs
grep "172\.18\.20\.254" all_log > ../../tijdelijk/172.18.20.254_all_logs
grep "10\.10\.240\.254" all_log > ../../tijdelijk/10.10.240.254_all_logs
```

10.10.200.254_all_logs
Als we de icmp eruit halen worden er maar een paar connecties gedaan. Opvallen zijn de connecties vanaf op 4 juli de hsm naar andere systemen. Port scan? Geownde hsm?
Port 9004 is normaal?

Further investigations on these servers can give a more definite answer if these were misused.

15 References

RSA Keon Ready Implementation Guide For PKI 3rd Party Applications,
http://www.rsa.com/rsasecured/guides/keonca_pdfs/nCipher_netHSM_KCA651.pdf

incident logbook

15.1 Terminology

Term	Meaning
ASN	Autonomous System Number Identification of a registered network operator, usually an ISP.
ASN.1	
BAPI	Belastingdienst Advanced Program Integration (Dutch tax administration)
CA	Certificate Authority, an issuer of certificates.
CAP	Control Application [for ...]
Certificate	A digital file used amongst others to authenticate a website and to encrypt networktraffic. The validity of a certificate is generally verified with the issuer (CA)
CSR	
CSP	
DARPI	DigiNotar "Abonnementen Registratie" (Subscription Registration) Production Interface
ISP	Internet Service Provider.
MiTM	Man-in-the-Middle. In this type of attack an attacker places himself between two parties in order to spy on the traffic between them
PIN mailer	
OCSP	Online Cretificate Status Protocol, a protocol that is used to obtain the revocation status of certificates as described in RFC2560.
(net)HSM	(Over the network accessible) hardware security module
PKI	Public Key Infrastructure
SVO	

15.2 tools used

python
Microsoft Excel
FTK imager
ASN1.Editor (`www.lipingshare.com/Asn1Editor`)
RapidMiner
OpenSSL

Appendix I {references to equipment}

{lijst van list van SVOs waarnaar wordt gerefereerd in het rapport}

Name[27]	Server Id[28]	SVO number(s)	IP address(es)	Network segment	Remarks
CA servers					
Root-CA	winsvr167	SVO1	172.18.20.247	secure-net	
Qualified-CA	winsvr022	SVO2	172.18.20.249	secure-net	
CCV-CA	winsvr057	SVO3	172.18.20.246	secure-net	
Nova-CA	winsvr021	SVO4	172.18.20.252	secure-net	Also called 'Orde-CA'.
Taxi-CA	winsvr053	SVO5	172.18.20.251	secure-net	
Test-CA	winsvr054	SVO7	172.18.20.250	secure-net	
Relatie-CA	winsvr055	SVO12 DD.055	172.18.20.244	secure-net	
Public-CA	winsvr056	SVO13 DD.056	172.18.20.245	secure-net	
DNTest-CA	winvm012	SVO149	10.10.240.39	test-net	
DNAcceptance-CA	winvm032	SVO114	10.10.230.39	acceptance-net	
Public-CA-Colo	winsvruw07		172.27.20.19	secure-colo-net	
Qualified-CA-Colo	winsvruw08		172.27.20.20	secure-colo-net	
Relatie-CA-Colo	winsvruw09		172.27.20.17	secure-colo-net	
Root-CA-Colo	winsvruw10		172.27.20.15	secure-colo-net	
Nova-CA-Colo	winsvruw11		172.27.20.16	secure-colo-net	Also called 'Orde-CA'.
CCV-CA-Colo	winsvruw18		172.27.20.23	secure-colo-net	
Taxi-CA-Colo	winsvruw19		172.27.20.26	secure-colo-net	
netHSMs					
netHSM-CAs	dnhsm01		172.18.20.254	secure-net	
netHSM-web	dnhsm02		10.10.200.254	DMZ-int-net	
netHSM-test	dnhsm04		10.10.240.254	test-net	Also called "Stichting continuïteit hsm"
netHSM-CAs-Colo	dnhsmuw01		172.27.20.254	secure-colo-net	
XXX					
BAPI-db	winsvr007		172.17.20.4		
eHerkenning-AD	winsvr155		10.10.20.134 62.58.44.101		
auth.pass.nl	winsvr108		10.10.20.16 10.10.20.35 143.177.11.12 143.177.11.3		
Source-build	winsvr003		172.17.20.25		
Load-balancer-1	dnlb01		10.10.20.8		
Load-balancer-2	dnlb02		10.10.20.9		

IP addresses of firewall

From the file systemroot\System32\Inetsrv\MetaBase.xml taken from WINSRV118 (nieuwe? DocProof; svo11) the following IP address bindings were present:

- 10.10.20.37 Docproof

[27] Server name as it is used in this report.
[28] Server Id as it is used by DigiNotar

From the WINSRV119 (old docproof) image from ITSec:

- WINSRV119
- IP address: 10.10.20.65
- Primary Domain Name: DNDMZEXT

From the file systemroot\System32\Inetsrv\MetaBase.xml the following IP address bindings were present:

- :80: :443: Docproof (local addresses)

Winsrv108: NTP, Pass, Tim (SVO35)

ServerBindings="10.10.20.16:80:"
ServerComment="PassWeb - PASS15"
SecureBindings="10.10.20.40:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.40:80:"
ServerComment="NTP"
SecureBindings="10.10.20.35:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.35:80:"
ServerComment="TIM_tim.diginotar.nl"

Winsrv109: (SVO46)

SecureBindings="10.10.20.98:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.98:80:"
ServerComment="SS_Provincie-Utrecht.signing.diginotar.nl"
SecureBindings="10.10.20.129:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.129:80:"
ServerComment="SS_Gelderland.signing.diginotar.nl"
ServerBindings="10.10.20.42:80:"
ServerComment="TimeStampServer"
ServerBindings="10.10.20.92:80:"
ServerComment="SoapSigning"
SecureBindings="10.10.20.84:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.84:80:"
ServerComment="SS_Lelystad.Signing.diginotar.nl"
SecureBindings="10.10.20.85:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.85:80:"
ServerComment="SS_Waterschapdedommel.signing.diginotar.nl"
SecureBindings="10.10.20.86:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.86:80:"
ServerComment="SS_Signing.diginotar.nl"
SecureBindings="10.10.20.137:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.137:80:"
ServerComment="DigiDownload"
SecureBindings="10.10.20.87:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.87:80:"
ServerComment="SS_Teylingen.signing.diginotar.nl"
SecureBindings="10.10.20.88:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.88:80:"
ServerComment="SS_PZH.signing.diginotar.nl"
SecureBindings="10.10.20.89:443:"
ServerAutoStart="TRUE"

ServerBindings="10.10.20.89:80:"
ServerComment="SS_sintanthonis.signing.diginotar.nl"
SecureBindings="10.10.20.130:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.130:80:"
ServerComment="SS_Leeuwarden.Signing.diginotar.nl"
SecureBindings="10.10.20.90:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.90:80:"
ServerComment="SS_PNB.signing.diginotar.nl"
SecureBindings="10.10.20.91:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.91:80:"
ServerComment="SS_Leiderdorp.Signing.diginotar.nl"
SecureBindings="10.10.20.99:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.99:80:"
ServerComment="SS_Drenthe.Signing.diginotar.nl"
SecureBindings="10.10.20.93:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.93:80:"
ServerComment="SS_Overijssel.Signing.diginotar.nl"

winvm028: geen SVO aanwezig?

winvm045:

winsrv155 (SVO51): Geen matebase.xml

SVO55 WINVM045 [P] WebServer (www.diginotar.nl etc.)
SecureBindings="10.10.20.172:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.172:80:"
ServerComment="evssl.diginotar.nl"
SecureBindings="10.10.20.164:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.164:80:"
ServerComment="BapiViewer"
SecureBindings="10.10.20.165:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.165:80:"
ServerComment="DarWizard"
ServerBindings="10.10.20.182:80:"
ServerComment="bct.csp.minienm.nl"
SecureBindings="10.10.20.173:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.173:80:"
ServerComment=www.diginotar.com
SecureBindings="10.10.20.167:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.167:80:"
ServerComment="OCSPClient"
SecureBindings="10.10.20.174:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.174:80:"
ServerComment="service.diginotar.nl"
SecureBindings="10.10.20.169:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.169:80:"

ServerComment="BapiOphalenCert"
ServerBindings="10.10.20.183:80:"
ServerComment="test.bct.csp.minienm.nl"
SecureBindings="10.10.20.175:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.175:80:www.evssl.nl"
ServerComment=www.evssl.nl
SecureBindings="10.10.20.158:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.158:80:www.diginotar.nl
10.10.20.158:80:www.diginotar.com
10.10.20.158:80:diginotar.com
10.10.20.158:80:diginotar.nl
10.10.20.158:80:www.evssl.nl
10.10.20.158:80:evssl.diginotar.nl"
ServerComment="diginotar.nl"
ServerBindings="10.10.20.184:80:"
ServerComment="test.csp.minienm.nl"
ServerBindings="10.10.20.181:80:"
ServerComment="csp.minienm.nl"
SecureBindings="10.10.20.176:443:"
ServerAutoStart="TRUE"
ServerBindings="10.10.20.176:80:"
ServerComment="sha2.diginotar.nl"

SVO11:

SecureBindings="10.10.20.37:443:"
ServerAutoStart="FALSE"
ServerBindings="10.10.20.37:80:"
ServerComment="Docproof"

Appendix II Certificate issuers

Based on the investigations of the database files of the CA management software the issuing CAs were determined.

Root-CA

Issuers and number of occurrence of certificates found in database files on the Root-CA.
{moet nog worden herzien}

Root-CA: Issuer	#
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA	2
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA	33
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	24
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2	6
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA	2
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA	2
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA	33
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA	33
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020	1
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	24
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	24
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2	6
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2	6

Certificates with the basic constraints attribute set found in database files on the Root-CA.
{moet nog worden herzien}

Root-CA: Basic constraints = TRUE
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA

/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA

Certificates with CA in the common name without the basic constrains attribute found in database files on the Root-CA.
{moet nog worden herzien}

Root-CA: CA in name CA attribute not set
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA CA Administrative Certificate
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA CA Administrative Certificate
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA

Self signed root certificates found in database files on the Root-CA.
{moet nog worden herzien}

Root-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2

Qualified-CA

Issuers and number of occurrence of certificates found in database files on the Qualified-CA.
{moet nog worden herzien}

Qualified-CA: Issuer	#
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2	142
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2	1
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2	1560
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven	5358
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA	5
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA	33
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr022	1
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl	16515
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	2
/C=NL/O=PKIoverheid TEST/CN=TRIAL PKIoverheid Organisatie TEST CA - G2	1

/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Organisatie CA - G2	1
/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Overheid CA	1

Certificates with the basic constraints attribute set found in database files on the Qualified-CA.
{moet nog worden herzien}

Qualified-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

Self signed root certificates found in database files on the Qualified-CA.
{moet nog worden herzien}

Qualified-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr022
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

CCV-CA

Issuers and number of occurrence of certificates found in database files on the CCV-CA.
{moet nog worden herzien}

CCV-CA: Issuer	#
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010	1
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010	2
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010	1
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010	1
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010	1
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010	14
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA	1
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA	14
/C=NL/O=DigiNotar B.V./OU=IT/CN=RSA CCV CA Administrative CA	1
/C=NL/O=DigiNotar B.V./OU=IT/CN=RSA CCV CA System CA	15
/C=NL/O=DigiNotar B.V./OU=IT/CN=winsvr057.DNproductie	2
/CN=ids CA	10

Certificates with the basic constraints attribute set found in database files on the CCV-CA.
{moet nog worden herzien}

CCV-CA: Basic constraints = TRUE
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=CCV-CH-TMS 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-110-364
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-160-364
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-179-095
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-237-323
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-300-362
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-310-362
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-399-095
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-507-524
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-537-524
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-569-094
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-659-094
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=RSA CCV CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=RSA CCV CA System CA

Self signed root certificates found in database files on the CCV-CA.
{moet nog worden herzien}

CCV-CA: Self signed

/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=RSA CCV CA System CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=winsvr057.DNproductie
/CN=ids CA

Nova-CA

Issuers and number of occurrence of certificates found in database files on the Nova-CA.
{moet nog worden herzien}

Nova-CA: Issuer	#
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA	4
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA	31
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr021	1
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl	29
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl	108
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl	40329
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	7
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl	484
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl	8
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA	4
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA	29
/C=NL/O=DigiNotar/OU=IT/CN=winsvr056	1
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association	37830
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root	1

Certificates with the basic constraints attribute set found in database files on the Nova-CA.
{moet nog worden herzien}

Nova-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association

Self signed root certificates found in database files on the Nova-CA.
{moet nog worden herzien}

Nova-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr021
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA
/C=NL/O=DigiNotar/OU=IT/CN=winsvr056

Taxi-CA

Issuers and number of occurrence of certificates found in database files on the Taxi-CA.
{moet nog worden herzien}

Taxi-CA: Issuer	#
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA	4
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA	15
/C=NL/O=DigiNotar/OU=IT/CN=Winsvr053.DNproductie	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2	3
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA	13
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2	639

/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2	230
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2	3
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2	4
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Root CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2	420
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2	7
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA	5
/CN=ids CA	5

Certificates with the basic constraints attribute set found in database files on the Taxi-CA.
{moet nog worden herzien}

Taxi-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA

Self signed root certificates found in database files on the Taxi-CA.
{moet nog worden herzien}

Taxi-CA: Self signed
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=DigiNotar/OU=IT/CN=Winsvr053.DNproductie
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA
/CN=ids CA

Test-CA

Issuers and number of occurrence of certificates found in database files on the Test-CA.
{moet nog worden herzien}

Test-CA: Issuer	#
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010	8
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA	25
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl	2
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010	4
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010	4
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010	1
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA	91
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2	1
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIOverheid CA Overheid en bedrijven	562
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA	3
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA	20
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl	5
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl	1
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl	606
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl	1134
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl	47
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA	6
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA	42
/C=NL/O=DigiNotar/OU=IT/CN=RSATESTCA	1
/C=NL/O=Hypotrust/CN=Hypotrust CA	87
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.	1
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA	29
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association	97
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA	11

/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA	16
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA	52
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA	174
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL	30
/CN=Test Renault Nissan Nederland CA/O=Renault Nissan Nederland N.V./C=NL	42
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/OU=TEST/CN=TEST Key Recovery CA	1

Certificates with the basic constraints attribute set found in database files on the Test-CA.
{moet nog worden herzien}

Test-CA: Basic constraints = TRUE
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-219-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-269-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-429-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-439-072
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=CCV Group/CN=oltp.ccvpay.nl
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Group/CN=Test.SSL3.certificate.erwin.nl
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIOverheid CA Overheid en bedrijven
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Schuberg Philis/CN=Schuberg Philis Class 1 Issuing CA
/C=NL/O=Schuberg Philis/CN=Schuberg Philis Class 2 Issuing CA
/C=NL/O=Schuberg Philis/CN=Test Schuberg Philis Class 1 Issuing CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA
/CN=oltp.ccvpay.nl/OU=DMT/O=CCV Group/L=Arnhem/ST=Gelderland/C=NL
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL
/CN=Test.SSL3.certificate.erwin.nl/OU=Systems/O=CCV Group/L=Arnhem/ST=Gelderland/C=NL
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA

Self signed root certificates found in database files on the Test-CA.
{moet nog worden herzien}

Test-CA: Self signed
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA
/C=NL/O=DigiNotar/OU=IT/CN=RSATESTCA

Relatie-CA

Issuers and number of occurrence of certificates found in database files on the Relatie-CA.

{moet nog worden herzien}

Relatie-CA: Issuer	#
/C=FR/O=EASEE-gas/CN=EASEE-gas CA	47
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA	5
/C=NL/O=Delft University of Technology/CN=TU Delft CA	274
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA	3
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA	31
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr055	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	11
/C=NL/O=Hypotrust/CN=Hypotrust CA	977
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA	1
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA	1192
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA	6139
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA	155
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA	379
/C=NL/O=Stichting SHOCK/CN=SHOCK CA	1
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA	2320
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011	135

Certificates with the basic constraints attribute set found in database files on the Relatie-CA.
{moet nog worden herzien}

Relatie-CA: Basic constraints = TRUE
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011

Self signed root certificates found in database files on the Relatie-CA.
{moet nog worden herzien}

Relatie-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr055
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011

Public-CA

Issuers and number of occurrence of certificates found in database files on the Public-CA.
{moet nog worden herzien}

Public-CA: Issuer	#
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA	2
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA	34
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020	1
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl	124
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl	226
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl	54
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl	45002
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	3
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	25
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl	564
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl	86
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA	4
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA	29
/C=NL/O=DigiNotar/OU=IT/CN=winsvr056	1
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root	1
/CN=ids CA	5

Certificates with the basic constraints attribute set found in database files on the Public-CA.
{moet nog worden herzien}

Public-CA: Basic constraints = TRUE
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA

Self signed root certificates found in database files on the Public-CA.
{moet nog worden herzien}

Public-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA
/C=NL/O=DigiNotar/OU=IT/CN=winsvr056
/CN=ids CA

Appendix III Private keys

{uit de tekst naar hier?}

Appendix IV Unknown serial numbers

{opmaak}

Root-CA server

On the 'Root-CA' server the following serial numbers were encountered {that were...}:

83120A023016C9E1A59CC7D146619617
68E32B2FE117DFE89C905B1CCBE22AB7
711CE18C0423218425510EF51513B7B8
B7ABEFC8A1F844207B774C782E5385B3
6E0088D11C7E4E98CC9E0694D32A0F6B
80C990D339F177CA9FDAC258105882AB
7F73EC0A14C4BA065BECFAD69DC5A61D

Qualified-CA server

On the 'Qualified-CA' server the following serial numbers were encountered:

C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4

Taxi-CA

On the 'Taxi-CA' server the following serial numbers were encountered:

25B6CA311C52F0E4F72A1BD53774B5B3
A0CF459D0D1EA9A946861A0A02783D88
71A10FA4C491D3A72D18D33E3CCF576C
FE456B099700A6C428A193FE5968C9FD
E7E2B46B8C9AA64679E03841F88CA5A0
AEC9F2324D80020B6E2B2A1103D6A4E8
CB20C25F14583AFC86465F14E621FBC1
947FF1DB66A41D809A9BC7E7344E342A
90BCA541B4DF5E77FB1349684F84A930
AB4967CE8B94FCF8DA7691922E6FD59C
BA479991C9103C005726FAB83088A8D6
363E9AAF4DAC7085F31B89B2AC49059A
8A63042B8A8FA256035773BC9417435A
963CCB2601B15C73DCA821F4BC4C7458
6B7057D5DE0170842C372821D3F17DB2
C391438C15FF31BD89544A7F68DDF3B3
7278CB2A8270A3E66A021A7CD75F1211
F401D4C50FCA9161A70ED9D91D40E684
6C396359C423417E20C54CFC6690F3FF
9916C8350225BB607857375A02B6DC72
0F48A14121370B5CF4828EF826749FBC
DB43E2CE6110750785FCBBE9A8EAE061
C641E4B7F19B63C4FF1EA6D3833FC874
D8B771F90BC01C9ED1333C23EF24CFC1

'Public-CA server

On the 'Public-CA' server the following serial numbers were encountered:

79C03FE0C81A3022DBF8143B27E40223
FCCF53CB3D0A71494AF9664690FFCF84
82BC18B1AA5D59C61D0EFDBEA7664C08
5D4352671C39616670B2F34C173A1F63
6FA3C48173B3B289943F113A8CD9DB8C
CFAF9BE4E5BD0F5A75F628E45E0178C9
4ADA28D281D3D14D19FB782D64086D0C
0B41ABEE6F4168D3CDE5A7D223B58BC1
13548FC160BC5C9F315AE28CDB490E36
5D8D0D436112759826A5490E7F87BD7
C880AE4D7927E6A8FA7D456CB03E9763
82072FC8F8DD7E6C0ECE9B47185F0521
90DB656E2734760CC836778255582FA8B
171A8599EDE711A3315BC7D694CEBEC6
E9EB8075F7FE3683B431552C2D962CB0
E6F9E095464F64448840A832FB3443DB
C83D16E9CB29DCF35F3B351CB942FE0D
39B5DD0ECC85C3F62A72391DC055F561
DF3FD6AFBBFBC30C9AD80BF764A102DB
327B9A443C49018D7B0A97B6EC2254B8
8B0EABAF922D4C6E6917FCBE365DD64A
4FC2D72D6427CABBE3E859453865F43B
53B53BF2F74997EBEB2577D63DA692B7
ABB21F43553F2695031A1C85355D7F1C
5563605FDC2DC865E2A1C32995B5A086
5DD6A72747D90C018B63F959DFE7C976
CAB736FFE7DCB2C47ED2FF88842888E7
9C79C9FE16727BAC407B4AA21B153A54
2D711C9CB79EC15445747BFE3F8BC92F
752A2D0325A3D34D9F5198C2F5C92A6C
BC01852405D3F4E22C48600266655026
9F7DDFE3CAAD224EC6BD68B60DE78550
A67C22A6E1F9D87799548EBFC7D5527E
11661878CCE9DC337CEEBB16E30F9A3A
6BF3BEB26AFF31116200B14F4378C33B
7A61A7778842E502E2291166C4574485
82C42F0EDC18BD751727BE5C54413EF7
03124C25849D9E49BC2A2FAD3E10C8A4
EFF0DD4B4927DF64232C5D2FF280C1E4
9EDCB5E1FE1255A2F1D7FC52C4AFA3B1
3A32AAA9DFE2CA7F9E003885E316944B
4455B43B9173CBAE4E247272EE2573D5
B95F62E86194734C9F68D4BF8B200C49
FE873B742B230B22AE540E840490A2F4
8779917563EC38B7746B8ECAFE239BE6
72CBC4824C6215B139FDE6BA10DAC6AD
8D09D4B98DE67C9E9C7C18CB72AD2418
07BC72A463D4DE33B2BE733D6FAC991D
D3E2205C3B899FC99D77FE802985283F
A5029D6A057D50D20ECFE0E528EDA067
C8B2487ADFAF969E34306029AC934406
5F3C1BDC7A2BCD47ABAF0C8E62D9F757
601315BB085FECF29538DA3F9B7BA1CE
30170F15A240446E6B482E0A364E3CCA
0590B310AEFC7A3EDC03ECA2A6F6624F
FDEB145AAC81B8CD29B8DA018E71456F
C3F9F45F19E334C8303F44288856D843
028CF7556F8BE27026800448FA6AA527
E93B28B47C34B243EBA62E58FE2FF46F
F89F5DE575755A3B4C0DECC6EDA7C804
E3E120935934CBD77E1DA7F00431F745
0A6DFACFDEAE74A816031534BE90B75A
9AD82BE2FED538B10BDFBD229A8A5AEA
C0F216CA8197AD00F0D98927EAE29E64
DE76B17BFB1B6D6D6634C8C104A6E59F
A90F1BB43E9DB5EDFC60C15FB897C593
8625B32398C2722D96E7B972580A0238
D1FDE3A78C9D2E80C2303CC4E3E92A4C
B355E909FD55C5E9EF1A6E67E9C18203
ADB59A303C6260DBE466F0149AB11A4A
5CEBD524469A075FB6B42D06C9BF27AD
0E0886EEAA119CF14F1C54387060929A
B4F9299F05A327E60543C4CDE3277FC0
E4B2F09505726306314DF05B734FD9D0
4DD0497CBAABBA058574A611B26151BA
7073C6C01DEE4E158F554555F697F7D9
EB72415ECD0B4AACBDEEA3734F4349BF
BED90D98FA3A1E0A5BD78AD54E55774D
3CDCD81930F91AC0B990664931E5412E
763B0C2A7B83066A9D995C8C4FD9E35E
720DF591261D710ADC73127C1BC4303D
C06C12DBBC7055FE40950803238EC104
62BF5A170CC779ADE7EF0090F395D5E6
61BF9A0FF2CE9D55D86BC063839F72F4
B5D7A148CA6C1F9693A2C16ACDD66226
35FBDCDF923F99B5E1C5FF4423B715B8
F1EBE73557546DC8B21E0A2DE5E3A33E
EBE7561CA573DA5DBB8EFAA250A40FD3
6BACB6C5B74FA747A3CF375EC3095035
6C1950AA83F4663F1BA063B5275C25EC

```
39936336286F843756FC4BC296D7A8E0
4A6D90618A5CA6797C768C03C860C4F8
0954E1AB9141ED7E8B640FE681046451
8259C3E1DB6C2C9B7FCD6A305EADEFE4

022E35B1ACD40F040C444DF32A7B8DE6
170370B60D515F164119BE54FD55E1ED
CBFE437C9B62805C4353516699E44649
5FFA79AB76CE359089A2F729A1D44B31
5298BCBD11B3952E3FDDC6FDD6711F5C
1836289F75F74A0BA5E769561DE3E7CD
DEB427AC9F1E8A0D0237049C80DF7E7F
FD8FE350325318C893AFE03F9DFC7096
A8031D608F65499418799817646 74DD7
DDAD29B8B1215191E7EB5AAEE0219338
3F8A5EA1756DDF4A6B6F2645B4911486
30DF96D87EEC8CA77A135ECCAB1AD25E
7DD8E0E1906C1754E11E901927CCABBD
DAC51C3D23B163601305AF99DF129689
D77EC92400AE0D9FA57DEF4DD8CFA4D4
09369288E36D7AFFEE94EA81998FA316
EEBE1885532234328919 1913F6D769EB
C00132DA154BDEE361EDEE727226D0F5
6580BE22A0566352B9622777BFCB7164
7352C61297D6B04E874EDAD12480F78E
F658C0D52B3EEF71DDE6C284E7E1B337
E1253D04A17AB8E47F4A5916B9BF9D23
8922A9A23BE960FFE9707A0B3F4D75BD
EAE97F465015E49A14F3B23403ACFA11
13A757022817C0514A5C142FE9BF143A
5132F0FCB3F8DCAA501C620575D33FEE
39953BF6383A00D29BEB377568E3DE7A
67887932934DFF086153CA905E7DE9EE
DCD1072719692871126E4159D80EFDA8
C6741E3D08C0FFD4617B94E654DD89F1
8CC74931E64061491652CC169C8BAAB3
4157D99E46A3E45E6130A95645410DAC
E34C4FC7488C4DFEF0EA475A17AF2C7B
59F8BDDA3F56D8026FAB6E3130F5D843
FAB79682C8EAE556F11ECF6DAD7121BA

5D8F8D78B0C19EF4479F744DECBD84BC
EAACDC2F46D4A86F39B035B793F4A94F
9D06313F21A4EDF734C324FFBCB9E2B5
35C54E845AE855F818504C8C189F52C7

D0BA58BA609CC1A001F612987A822BEF
6B339433956F1505104BB231314A153E
C1366C7246041A3089E1C244C5DC42E7
61D11B35765ECB85890D5349786D9FCA
44C287C1C3697367B0E6CB78A78C1DF5
DAACF72BC91FB6DA90A804933CB72E23
2ACBA14BB6F65F7BD0A485BFCB6D023F
84BE5D762F37E9018D623C8E91F4D924
1A89324D6D3E6DE6726C688BFF225DDD
F5FA42A5B421705E4803DA93C4F7E099
A869B96BCDF1D474C0714763AA34A8C9
3EA0F90DE57187FC7E1AC45AE44D16C6
F7DE638B76C3958AA3413A9785A19900
3F8C9CDAACBB533AE94F47456819FA0E
209920C169512D3EB4A1ED7CAD17D033
B2F57BD01BAAF7AF01EF442910CEBBA0
C0766829AA4D2E1A5D97213A4E4A654E
FC9993EA7A4E761B6CB79ABE2BD3CDE1
4D556B338FAA020979A740B4C3AEE28C
8ED896B9A622FF24559A3429E5888E0A
8CF1F45323EC5AB449451E7A9476CFDC
D1718E9BD91257D2169C81197D508A67
E4A691D60266784968DF971D6BF473AF
B3B64F1925F759A2E145190333D1D6D2
ED4C2EBC14B85F46A9A75F159DF8BEB3
CDBC0441C10DB5ABA43120E63A048425
DC1665266A0198728861AC99ED368928
706BBC770C62D41DD799721ABD1868AB
B2205D8CBDDFE49D7C5F0F95D506718F
901F30DB86EEB1666F5A8CAE1C7BD08B
C731140FAA7690918BABF17BECB7938D
8C605DFAA0EC88CDB7D12F7250C9F53A
68F252CD36F2798A2182F6406A31A5A2
BD7CB0D124DFDE784CD5B9EF288C304E
3D2BC95A85EF539A68DAC84542A1AE7A

56EF1EE54D65EF7B39AF541E95BB45A9
2B1EA767EC59E46364BC2DF9B1F30B97
3913B1E1C35BDDF02CE03C916E8AA638
AFA2F7E964280B36DB0D714B86256F54

9A3A951BE27E0729726FD8B80060E7E1
6410577C738133297472F6C22C2BB397
C8C06B0C6B7FE7CA66BCFE617AB6C4E6
58C18B290620E18B8C78AC1912E5DCD7
2F5ABFDCCAB1A2927E54283296F19FB8
A07CB7881E35C91FD9C5D20F6102572C
05E2E6A4CD09EA54D665B075FE22A256
8BA800DDDD865B6BF3A85ADEC4C29730
07B546E8E002FC5854651BE31802F96D
DF2AD7F766E2EEFAF0FD1FB5C6883AB4
1C6EA2DA6ECED5C5C761BCA9CA4C5308
A640A29E706AF38557B86619EAF45E7A
F88885670C3D55EBA52096A65310DACA
B85E7BB83667097F15D8A3DEAAA1B198
A5F6F149B468683318DC178F4208E237
04841B82A9D81E44CB4F2D98CFE7C374
A81686CEFDEFFCE82B8DBF100E1395F1
9952073595776A3D7A8101664A56AB96
A076DA72A8C8E2137F05FE3FA59870EB
121378A6DE0A13DDB295106E912A4E14
65A925E578098658FADA30E9FB67B5E4
5B8E5202EC6769F2389605D33DC245B2
EA71F746BD17D1B05450329818572F2E
DD8C315D2CA61870CBCF9D56ED7474E2
F346A1E62FED476F472560C6DDE0CADC
CBBCB9E06F9FC92C533B2F2A5284BA22
79DCFDA2700E06F8EAA640BA9B827810
17CF5474D5A8B4E735E69E017CEC2F37
7034FBF641CEB257FC109A6819D19DA0
6E6D052B5ABC015C779EA3500FA11A28
0370390E48A7F26AA62188A79E612DC3
```

Appendix V Suspicious files

Found on the servers:

- winsrv022 Qualified-CA
- winsrv053 Taxi-CA
- winsrv055 Relatie-CA
- winsrv056 Public-CA
- winsrv119 docproof
- winsrv167 Root-CA
- winsvr007 BAPI-db
- winsvr057 CCV-CA
- winsvr065 Office-fileserver
- winsvr101 Diginotar.nl-server

{admin names vervangen!}

Server	File name	Full path	Size
winsvr007	hosts	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\drivers\etc\hosts	792
winsvr007	savrt.dat	Partition 1\NONAME [NTFS]\[root]\Program Files\Symantec AntiVirus\savrt.dat	3220
winsvr007	SRTSEXCL.DAT	Partition 1\NONAME [NTFS]\[root]\Program Files\Symantec AntiVirus\SRTSEXCL.DAT	76
winsvr007	default	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\default	262144
winsvr007	SAM	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\SAM	262144
winsvr007	SECURITY	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\config\SECURITY	262144
winsvr007	SchedLgU.Txt	Partition 1\NONAME [NTFS]\[root]\WINDOWS\Tasks\SchedLgU.Txt	10364
winsvr007	ipconfig.exe	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ipconfig.exe	63488
winsvr007	$I30	Partition 1\NONAME [NTFS]\[root]\Program Files\Symantec AntiVirus\$I30	12288
winsvr007	Symantec AntiVirus	Partition 1\NONAME [NTFS]\[root]\Program Files\Symantec AntiVirus\	288
winsvr007	settings.dat	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\Symantec\Common Client\settings.dat	20204
winsvr007	BBConfig.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBConfig.log	3676
winsvr007	BBDebug.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBDebug.log	64
winsvr007	BBDetect.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBDetect.log	64
winsvr007	BBNotify.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBNotify.log	64
winsvr007	BBRefr.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBRefr.log	64
winsvr007	BBSetCfg.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetCfg.log	64
winsvr007	BBSetDev.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetDev.log	64
winsvr007	BBSetLoc.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetLoc.log	2108
winsvr007	BBSetUsr.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetUsr.log	64
winsvr007	BBStHash.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBStHash.log	64
winsvr007	BBStMSI.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBStMSI.log	7576
winsvr007	BBValid.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBValid.log	64
winsvr007	SPPolicy.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPPolicy.log	64
winsvr007	SPStart.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPStart.log	64
winsvr007	SPStop.log	Partition 1\NONAME [NTFS]\[root]\Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPStop.log	64
winsvr007	finance01_Log.LDF	Partition 5\Log [NTFS]\[root]\MSSQL\Log\finance01_Log.LDF	1048576
winsvr007	Applog01_Log.LDF	Partition 5\Log [NTFS]\[root]\MSSQL\Log\Applog01_Log.LDF	2359296
winsvr007	Web.config	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\wschmitt\Bureaublad\WebRAOBeheer02\Web.config	7415
winsvr101	web.config	Partition 3\Data [NTFS]\[root]\Websites\Bapiviewer\BapiViewer\web.config	5471
winsrv056	mofcomp.log	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\wbem\Logs\mofcomp.log	14664
winsvr007	wietse_log.ldf	Partition 5\Log [NTFS]\[root]\MSSQL\Log\wietse_log.ldf	3145728
winsrv119	b.aspx	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\js\b.aspx	72689
winsrv119	RunAs.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\RunAs.exe	24576
winsvr007	06172011.Log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\06172011.Log	262
winsvr007	06172011.Log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\06172011.Log	262
winsvr007	archive.zip	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\archive.zip	198024801
winsvr007	mswinsck.ocx	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\mswinsck.ocx	127808
winsvr101	demineur.dll	Partition 3\Data [NTFS]\[orphan]\demineur.dll	151552
winsvr101	klock.dll	Partition 3\Data [NTFS]\[orphan]\klock.dll	153600
winsvr101	mimikatz.exe	Partition 3\Data [NTFS]\[orphan]\mimikatz.exe	368128
winsvr101	sekurlsa.dll	Partition 3\Data [NTFS]\[orphan]\sekurlsa.dll	200704
winsvr101	Nieuw - Tekstdocument.txt.lnk	Partition 2\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\Nieuw - Tekstdocument.txt.lnk	872
winsvr007	WINSVR007_MS IIS DCOM Server.pvk	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_MS IIS DCOM Server.pvk	332
winsvr007	WINSVR007_SELFSIGN_DEFAULT_CONTAINER.pvk	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_SELFSIGN_DEFAULT_CONTAINER.pvk	620
winsvr007	WINSVR007_Microsoft Internet Information Server.pvk	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_Microsoft Internet Information Server.pvk	332
winsvr007	WINSVR007_tmpHydraLSKeyContainer.pvk	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_tmpHydraLSKeyContainer.pvk	332
winsvr007	WINSVR007_0_winsvr007.diginotar.nl.pfx	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\WINSVR007_0_winsvr007.diginotar.nl.pfx	1737
winsvr007	Documents.7z	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Documents.7z	1015873568
winsvr007	bsqweyec.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\bsqweyec.dll	65536
winsvr007	xjegjvhr.exe	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\xjegjvhr.exe	53760
winsvr007	uploader	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\uploader\	48

winsrv119	94.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\94.exe	37888
winsrv119	Troj65.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\Troj65.exe	61440
winsrv119	PwDump.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\PwDump.exe	393216
winsrv119	cachedump.exe	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\cachedump.exe	45056
winsrv119	test.txt	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\test.txt	127
winsvr007	rdp.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\rdp.exe	553472
winsvr007	rdp.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\rdp.exe	553472
winsvr007	Default.rdp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\Default.rdp	2458
winsvr065	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	141
winsvr065	sfk.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\sfk.exe\	1155072
winsvr065	sfk.exe	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\sfk.exe\	1155072
winsvr007	13480.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Desktop\13480.exe	37888
winsvr007	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	141
winsvr007	pki.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\pki.zip.lnk	424
winsvr007	DARPI.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\DARPI.lnk	941
winsrv053	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	139
winsrv053	Crypto	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Microsoft\Crypto\	136
winsrv053	MachineKeys	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Microsoft\Crypto\RSA\MachineKeys\	48
winsrv053	RSA	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Microsoft\Crypto\RSA\	256
winsrv053	Desktop.ini	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\Desktop.ini	150
winsrv053	Recent	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator\Recent\	152
winsrv022	certs.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\certs.lnk	598
winsrv022	ssl.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\ssl.crt.lnk	720
winsrv022	root.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\root.crt.lnk	725
winsrv022	cas.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\cas.crt.lnk	720
winsrv022	a.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\a.crt.lnk	736
winsrv022	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	141
winsrv022	qualifiedData.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\qualifiedData.zip.lnk	448
winsrv022	qualifiedData.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\qualifiedData.zip.lnk	448
winsrv022	457718b9-fa34-41e3-8d9d-3ecf7391929c	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\Microsoft\Protect\S-1-5-18\User\457718b9-fa34-41e3-8d9d-3ecf7391929c	388
winsrv022	nfmodexp.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\nfmodexp.dll	742680
winsrv022	nfmodexp.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\nfmodexp.dll	742680
winsrv022	ncspmess.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspmess.dll	357656
winsrv022	ncspmess.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspmess.dll	357656
winsrv022	ncsp.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncsp.dll	1041688
winsrv022	ncsp.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncsp.dll	1041688
winsrv022	ncspdd.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspdd.dll	1041688
winsrv022	ncspdd.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspdd.dll	1041688
winsrv022	ncspsigdd.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspsigdd.dll	1033496
winsrv022	ncspsigdd.dll	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system32\ncspsigdd.dll	1033496
winsrv167	DNproductie.sch	Partition 1\NONAME [NTFS]\[root]\WINDOWS\SchCache\DNproductie.sch	370536
winsrv167	SchCache	Partition 1\NONAME [NTFS]\[root]\WINDOWS\SchCache\	272
winsrv167	9cb4f8bdfaa302f85333ef07fa3fb192_60643e52-42b0-4d55-aea2-38a5b64b11ec	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\Crypto\RSA\S-1-5-21-4190788878-266275749-1156481715-500\9cb4f8bdfaa302f85333ef07fa3fb192_60643e52-42b0-4d55-aea2-38a5b64b11ec	2073
winsrv167	40F1C4C24E802122FBC4DB5061CADF1DDCEB33DD	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\Certificates\40F1C4C24E802122FBC4DB5061CADF1DDCEB33DD	858
winsrv167	Certificates	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\Certificates\	320
winsrv167	CRLs	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\CRLs\	48
winsrv167	CTLs	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\CTLs\	48
winsrv167	Request	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\	456
winsrv167	MinIenM Organisatie CA - G2.p7b.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\MinIenM Organisatie CA - G2.p7b.lnk	560
winsrv167	keysafe.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\nCipher\Log Files\keysafe.log	566
winsrv167	cmdadp.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\nCipher\Log Files\cmdadp.log	388
winsrv167	cmdadp-debug.log	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\All Users\Application Data\nCipher\Log Files\cmdadp-debug.log	0
winsrv167	httpd.conf.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\httpd.conf.lnk	696
winsrv167	ErrorRep	Partition 1\NONAME [NTFS]\[root]\WINDOWS\PCHealth\ErrorRep\	256
winsrv167	ErrorRep	Partition 1\NONAME [NTFS]\[root]\WINDOWS\PCHealth\ErrorRep\	256
winsrv167	UserDumps	Partition 1\NONAME [NTFS]\[root]\WINDOWS\PCHealth\ErrorRep\UserDumps\	576
winsrv167	UserDumps	Partition 1\NONAME [NTFS]\[root]\WINDOWS\PCHealth\ErrorRep\UserDumps\	576
winsrv167	dist.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\dist.lnk	531
winsrv167	schema.conf.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\schema.conf.lnk	677
winsrv167	iXudad.conf.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\iXudad.conf.lnk	677
winsrv167	xudad.oc.conf.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\xudad.oc.conf.lnk	683

winsrv167	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	140
winsrv167	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	140
winsrv167	origrsa.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\origrsa.zip.lnk	416
winsrv167	CertiID Enterprise Certificate Authority.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\CertiID Enterprise Certificate Authority.crt.lnk	804
winsrv167	d$ on winsvr057	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\	256
winsrv167	d$ on winsvr057	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\	256
winsrv167	Desktop.ini	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\Desktop.ini	75
winsrv167	Desktop.ini	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\Desktop.ini	75
winsrv167	muh.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\muh.lnk	571
winsrv167	target.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\target.lnk	463
winsrv167	target.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on winsvr057\target.lnk	463
winsrv167	USPP-Perso Certificate ST4000 260-160-364.crt.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\USPP-Perso Certificate ST4000 260-160-364.crt.lnk	879
winsrv167	certs.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Recent\certs.lnk	631
winsvr057	winsvr022.txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\winsvr022.txt	461
winsvr057	winsvr167.txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\winsvr167.txt	272
winsvr057	kcavkfsc.dll	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\kcavkfsc.dll	65536
winsvr057	njnypgqa.exe	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\njnypgqa.exe	53760
winsvr057	winsvr056.txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\administrator.DNPRODUCTIE\Desktop\winsvr056.txt	458
winsrv055	get.xuda	Partition 2\Data [NTFS]\[root]\Progs\rsa_cm_68\WebServer\enroll-server\ca\get.xuda	254
winsrv055	dbpub.zip	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Desktop\dbpub.zip	59545925
winsrv055	administrator@10.10.20[1].txt	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\npost\Desktop\administrator@10.10.20[1].txt	141
winsrv055	dbpub.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\dbpub.zip.lnk	404
winsrv022	m.zip.lnk	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\Recent\m.zip.lnk	380
winsrv056	add-pkcs10-request[16].htm	Partition 5\NONAME [NTFS]\[orphan]\add-pkcs10-request[16].htm	96617
winsrv056	osvchost.exe	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system\osvchost.exe	36864
winsrv056	Desktop.ini	Partition 5\NONAME [NTFS]\[root]\Documents and Settings\ljensma\Recent\Desktop.ini	150
winsrv056	C8463ECBE33BC240263A0B094E46D510.mof	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\wbem\AutoRecover\C8463ECBE33BC240263A0B094E46D510.mof	2826402
winsrv056	23BDE61F1F4FACE17E9B0C01F2A1FD9B.mof	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\wbem\AutoRecover\23BDE61F1F4FACE17E9B0C01F2A1FD9B.mof	36574
winsrv056	Settings[2].htm	Partition 5\NONAME [NTFS]\[orphan]\Settings[2].htm	3097
winsrv056	direct83[1].exe	Partition 5\NONAME [NTFS]\[orphan]\direct83[1].exe	37888
winsrv056	csrsss.exe	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\csrsss.exe\	37888
winsrv056	Zone.Identifier	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\csrsss.exe\Zone.Identifier	26
winsrv056	139[1].exe	Partition 5\NONAME [NTFS]\[orphan]\139[1].exe	37888
winsrv056	svhost.exe	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\svhost.exe\	37888
winsrv056	Zone.Identifier	Partition 5\NONAME [NTFS]\[root]\WINDOWS\system32\svhost.exe\Zone.Identifier	26
winsrv053	svchost.exe	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system\svchost.exe\	19702
winsrv053	Zone.Identifier	Partition 1\NONAME [NTFS]\[root]\WINDOWS\system\svchost.exe\Zone.Identifier	26
winsrv055	Default.rdp	Partition 1\NONAME [NTFS]\[root]\Documents and Settings\Administrator.DNPRODUCTIE\My Documents\Default.rdp	1214
winsrv056	x-select-settings.xuda	Partition 2\NONAME [NTFS]\[orphan]\x-select-settings.xuda	28875

Appendix VI (Confidential)

The information in this appendix must be kept confidential due to the ongoing investigation or due to the privacy of the employees of DigiNotar.

Appendix V-I List of attackers IP addresses

Reference	IP address	Source	Remark
	109.131.139.148	IIS logs winsrv101	
	184.73.172.213	IIS logs winsrv101	
	188.34.57.139	IIS logs winsrv101	
	202.60.66.32	IIS logs winsrv101	
	204.12.8.116	IIS logs winsrv101	
	207.232.7.167	IIS logs winsrv101	
	209.190.184.207	IIS logs winsrv101	
	213.229.81.34	IIS logs winsrv101	
	217.122.166.160	IIS logs winsrv101	
	217.169.64.30	IIS logs winsrv101	
	50.17.249.10	IIS logs winsrv101	
	50.57.92.77	IIS logs winsrv101	
	62.75.181.81	IIS logs winsrv101	
	66.249.66.23	IIS logs winsrv101	
AttIP5	67.202.50.234	WINSRV119	Not in the IIS logs of winsrv101
	74.220.215.87	IIS logs winsrv101	
	77.104.76.200	IIS logs winsrv101	
	77.104.76.95	IIS logs winsrv101	
AttIP7	77.104.76.96	IIS logs winsrv101	OCSP request test run. Resolved to an ADSL user in Iran.
AttIP3	77.104.76.97	IIS logs winsrv101	
	77.104.76.98	IIS logs winsrv101	
	80.101.202.176	IIS logs winsrv101	
	81.164.210.31	IIS logs winsrv101	
	81.242.49.214	IIS logs winsrv101	
AttIP1	83.170.68.10	Malware WINSRV119	csrsss.exe Not in the IISlog of {SVO8}? Resolves to warfit.com
AttIP6	83.220.51.66	IIS logs winsrv101	
AttIP4	85.17.182.207	IIS logs winsrv101	
	88.80.216.130	IIS logs winsrv101	
AttIP2	94.236.23.234	Malware WINSRV119	Niet in de IISlog van SVO8?

Appendix V-II List of administrators

Reference	Real name

Admin1	ljensma

Van: [redacted](Fox-IT) [[redacted]@fox-it.com]
Verzonden: woensdag 25 juli 2012 19:07
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: het rapport!

Kan je al iets aangeven van de hoeveelheid 'changes'. Er is dan maar korte doorlooptijd over immers.

[redacted] heb jij de tijd om dit op te pakken?

From: [redacted] [mailto:[redacted]@minbzk.nl]
Sent: woensdag 25 juli 2012 18:23
To: [redacted](Fox-IT)
Cc: [redacted]
Subject: RE: het rapport!

Beste [redacted]
we zouden het rapport begin augustus definitief willen hebben (bv. 6 aug.)
Volgende week kom ik met een aantal vragen en opmerkingen over het rapport naar je toe.

Met vriendelijke groet,

[redacted]
Portefeuillehouder Informatiebeveiliging en privacy .....
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
DGOBR, Informatiseringsbeleid Rijk
Schedeldoekshaven 200 | 2511 EZ | Den Haag | H 1041
Postbus 20011 | 2500 EA | Den Haag .....
M 06-[redacted]
T secretariaat IR: 070-426 7235
[redacted]@minbzk.nl
http://www.rijksoverheid.nl
Samen met de ministeries optimaliseert en faciliteert DG OBR de bedrijfsvoering en organisatie van het Rijk. Zo kan het Rijk zijn maatschappelijke functie beter vervullen.
Beveiligingsbeleid rijksoverheid:
- Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement
- Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement
- De klassieke informatiebeveiligingsaanpak waarbij inperking van mogelijkheden de boventoon voert maakt plaats voor veilig faciliteren
- Methoden voor rubricering en continue evaluatie ervan zijn hanteerbaar om onder- en overrubricering te voorkomen
- Naast aandacht voor netwerkbeveiliging meer aandacht voor gegevensbeveiliging
- Verantwoord en bewust gedrag van mensen is essentieel voor een goede informatiebeveiliging
- Kaders en maatregelen worden overheidsbreed afgesproken en ingezet. In uitzonderingsgevallen wordt – in overleg – afgeweken
- Kennis en expertise zijn essentieel voor een toekomstvaste informatiebeveiliging en moeten (centraal) geborgd worden
- Informatiebeveiliging vereist een integrale aanpak

-----Oorspronkelijk bericht-----
Van: [redacted](Fox-IT) [mailto:[redacted]@fox-it.com]
Verzonden: dinsdag 10 juli 2012 9:50
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: het rapport!

Hoi [redacted]

Ik neem aan dat jullie hard aan het lezen zijn? Heb je een planning voor ogen, wanneer wij eventuele wijzigingen kunnen bespreken en wanneer je de definitieve wilt hebben?

From: [redacted](Fox-IT)
Sent: woensdag 4 juli 2012 9:02
To: [redacted]@minbzk.nl)'
Cc: [redacted]; [redacted]@minbzk.nl; [redacted]
Subject: het rapport!

[redacted]

[redacted] heeft me aangegeven dat de overeenkomst die ik op 28 juni naar jullie gestuurd heb, door [redacted] ondertekend is en retour naar ons komt.

Op basis van dat goede nieuws bij deze bijgevoegd een pdf van het rapport. Mochten jullie opmerkingen hebben, dan hoor ik dat natuurlijk graag.

In de zip zit het originele word bestand dat gebruikt kan worden om changes aan te geven.

Met vriendelijke groet,

[redacted]

[redacted]@fox-it.com | [redacted] linkedin | [redacted]

FOX IT
FOR A MORE SECURE SOCIETY

Olof Palmestraat 6, Delft
Postbus 638, 2600 AP Delft
T +31152847999 M + 316[redacted]

FOX-IT.COM

FOX-IT
EXPERTS IN IT SECURITY

Black Tulip

Report of the investigation into the DigiNotar Certificate Authority breach

Classification	**CONFIDENTIAL**
Customer	Ministry of the Interior and Kingdom Relations
Project no./Ref. no.	PR-110202_CC
Date	19 June 2012
Version	0.9
Team	Hans Hoogstraaten (Team leader) Ronald Prins (CEO) Daniel Niggebrugge Danny Heppener Frank Groenewegen Janna Wettinck Kevin Strooy Pascal Arends Paul Pols Robbert Kouprie Steffen Moorrees Xander van Pelt Yun Zheng Hu
Business Unit	Cybercrime
Pages	101

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

WARNING
Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. Fox-IT cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by any information this document contains.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
Email: fox@fox-it.com
Internet: www.fox-it.com

Management summary

DigiNotar and the initial incident response

DigiNotar B.V. was founded as a privately-owned notarial collaboration in 1998. DigiNotar provided digital certificate services as a Trusted Third Party (TTP) and hosted a number of Certificate Authorities (CAs). The certificates issued by DigiNotar were trusted worldwide to secure communication on the basis of a Public Key Infrastructure (PKI). The services that DigiNotar provided included issuing SSL certificates to secure websites, issuing accredited qualified certificates that could be used as the legal equivalent of a handwritten signature and issuing PKIoverheid[1] certificates for various Dutch eGovernment purposes.

On July 19, 2011, a DigiNotar employee discovered that rogue certificates were issued by one of its Certificate Authorities. The company immediately took several measures to control the incident, including the hiring of a third party specialized in IT security to investigate the intrusion. At the end of July 2011, DigiNotar was under the impression that the intrusion of its network and services had been contained. On August 28, 2011, the content of a rogue wildcard certificate that was issued by DigiNotar for the Google.com domain was posted. The rogue certificate was being abused in a large scale man-in-the-middle (MITM) attack on users in the Islamic Republic of Iran.

Commissioning of Fox-IT and subsequent measures

On August 30, 2011, Fox-IT was asked by DigiNotar to investigate the intrusion of its network. One of the first measures taken by Fox-IT was to place an incident monitoring service on DigiNotar's network, to determine if unauthorized activity was still taking place. A sensor captures and monitors all traffic between the internal network and the Internet. For the Fox-IT monitoring service, at least one person is on standby at all times to analyze suspicious traffic in real time. Additionally, the behavior of the Online Certificate Status Protocol (OCSP) responder[2] at DigiNotar was changed on September 1, 2011 as a precautionary measure at the initiative of Fox-IT, which effectively revoked all remaining rogue certificates that had been issued by the intruder.

An interim report with preliminary findings was provided to DigiNotar and was published on September 5, 2011 by the Dutch state. On this date an operational director that acted on behalf of the Dutch state was appointed by the board of DigiNotar under Power of Attorney. At the instruction of the Dutch National Police Services Agency (KLPD) and the public prosecutor's office (OM), identifying evidence regarding the intruder was specifically included in the continued investigation. This definitive report is the outcome of that fact finding investigation performed by Fox-IT into the intrusion of DigiNotar's network and the subsequent MITM attack.

The primary aims of the combined investigation that Fox-IT performed at the request of DigiNotar and the Dutch Ministry of the Interior and Kingdom Relations (BZK) were to determine how DigiNotar's network had been breached, to what extent it had been breached, if the various Certificate Authorities that DigiNotar operated had been compromised and if evidence that could lead to a potential criminal indictment of the intruder could be safeguarded. For these purposes, various sources of information were gathered and examined, including the log files from the web servers, firewalls and the various CA servers. Additionally, the images of relevant systems in DigiNotar's network were analyzed. Approximately 400 forensically sound disk images were created during the course of the investigation of 265 systems, amounting to a total of seven terabytes of compressed data.

The investigation of DigiNotar's network and the intrusion

The DigiNotar network was divided into 24 different internal network segments. An internal and external Demilitarized Zone (DMZ) separated most segments of the internal network from the Internet. The zones were not strictly described or enforced and the firewall contained many rules that specified exceptions for network traffic between the various segments. The main production servers of DigiNotar, including the CA servers and the accompanying hardware security module (netHSM), were located in a physically highly-secured room and in the Secure-net network segment. The Certificate Authorities that were hosted by DigiNotar were managed by software running on eight different CA servers.

[1] A Public Key Infrastructure for the Dutch government facilitating trusted digital communication.
[2] A responder that informs the inquirer of the validity of a certificate using the Online Certificate Status Protocol (OCSP); further details are included in paragraph 10.2.

The investigation showed that web servers in DigiNotar's external Demilitarized Zone (DMZ-ext-net) were the first point of entry for the intruder on June 17, 2011. During the intrusion, these servers were used to exchange files between internal and external systems, with scripts that were placed on these systems serving as rudimentary file managers. The (recovered) log files from the Main-web server from the period of the intrusion showed a list of 12 internal and 21 suspicious external systems that connected to these scripts and a list of more than 100 unique filenames that were exchanged. Internal systems that requested these scripts were most likely to have been compromised[3], while external systems that requested these scripts were most likely used by the intruder to access DigiNotar's network.

From the web servers in DMZ-ext-net, the intruder first compromised systems in the Office-net network segment between the 17th and 29th of June 2011. Subsequently, the Secure-net network segment that contained the CA servers was compromised on July 1, 2011. Specialized tools were recovered on systems in these segments, which were used to create tunnels that allowed the intruder to make an Internet connection to DigiNotar's systems that were not directly connected to the Internet. The intruder was able to tunnel Remote Desktop Protocol connections in this way, which provided a graphical user interface on the compromised systems, including the compromised CA servers.

Recovered log files showed that the first extraordinary certificate signing attempts on a CA server occurred on July 2, 2011 on the Relation-CA server. The first rogue certificate was successfully issued on July 10, 2011. The investigation by Fox-IT showed that all servers that managed Certificate Authorities had been compromised by the intruder, including the Qualified-CA server, which was used to issue both accredited qualified and government certificates. In total, a non-exhaustive list of 531 rogue certificates with 140 unique distinguished names (DNs) and 53 unique common names (CNs) could be identified. The last known date for traffic that was initiated from within DigiNotar's network to an IP address that was presumably (ab)used by the intruder was on July 22, 2011. Traces of activity by the intruder in DMZ-ext-net were found up to July 24, 2011.

Investigation of compromised CA servers and Certificate Authorities

The logging service for the CA management application ran on the same CA servers that were compromised by the intruder. The investigation also showed that the intruder had full administrative rights and that database records on these CA servers were deleted or otherwise manipulated. Consequently, suspicious entries in the log files of the CA servers can only be used to make inconclusive observations regarding unauthorized actions that took place, but the absence of suspicious entries cannot be used to infer that no unauthorized actions took place.

In order to successfully issue rogue certificates, compromising a server that hosted a Certificate Authority was not enough, as it also required the abuse of an active corresponding private key in the netHSM. This means that the unauthorized actions that might have taken place could not have included the issuing of rogue certificates if the corresponding private key had not been active during the intrusion period. The private keys were activated in the netHSM using smartcards. No records could be provided by DigiNotar regarding if and when smartcards were used to activate private keys, except that the smartcard for the Certificate Authorities managed on the CCV-CA server, which is used to issue certificates used for electronic payment in the retail business, had reportedly been in a vault for the entire intrusion period.

In the log files of some CA servers, log entries were found that indicated the automatic generation of a Certificate Revocation List (CRL). Certificate Authorities usually issue CRLs at regular intervals according to their policies. These CRLs are signed by the issuing Certificate Authorities, which can only occur if a private key was active on the netHSM. The log entries referring to such an automatic process thus indicated that the private keys in the netHSM were activated and that there was potentially an opportunity for the intruder to abuse these private keys.

Given the inevitable uncertainty if the other Certificate Authorities had been abused to issue rogue certificates, PKI standards required all certificates that were issued by these Certificate Authorities to be revoked and the Certificate Authorities themselves to be removed from trust lists in the software products that contained them. The impact of revoking the certificates that were issued by DigiNotar varied depending on their usage and had to be assessed on a case by case basis. None of the issued

[3] In information security, a system is regarded as being compromised if its confidentiality, integrity and/or availability can no longer be guaranteed.

certificates could be validated by PKI and therefore could not be trusted anymore, which included all certificates issued prior to the intrusion.

Investigation into the intruder

In one of the scripts that were found on a CA server, the intruder left a signature that was also identified after the breach of the certificate service provider Comodo. The vast majority of the external IP addresses that were identified during the investigation were probably used as proxies to obscure the identity of the intruder. The true IP address of the intruder may have been revealed by error however, when the intruder erroneously connected to the Main-web server without using one of the proxies that was regularly used. The error occurred only once and was corrected within seconds. This IP address was also identified in other parts of the investigation.

More specifically, during the investigation a tool was identified that connected back to an external IP that was used as a proxy by the intruder. When this external system was examined, after an official request for assistance by the proper authorities, its log files also showed connections from the IP address that had erroneously been revealed. Furthermore, eight requests were made by this IP-address for a rogue Yahoo certificate, presumably to test DigiNotar's OCSP responses. The first three OCSP requests for the wildcard Google.com certificate used for the MITM attack came from an IP address that also connected to the Main-web server once. These two IP addresses and three other IP addresses that were used by the attacker are in a close range, located in the Islamic Republic of Iran. A complete list of all the identified IP addresses that are suspected to have been abused by the intruder was shared with the proper authorities.

Investigation of the MITM attack

The fact that the chain of trust of PKI had been broken due to the intrusion at DigiNotar did not just result in a hypothetical threat, as at least one rogue certificate was subsequently abused in practice. A rogue certificate for `*.google.com` was abused to perform a massive man-in-the-middle (MITM) attack. In such an attack, the attacker places himself between two parties to intercept or modify the traffic between them. The investigated MITM attack was compounded with a form of redirection, where users who tried to reach legitimate websites that were hosted by Google were redirected to fraudulent versions of these websites. The traffic which was meant for Google and that was intercepted was not necessarily forwarded to Google, as users may have been presented with a page specifically intended to phish for their credentials.

The requests made to the OCSP responder for the rogue `*.google.com` certificate indicated that a total number of 298,140 unique IP addresses could be identified as having been victimized by the MITM attack. The number of unique IP addresses can only be regarded as a very rough approximation of the number of users affected. Multiple users can be masqueraded behind a single external IP address, while a single user can also make requests from multiple IP addresses. Moreover, relatively old software such as Internet Explorer 6 does not support OCSP requests and these users are therefore not included in the aforementioned approximation.

The IP addresses in the OCSP log files were enriched with GeoIP information, which showed that 95% of these IP addresses originated from the Islamic Republic of Iran. These IP addresses originated from 143 different autonomous systems (often Internet Service Providers), while 60% of the requests originated from only 4 Iranian autonomous systems. A sample of the remaining 5% of the affected IP addresses was inspected, which mainly showed exit nodes for The Onion Router (Tor), proxies and VPN servers. On this basis it can be concluded that the MITM attacks almost exclusively targeted at users who were located in the Islamic Republic of Iran.

The most likely modus operandi used during the MITM attack, based on the accumulated OCSP data, is that of DNS cache poisoning. A DNS cache poisoning attack relies on the fact that DNS servers cache the responses of DNS servers at a higher level in the infrastructure. By flooding a DNS server with forged responses for a particular domain, as if it had received the response from a higher DNS server, it is possible to "poison" the entries in the DNS server and thus its responses to clients at a lower level in the infrastructure. The poisoned entries are valid for as long as the Time To Live (TTL) allows, after which these entries expire and another DNS request would be made to a higher DNS server for the domain if requested by a client. This modus operandi would explain why traffic that went through proxies, Tor exit nodes and VPNs was also affected by the MITM attack and would also correspond with the peak-like

behavior and the occurrence of repeated and sudden declines in OCSP requests that were made for rogue certificates.

Lessons learned

The modus operandi that was used in the intrusion of DigiNotar is unusual when compared to what is more generally encountered, which is the modus operandi of a criminal organization, where the aim is to make money or obtain information and intrusions are performed covertly or the modus operandi of hacktivists. The intruder of DigiNotar seems to have had the specific intention to abuse the private key of a trusted Certificate Authority to spy on a large number of Iranian users. The intrusion at the certificate service provider DigiNotar and the ensuing MITM attack resulted in an erosion of trust of the general public in the existing Public Key Infrastructure, which is central to its operation.

Average users have a very limited capacity to protect themselves properly against attacks such as those against Trusted Third Parties in the Public Key Infrastructure. Given the impact that a breach in the security of a Certificate Authority has on the Public Key Infrastructure as a whole, and the Internet in general, ensuring the security of every Certificate Authority is paramount to the trust in PKI and its role in providing security for a diverse range of activities on the Internet. While the approach to protecting the potential targets from this type of intrusion does not differ significantly from other threats, the range of scenarios that need to be taken into account is rapidly expanding.

Table of Contents

1 Introduction

1.1 Background

The confidentiality and security of the communication that occurs over the Internet in large part relies on the use of the cryptographic protocols Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL). An essential element of these protocols is the use of public key certificates, which use a digital signature to bind a public key with the identity of a specific system or a website. These public key certificates are issued by Certificate Authorities (CAs). A certificate authority is a third party that is trusted by both the holder of the certificate and the party that relies on the certificate to identify the holder. Together with the necessary hardware, software and corresponding procedures, the Certificate Authorities form the basis of a Public Key Infrastructure (PKI).

DigiNotar B.V. [4] was a Certificate Authority that provided digital certificate services. The digital certificates were used to secure Internet traffic, to issue (qualified) electronic signatures and to provide data encryption. DigiNotar also issued government accredited PKIoverheid certificates. During the months of June and July of 2011, the security of DigiNotar was breached and rogue certificates were issued. One of these certificates, a rogue Google certificate, was abused on a large scale in August of 2011 targeting primarily Iranian Internet users. At the end of August the intrusion became public knowledge and set into motion a chain of events that eventually led to the removal of all the Certificate Authorities that were hosted by DigiNotar from trust lists and ultimately the bankruptcy of the company.

On September 3 of 2011 the Dutch state expressed the intention to take over the operational control of DigiNotar, including the responsibility for the commissioned investigation into the intrusion of DigiNotar's network by Fox-IT. The interim report with the preliminary findings of Fox-IT was provided to DigiNotar and was published on September 5, 2011 by the Dutch state. On this date an operational director that acted on behalf of the Dutch state was appointed by the board of DigiNotar under Power of Attorney. At the instruction of the Dutch police (KLPD) and the public prosecutor's office (OM), identifying evidence that could lead to the intruder was specifically included in the continued investigation. This report is the outcome of the technical fact finding investigation by Fox-IT into the intrusion of DigiNotar's network and the subsequent man-in-the-middle (MITM) attack. Former employees of Diginotar B.V. were given the chance to respond to a draft version of this report for the purpose of verification and their relevant input was incorporated where appropriate.

This report provides an overview of the results of the investigation by Fox-IT and evidence that was left by the intruder in the internal network of DigiNotar. More detailed information that was uncovered in regard to the identity and/or location of the intruder has been excluded from this report and was made available only to the proper authorities. Once this information was obtained, the focus shifted from tracing the intruder's steps in detail to concluding the investigation and this report.

Questions that lie outside the scope of the investigation will not be answered in this report, but may be answered after further research. The findings in this report are reported in such a way that they can be continued or repeated by other parties if they are provided access to the source material. Potential follow-up questions for further research are included in Chapter 12.

References to servers are made using descriptive names. A comprehensive list of the referenced servers including their IP addresses and exhibit numbers can be found in Appendix I. All dates and timestamps are in Central European (Summer) Time (CEST; UTC+2), unless explicitly stated otherwise.

1.2 Events leading up to the report

The rogue certificates that had been generated on July 10, 2011 were first discovered when an automated routine test that had failed to work was restored on July 19, 2011. The test signaled that there was a mismatch between the certificates that had been issued and the administrative records in the back office of DigiNotar. The staff of DigiNotar proceeded to examine the CA management applications and found that rogue certificates had been issued. In response DigiNotar took several measures to

[4] A B.V. (*Besloten Vennootschap*) is a limited liability company, a commonly used legal entity for corporations in the Netherlands.

control the incident and its employees were under the impression that the incident had been contained at the end of July of 2011.

On August 28, 2011, a concerned Gmail user posted a warning that his web browser had displayed on a Google support forum. The Google Chrome web browser that he used blocked access to the Google website because Chrome detected the usage of an invalid certificate[5]. This certificate had been issued by one of the Certificate Authorities that were controlled by DigiNotar. Subsequently, similar reports were posted on the Internet by others. According to DigiNotar, the Dutch Government Computer Emergency Response Team (GOVCERT.NL) was notified on August 29, 2011 and various other stakeholders were notified in the morning of August 30.

Fox-IT was asked to start an investigation into the breach of DigiNotar's network on August 30, 2011 with the purpose to help DigiNotar to identify if unauthorized activity was still taking place, to reveal to what extent DigiNotar's systems in general and PKIoverheid specifically had been compromised and to identify the path of the intruder through the network, if remarkable OCSP requests were taking place and to ascertain the impact of the rogue certificate that was being abused in the Islamic Republic of Iran. An incident response team was assembled by Fox-IT that started the investigation immediately. The team included forensic IT experts, cybercrime investigators, malware analysts and a security expert with PKI experience.

In the days that followed several actions were taken by DigiNotar with the help of Fox-IT to further control the incident and to limit the damage to its business. On September 2, 2011 an interim report with preliminary findings was drafted for DigiNotar stakeholders in consultation with DigiNotar. These results were shared verbally with GOVCERT.NL by DigiNotar. Once the full impact of the intrusion became clear to the Dutch Ministry of the Interior and Kingdom Relations (BZK) it took over the lead role in Fox-IT's ongoing investigation.

The focus of the investigation shifted as a result of the involvement of the ministry BZK. The focus of the continued investigation was primarily to determine the extent of the breach and its impact on PKIoverheid, to assist the KLPD by investigating the infrastructure to produce evidence against the intruder and to describe the lessons that could be learned from such an incident. As a result, questions into the path of the intruder through DigiNotar's network became less relevant and the level of certainty of statements that are made in regard to the attacker's path will reflect this shift in focus. Once it became clear to what extent the CA servers had been compromised and all the IP addresses that could be connected to the intruder were collected, the investigative stage was concluded. This report is the culmination of the incident response investigation that was performed at the request of both DigiNotar and the ministry BZK.

In this report, the term "intruder" should not be read to convey any information in regard to whether one or more persons were involved in the various stages of the intrusion or if these acts were perpetrated by a male or a female. The term "attacker" is used similarly to describe the person or persons who perpetrated the man-in-the-middle (MITM) attack on primarily Iranian users of Google services.

1.3 Involved parties

Multiple parties were involved in the DigiNotar incident response and the subsequent investigation. The parties were as follows:

Party	Role
AIVD	The General Intelligence and Security Service of the Netherlands.
BZK	The Dutch Ministry of the Interior and Kingdom Relations is responsible for national affairs, including the Dutch PKI infrastructure (PKIoverheid) in which DigiNotar took part.
Cert-Bund	Computer Emergency Response Team der Bundesverwaltung is the German equivalent of GOVCERT.NL.
DigiNotar B.V.	Former notarial collaboration that provided various certificate services including issuing digital certificates.

[5] Google Chrome performs additional certificate verification on Google certificates (certificate pinning) in addition to the standard in PKI prescribed verification.

Party	Role
Fox-IT B.V.	Security company that provides solutions for the protection of state secrets, the investigation of digital crimes, audits, managed security services and consultancy.
GOVCERT.NL	Cyber security and emergency response team of the Dutch government.
Hoffman B.V.	A company that offers investigative, forensic and strategic risk management services.
KLPD	The Dutch National Police Services Agency and its Team High Tech Crime Unit.
Manufacturers	Manufacturers of software that uses certificates, such as Mozilla, Microsoft, Adobe and the Tor Project.
OM	The Dutch Public Prosecutor.
OPTA	The Independent Post and Telecommunications Authority of the Netherlands is responsible for the registration of Certificate Service Providers (CSPs) that issue qualified electronic signatures.
Parties relying on DigiNotar B.V.	Enterprise customers of DigiNotar who used certificates issued by DigiNotar, such as lawyers, notaries, judicial officers and ministries (and their customers).

1.4 Timeline of events

The timeline below shows the most relevant events that occurred after the public disclosure of the existence of a rogue certificate that had been issued by DigiNotar. An overview of the events that took place before this public disclosure is detailed in paragraph 2.1.

Date	Description
28-Aug-2011	On a Google support forum, a customer of the Iranian ISP ParsOnline posted details about a certificate warning that was presented to him by Google Chrome for a rogue `*.google.com` certificate[6].
29-Aug-2011	Google received multiple reports about an attempted SSL MITM attack. Articles about a rogue `*.google.com` certificate appeared on the blogs of Mozilla, Google, Microsoft and other manufacturers. The rogue `*.google.com` certificate was revoked by DigiNotar. Additionally, GOVCERT.NL was notified by Cert-Bund.
30-Aug-2011	Fox-IT was asked by DigiNotar to initiate an investigation into the intrusion at DigiNotar to detect whether the intruder was still active.
01-Sep-2011	At the advice of Fox-IT, the behavior of the OCSP responder was changed so its responses were based on a white list of known valid certificates, effectively revoking all unknown certificates (see paragraph 2.2.1).
02-Sep-2011	The preliminary investigation by Fox-IT indicated that the integrity of the CA server that was used for managing qualified certificates and PKIoverheid was breached (Qualified-CA). DigiNotar informed GOVCERT.NL about the details of this finding.
03-Sep-2011	The Dutch government publicly revoked trust in DigiNotar and the certificates that had been issued by the company. Following this announcement, most browser manufacturers also revoked their trust in DigiNotar, if they had not done so already.
05-Sep-2011	The interim report on the breach of the DigiNotar Certificate Authority was published[7]. DigiNotar formally reports the intrusion to the police.
14-Sep-2011	OPTA ended the registration of DigiNotar B.V. as a certificate authority for qualified signatures on the basis of the Dutch Telecommunicatiewet (the Dutch law on telecommunication).
19-Sep-2011	DigiNotar filed a bankruptcy petition under Article 4 of the Dutch Bankruptcy Act.
20-Sep-2011	The Court of Haarlem declared DigiNotar B.V. to be bankrupt.
28-Sep-2011	All qualified and PKIoverheid certificates issued by DigiNotar were revoked.
01-Nov-2011	Most of the remaining active public certificates were revoked. BAPI (used for the Dutch Tax administration) and two private DigiNotar Certificate Authorities were excluded from this revocation[8].

[6] Google Groups, "Is This MITM Attack to Gmail's SSL?" at http://groups.google.com/a/googleproductforums.com/d/topic/gmail/3J3r2JqFNTw/discussion

[7] Rijksoverheid, "Interim Report DigiNotar Certificate Authority breach" at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

[8] The Dutch tax administration took additional security measures and accepted the minimal risks that remained. This also applies to the operation of the internally used private CAs.

1.5 Structure of the report

In this introductory chapter, the background of the events against which the incident occurred is described. The overview includes a summary of how DigiNotar's internal network was set up and operated. Chapter 2 provides insight into the incident response investigation that was performed by Fox-IT at the request of DigiNotar and the ministry BZK. More specifically, it details how the investigation was approached and what actions were taken. Chapter 3 provides a general overview of the state of affairs that Fox-IT encountered at DigiNotar when its incident response investigation was initiated.

Chapters 4 through 8 describe the relevant results of the investigation that was performed by Fox-IT. More specifically, Chapter 4 details the investigation into the web servers that were used as stepping stones by the intruder; Chapter 5 details the investigation into the firewall logs; and Chapter 6 details the investigation into the CA servers. Chapter 7 contains an overview of the investigation that was performed on safeguarded hard disks. Assorted smaller sources of information for the investigation are discussed in Chapter 8. Chapter 9 contains the investigative conclusions on the basis of the preceding chapters, which includes an image of the referenced systems and network segments.

The large-scale MITM attack that took place in the aftermath of the intrusion of DigiNotar's network is the subject of Chapter 10. In this chapter the results of scrutinized OCSP log files provide more details about this attack.

Lessons that can be learned from the intrusion of DigiNotar's network are discussed in Chapter 11. In Chapter 12 a number of questions are formulated that could serve as the basis for further investigation on the source material. References and a description of some of the commonly used terms in this report are included in Chapter 13.

There are nine appendices to this report that are referenced throughout the report. Appendix I includes the detailed references to the equipment that was present in DigiNotar's internal network. Appendix II provides details about IP addresses that are suspected to be linked to the attacker. Due to the ongoing investigation, the actual IP addresses have been removed. Appendix III provides a timeline of notable traffic that was found when investigating the firewall logs. Appendix IV contains a list of Certificate Authorities that were automatically generating CRLs. Appendix V includes the Certificate Authorities that were hosted at DigiNotar. Appendix VI lists references to private keys that were present in the databases of the CA servers. Appendix VII lists serial numbers encountered in the `serial_no.dbh` database on servers managing Certificate Authorities that could not be related to any found certificates. Appendix VIII provides a list of the unique Common Names of the rogue certificates. Appendix IX lists a number of suspicious files that were encountered on various DigiNotar systems.

While every reasonable precaution was taken to ensure that all the data, facts and conclusions in this report are correct, the information in this report may include errors and facts may have been omitted. The limited degree of inevitable uncertainty is because the results are in part based on information that had to be extracted from systems that had been compromised and thus on data that had or may have been tampered with. Fox-IT performed a time boxed investigation into the intrusion of DigiNotar and the subsequent MITM attack for the ministry BZK. While the time provided allowed Fox-IT to perform the necessary research to support the conclusions in this report, further investigation could still be performed, which may yield new information, given the size of the breach described in this report and the amount of available data.

2 Incident response investigation

2.1 Preliminary research and actions

Prior to the involvement of Fox-IT on August 30, 2011, DigiNotar took several actions during their preliminary research. The timeline below is intended to provide the necessary context and should not be regarded as exhaustive. Based on DigiNotar's incident reports and interviews with the persons involved, the following timeline could be reconstructed:

Date	Description
19-Jul-2011	A daily routine check revealed that rogue certificates had been issued. An incident response team was formed and the identified rogue certificates were revoked.
20-Jul-2011	A script with a message of the Iranian intruder was found. More rogue certificates were discovered.
21-Jul-2011	The rogue certificates that were discovered on July 20, 2011 were revoked. CA servers were shut down at night.
25-Jul-2011	An external firm specialized in IT security was consulted to investigate the incident.
27-Jul-2011	More rogue certificates were discovered and revoked. The external security firm delivered their report. The report showed that a server in the DMZ-ext-net (Docproof2) was compromised by utilizing a known vulnerability in the DotNetNuke software and that a CA server (Relation-CA) was compromised.
28-Jul-2011	It was discovered that a rogue certificate was verified by an IP-address originating from the Islamic Republic of Iran.
29-Aug-2011	The rogue wildcard Google.com certificate that was used in the large-scale MITM attack.

2.2 Investigational approach

On August 30, 2011, Fox-IT was hired by DigiNotar. Fox-IT assisted DigiNotar by:

- Mitigating the intrusion of the network and systems within it. This included monitoring the network traffic to determine if unauthorized activity was still taking place and giving advice in regard to firewall changes, changes in the infrastructure (disconnecting network segments), rebuilding servers in the DMZ, shutting down services, et cetera.
- Managing the trust of the certificate authority:
    - Initiating a change of the behavior of the OCSP responder to be based on a white list, effectively revoking any unknown certificate serial numbers;
    - Monitoring all OCSP requests for irregularities such as unknown certificate serial numbers, unusual senders or unusual volumes;
    - Investigating which and how many rogue certificates had been issued;
    - Determining the chance that the PKIoverheid environment had been breached.

From September 3,2011 onwards, after the ministry BZK had intervened, Fox-IT additionally assisted by:

- Determining the extent of the breach in DigiNotar's security and specifically if the CA servers that were used to issue qualified certificates and/or certificates for PKIoverheid had been compromised.
- Identifying evidence that could lead to the location and identity of the intruder. This was done by investigating the relevant servers, workstations and network equipment and by assisting the High Tech Crime team of the KLPD.
- Describing the lessons that can be learned from an incident such as the intrusion at DigiNotar.

The main strategy to accomplish the aims was to determine the extent to which servers within the DigiNotar network had been compromised and to identify IP addresses and other evidence that could provide more information about the intruder.

2.2.1 Incident response monitoring

One of the first measures taken by Fox-IT was to place an incident monitoring service in the form of a network sensor on the boundary of the DigiNotar network, to determine if unauthorized activity was still taking place. The sensor captures and monitors all traffic between the internal network and the Internet. Suspicious traffic is detected by the sensor using Intrusion Detection System (IDS) functionality. All

network traffic and flow data is stored on disk so that it can be evaluated afterwards if necessary. The Fox-IT monitoring service has a person on standby at all times to analyze all suspicious traffic in real time. Detected incidents can be escalated to administrators so that further actions can be taken, such as blocking an IP address or IP range, or changing the rules on the firewall for specific ports.

In this particular case, a tailored OCSP responder monitoring service was added to the incident response sensor on August 30, 2011. This addition included a custom sniffing service for logging OCSP requests and scripts that were written to check the OCSP logs against all valid certificates, to check if OCSP requests persisted for known rogue certificates and to detect serial numbers that were unknown and could correspond with rogue certificates. Also irregularities in volumes or originating IP addresses were checked for possible other MITM attacks. As a precautionary measure, any serial number presented to the OCSP responder that did not exist in the back office records was presumed to be invalid and the OCSP responder was set to answer that the serial had been revoked.

2.2.2 Safeguarding evidence

Forensically-sound disk images were created by Fox-IT of the systems that were prone to be compromised. Initially this process was restricted to the servers that hosted the CA software and the firewall management system that contained the firewall logs. At the request of the KLPD, the process was extended to include the creation of images of additional computer systems within DigiNotar's premises.

The disk images that were produced as evidence were numbered with the prefix SVO, which refers to "Stuk Van Overtuiging" (and translates to "evidentiary item"). References within this report to (images of) machines that can also serve as evidence will be made using the function of the server. Approximately 400 disk images were created of 265 systems amounting to a total of seven terabytes of compressed data.

In addition to manually safeguarding servers, an investigational infrastructure was set up using Encase Enterprise. This method provided the means to safeguard servers and workstations without shutting them down thus limiting the impact on the operation of the business. Encase Enterprise provided the means to do a live examination on the connected servers and workstations within DigiNotar's infrastructure. The live investigation was done in an iterative and forensically-sound manner. The infrastructure aided the researchers by allowing them to instantly follow up on their results and to perform further research. Most of the computer systems were still in use during the investigation, which had a negative effect on the overall progress of the investigation, as it slowed down the process of imaging the systems and resulted in the possibility that traces could be overwritten by a running process.

During the investigation, several servers were needed for the purpose of rebuilding a new production infrastructure. If these systems were not already secured they were secured manually before they were used in the new setup. The impact of this was that the systems that were reinstalled were not a part of the network anymore and therefore could not be investigated live. Two systems could not be shut down because of the critical function that they performed for the Dutch tax and customs administration and therefore were not safeguarded or investigated. Conforming to the wishes of the ministry BZK, the following systems were not safeguarded: all but one system in the co-location, approximately 40 workstations, the backup tapes and an unknown number of laptops[9].

[9] Since no complete administration could be presented of the equipment that was in use by DigiNotar.

3 State of affairs

3.1 Organization

DigiNotar B.V. was founded as a privately-owned notarial collaboration in 1998. The customer base of DigiNotar consisted of government institutions, profit and non-profit organizations and individual citizens. The company provided digital certificate services as a Trusted Third Party (TTP) and hosted a number of Certificate Authorities (CAs). Certificates that were issued by DigiNotar included SSL certificates used to secure websites, qualified certificates used to make legal digital signatures and government accredited certificates used by the Dutch government and its citizens. The government accredited 'PKIoverheid'-certificates were used for a wide range of critical eGovernment services in The Netherlands, such as a citizen authentication service, vehicle registration and real-estate registration. The bankruptcy of DigiNotar B.V. was declared by the court of Haarlem on September 20, 2011.

3.2 Services

DigiNotar hosted multiple Certificate Authorities and provided various services based on certificates. The most important Certificate Authorities that were hosted by DigiNotar were:

- *DigiNotar PKIoverheid CA Organisatie - G2*. This is one of the sub-CAs of the root "Staat der Nederlanden Root CA" (translates to "State of the Netherlands"), which was part of the PKIoverheid infrastructure. These certificates are used for organizations in their communication with the Dutch government.
- *DigiNotar Root CA*. The root certificate was in the trust list of several web browsers, operating systems and document readers.
- *DigiNotar Qualified CA*. This sub-CA of the DigiNotar Root CA was a registered authority and the qualified certificates that it issued could be used to legally sign documents on the basis of directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.
- *DigiNotar Extended Validation CA*. This sub-CA of the DigiNotar Root CA could issue generally accepted EV-SSL certificates that are used to protect websites.

Several other sub-Certificate Authorities of the DigiNotar Root CA existed in the infrastructure of DigiNotar. Also, various other root certificates existed for various services. During the investigation a complete list of Certificate Authorities that were hosted by DigiNotar was created, which is included in Appendix VI.

3.3 Network infrastructure

In order to clarify the investigative results in chapters 4 through 8, a general overview of the network infrastructure is provided in this chapter. The overview of the network infrastructure and its normal operation is based on information that was provided by DigiNotar.

The DigiNotar network had two connections to the Internet that were provided by two different Internet Service Providers, one at the main location and one at the co-location. Behind the router that is responsible for Internet connectivity at the main location, a TippingPoint 50 Intrusion Prevention System (IPS) was present. The IPS was running a default configuration and was not used optimally, as it was placed in front of the firewall and consequently gave a lot of false positives. The IPS was planned to be placed behind the firewall. Behind the IPS the traffic was routed to a redundant Nokia firewall appliance, which was running Check Point Firewall-1 / VPN-1 (Check Point SecurePlatform NGX R65 HFA 50) with a separate management server. A third party assisted DigiNotar in operating the firewalls with support and technical fallback. A load balancer routed the traffic to the web servers.

A number of co-located servers were part of the network for the purpose of disaster recovery and business continuity. The co-located servers were not located in the same building or in a building near the main location.

Most of the systems in the DigiNotar network were running a Microsoft Windows operating system.

3.3.1 Network segments

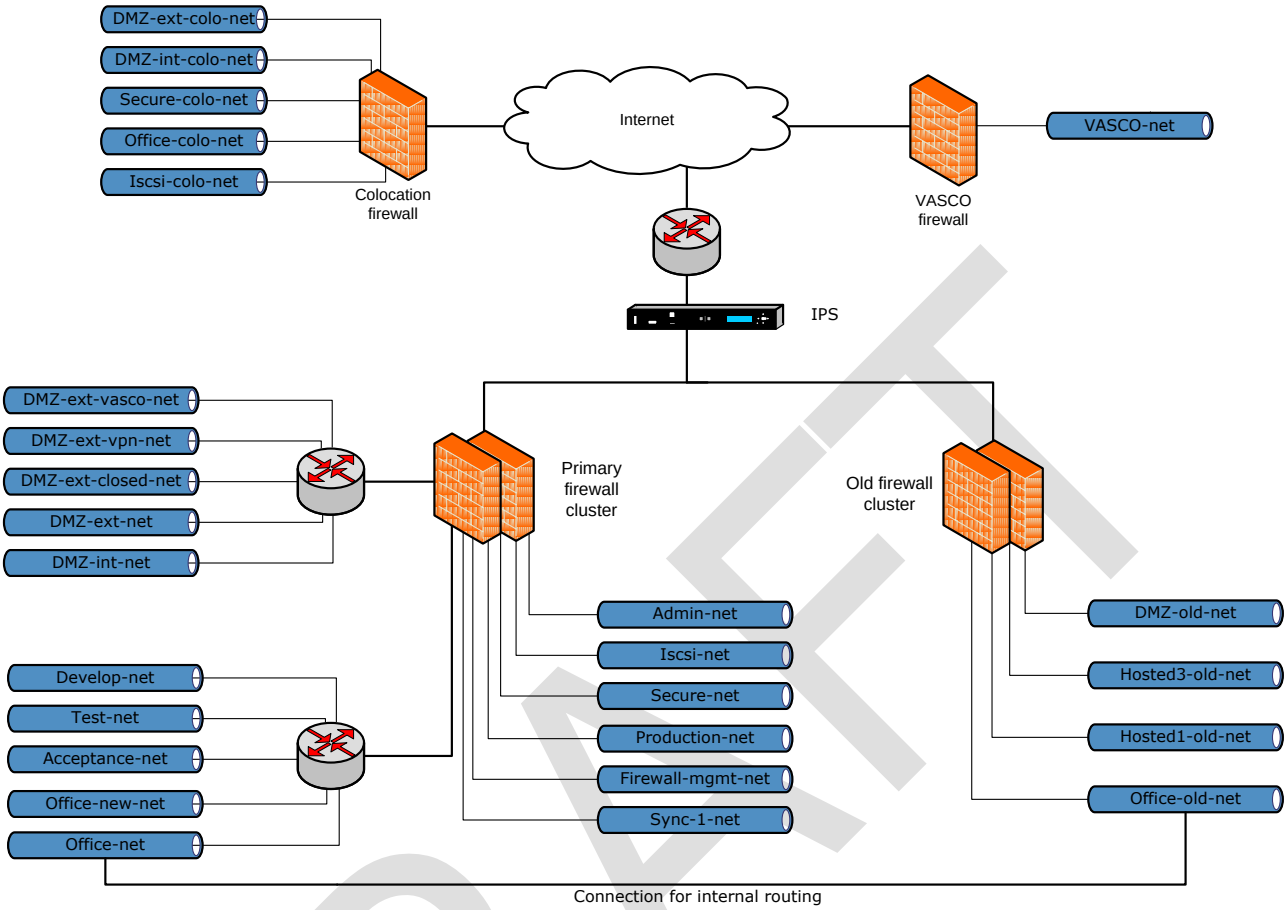


Figure 1 A sketch of the DigiNotar network[10]

The DigiNotar network was divided into 24 different internal network segments. The following list of segments was enforced, as extracted from the firewall settings on August 30.

Net name[11]	IP range	Description
DMZ-old-net	10.10.0.0/24	Old DMZ network
DMZ-ext-net	10.10.20.0/24	External DMZ network
DMZ-ext-closed-net	10.10.30.0/24	Closed external DMZ network
DMZ-ext-vpn-net	10.10.40.0/24	VPN network
DMZ-ext-vasco-net	10.10.50.0/24	Vasco external DMZ network
Production-net	10.10.110.0/24	Secure production network
DMZ-int-net	10.10.200.0/24	Internal DMZ network
Admin-net	10.10.210.0/24	Management network
Acceptance-net	10.10.230.0/24	Acceptance network
Test-net	10.10.240.0/24	Test network
Develop-net	10.10.250.0/24	Development network
Office-new-net	10.31.32.0/23	New office network
Vasco-net	10.32.0.0/16	Connection to the Vasco network
Iscsi-net	10.200.200.0/23	Internal ISCSI network
Iscsi-colo-net	10.200.202.0/23	Co-location - ISCSI DMZ network
Office-net	172.17.20.0/25	Office network and temporary network
Hosted1-old-net	172.17.20.128/28	Old ”hosted1” network

[10] Based on a drawing provided by DigiNotar. The exact lay-out of the layer-2 network (switches) in this sketch was not verified.
[11] Network segment name as it is used in this report.

Net name[11]	IP range	Description
Hosted3-old-net	172.17.20.160/28	Old "hosted3" network
Secure-net	172.18.20.0/24	Secure network locating the CAs and netHSMs
DMZ-ext-colo-net	172.25.20.0/24	Co-location – external DMZ network
DMZ-int-colo-net	172.26.20.0/24	Co-location – internal DMZ network
Secure-colo-net	172.27.20.0/24	Co-location – Secure network
Office-colo-net	172.28.20.0/24	Co-location – office network
Sync-1-net	192.168.1.0/29	First FireWall-1 synchronization network
Ext-net	62.58.35.96/28	External network addresses
Firewall-mgmt-net	62.58.74.128/27	Remote access for the management of the firewall

The construction of the network security zones corresponded with best practices as the following sketch depicts. A more detailed figure of the systems and network segments that are mentioned in this report is included in chapter 9.

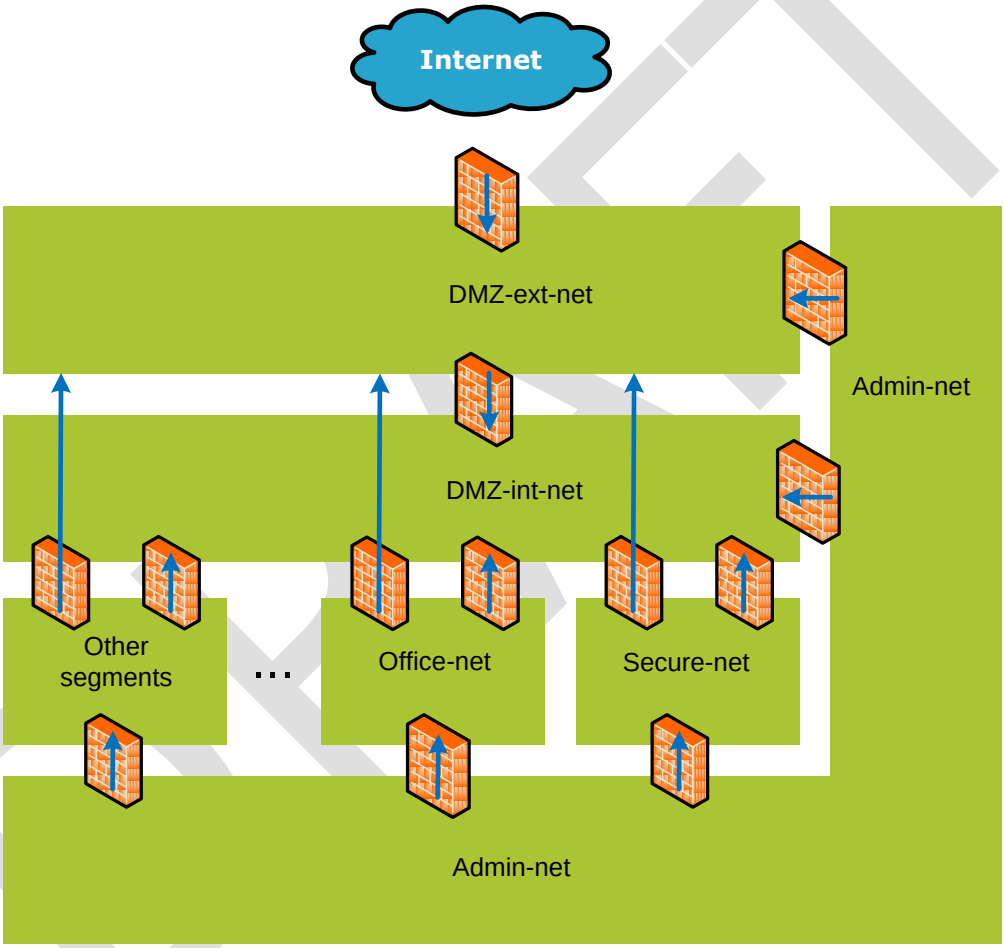


Figure 2 Network security zones

An internal and external DeMilitarized Zone (DMZ) prohibited direct connections between the Internet and the internal network. The firewall prohibited any connections initiated from DMZ-int-net to DMZ-ext-net as well as connections that were initiated from DMZ-int to Secure-net[12]. The administrators could access all the systems through remote desktop connections from their workstations, which were located in a room that was physically only accessible to administrators. Several exceptions existed in the firewall configuration for network traffic between the various segments[13].

[12] The description of the operation of the firewall is based on interviews with the administrators of DigiNotar.
[13] A total number of 156 rules existed in the firewall. Firewall rules influence the interconnections that are allowed and disallowed between zones.

3.3.2 Network operation

During normal operation, a customer requested a certificate on one of the websites running on a web server in the external DMZ (DMZ-ext-net). The request was then stored by the web server on a server in the internal DMZ (DMZ-int-net). These requests were periodically collected by a service in Secure-net. In the CAP (Control Application) administrative application, the request was stored and administrative procedures such as vetting were initiated.

When a request was approved using the four-eye principle, the request was marked as such in the database. Subsequently, an administrative employee logged onto a workstation running a DARPI client (*DigiNotar Abonnementen Registratie Production Interface*[14]) in a separate room and processed the request. Depending on the procedure, a private key was generated if it was not generated by the customer and a certificate request was sent to one of the CA servers. The CA software automatically signed the request and returned the certificate.

In order for the CA software to automatically sign the certificate request, the appropriate private key needed to be activated in the netHSM. This was done by authorized employees by entering a smartcard into the netHSM combined with a PIN code.

It was also possible for the CA operator to manually create certificates, for certificate requests that could not be processed by the DARPI application. In order to issue these certificates the CA operator had to log into the CA application with its smartcard, provided someone else had given the operator physical access to the secured room. After verification by another person the certificate was created.

The main servers and network devices of DigiNotar, including the CA servers and netHSM, were located in a physically highly-secured room at the main location. This room could be entered only if authorized personnel used a biometric hand recognition device and entered the correct PIN code. This inner room was protected by an outer room connected by a set of doors that opened dependent on each other creating a sluice. These sluice doors had to be separately opened with an electronic door card that was operated using a separate system than for any other door. To gain access to the outer room from a publicly accessible zone, another electronic door had to be opened with an electronic card.

Systems that needed the most protection were located in the Secure-net network segment. These systems included the servers that ran the CA management software, the "production" servers and the hardware security module that was accessible over the network (netHSM). The workstations and servers in this production network were used, among others, to initialize and personalize smartcards or other PKI tokens, issue certificates and create PIN letters. These production workstations could access the back-end records in Office-net as well as the CA servers in Secure-net. The custom applications used for production are called CAP, DARPI and BAPI (*Belastingdienst*[15] *Advanced Program Integration*) and were all developed in-house.

The CA management software that ran on the CA servers connected over the network to the netHSMs, where the private keys of the Certificate Authorities were stored in encrypted form. At the main location, at least eight CA servers were present, including one test CA server and one root CA server. At the co-location, seven redundant (virtual) CA servers were located for the purpose of business continuity[16]. In total DigiNotar used four netHSMs, one of which was in the secure segment for the CAs, a second in the internal DMZ (DMZ-int) for the "Parelsnoer" service, a third in the test environment and the fourth in the co-located secure network segment (Secure-colo-net).

3.3.3 Internet connectivity

For the purpose of the investigation, it was helpful to know how DigiNotar was connected to the Internet. Although no exhaustive inventory was made, it became clear during the investigation that many websites were hosted by DigiNotar. A survey was made of the connection to the Internet.

[14] Translates to "Subscription Registration Production Interface".
[15] The Dutch tax and customs administration.
[16] The systems were on 'warm' standby; the servers were switched on and backups were stored there on a regular basis.

3.3.3.1 Registered Internet IP addresses

The following IP address ranges were identified to be used by DigiNotar:

IP start	IP end	net name
62.58.35.96	62.58.35.111	TELE2-CUST-DIGINOTAR-BV
62.58.36.112	62.58.36.127	VERSATEL-CUST-Diginotar-B-Vx
62.58.44.96	62.58.44.127	VERSATEL-CUST-Diginotar-B-Vx
81.58.241.160	81.58.241.175	VERSATEL-CUST-Diginotar-B-Vx
87.213.105.80	87.213.105.95	TELE2-CUST-Diginotar
87.213.114.0	87.213.114.15	VERSATEL-CUST-Diginotar-B-Vx
87.213.114.160	87.213.114.191	VERSATEL-CUST-Diginotar-B-Vx
143.177.3.40	143.177.3.47	-
143.177.11.0	143.177.11.15	-
193.173.36.32	193.173.36.47	OTS25849

3.3.3.2 Web service scan

During a service scan performed by Fox-IT on September 14, 2011, a long list of servers were identified as accessible from the Internet.

IP address	Port 80 HTTP	Port 443 HTTPS
62.58.35.107	X	X
62.58.36.113	X	X
62.58.36.116	X	X
62.58.36.117	X	X
62.58.36.118	X	X
62.58.36.119	X	X
62.58.36.121	X	X
62.58.36.122	X	X
62.58.36.123		X
62.58.36.124		X
62.58.36.125	X	X
62.58.36.126	X	X
62.58.36.127	X	X
62.58.44.96	X	X
62.58.44.97	X	X
62.58.44.98	X	X
62.58.44.99	X	X
62.58.44.100		X
62.58.44.102	X	X
62.58.44.103	X	X
62.58.44.104	X	X
62.58.44.105	X	
62.58.44.107	X	X
62.58.44.109	X	X
62.58.44.110		X
62.58.44.112	X	X
62.58.44.113	X	X
62.58.44.114	X	X
62.58.44.118	X	X

IP address	Port 80 HTTP	Port 443 HTTPS
62.58.44.119	X	X
62.58.44.121	X	X
62.58.44.123	X	X
62.58.44.125	X	X
62.58.44.126	X	X
62.58.44.127	X	X
81.58.241.160	X	X
81.58.241.161	X	X
81.58.241.162	X	
81.58.241.163	X	X
81.58.241.164	X	
81.58.241.165	X	X
81.58.241.167	X	X
81.58.241.168	X	X
81.58.241.171	X	X
81.58.241.172	X	X
81.58.241.173	X	X
81.58.241.174	X	X
81.58.241.175	X	
87.213.105.80	X	
87.213.105.81	X	X
87.213.105.82	X	
87.213.105.83	X	
87.213.105.84	X	
87.213.105.85	X	
87.213.105.87	X	X
87.213.105.89	X	
87.213.105.90	X	X
87.213.105.91	X	X

IP address	Port 80 HTTP	Port 443 HTTPS
87.213.105.92		
87.213.105.93	X	
87.213.105.94	X	X
87.213.105.95	X	X
87.213.114.3	X	X
87.213.114.4	X	X
87.213.114.5	X	X
143.177.3.40	X	X
143.177.3.41		X
143.177.3.44	X	X
143.177.3.45	X	
143.177.3.46	X	
143.177.3.47	X	X
143.177.11.1	X	X
143.177.11.2	X	
143.177.11.3	X	X
143.177.11.4	X	
143.177.11.5	X	X
143.177.11.6	X	X
143.177.11.7	X	X
143.177.11.8	X	X
143.177.11.9	X	
143.177.11.10	X	X
143.177.11.11	X	X
143.177.11.12	X	
143.177.11.14	X	X
143.177.11.15	X	X

A DNS query of the IP addresses that were used (among others) showed the following entries:

IP address	DNS lookup
62.58.36.114	mailhost.diginotar.nl
62.58.36.116	mail.diginea.nl
62.58.36.118	www.diginotar.nl
62.58.36.120	authenticatie.pass.nl
62.58.36.121	belastingdienst.diginotar.nl
62.58.36.125	service.diginotar.nl

IP address	DNS lookup
62.58.36.126	Registratie.diginotar.nl
62.58.44.107	digi01.mailwitness.net
62.58.44.108	digibackup.mailwitness.net evssl.diginotar.nl
62.58.44.109	sha2.diginotar.nl
62.58.44.111	ftp.diginotar.nl
62.58.44.113	www.evssl.nl
62.58.44.116	genghini.mailwitness.net
62.58.44.121	danka.mailwitness.net
62.58.44.122	bgg.mailwitness.net
62.58.44.123	diginotar.mailwitness.net
62.58.44.124	test.pass.nl
62.58.44.125	*.diginotar.com diginotar.com diginotar.net
143.177.3.41	mailhost1.diginotar.nl mail.digifactuur.nl mail.diginotar.com
143.177.3.42	directory.diginotar.nl
143.177.3.43	www.servicecentrum.diginotar.nl
143.177.3.45	validation.diginotar.nl
143.177.11.2	servicecenter.diginotar.nl
143.177.11.4	demonstratie.pass.nl
143.177.11.10	onlineaanvraag.diginotar.nl
143.177.11.11	www.pass.nl
193.173.36.36	ns1.diginotar.nl
193.173.36.39	mailhostuw.diginotar.nl

Additionally, a service scan showed a number of noteworthy services:

IP address	Service
62.58.44.111 (ftp.diginotar.nl)	FTP server
87.213.105.92 (port 8888)	Web server
62.58.35.108, 62.58.35.109 & 62.58.35.110	VPN server
62.58.36.114	Mail server
87.213.114.2	DNS server

3.3.3.3 Web server configuration

From some of the web servers that were present in DMZ-ext-net, the following internal IP addresses were extracted from their configuration.

Server	Internal IP	Site name
Main-web server	10.10.20.11	Notarisgombert.nl
	10.10.20.14	Darwizard
	10.10.20.28	evssl.diginotar.nl
	10.10.20.41	DigiNotar.nl
	10.10.20.46	www.evssl.nl
	10.10.20.58	DigiNotar.com
	10.10.20.61	OCSPclient
	10.10.20.69	sha2.diginotar.nl
	10.10.20.73	BapiOphalen
	10.10.20.97	Bapiviewer
Docproof1 server	10.10.20.37	Docproof
Docproof2 server	10.10.20.65	Docproof
Pass-web server	10.10.20.16	PassWeb - PASS15
	10.10.20.40	NTP
	10.10.20.35	TIM_tim.diginotar.nl

Server	Internal IP	Site name
Soap-signing web server	10.10.20.98	SS_Provincie-Utrecht.signing.diginotar.nl
	10.10.20.129	SS_Gelderland.signing.diginotar.nl
	10.10.20.42	TimeStampServer
	10.10.20.92	SoapSigning
	10.10.20.84	SS_Lelystad.Signing.diginotar.nl
	10.10.20.85	SS_Waterschapdedommel.signing.diginotar.nl
	10.10.20.86	SS_Signing.diginotar.nl
	10.10.20.137	DigiDownload
	10.10.20.87	SS_Teylingen.signing.diginotar.nl
	10.10.20.88	SS_PZH.signing.diginotar.nl
	10.10.20.89	SS_sintanthonis.signing.diginotar.nl
	10.10.20.130	SS_Leeuwarden.Signing.diginotar.nl
	10.10.20.90	SS_PNB.signing.diginotar.nl
	10.10.20.91	SS_Leiderdorp.Signing.diginotar.nl
	10.10.20.99	SS_Drenthe.Signing.diginotar.nl
	10.10.20.93	SS_Overijssel.Signing.diginotar.nl
Main-web-new[17]	10.10.20.172	evssl.diginotar.nl
	10.10.20.164	BapiViewer
	10.10.20.165	DarWizard
	10.10.20.182	bct.csp.minienm.nl
	10.10.20.173	www.diginotar.com
	10.10.20.167	OCSPClient
	10.10.20.174	service.diginotar.nl
	10.10.20.169	BapiOphalenCert
	10.10.20.183	test.bct.csp.minienm.nl
	10.10.20.175	www.evssl.nl
	10.10.20.158	www.diginotar.nl www.diginotar.com diginotar.com diginotar.nl www.evssl.nl evssl.diginotar.nl
	10.10.20.184	test.csp.minienm.nl
	10.10.20.181	csp.minienm.nl
	10.10.20.176	sha2.diginotar.nl

[17] Main-web server was replaced by Main-web-new: the first firewall entries of 10.10.20.158 from the main-web-new server appeared on July 18, 2011. Logs of the old Main-web server showed activity up until August 1, 2011. More details are included in Chapter 4.

4 Investigation of web server log files

During the initial incident response investigation that was performed before the involvement of Fox-IT, it was identified that at least two web servers were running outdated versions of the DotNetNuke software. There are known security vulnerabilities in these outdated versions of the DotNetNuke software and the initial incident response investigation concluded that these vulnerabilities had been exploited to gain first entry into DigiNotar's network.

These compromised web servers were used by the intruder as stepping stones to transfer data and tools between DigiNotar's internal network and the Internet. Both the Main-web and Docproof2 web servers were investigated in order to examine what files and tools were transferred and what internal and external systems had connected to these compromised systems in DMZ-ext-net.

4.1 Sources

After a crash of the main web server of DigiNotar, an employee of DigiNotar found evidence that the Main-web server had been compromised. A new web server was installed on other hardware using an old backup, which left the data of the compromised web server, including the log files up to August 1, 2011, intact for further investigation.

During the incident response investigation by Fox-IT on the Taxi-CA and Qualified-CA servers, evidence was found indicating that these systems had connected to a specific file (`settings.aspx`) on the Main-web server that acted as a rudimentary file manager, among other things. With this file manager the directory `/beurs` could be used to store and exchange hacking tools and other unauthorized files. Other investigated systems within the network later showed cached web pages originating from this directory, as detailed in Chapter 7. A sample of a cached version of `settings.aspx` is shown below.

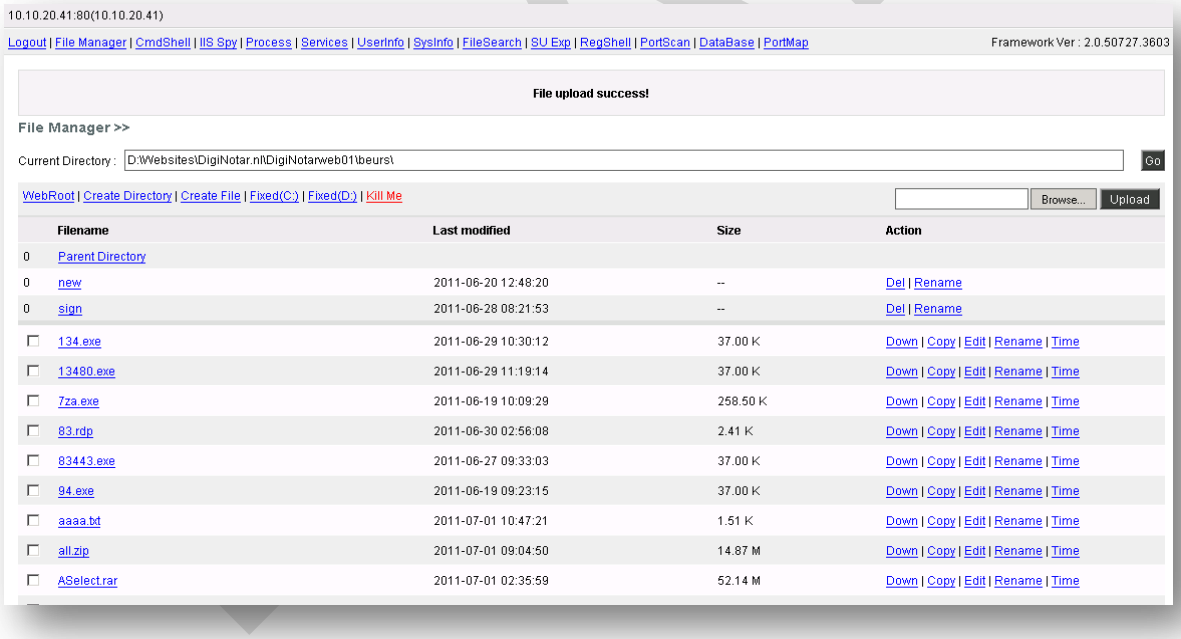


Figure 3 A sample of a cached version of `settings.aspx`

4.2 Web server log file analysis

The directory `/beurs` was located on the Main-web server at `D:\Websites\DigiNotar.nl\DigiNotarweb01\beurs` and was available internally at `http://10.10.20.41/beurs` and publicly at `http://www.diginotar.nl/beurs`. When the directory `/beurs` was examined, no files were present in the disk image, but the evidence on Taxi-CA and Qualified-CA servers indicated that files had indeed been present in this directory (see paragraph 7.2.2).

The Microsoft IIS log files of the Main-web server were subsequently examined in order to determine which internal and external systems had made a connection to the directory `/beurs` including all files in that directory. The log files were stored in `C:\WINDOWS\system32\LogFiles\W3SVC1062701327\` and `C:\Data\Websites\Logging\W3SVC1062701327\` and were named `EX<YYMMDD>.log`. The timestamps in the logs are based on Coordinated Universal Time (UTC) and the time deviation of the server was minimal. The log files have the following format:[18]

```
2011-07-11 00:30:48 W3SVC1062701327 10.10.20.41 GET /beurs/settings.aspx - 80 -
aaa.bbb.ccc.ddd Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1)
+Gecko/20100101+Firefox/4.0.1 200 0 0
```

In a log entry such as the one above, one can distinguish when a system identifiable by its IP address (`aaa.bbb.ccc.ddd`) made a connection to the Main-web server (10.10.20.41) and which operating system and browser were most likely used to do so (`Mozilla/5.0+(Windows+NT+6.1;+rv:2.0.1`). Furthermore, one can distinguish the request that was performed (`GET /beurs/settings.aspx`) and the web server's response to this request (status OK: `200`).

During the incident response investigation, it became clear that a number of log files were missing, which included log files from the period around the intrusion. More specifically, access log files for the period up to July 11, 2011 had been removed from the Main-web server. However, the error logs in the `HTTPERR` directory were still present on the Main-web server and contained entries prior to July 11, 2011. According to DigiNotar, the log files were most likely deleted by an administrator of DigiNotar during an incident where the available space on the hard disk was filled by large log files. According to DigiNotar, the files were deleted after a brief inspection that showed no remarkable entries.

The files `Default.aspx` and `old_Default.aspx` that had originally been located in the `/beurs` directory were recovered in a backup that was made on August 27, 2009 and which was located at `D:\Websites\BackUp\Diginotar01.old`. This could mean that the `/beurs` directory had been inactive for a while, which may have been a reason to use this directory, as well as that it may have been emptied by the intruder.

4.3 Results

Since the removed log files had partially been overwritten, recovery software could not be used. Therefore a pattern matching text search was performed on the entire disk image searching for log entries that contained `/beurs`. This method recovered 1,583 log entries. It showed that uploading a file to the web server was done with a post-request to the `aspx` script, and downloading a file could be done by connecting to the `/beurs` directory. The scripts `settings.aspx` and `up.aspx` were used to upload files. The recovered logs revealed a list of internal and external IP addresses that had connected to the `/beurs` directory, which was used as a stepping stone.

4.3.1 Internal systems

Based on entries in the log files, the following 13 internal systems could be identified as having connected to the `/beurs` directory on the compromised Main-web server.

Network	Server
DMZ-int-net	Docproof-db
Office-net	BAPI-db
	Production121
	Squid-proxy server
	Office-file
Secure-net	CAP-app-web
	CAP-app-db
	Relation-CA

[18] More details can be found at Microsoft Technet, "W3C Extended Log File Format (IIS 6.0)" at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/iis/676400bc-8969-4aa7-851a-9319490a9bbb.mspx

Network	Server
	Public-CA
	CCV-CA
	Root-CA
	Qualified-CA
	Taxi-CA

All the internal systems that had connected to the `/beurs` directory, which was used as a stepping stone by the intruder during the intrusion, should be regarded as compromised unless specific evidence would indicate otherwise. This was the case for Squid-proxy, which was probably not compromised but used as a proxy by other machines in the Office-net.

It was noticed that the connections from the Public-CA server to the script `up.asxp` showed a regular pattern of connections.

4.3.2 External IP addresses

The IP addresses of external systems that had accessed the directory `/beurs` were likely to have been utilized by the intruder and are included in Appendix II (referenced as AttIPxx). This list of IP addresses is not exhaustive, as a number of log files had been removed, were overwritten, and were beyond recovery. In total, 26 unique external IP addresses were identified during the investigation of the web server log files.

Some of these IP addresses were probably not related to the intruder. For example, requests from four different IP addresses originating from the Netherlands and Belgium were only seen during the internal incident response investigation that started on July 19, 2011. Another IP address resolved to a Googlebot web crawler and was therefore excluded. The remaining 21 IP addresses were suspicious and were probably utilized by the attacker, because files were up or downloaded and the `aspx`-scripts were used by these IPs. Results from other parts of the investigation also point to seven of these IP addresses that are referenced as AttIP3, AttIP4, AttIP5, AttIP6, AttIP13, AttIP19 and AttIP22.

4.3.3 Suspicious files

From the results of pattern matching text searches, a list of files was composed that had been present in the directory `/beurs` of the Main-web server over time. The following list of 125 files is not exhaustive, as a number of log files appear to had been removed and overwritten and were beyond recovery.

File name	File name	File name	File name
aaaa.txt	darv28.exe	ids.zip	saerts.zip.part3.txt
all.zip	darv28.zip	jobdone.zip	saerts.zip.part4.txt
asdasd.zip	darv29.zip	keo.zip	settings
aselect.rar	darv3.zip	last.zip	Settings.aspx
bapi.zip	darv30.zip	lastdb.zip	settings.aspx
beurs.aspx	darv31.zip	lb.msi	settings.zip
bin.zip	darv33.zip	ldap.msi	sms.msi
c.zip	darv34.exe	ldap.msi	SQLServer2005_SSMSEE.msi
cachedump.exe	darv34.zip	md5s.txt	ssl.zip
certcontainer.dll	darv35.zip	mimi.zip mohem.zip	tijdstempel.pfx
code.zip	darv36.zip	mswinsck.ocx	Troj25.exe
csign.zip	darv37.zip	msxml6.msi	twitter.zip
dar.rar	darv38.zip	nc.exe	up.aspx
dar.zip	darv4.zip	newjob.zip	USBDeview.exe
darpi.zip	darv5.zip	nfast.zip	validate.zip
darv11.zip	darv6.zip	nssl.zip	vcredist_x86.exe
darv12.zip	darv7.zip	origrsa.zip	webapp.zip
darv13.zip	darv8.zip	passadmin.rar	websign.rar
darv15.zip	darv9.zip	pki.zip	win.exe
darv16.zip	data.zip	PortQry.exe	win2.exe
darv17.zip	dbpub.zip	psexec.exe	win3.exe
darv18.zip	Default.aspx	putty.exe	z3.exe
darv19.zip	Depends.exe	PwDump.exe	z4.exe
darv20.zip	depends.exe	qualifieddata.zip	z5.exe
darv21.zip	DigiNotar_Services_CA.cer	Read1.exe	Zip2.exe
darv22.zip	direct.exe	Read2.exe	zip3.exe
darv23.zip	direct.zip	Read3.exe	zipped.zip
darv24.exe	direct83.exe	Repositories.zip	Zipper.exe
darv24.zip	elm.zip	rsa_cm_68.zip	
darv25.zip	ev-add.zip	rsaservice.rar	
darv26.zip	f1.cer	saerts.zip.part1.txt	
darv27.zip	final.zip	saerts.zip.part2.txt	

Some of these names are related to internally used names. For example:

- A-select is a service provided by DigiNotar
- BAPI is an administration application for the Dutch tax administration
- DAR is the administration application hosting all customers information (*DigiNotar Abonnementen Registratie*)
- Qualified is the name of one of the CA servers (Qualified-CA)
- Public (pub) is the name of another CA server (Public-CA)
- rsa_cm_68 is the directory where the CA management software is installed on the CA servers

4.3.4 Noteworthy log entries

In the access logs of the Main-web server a remarkable piece of evidence was found.

```
2011-07-24 13:16:48 10.10.20.41 GET /settings.aspx - 80 - AttIP3
      Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0
2011-07-24 13:16:53 10.10.20.41 POST /settings.aspx - 80 - AttIP4
      Mozilla/5.0+(Windows+NT+5.1;+rv:5.0)+Gecko/20100101+Firefox/5.0
```

The entries in the log files indicate that the intruder regularly used the proxy on AttIP4 to connect to the stepping stone in order to obscure his identity. It appears that the intruder erroneously connected to the stepping stone without using the proxy on AttIP4 (possibly in a proxy chain) which revealed AttIP3. Five seconds later the error was corrected and the request was repeated using the proxy on AttIP4. AttIP3 had previously been used to test the OCSP response for a rogue Yahoo certificate that had been issued by DigiNotar. AttIP3 resolved to a DSL user in the Islamic Republic of Iran (see also paragraph 10.2.2).

4.4 Conclusion

Some of the incriminating files and logs were deleted from the Main-web server by DigiNotar, the intruder or by an automated process. However, by searching through the images of the entire disk the remains of deleted web server access log entries were found. Additionally, error log files were present on the Main-web server and log files were present on the Docproof2 server. From these log entries, a list of IP addresses that had connected to the directory `/beurs`, which was used as a stepping stone, was generated. Of the internal systems that were found to have connected to this directory and the corresponding script, 12 were most likely compromised by the intruder. A total of 125 file names were extracted, which were copied to or from the stepping stones.

Moreover, the log entries that were recovered produced a list 26 external IP addresses that had been used to connect to the Main-web server stepping stone. On this basis of this part of the investigation, Fox-IT deems it very likely that 21 of these IP addresses were (ab)used by the intruder. The vast majority of these IP addresses were most likely used as a proxy to obscure the identity of the intruder, but the true IP address of the intruder may have been revealed by error. All these IP addresses were handed over to the KLPD.

5 Investigation of firewall log files

Within DigiNotar's infrastructure there was a central position for the firewall. The firewall was configured so that all violations of firewall rules as well as all the accepted traffic connections were logged, which resulted in up to 2 million log entries per day. The large amount of log data that was generated has great potential for tracing the intruder's steps, even though data mining on such a large amount of data is time intensive.

The firewall was only able to log connections between the network segments that it segregated. Traffic within a segment was not logged by the firewall, with the exception of traffic that had the firewall as its destination.

5.1 Sources

A Check Point appliance on a redundant Nokia IP390 platform with a separate management server was used as the firewall within the main infrastructure. A previously-used redundant Sun firewall platform was also present in the network. At the co-location, another Check Point firewall based on a Nokia appliance platform was present.

Fox-IT created a forensic image of the disk of the firewall management server located at the main location. In our forensic lab, a copy of the disk image was virtualized and the management station was accessed using the Check Point SmartConsole software. The log files were exported for further processing and examination.

For the purpose of this investigation, the traffic logs were of primary interest. The traffic logs contain the following fields:

- Timestamp
- Action (accept / drop / reject / encrypt / decrypt / keyinst)
- Firewall interface name and traffic direction
- Firewall rule (name, ID and number)
- Source and destination IP and port
- Protocol
- ICMP (code and type)
- NAT (rule number, translated IP / port)
- DNS query
- VPN (scheme, method, peer gateway)
- TCP out of state, flags
- IPSec specification
- Attack details

The timestamps of the firewall logs are based on Central European (Summer) Time (CEST).

5.2 Log file analysis

Not all the fields in the log files were relevant for the investigation. Only the source and destination IP addresses, port numbers and the "accept" and "drop" actions were used. The investigated log files date from May 31, 2011 at 23:51:57 up to July 31, 2011 at 23:51:36 and contain a total of 112,840,345 records. Logs that date back further were also available but were irrelevant for the purpose of this investigation.

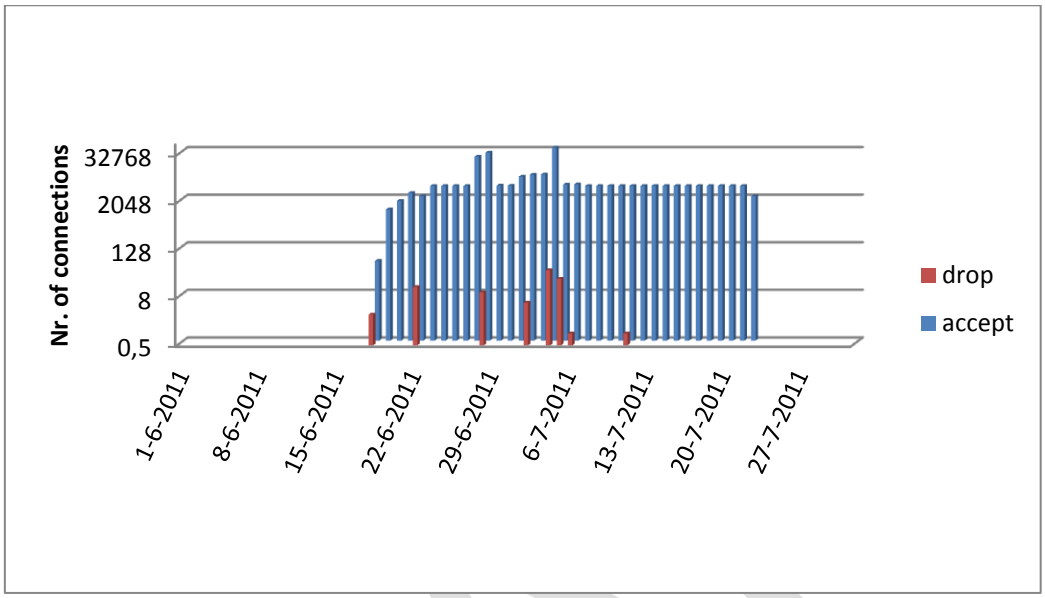
The approach for the analysis of the firewall logs was based on the results of the investigation performed on other exhibits. The search for anomalies was guided by the expertise of the investigators and the situation at hand. The degree of certainty in which the identified anomalies can be linked to the intruder on the basis of the firewall log files alone varies. Anomalies that cannot conclusively be connected to the intruder are included in paragraph 5.2.8.

5.2.1 Connections from internal IPs to AttIPs

During the investigation, a list of external IP addresses that were suspected to have been used by the intruder was created. This list was based on the web server log files that the intruder used as a stepping stone (as described in paragraph 4.3.2) and the IP addresses that were found in the tools that were left

by the intruder (as described in Chapter 7). The complete list of these IP addresses is included in Appendix II.

On June 18, 2011 connections started to appear that were initiated from systems with internal IP addresses of DigiNotar to the suspected intruder's IP addresses. The log entries with source IP addresses in the ranges 10.0.0.0/8 and 172.16.0.0/12 to the intruders IP addresses in the firewall log files are visualized in the following graph.[19]



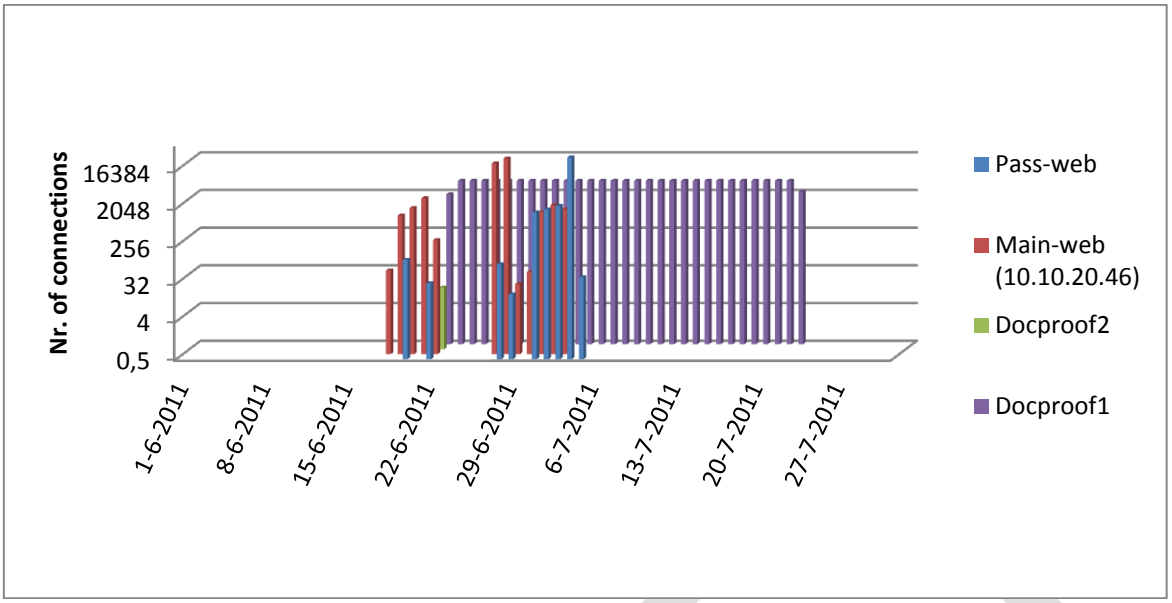
Internal IPs → suspicious intruder IPs

The data indicates that the first connections back to the intruder were established from two machines in the external DMZ network (DMZ-ext-net), namely the Main-web and Docproof1 web servers. The last connection back to the suspicious intruder IP addresses occurred on July 22, 2011. This part of the investigation also showed that successful connections only took place from internal IP address to AttIP1, AttIP2, AttIP19 and AttIP22. Additionally, unsuccessful connections (dropped by the firewall) were attempted to AttIP13.

5.2.2 Tunnels from DMZ-ext-net to AttIP1

Early on in the investigation, a tool was identified that had been created by the intruder which contained an external IP address used by the intruder (AttIP1). It was then discovered that connections from the ext-DMZ-net to this IP address had taken place. Based on entries in the log files, it was examined if other connections from DMZ-ext-net to this specific IP address could be found.

[19] Please note the use of a logarithmic scale. This scale is used to emphasize the occurrence of the connections rather than the number of connections. One bar indicates the connections of one day.

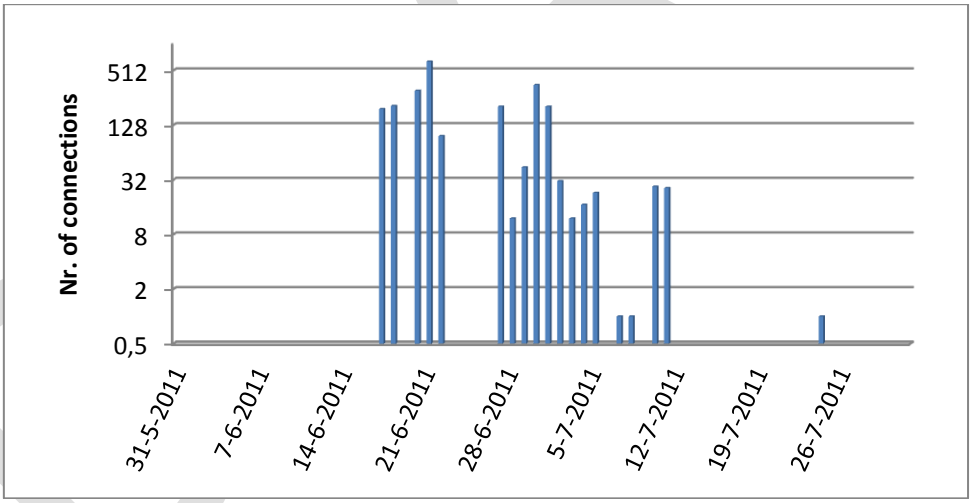


Web servers → AttIP1 port 443

This showed that at least 4 servers in DMZ-ext-net had connected back to the intruder since June 18, 2011. It also showed a regular pattern for the connections between the Docproof1 server and AttIP1.

5.2.3 Access to Office-net

As of June 17, 2011 at 11:28, accepted connections started to appear between the Main-web server and the BAPI-db server on port 1433, which is used for the Microsoft SQL service.



Main-web (10.10.20.46) → BAPI-db on port 1433

This indicated that the firewall accepted connections on this port between DMZ-ext-net and Office-net, but that no such connection had taken place between June 1, 2011 and June 16, 2011. The identified traffic from June 17, 2011 onwards indicated that the MSSQL database server on BAPI-db was probed from Main-web. This activity matched with a file that was identified on the Main-web server which contained a string with credentials to access the database on BAPI-db (see paragraph 7.3).

5.2.4 Tunnels from Office-net

A number of tools that were left by the intruder were used to create network tunnels (see also paragraph 7.2.3). These tunnels were setup between an internal server (TCP port 3389) and a server in the DMZ-ext segment (TCP port 443). Port 3389 indicates that the tunnels were used to tunnel Terminal Services or Remote Desktop Protocol (RDP) traffic. Port 443, which is generally used for HTTPS, was utilized so

that the traffic could pass through the firewall. Analysis of the traffic log files of the firewall showed that these tunnels had been used.

File name	troj134.exe
Connect from	BAPI-db server
Connect to	eHerkenning-AD server
Connections	

Date	Nr. of log entries
2011-06-30	74522
2011-07-01	124510
2011-07-02	26351
2011-07-03	49021
2011-07-04	530
2011-07-05	11

File name	troj172.exe
Connect from	BAPI-db server
Connect to	Pass-web server
Connections	

Date	Nr. of log entries
2011-06-29	1

File name	troj25.exe
Connect from	Source-build server
Connect to	eHerkenning-AD server
Connections	None were found

Although a tool was found to tunnel remote desktop traffic, no conclusions can be drawn that the Source-build was compromised. Also, the investigation of the firewall logs showed no connections of this tunnel.

The tunnels allowed the intruder to connect to a remote desktop service on systems in the Office-net segment. The data showed that the intruder had created tunnels to access systems in the Office-net on and after June 29, 2011.

5.2.5 Access to Secure-net

The earliest suspicious traffic identified from the Secure-net was encountered when traffic from Secure-net with destination port 80 was examined. The following extraordinary log entries were identified:

```
2011-07-01 01:16:36 - drop - [tcp] 172.18.20.230:2404 -> 172.18.20.2:80
2011-07-01 01:16:39 - drop - [tcp] 172.18.20.230:2404 -> 172.18.20.2:80
2011-07-01 01:16:45 - drop - [tcp] 172.18.20.230:2404 -> 172.18.20.2:80
2011-07-01 01:17:07 - drop - [tcp] 172.18.20.230:2408 -> 172.18.20.2:80
2011-07-01 01:17:10 - drop - [tcp] 172.18.20.230:2408 -> 172.18.20.2:80
2011-07-01 01:17:16 - drop - [tcp] 172.18.20.230:2408 -> 172.18.20.2:80
2011-07-01 01:18:04 - drop - [tcp] 172.18.20.230:2422 -> 172.18.20.2:80
2011-07-01 01:18:07 - drop - [tcp] 172.18.20.230:2422 -> 172.18.20.2:80
2011-07-01 01:18:13 - drop - [tcp] 172.18.20.230:2422 -> 172.18.20.2:80
2011-07-01 01:19:28 - drop - [tcp] 172.18.20.230:2436 -> 172.18.20.2:80
2011-07-01 01:19:31 - drop - [tcp] 172.18.20.230:2436 -> 172.18.20.2:80
2011-07-01 01:19:37 - drop - [tcp] 172.18.20.230:2436 -> 172.18.20.2:80
2011-07-01 01:20:10 - drop - [tcp] 172.18.20.230:2446 -> 172.18.20.2:80
2011-07-01 01:20:13 - drop - [tcp] 172.18.20.230:2446 -> 172.18.20.2:80
2011-07-01 01:20:19 - drop - [tcp] 172.18.20.230:2446 -> 172.18.20.2:80
```

The entries concern traffic within the Secure-net segment, but which was still logged by the firewall. The reason for this is that the destination IP (172.18.20.2) is the firewall itself. The earliest suspicious log entry from the secure network segment occurred on July 1, 2011 at 01:16 CEST. About an hour later, more dropped traffic to ports 139, 443 and 445 on the firewall IP was logged originating from 172.18.20.230 (the BAPI-production workstation).

This led to the presumption that the intruder first entered the Secure-net segment on the BAPI-production workstation and then conducted a port scan on ports 80, 139, 443 and 445 within the subnet, which included the firewall and thus resulted in the aforementioned log entries.

5.2.6 Tunnels from Secure-net

Servers located in DMZ-ext-net acted as an intermediate hop or stepping stone between the internal network of DigiNotar and the Internet. For this purpose the intruder used tunnels through port 443 that allowed him to connect to servers that were not directly connected to the Internet.

All traffic originating from Secure-net to other network segments on port 443 was examined. This resulted in 3,062 logged traffic connections. The majority of these connections (2,970) originated from CAP-app-web and CAP-web server to the cluster address Cluster-prodpass in DMZ-ext-net. This traffic occurred before and after the intrusion and was probably ordinary traffic.

When this traffic is ignored, it leaves 92 traffic connections out of the original 3,062 that were further investigated. Out of these 92 connections, 54 relate to blocked traffic that originated from Public-CA server on July 4, 2011 between 03:25 and 04:42. The blocked traffic was intended for the following IPs:

- AttIP1:443 (see Appendix II);
- Pass-web server;
- Docproof1 web server;
- 10.10.2.139:443 (not in the server list - presumably a typing error made by the intruder).

Due to the unusual time that these attempts occurred, it was safe to assume that the intruder had access to the Public-CA server at this time.

The remaining 38 of the 92 connections that were further investigated relate to accepted traffic. These log entries show that direct connections were made from the Secure-net segment to the DMZ-ext-net segment:

From	To	Nr. of conn.
CAP-app-db server	Main-web server	5
Relations-CA server	Main-web server	2
Public-CA server	eHerkenning-AD	15
Public-CA server	eHerkenning-HM	7
Public-CA server	Pass-web	3
Public-CA server	Main-web server	2
CCV-CA server	Main-web server	2
Taxi-CA server	Main-web server	2

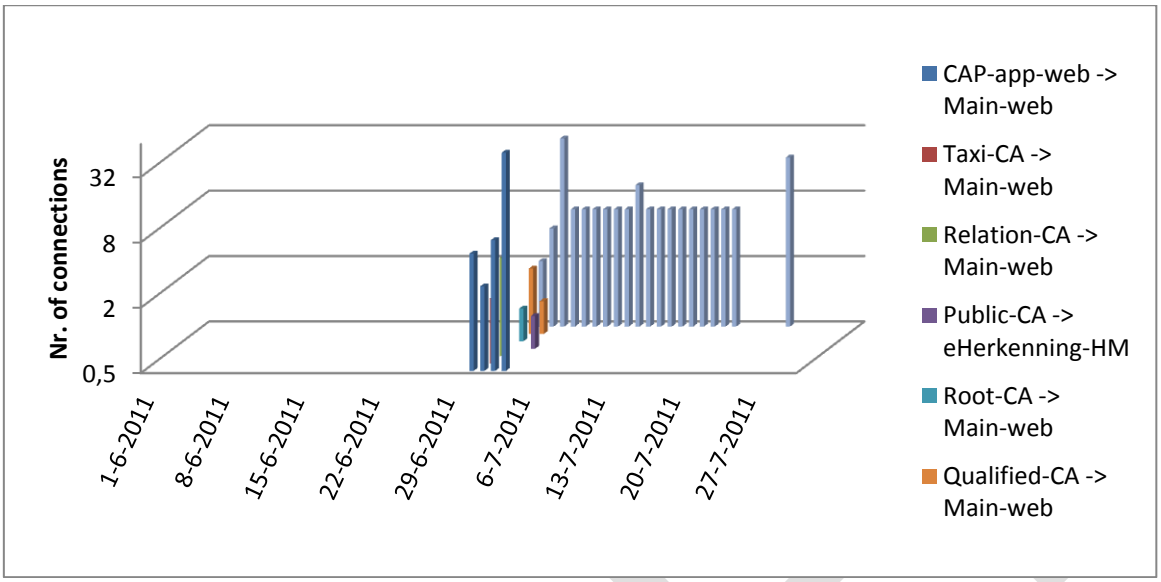
This confirmed that suspicious connections from Secure-net to DMZ-ext-net took place as of on July 2, 2011 at 06:40:44. Further investigation could conclusively establish if this traffic is related to the intruder.

5.2.7 Access to stepping stone from Secure-net

When all traffic originating from Secure-net to DMZ-ext-net was examined it was noticed that connections over port 80 were accepted by the firewall. When ordinary traffic that also occurred before the intrusion was eliminated, the following suspicious traffic remained:

From	To	Nr. Of conn.
CAP-app-web server	Main-web server port 80	68
Relation-CA server	Main-web server port 80	4
Public-CA server	eHerkenning-HM server port 80	1
Public-CA server	Main-web server port 80	151
Root-CA server	Main-web server port 80	1
Qualified-CA server	Main-web server port 80	3
Taxi-CA server	Main-web server port 80	2

Over time this could be visualized as follows:



Abnormal connections Secure-net → DMZ-ext-net port 80

The investigation showed that on July 1, 2011 at 22:52, the first successful connection was made from the Secure-net (the CAP-app-web server) to one of the compromised stepping stone servers. The investigation also showed that on July 2, 2011 at 00:14:14, the first connection from a CA server (Taxi-CA) to the Main-web took place.

Another noticeable anomaly consisted of a regular connection pattern between Public-CA server and the Main-web stepping stone server. From July 4, 2011 to July 7, 2011, daily connections took place at 15:09:36, 18:09:36 and 21:09:36. From July 8, 2011 to July 20, 2011, these connections occurred daily at 01:09:38, 04:09:36 and 07:09:35. This indicated that some form of traffic generated by a scheduled process took place.

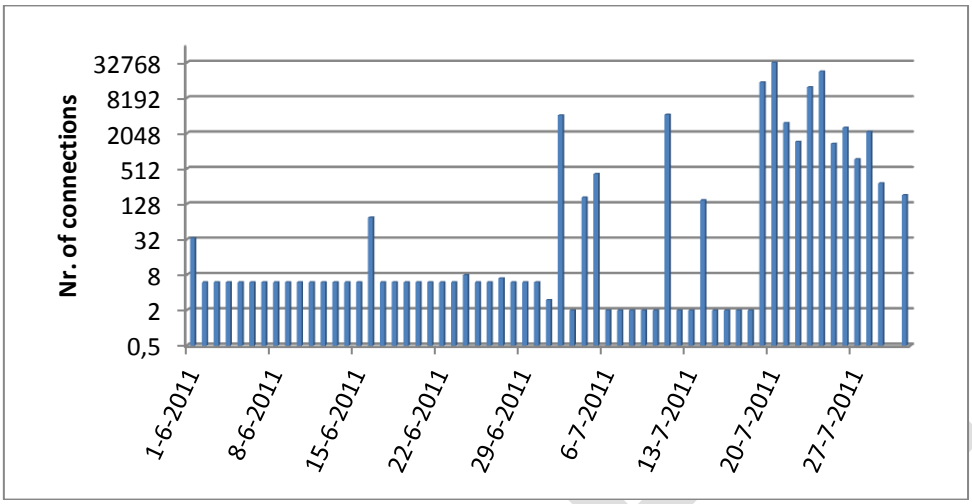
If we exclude the traffic peak on July 25, 2011, as this peak was probably due to incident response activities, the last traffic between the Secure-net and the stepping stone took place on July 20, 2011 at 07:09:35 from the Public-CA server.

5.2.8 Other noteworthy traffic

The previous paragraphs of the firewall log investigations show results based on the firewall logs that can be correlated with other exhibits to draw conclusions in regard to the attacker. The conclusions are mostly in regard to the exit path that was used to exfiltrate data and/or to create easy access for future visits. The following paragraphs detail the remaining results of the investigation that was performed on the firewall logs. Although the following anomalies cannot be unambiguously connected to activity of the intruder, they are noteworthy and provide sufficient reason for further investigation. An extensive list of the identified noteworthy traffic, complemented with investigation notes, is included in a timeline in Appendix III. In the following paragraphs, only the most remarkable anomalies are noted.

5.2.8.1 E-mail traffic

The firewall logs show unusual traffic with destination port 25 (SMTP) between the CAP-app-web server in the Secure-net segment and the Exchange-mail server in the Office-net segment. As port 25 is generally used for the purpose of e-mail, this could indicate intensive e-mail traffic that normally does not occur in these quantities. The figure below illustrates the anomaly.

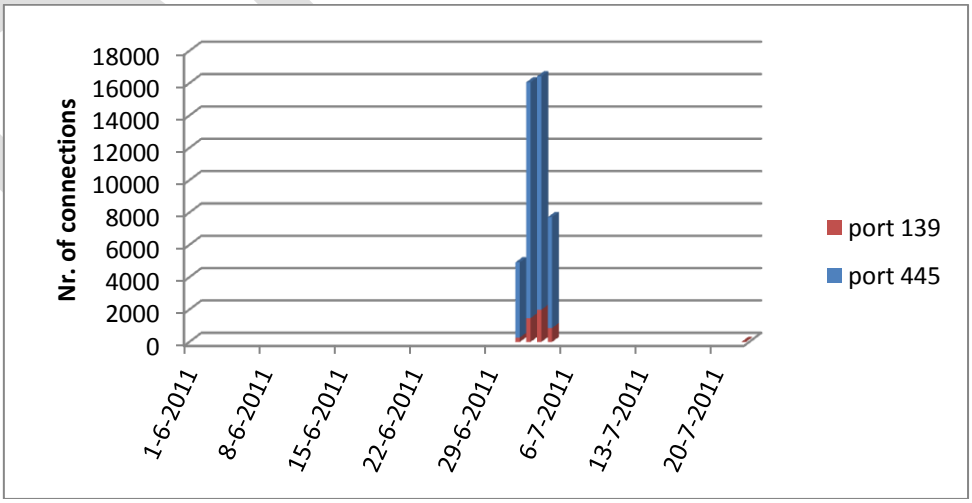


Anomaly CAP-app-web → Exchange-mail

The normal traffic on port 25 consists of six regular SMTP-connections each day at given intervals (four at 9:00 and two at 00:30), probably the result of a scheduled task. After June 30, 2011, the regular connections at 09:00 cease to take place. Then, suddenly, in the night of July 2, 2011, approximately 4,100 connections occurred. Then, additional spikes of traffic occurred on the 4th, 5th, 11th and 14th of July, 2011. Between July 19 and July 29, very large numbers of connections on port 25 took place. The last mentioned anomalous traffic coincides with the incident response actions that were initiated on July 19, 2011. According to DigiNotar, anomalous SMTP traffic may also have been caused by intensive testing of Taxi CA, which used SMTP as mode of transport.

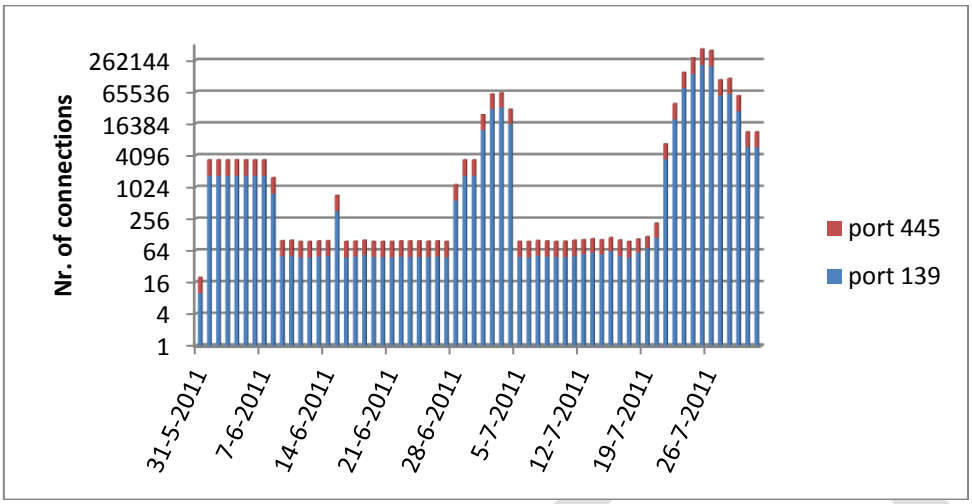
5.2.8.2 Co-location

At the co-location, suspicious (dropped) traffic was detected originating from the co-located secure network segment (Secure-colo-net) to the main secure network (Secure-net). The traffic occurred between the Admin-DNS server and the CAP-app-web server on ports 139 and 445.



Anomaly connections Admin-DNS → CAP-app-web on port 139 and 445

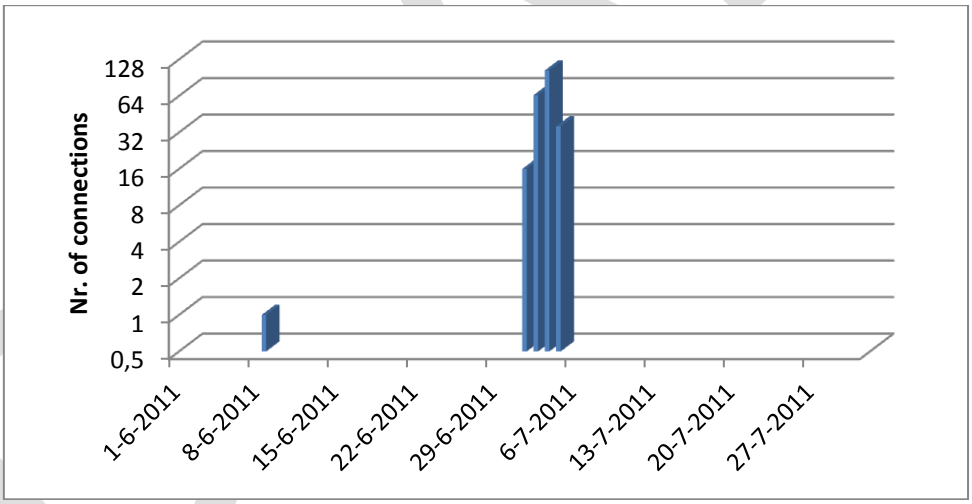
This could indicate that the intruder had gained a foothold in Secure-colo-net as of July 1, 2011. The reverse connection from Secure-net to Secure-colo-net showed the following pattern:



CAP-app-web → Admin-DNS port 139 and 445

This indicates some regular traffic (approximately 50 packets per day) and some monthly traffic. The spikes during the first four days of July are anomalous (the scale is logarithmic). The traffic after July 19 is extreme when compared to the ordinary traffic, but could be explained by incident response activity.

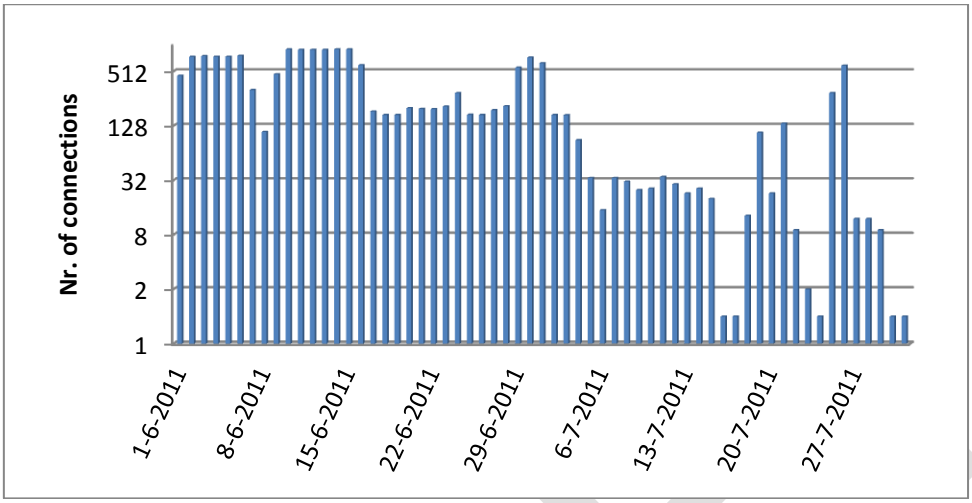
Other noticeable traffic was discovered on port 137 during the first four days of July (in addition to a connection on June 8, 2011):



Anomaly connections CAP-app-web port 137 → Admin-DNS on port 137

5.2.8.3 Internal DMZ-net

A noticeable change in the normal traffic between Secure-net and DMZ-int-net was found between the CAP-app-web and the Production-Notification server. Normal traffic between these segments depends on the amount of requests, which may vary significantly.



CAP-app-web server → Production-notification server port 80

The traffic shows a steep decrease in connections from July 4, 2011 onwards. From July 16, 2011 to the last-examined logs, a very erratic pattern occurs.

5.3 Conclusion

The examination and analysis of the firewall traffic logs provided some insight into the steps and foothold of the intruder. Connections initiated from internal IP addresses to external IP addresses that were suspected to have been used by the intruder were found. This indicated that from June 18, 2011 the intruder had a foothold on a server in the DMZ-ext-net. In total, four servers in the DMZ-ext-net were found to have been used to connect back to suspicious external IP addresses on the basis of the firewall log files. Other evidence confirmed that some of these servers were used as a stepping stone. During this part of the investigation four of the IP addresses suspected to have been used by the attacker were found to have been accessed from within the DigiNotar network.

From June 17, 2011, connections were initiated to a database server in the Office-net from the DMZ-ext-net. This indicates that the Microsoft SQL database running on that server was probed or used. From June 29, 2011, traffic initiated from the server in the Office-net started to appear, indicating tunneled remote desktop connections from servers in the DMZ-ext-net. This indicates that the foothold of the intruder was extended to the Office-net.

First signs of suspicious traffic from the Secure-net were found on July 1, 2011, possibly a network scan. This traffic originated from the BAPI-production workstation. Due to limitations on the investigation this workstation was not examined. Later on July 2, 2011, traffic from CA server and other servers in the Secure-net was initiated towards the stepping stones in the DMZ-ext-net.

Based on the firewall logs the following servers were identified as likely to have been compromised:

Network	Server
DMZ-ext-net	Main-web server
	eHerkenning-AD server
	eHerkenning-HM server
	Pass-web server
	Docproof1
	Docproof2
Office-net	BAPI-db server
	Source-build

Network	Server
Secure-net	BAPI-production (workstation)
	CAP-app-db server
	Relations-CA server
	Public-CA server
	CCV-CA server
	Taxi-CA server
	CAP-app-web server
	Root-CA server
	Qualified-CA server

Based on investigation of the firewall logs, the following external AttIP addresses are likely to been utilized by the attacker (see also Appendix II):

Intruder IP	Remark
AttIP1	Successful connections initiated from DMZ-ext-net and specifically tunnels from DMZ-ext-net. Blocked attempts from Secure-net.
AttIP2	Successful connections initiated from DMZ-ext-net.
AttIP13	Dropped connections initiated from DMZ-ext-net.
AttIP19	Successful connections initiated from DMZ-ext-net.
AttIP22	Successful connections initiated from DMZ-ext-net.

6 Investigation of CA servers

The rogue certificates that had first been generated on July 10, 2011 were first discovered when an automated routine test that had failed to work was restored on July 19, 2011. The test verified certificates that had been issued with the records in the back office and showed that a number of these certificates lacked any records in the back office of DigiNotar. The staff of DigiNotar proceeded to examine the CA managing applications and found that rogue certificates had been issued. The serial numbers that corresponded with these rogue certificates were revoked immediately. An initial incident response team was formed and a further investigation was launched. As a result, more rogue certificates were found and revoked on July 21, 2011 and on July 27, 2011. At the end of July, DigiNotar was convinced that the breach of its infrastructure was under control and that the damage had been repaired.

On August 28, 2011, another rogue certificate issued for all services on the Google.com domain and its sub domains, which had not been revoked, was found by a Gmail user[20]. A search through the management software did not reveal the serial number that belonged to this certificate. In order to revoke the rogue `*.google.com` certificate, another certificate was created with the same serial number and revoked effectively on August 29, 2011 at 19:09:05 (CEST).

Fox-IT investigated the CA management software to determine if any additional certificates were falsely issued. Fox-IT also investigated if other Certificate Authorities had been compromised.

It is important to note that the CA servers did not log to a separate secure log server. All the investigated log files originated from servers that had been compromised. As a result, all the identified log files may have been tampered with, log files may have been replaced by earlier versions or the log service may have been shut down intentionally. Consequently, suspicious entries in the log files can only be used to make inconclusive observations regarding unauthorized actions that took place, but the absence of suspicious entries cannot be used to infer that no unauthorized actions took place.

6.1 Sources

Eight systems that operated as CA servers were investigated:[21]

- **CCV-CA server.** This server managed the certificates that were used for electronic payment in the retail business. The name CCV refers to the company that used these certificates (www.ccv.eu).
- **Nova-CA server.** Also called Orde-CA, which managed certificates of the Nederlandse Orde van Advocaten (Dutch Bar Association) (www.advocatenorde.nl).
- **Public-CA server.** This server managed the certificates that were used for public services, including the DigiNotar Extended Validation Certificate Authority, which was used for protecting websites with SSL.
- **Qualified-CA server.** Managed the certificates that DigiNotar issued on behalf of the Staat der Nederlanden (the Dutch state). This was a sub-Certificate Authority in the PKI hierarchy called PKIoverheid (PKI government). This server also managed the DigiNotar Qualified Certificate Authority, allowing documents that had been signed with these certificates to be used as the legal equivalent of a handwritten signature as determined in the European Union Directive 1999/93/EC. DigiNotar was registered to issue these qualified signatures.[22]
- **Relation-CA server.** On this server the Certificate Authorities of other important clients of DigiNotar were hosted such as:[23]
    - TenneT, a large Dutch electricity supplier (www.tennet.org)
    - Koninklijke Notariële Beroepsorganisatie (Royal Netherlands Notarial Organisation at `www.knb.nl`)

[20] Google Groups, "Is This MITM Attack to Gmail's SSL?" at http://groups.google.com/a/googleproductforums.com/d/topic/gmail/3J3r2JqFNTw/discussion and Pastebin, "Gmail.com SSL MITM ATTACK BY Iranian Government – 27/8/2011" at http://pastebin.com/ff7Yg663

[21] Other systems found running CA managing software were WINVM012 and WINVM032. No exhaustive search was undertaken to identify all the systems running CA management software because these eight systems managed the most important Certificate Authorities.

[22] This registration was ended on September 14, 2011.

[23] A complete list is included in Appendix VI.

- **Root-CA.** Managed the root Certificate Authority certificates of DigiNotar and all the certificates of the Ministerie van Infrastructuur en Milieu (Dutch ministry of Infrastructure and the Environment).
- **Taxi-CA.** Hosted the Certificate Authorities that were used for a project for the registration of taxi drivers in The Netherlands for the Ministerie van Infrastructuur en Milieu. The test CA environment of the Ministerie van Infrastructuur en Milieu was also hosted on this server.
- **Test-CA.** Different kinds of test Certificate Authorities were managed on this server. They all had "test" in the common name of their certificates with the exception of three CA certificates (appendix VI).

The CA servers had access to the nCipher netHSM that was also located in Secure-net. The netHSM devices store private key material in a secure way, so that the key material cannot leave the device unencrypted. The private keys can only be used if a smartcard, which is secured with a PIN code, is present in the netHSM.

On the CA servers, software from RSA was installed in order to manage certificates. The product used was the RSA Certificate Manager (RSA CM).[24] The CA software consists of several services. One of the services provides a web interface for users and administrators. Another service logs the activity of the software into log files. The CA software also provides an application programming interface (API) that enables programmers to develop PKI applications. These applications can be developed using a scripting language called XUDA (Xcert Universal Database API). Since no information that could be used for a public report could be exchanged with RSA, Fox-IT used reverse engineering techniques to perform the investigation.

For the purpose of the investigation, Fox-IT used a list that was provided by DigiNotar, which contained all the certificates that had been issued by DigiNotar. This list `allcerts.csv` was created by exporting the CA databases and contained the following information regarding the certificates:

Value	Meaning
md5	The MD5 checksum of the certificate as calculated by the CA software
CA md5	The MD5 checksum of the issuing CA certificate
Serial nr.	The serial number of the certificate
Cert dn	The distinguished name field of the certificate
Valid from & valid until	The date fields of the certificate
Revocation date	The date of revocation (if applicable)

6.2 CA software log files

6.2.1 Sources

All CA servers were outfitted with software that logged relevant information for the ongoing processes. The information was stored in log files that were in the format `xslog_{yyyyMMdd}.xml`. It appears that the log files were not being rotated or removed automatically. A new log file was created whenever the machine was rebooted or when the logging service was restarted. The following log files from the period within which the intruder was active were investigated:

Server	Log files
CCV-CA	`xslog_20110616.xml`
Nova-CA	`xslog_20110401.xml`

Public-CA	`xslog_20110325.xml`
	`xslog_20110711.xml`
	`xslog_20110711_1.xml`

Qualified-CA	`xslog_20110224.xml`
	`xslog_20110702.xml`
	`xslog_20110704.xml`
	`xslog_20110723.xml`

Relation-CA	`xslog_20110407.xml`
Root-CA	`xslog_20110616.xml`

[24] Older versions of this software are known as RSA Keon.

Server	Log files
Taxi-CA	xslog_20110517.xml xslog_20110711.xml
Test-CA	xslog_20110224.xml

The integrity of blocks of data within the log files can be verified using a signature. The CA software can be used to verify the integrity of the log files, which was done for all CA management application instances by an employee of DigiNotar. Two log files failed the verification by the CA software, which originated from Public-CA server:

- xslog_20110711_1.xml
- xslog_20110720.xml

The integrity of other log files was verified by the CA software without failure. The breached integrity of xslog_20110711_1.xml corresponds with descriptions that were found in the incident log book. The log book contains log entries showing that when the console on the Public-CA machine was started on July 20, 2011, rogue certificates were being issued and that the machine was shut down. The corresponding customary entries "Log Server Stopped" and "Final Entry" are missing from this log file.

The entries in the log files contain the following information:

- LOG_NUMBER: a sequential unique log entry number
- LOG_SOURCE: the source of the log entry (either from the Certificate Administration management, Secure Directory or Logging Server)
- EVENT_CONDITION: either ATTEMPT or COMPLETION of an action
- DATE,TIME: the date and time of the entry (in CEST time zone)
- ID: a hexadecimal value consisting of 32 characters (29 unique IDs have been encountered - 6 of these were encountered more than 100,000 times)
- IP_ADDR: the IP address associated with the action
- LOG_DATA: the structure of this field varies depending on the data that it contains. A "Certificate signing" entry has the following fields:
  - Succeeded or failed
  - Certificate presented: an MD5 value of 32 characters of the certificate presented to the CA software with the request
  - certDN with distinguished name fields
  - MD5-value of the certificate
  - Issuing CA MD5

Note that no serial number was logged for the issued certificates. Therefore, no link could be established between a certificate and an entry in the log files on the basis of a serial number. The relation between a certificate and a log entry may have been established using the MD5 value of the certificate that was in the log file; however, the data that was used to calculate the MD5 was not known.[25] The certificates that were stored in the databases also contained the MD5 value of the certificate. Therefore, it was attempted to make a definitive link between entries in the log files and the certificates on the basis of the MD5 value in these databases.

6.2.2 CA software log analysis

In the log files of some CA servers, log entries were found indicating the automatic generation of a Certificate Revocation List (CRL). Certificate Authorities usually issue CRLs at regular intervals according to their policies. These CRLs are signed by the issuing Certificate Authorities, which can only occur if a private key was active on the netHSM. The log entries referring to such an automatic process thus indicated that the private keys in the netHSM were activated and that there was potentially an opportunity for the intruder to abuse these private keys. According to DigiNotar, this practice is based on requirements of PKIoverheid.

[25] The MD5 value did not correspond with the MD5 fingerprint or the MD5 sum of the certificate in PEM or DER format.

In the examined log files, a large number of automatically generated CRLs were found. The complete list is included in Appendix IV.

Server	Number of Certificate Authorities
Nova-CA	3
Public-CA	10
Root-CA	6
Qualified-CA	8
Test-CA	27
Relation-CA	8

CCV-CA server
The logs of the CCV-CA server showed no activity between June 17, 2011 and July 22, 2011. No automated CRL generation process was found.

Public-CA server
The log entries of Public-CA server showed the automated generation of CRLs for (among others) the Certificate Authorities of *Cyber CA*, *Extended Validation CA*, *Public CA - G2*, *Public CA 2025* and *Services 1024 CA*.

The analysis of the log file `xslog_20110325.xml` on the Public-CA server showed that the first signs of abnormal activity and certificate signing attempts occurred on Sunday July 3, 2011 at 12:15:44. Between Thursday July 7, 2011 at 23:19:33 and Sunday July 9, 2011 at 12:53:16, it appears that experiments took place by the intruder outside of office hours. During this timeframe old certificate requests appear to have been reissued. For example, `beveiligd.gemeentesudwestfryslan.nl` was issued twice with different CA keys. On July 10, 2011 at 19:55:56, the log files showed that the first rogue certificate was successfully issued on the Public-CA server (a `*.google.com` certificate). Between 19:55:56 and 23:55:57 on July 10, 2011, a total of 198 rogue certificates were issued on the Public-CA server. The log server was stopped on 11-Jul-2011 at 01:41:19.

The log file `xslog_20110711.xml` started on July 11, 2011 at 08:18:42, leaving a gap in the logs of about six and a half hours. The next log file (`xslog_20110711_1.xml)` contained only a few entries, most of them logging failed certificate signing attempts.

The next log file (`xslog_20110711_1.xml`) started on July 11, 2011 at 11:24:49, most likely after a reboot of the system or the logging service. On July 18, 2011 at 16:19:27, a burst of 124 rogue certificates were created. Another burst of 124 rogue certificates were issued on July 20, 2011 at 08:56:41. According to DigiNotar, this burst was an isolated incident that produced a copy of generated rogue certificates in the previous burst and prior measures had been taken to prevent the certificates from being published. No other rogue certificates were found in the logs of the Public-CA server after this point in time. The log file was not properly terminated. The last log entry dated from July 20, 2011 at 08:57:11.

The following log file (`xslog_20110720.xml`) started on July 20, 2011 at 12:19:37, has no entries and was terminated at 12:21:41. The next log file (`xslog_20110720_1.xml`) started on July 20, 2011 at 12:34:52. No obvious suspicious activity was found in this file. The final entry was on July 20, 2011 at 18:20:14. After that all entries in the log files appeared to relate to normal activity. The servers were shut down daily.

Based on logs of the Public-CA server, 446 certificates were issued between July 10, 2011 at 19:55:56 and July 20, 2011 at 08:57:11 on the Public-CA server that were evidently rogue based on the common name that was used.

Relation-CA server
The log entries of Relation-CA server showed the automated generation of CRLs for (among others) the Certificate Authorities of *KNB CA 2*, *Ministerie van Justitie CA* and *Stichting TTP Infos CA*.

The analysis of the log file `xslog_20110407.xml` on Relation-CA server showed that the first signs of extraordinary activity and certificate signing attempts occurred on July 2, 2011 at 19:59:34. The first

successful rogue certificate was created on the Relation-CA server on July 10, 2011 at 13:05:10 with the common name `*.google.com`. The log file ended normally on July 20, 2011 at 18:20:29.

The logs of the Relation-CA server showed that a total of 85 rogue certificates were successfully created on the Relation-CA server between 13:05:10 and 23:35:54 on July 10, 2011.

Root-CA, Nova-CA and Test-CA servers
The examination of the log files showed an automated CRL generation process on all three CA servers, including the Certificate Authorities of *DigiNotar Root CA*, *Root CA G2* and *MinIenM Organisatie CA - G2* on the Root-CA server, and the Certificate Authority *Nederlandse Orde van Advocaten* on the Nova-CA server. Very few certificates were issued by these Certificate Authorities during the intrusion, according to the log files. No unusual or remarkable log entries were found.

Taxi-CA server
The logs of the Taxi-CA server showed no activity between June 16, 2011 and July 11, 2011. No unusual or remarkable log entries were found. No automated CRL generation process was found.

Qualified-CA server
The log entries of the Qualified-CA server showed automated backup processes and generation of CRLs, which included the Certificate Authorities *DigiNotar PKIoverheid CA*, *PKIoverheid CA Organisatie - G2*, *Overheid en Bedrijven*, *DigiNotar Qualified CA* and *DigiNotar Qualified CA - G2*.

When the log files of the Qualified-CA server were examined, the two successive log files, `xslog_20110224.xml` and `xslog_20110702.xml`, showed that the log server was turned off on July 2, 2011 at 02:13:40 presumably by the intruder and turned on again at 10:12:43. This leaves a gap of approximately eight hours during which no activity was logged. No other unusual or remarkable log entries were found.

6.3 CA databases

The CA management software used databases to store various application data. Several database files were stored in the directory `{install directory}\Xudad\db\`. The main database file was named `id2entry.dbh`. The main database file contained records of the certificates that had been issued, including several characteristics for the issued certificates.

During its investigation, Fox-IT encountered database files named `serial_no.dbh` that contained serial numbers plausibly identifying the certificates issued by the software. All the found `id2entry.dbh` and `serial_no.dbh` database files were examined, including recoverable deleted files. All these database files were in the Berkeley DB format.

6.3.1 Certificates

The certificates stored in the main database file were extracted and converted into the PEM (Privacy Enhanced Mail) format. The following methodology was used in order to do this:

- Perform a case insensitive search for the string `pem_x509::` in the `id2entry.dbh` files
- Extract the trailing data block
- Decode the text from its base64 format
- Encapsulate the text with `-----BEGIN PUBLIC KEY-----` and `-----END PUBLIC KEY-----`.

When the certificates were extracted in this way, some extracted data blocks were invalid. An attempt to read them with, for instance, OpenSSL would result in an error. A check revealed that complete versions of these data blocks were also present in the database. This led Fox-IT to conclude that no certificates were missed using this method.

Additionally, some certificates were stored more than once in the database or were found in a backup database. Comparing the fingerprints[26] of the certificates identified the duplicates. The incomplete and duplicate certificates were excluded from further analysis.

[26] In public key cryptography, a public key fingerprint is a short sequence of bytes used to authenticate or look up a longer public key.

The following numbers of certificates were identified. The validity period has not been taken into account. Details of these certificates are provided in Appendix V.

	Root-CA server	Qualified-CA server	CCV-CA server	Nova-CA server
Total number of certificates	73	23621	36	37868
Unique subject name	45	22483	26	35742
Different issuers	10	13	9	5
Basic constraints = TRUE	29	7	20	2
Self signed	5	4	8	4

	Public-CA server	Taxi-CA server	Test-CA server	Relation-CA server
Total number of certificates	46101	1348	3111	11671
Unique subject name	44161	601	2088	11168
Different issuers	13	17	32	16
Basic constraints = TRUE	9	15	42	12
Self signed	4	5	11	6

6.3.2 Private keys

The `id2entry.dbh` database files contained entries labeled `privatekey::`. After decoding the base64 data, these entries showed the following ASN.1 structure (Root-CA server is used for this example):

```
 0:d=0  hl=2 l= 111 cons: SEQUENCE
 2:d=1  hl=2 l=   1 prim: INTEGER    :02
 5:d=1  hl=2 l=  19 prim: IA5STRING  :XCSP nCipher Native
26:d=1  hl=2 l=   1 prim: INTEGER    :53
29:d=1  hl=2 l=  64 prim: cont [ 0 ] :30 3E 16 0E 72 73 61 2D 6B 65 6F 6E 2D 63 61 2D  0>..rsa-keon-ca-
                                      36 38 16 10 31 33 30 38 32 32 33 37 36 30 33 32  68..130822376032
                                      37 30 30 30 16 11 53 45 43 55 52 45 20 4F 50 45  7000..SECURE OPE
                                      52 41 54 49 4F 4E 53 01 01 FF 02 01 02 02 01 04  RATIONS.........
95:d=1  hl=2 l=  16 prim: cont [ 1 ] :30 0E 80 01 01 81 01 00 04 06 02 04 84 8D A7 10  0.?.............
```

The decoded ASN.1 structure led investigators to believe that these are references to private keys in the netHSM. If this is the case, then investigators can conclude that the software installed on the server could use these keys and could show what Certificate Authorities were used on what server.

In the records surrounding the private key entries, there was no indication of the certificate or common name linked to these keys. However, a data block labeled `publickey::` was present. For the example mentioned above, investigators extracted the public key and matched it with the public keys of the extracted certificates. This resulted in the Certificate Authority certificate with the common name '`CN=MinIenM Autonome Apparaten CA - G2`'. Using this method, investigators were able to determine what CA servers could use which private keys in the netHSM, lookup the corresponding certificate and thus identify the Certificate Authority.

In some instances, different keys were used for the same distinguished name (DN). This occurred, for example, if a certificate expired and a new key was generated. A complete list of the references to private keys and the matching distinguished name is provided in Appendix VI. The validity period has not been taken into account.

Server	Total number of keys	Unique subject Name	Unknown key
Root-CA	11	11	None
Qualified-CA	8	8	None
CCV-CA	10	8	2
Nova-CA	3	3	None
Taxi-CA	17	15	2
Test-CA	43	34	4
Relation-CA	15	14	1
Public-CA	10	10	None

Also note that for some keys no matching certificate was found. This means that a reference to a private key in the netHSM could not be matched with a corresponding certificate.

6.3.3 Serial numbers

Removed database files were discovered on multiple CA servers, raising the suspicion that the intruder had manipulated database and log files. For example, the serial number of the rogue `*.google.com` certificate that was abused in the MITM attack was only present in a `serial_no.dbh` database that had been removed from the server and was recovered during the investigation.

The assumption was made that the `serial_no.dbh` database contained all serial numbers for certificates, including rogue certificates that had been issued by the CA software. To establish if serial numbers corresponding with rogue certificates were indeed present, all `id2entry.dbh` and `serial_no.dbh` files were collected for each CA server, including all recoverable files that had been removed. It was investigated whether every serial number in `serial_no.dbh` could be matched with an issued certificate.

In order to determine this, two sets of serial numbers were created. Set A included serial numbers from all `serial_no.dbh` files. Set B included serial numbers from all `id2entry.dbh` files. The difference between these lists resulted in set C, containing the unknown serial numbers. As an extra check, these serial numbers were matched against the `allcerts.csv` list of issued certificates that was provided by DigiNotar.

This method was applied for all the CA servers. The results showed unknown serial numbers originating from four of the eight CA servers. A complete list of unknown serial numbers for the CA servers can be found in Appendix VII. It was impossible to match a serial number to a specific common name or to match it to a specific issuing Certificate Authority since this information was not present in the database.

CA server	Number of unknown serial numbers
Root-CA	7
Qualified-CA	2
Taxi-CA	24
Public-CA	203

In the time available for the investigation, it could not be established conclusively for all instances why the discrepancy between the `serial_no.dbh` and `id2entry.dbh` databases existed. The examination of the OCSP responder logs showed that five of these unknown serial numbers were validated, including the `*.google.com` certificate used for the large-scale MITM attack (see paragraph 10.2). Given the fact that a number of unknown serial numbers were known to correspond with rogue certificates, it is plausible that most or even all unknown serial numbers are the result of rogue certificates that had been issued. However, unknown serial numbers may also have been caused by software errors or as a result of aborting the issuing process. As a precautionary measure, all the unknown serial numbers were revoked.

6.4 Conclusion

The CA management software of eight CA servers at DigiNotar was investigated by Fox-IT. After a thorough search, it was found that the number of issued rogue certificates in the log files exceeded the number of rogue certificates in the CA management application. This led to the conclusion that the CA software had been manipulated and records in the database had been deleted.

An important goal of this part of the investigation was to determine what Certificate Authorities had issued rogue certificates and thus could no longer be trusted. Since the logging service was running on the same systems that had been compromised and that records had been manipulated, the log files could only be used to make inconclusive observations regarding unauthorized actions. The absence of suspicious entries in the log files could not be used to infer that no unauthorized actions took place.

However, in order to issue certificates by a Certificate Authority on a CA server, the corresponding private key of the Certificate Authority in the netHSM needed to be active. This meant that the unauthorized actions that might have taken place could not have included the issuing of rogue certificates if the corresponding private key had not been active during the period in which the intrusion took place.

The log files recorded the distinguished name of a certificate but not its serial number. To revoke a certificate, however, the serial number of the certificate was essential. The revocation process was therefore changed to be based on the known valid certificates (a white list method) at the advice of Fox-IT (see also paragraph 2.2.1).

6.4.1 Rogue certificates

Based on the investigation of the log files, a total number of 531 rogue certificates were identified (446 on the Public-CA server and 85 on the Relation-CA server). These were identified as rogue because of the blatant common name of the certificates. Other certificates that were issued during the time the intruder was active on the CA servers may also have been fraudulent. Further investigation could determine if this is indeed the case.

Of the 531 rogue certificates found in the logs, 332 certificates were recovered in the databases and their serial numbers were known. One previously unknown certificate was posted by the Google.com user. For the remaining 198 log entries, no certificate was found and therefore the serial was marked as unknown.

The number of rogue certificates that could be connected to the issuing Certificate Authorities was:

Certificate Authority Common Name (Issuer)	Total	Unknown serial[27]	Cert.[28]	CA server
DigiNotar Cyber CA	108	1	107	Public-CA
DigiNotar Extended Validation CA	98	14	84	Public-CA
DigiNotar Public CA - G2	56	0	56	Public-CA
DigiNotar Public CA 2025	184	183	1 [29]	Public-CA
Koninklijke Notariele Beroepsorganisatie CA	67	0	67	Relation-CA
Stichting TTP Infos CA	18	0	18	Relation-CA
Total	**531**	**198**	**333**	

The investigation identified 236 serial numbers in the `serial_no.dbh` databases that have no obvious relation to log entries or recovered certificates. The following table compares the earlier list of serial numbers originating from CA servers with log entries without matching serial numbers.

CA server	Serials without matching certificate	Logs without matching serial
Root-CA	7	0
Qualified-CA	2	0
Taxi-CA	24	0
Public-CA	203	198
Relation-CA	0	0

Evidence of unmatchable certificates

Because it remains unknown when serial numbers were stored in the `serial_no.dbh` database, the total number of rogue certificates was unverifiable.

Of these rogue certificates, 344 have domain names as their common name. The remaining 187 have "Root CA" in their common name. This does not necessarily mean that they could have been used as an issuing certificate. Of the 333 rogue certificates that were found, none had the basic constraint attribute set, meaning that they could not be used for issuing certificates. Also in the logs of the CA management software, no logs were present of rogue-issued Certificate Authority certificates. However, no contraindication was found that it was impossible to issue rogue issuing certificates or that these were not created by the intruder either. Depending on the way the software verifies certificates, the basic constraint attribute can be ignored.

[27] Traces of these certificates were found in the logs and not in the databases, therefore the serial number is not known.
[28] The certificate is found in the database.
[29] The rogue wildcard Google.com certificate that was abused in the MITM attack.

The key usage of the 333 found certificates were all set as a critical attribute and were meant for the purpose of digital signature, key encipherment and data encipherment or a combination thereof. No code or certificate signing key usage was found.[30]

The 531 encountered rogue certificates contain 140 unique distinguished names and 53 unique common names. A list of the common names is included in Appendix VIII.

6.4.2 Trust in the Certificate Authorities

The situation that Fox-IT encountered was that the CA management software had clearly been manipulated. It was evident that the issuing Certificate Authorities of the rogue certificates, as identified on the basis of their Common Name, had to be revoked according to PKI standards[31]. Additionally, untraceable serial numbers on some of the CA servers raised suspicions in regard to the security of the Certificate Authorities that were managed on those machines. Gaps in log files of these CA servers added to the suspicions in regard to their security.

Some uncertainties in the operation of the CA management software still exist[32]. These uncertainties include if deleted log files could be detected, if the log settings had been manipulated, if the log service was stopped while the issuing software kept running, how the untraceable serial numbers were issued, et cetera. A scenario that may have been possible is that the intruder could have created a backup of the database and log files, then issued several certificates and restored the original backup thus removing all evidence.

The investigation of the suspicious files and, specifically, the presence of cached versions of the `/beurs` directory on the stepping stone showed that the operating systems of all CA servers had been compromised and were used at some point by the intruder (see Chapter 4).

Having compromised the CA servers, the only additional barrier for issuing rogue certificates that remained was the activation of the Certificate Authorities' private keys, which are activated with a smartcard on the netHSM. Some Certificate Authorities were continuously operational as evidenced by the automatic generation of CRLs, meaning that the corresponding private keys in the netHSM were always activated. If, for example, an offline record had been kept of when these smartcards were present or removed, a contraindication could have been given that a Certificate Authority could not have been abused to issue rogue certificates. However, no evidence could be produced by DigiNotar that private keys were not activated during the time of the intrusion. According to DigiNotar, the smartcard for CCV-Certificate Authority had been in a vault for the entire period of the intrusion and its private key was not activated during this period.

It remains possible that the CA software used was able to produce certificates that have identical certificate attributes as previously issued certificates, including the serial number and the validity dates, with the exception of the public key and its key identifier. If this was the case, the intruder could have issued seemingly identical certificates that were formally issued and trusted. It may also have been possible that the intruder used other CA management software to have certificates signed directly by the netHSM (bypassing even the XUDA interface). This was not investigated further.

The overall conclusion was that the possibility could not be excluded that all Certificate Authority keys managed by DigiNotar, with the exception of the private keys for the CCV-Certificate Authority, could have been abused to issue rogue certificates. Even certificates that would appear to have been issued before the intrusion took place could not be verified by the public key infrastructure and therefore could

[30] A user on Pastebin named 'ComodoHacker' created a binary (`calc.exe`) and signed it with the `*.google.com` certificate used in the MITM attack. Although this certificate had no explicit code signing key usage the Microsoft Windows operating system accepts the signature.

[31] RFC 5280 for instance stipulates that the "Existence of bogus certificates and CRLs will undermine confidence in the system. If such a compromise is detected, all certificates issued to the compromised CA MUST be revoked, preventing services between its users and users of other CAs". According to this RFC, certificates also need to be revoked if a CA and the corresponding private key are merely suspected to be compromised.

[32] RSA was contacted concerning the operation of the software, but no information that could be used by Fox-IT for a public report could be exchanged. Our efforts in this regard were abandoned after while due to the increasing irrelevancy of the specific issue for the overall investigation.

not be trusted. According to standards and best practices in the industry, the certificates had to be revoked, as the intruder could have issued seemingly identical certificates (including issuing dates in the past). All DigiNotar certificates therefore could no longer be trusted and the Certificate Authorities had to be removed from trust lists with the exception of the CCV certificates. The impact of the revocation of the certificates that had been issued by DigiNotar varied depending on their usage and had to be assessed on a case by case basis.

7 System access and tools

The goal of this part of the investigation was to identify tools that had been used during the intrusion and the purpose for which they were used. For this purpose, the images of systems were probed for anomalies and for files that could be connected to other parts of the investigation. In order to identify suspicious files, the timestamps of the files on disk images were examined, including recoverable files. Timestamps indicated when a file was created, copied, accessed or modified. In combination with the file location and file name, a file could be marked as suspicious for further examination.

This examination of the following servers is detailed in this chapter:

Network	Server
Secure-net	Qualified-CA
	Taxi-CA
	Relation-CA
	Public-CA
	Root-CA
	CCV-CA
Office-net	Office-file server
	BAPI-db
DMZ-ext-net	Main-web
	Docproof2

All the timestamps in this chapter are based on Coordinated Universal Time (UTC). A non-exhaustive list of the suspicious files that were found is included in Appendix IX.

7.1 Previous investigation

The initial internal investigation by DigiNotar was done on the file `svchost.exe` which was found on the Public-CA server. This investigation concluded that the file created a file `jobsdone.zip` and uploaded this file to the stepping stone Main-web in DMZ-ext-net using the `/beurs/up.aspx` script. The investigation also stated that the file `svchost.exe` created a connection to that same server on port 53. The file `svchost.exe` was created on the Public-CA server on July 3, 2011 at 23:56. These results indicated that an automated process might have been in place. This could mean that certificates were automatically issued and transferred via the stepping stone to the intruder.

7.2 Connection tools

7.2.1 Stepping stones

The intruder placed `aspx`-scripts on at least two compromised web servers in DMZ-ext-net. These scripts were used amongst others as a file manager in order to up- and download files between internal and external systems.

Timestamp	File name	Server
17-Jun-2011 02:33:35	b.aspx	Docproof2
17-Jun-2011 05:26:36	settings.aspx	Main-web

The results of the investigation show that as of June 17, 2011 the web servers had been compromised and files could be up- and downloaded to DMZ-ext-net. From that point onwards, the web servers could be used as stepping stones to exchange files between systems on the Internet and compromised systems inside of DigiNotar's network. The scripts also contained other functionality such as port scanning, port mapping and restarting services. No evidence was found that these functions were used however.

7.2.2 Accessing the stepping stones

The temporary Internet files of the investigated Windows systems hosting the CA management software showed cached copies of a file exchange location on the Main-web server in DMZ-ext-net. These cached copies showed a directory listing of the file manager on the web server with files sizes and modification

dates. This was discovered early on in the investigation and it therefore quickly became clear that the intruder had used the web servers in the external DMZ network as stepping stones to transfer files between arbitrary systems on the Internet and crucial systems in DigiNotar's network.

In addition to cached HTML pages, the temporary Internet files also showed other cached files from the web servers that were used as stepping stones. These locally cached files were the result of a file that was downloaded from a stepping stone. A number of files that were uploaded to the stepping stone could also be identified due to an upload notification in the cached HTML pages of the file manager. The path of the temporary Internet files on the hard disk also showed which Windows user accessed the web page or downloaded the file.

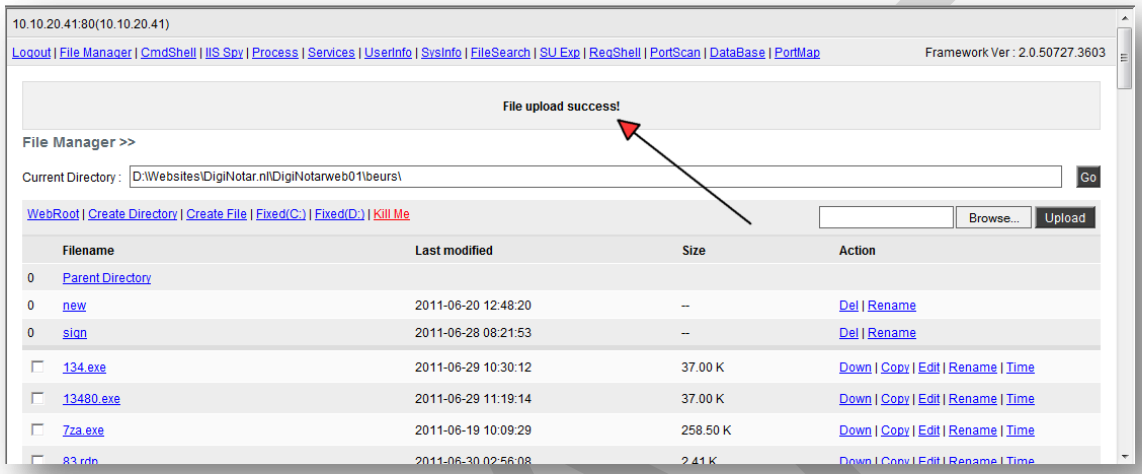


Figure 4 Example of a cached file upload page

If traces of a (recoverable) cached copy of the file exchange scripts from the stepping stones were identified on a system, the system could be marked as compromised by the intruder as only the intruder was aware of the existence of these scripts at that point in time. For this reason, the systems were probed for existing or recoverable `settings[*].htm` files (with * representing a number) and their content was inspected. The following systems showed traces of this cached page.

Server	File name	Size	First file create timestamp
BAPI-db	Settings[1].htm	3097	1-Jul-2011 14:33:59
Taxi-CA	Settings[1].htm	104502	1-Jul-2011 22:14:31
Qualified-CA	settings[1].htm	102048	1-Jul-2011 23:48:43
Root-CA	Settings[1].htm	3097	2-Jul-2011 2:40:06
Relation-CA	SETtings[1].htm	3097	2-Jul-2011 20:35:21
Public-CA	SETtings[1].htm	103156	3-Jul-2011 11:03:16

This led to the conclusion that the CA servers cited above were compromised by the intruder and that files may have been transferred to or from the stepping stone in the DMZ-ext-net. The fact that these files originated from Microsoft Internet Explorer also meant that a graphical user interface was available on these systems to the intruder using a tunneled remote desktop connection.

7.2.3 Network tunnels

A number of identified files that produced a tunnel between two IP addresses were examined more closely. The IP addresses were "hard coded" in the executable. Combined with the fact that the date and time of creation time was fairly recent led the investigators to believe that the files were specifically created (or modified) to run in the DigiNotar network.

The port numbers used suggested that a remote desktop connection (port 3389) was tunneled through port 443 (generally used for HTTPS).

File name	Source host	Destination host
troj134.exe	BAPI-db server	eHerkenning-AD server
troj172.exe	BAPI-db server	Pass-web server
troj25.exe	Source-build server	eHerkenning-AD server
troj65.exe	Docproof2 server	AttIP1

The earliest evidence of these tools in the examined servers was on June 29, 2011 at 22:13 on the BAPI-db server in Office-net.

Other created tools were partially investigated, specifically:

File name	Results
94.exe	Found on Docproof2. Created a connection to AttIP2.
134.exe	Created a connection to the server eHerkenning-AD on Port 443
13480.exe	Found on BAPI-db. Created a connection to the server eHerkenning-AD on Port 443

7.3 Gaining a foothold

Several tools found were used to scan for vulnerabilities and to increase the intruder's level of access in the network, such as scanning tools, port redirectors and remote process executor tools. Also, several files were found that indicated that the intruder had attempted to "brute force" terminal service or remote desktop credentials. These tools appeared on the stepping stone file exchange on June 18, 2011.

Traces in the "Documents and settings" directory on the BAPI-db server indicated that the intruder utilized the user account `MSSQLusr` starting on June 17, 2011 at 16:15:49. This user account was used by the Microsoft SQL service that was running on the BAPI-db server. Additionally, on the Main-web server the file `web.config` was identified that contained a string with credentials to access the database on BAPI-db:

```
<add key="connstring" value="Server=172.17.20.4;_Database=BAPI01;
uid=Bapi01usr;pwd=Bapi01usr12345!" />
```

This led to the conclusion that the intruder connected to the Microsoft SQL service running on the BAPI-db server from the Main-web using a found password and executed programs on the BAPI-db. The connections were not prohibited by the firewall as the investigation on the firewall log has shown in paragraph 5.2.3.

When the rights of the MSSQLusr account were examined it showed that MSSQLusr was part of the local administrators group, but the `LastWrite` date for the group was 18 June, 2011 at 02:18:48. The administrator rights could have been obtained after an effort by the intruder to escalate his rights or because the `MSSQLuser` had local administrator in the first place and that no further efforts were necessary. Event logs were not available to determine when MSSQLusr was first added to the local administrators group. On 1 July, 2011 at 14:33:59, the intruder used the local administrator account on the BAPI-db server.

The data shows that the intruder had used the administrator rights on the Qualified-CA server for the domain `DNPRODUCTIE` on July 1, 2011 at 23:48:43. Although this date is the first date seen in the investigation using a domain administrator account, it does not mean that the rights were not utilized earlier.

7.3.1 Password cracking tools

On the CCV-CA server, the well known `Cain & Abel` tool with `winpcap` had been installed. This tool can be used to extract and to crack password hashes. `Cain & Abel` can also be used to extract password hashes and to "brute force" the hashes to reveal the original passwords. Also the `pwdump` and `cachedump.exe` tools were found on the BAPI-db server and a stepping stone server.

On the desktop of the CCV-CA server, deleted files were found containing the output from the tool `pwdump`:

- `winsvr022.txt` (winsvr022 is the Qualified-CA server)
- `winsvr056.txt` (winsvr056 is the Public-CA server)
- `winsvr167.txt` (winsvr167 is the Root-CA server)

Evidence was found that `Cain & Abel` was used to capture credentials using a man-in-the-middle attack. More specifically, deleted Kerberos tickets and NTLM challenge-responses were found in the files `K5.LST`, `KRB5.LST`, `SMB.LST` and `HOSTS.LST`.

On the Docproof2 stepping stone, a file `test.txt` was found with the output of `cachedump.exe`. The file contained the `mscache` hash of one of the administrators. The administrator password could easily be brute forced on the basis of the hash, which indicated that the password that was used was relatively weak.

The earliest traces of a similar tool `PwDump.exe` in the examined servers in Office-net date from June 17, 2011 at 16:19 on the BAPI-db server. The earliest traces of the tool `cachedump.exe` in the examined servers in Office-net date from June 21, 2011 at 12:50 on the BAPI-db server.

Also the files `mimi.zip`, `mimikatz.exe`, `demineur.dll`, `klock.dll` and `sekurlsa.dll` were found in the cached web pages of the file exchange on the stepping stone. These files are part of the `mimikatz` security auditing tool. The earliest time of these tools in the examined servers in Office-net are from June 20, 2011 at 11:14 on the BAPI-db server. The traces on the Taxi-CA server showed that the intruder had logged in as administrator and downloaded the file `mimi.zip`.

7.4 Issuing certificates

7.4.1 CA management interface

The temporary Internet files also showed activity on the local CA software web service (by the user `Administrator.DNPRODUCTIE`):

Server	File name	Size	Create date	Create Time
Qualified-CA	domain-main[3].htm	4162	1-Jul-2011	23:22:03
Root-CA	domain-main[1].htm	4162	2-Jul-2011	1:01:41
Root-CA	request-cacert[1].htm	27449	2-Jul-2011	1:05:47
Root-CA	cert-search-results[1].htm	26718	2-Jul-2011	1:06:36
Root-CA	view-cert[1].htm	13557	2-Jul-2011	1:07:17
Root-CA	domain-main[1].htm	4166	2-Jul-2011	1:08:38
Root-CA	request-msie[1].htm	233043	2-Jul-2011	1:08:45
Root-CA	add-msie-request[1].htm	7332	2-Jul-2011	1:10:03
Root-CA	cert-search-results[1].htm	2309	2-Jul-2011	1:11:23
Root-CA	view-cert[1].htm	15164	2-Jul-2011	1:11:52
Root-CA	MinIenM Organisatie CA - G2[1].p7b	5239	2-Jul-2011	1:12:42
Root-CA	cert-search-results[1].htm	3711	2-Jul-2011	1:15:56
Relation-CA	cert-search-script[1]	20027	2-Jul-2011	20:42:08
Relation-CA	cert-search-results[5].htm	58415	2-Jul-2011	20:43:29
Relation-CA	view-cert[1].htm	13654	2-Jul-2011	20:43:43
Relation-CA	index[2].htm	5291	2-Jul-2011	21:20:20
Relation-CA	cert-search[1].htm	11192	2-Jul-2011	21:20:30
Relation-CA	cert-search-script[1].htm	19411	2-Jul-2011	21:20:30
Relation-CA	cert-search-results[4].htm	340	2-Jul-2011	21:22:25
Relation-CA	cert-search-results[6].htm	9966	2-Jul-2011	21:37:08
Relation-CA	get-ca-list[3].htm	3071717	2-Jul-2011	21:51:22
Relation-CA	get-ca-list[2].htm	3071717	2-Jul-2011	21:54:12
Relation-CA	index[1].htm	2525	2-Jul-2011	21:55:49
Relation-CA	get-ca-list[5].htm	332	2-Jul-2011	21:55:57

These traces showed that the intruder was experimenting with the CA management software. On the Relation-CA server, many `pkcs10` requests were made using the local CA software web interface. Also many Certificate Signing Requests (CSRs) were manually made with this interface.

7.4.2 XUDA scripts

The CA management software has an interface that can be used to execute custom applications. These applications can be developed using a scripting language called XUDA (Xcert Universal Database API).

On July 2, 2011 at 02:18:56, the Root-CA server created a Dr. Watson error dump of `Xuda.exe`. This means that `xuda.exe` had crashed, which was probably due to experimentation by the intruder given the time of occurrence (Saturday night local time).

On the Relation-CA server, the XUDA script `get.xuda` was recovered, which was created on July 2, 2011 at 16:58. This script was accessed by the local Internet Explorer on the Relation-CA server, as evidenced by a cached page showing a XUDA error.

Another XUDA script was found on the Public-CA server. This file `x-select-settings.xuda` was found with a modification timestamp of July 3, 2011 at 22:59:18. The script contained XUDA-code that uses the Xcert Universal Database API in order to utilize the CA software. In this script, two lists of 113 signing requests were included. The investigation on the CA management software as described in Chapter 6 shows more rogue certificates were issued than the amount of signing requests included in the XUDA script.

In this script, a personal message from the intruder was enclosed:

```
I know you are shocked of my skills, how i got access to your network
to your internal network from outside
how I got full control on your domain controller
how I got logged in into this computer
HoW I LEARNED XUDA PROGRAMMING
HOW I got this IDEA to write such XUDA code
How I was sure it's going to work?
How i bypassed your expensive firewall, routers, NetHSM, unbreakable hardware keys
How I did all xUDA programming without 1 line of resource, got this idea, owned your
. network accesses your domain controlled, got all your passwords, signed my certificates
. and received them shortly
THERE IS NO ANY HARDWARE OR SOFTWARE IN THIS WORLD EXISTS WHICH COULD STOP MY HEAVY
. ATTACKS
MY BRAIN OR MY SKILLS OR MY WILL OR MY EXPERTISE
That's all ok! EVerything I do is out of imagination of people in world
I know you'll see this message when it is too late, sorry for that
I know it's not something you or any one in this world have thought about
But everything is not what you see in material world, when God wants something to happen


My signature as always: Janam Fadaye Rahbar


Rahbare azizam mesle hamishe asoode bash, ta vaghti ke man va amsale man baraye in marzo
. boom
va baraye barafrashte negah dashtane parchame velayate faghih kar mikonand
daste har doshmano mozdouri ghat khahad bood
Rahbaram, Tamame vojoodam fadaye to ke ham jani o ham janani
```

The intruder left his fingerprint in the text: *Janam Fadaye Rahbar*[33]*.* The same text was found after the security breach at the Comodo certificate authority in March of 2011,[34] which also resulted in the issuing of rogue certificates.

[33] Supposedly translates to: "I will sacrifice my soul for my leader"
[34] Wired, "Independent Iranian Hacker Claims Responsibility for Comodo Hack" at http://www.wired.com/threatlevel/2011/03/comodo_hack/

7.4.3 nCipher DLLs

During the investigation on the Qualified-CA server, it appeared that some of the DLLs that were used to access the netHSM had been modified. These files were located in the `WINDOWS\system32` directory:

- `nfmodexp.dll`
- `ncspmess.dll`
- `ncsp.dll`
- `ncspdd.dll`
- `ncspsigdd.dll`

The unusual creation, modification and access times for these files were all around July 2, 2011 at 00:24:03, which was sufficient reason to mark these files as suspicious.

The manufacturer of the nCipher netHSM (Thales e-Security) provided us with the hash digest of the original DLLs. These hashes matched exactly with the hashes of the encountered DLLs. This led to the conclusion that the encountered DLLs had not been tampered with. It remains possible however that the DLLs had been modified but were later replaced by the original DLLs, which would explain the unusual creation date.

Related to this, nCipher logs were encountered with unusual timestamps. The following nCipher logs from the Root-CA server were created on July 2, 2011 at 01:28:19:

- `Application Data\nCipher\Log Files\keysafe.log`
- `Application Data\nCipher\Log Files\cmdadp.log`
- `Application Data\nCipher\Log Files\cmdadp-debug.log`

These traces on the DLLs and logs could indicate that the intruder had tried to use the netHSM and its stored private keys directly.

7.5 Conclusion

By examining the browser history and temporary Internet files of the compromised CA servers, it quickly became clear that the intruder used the Main-web and Docproof2 servers in DMZ-ext-net as stepping stones to transfer files. Scripts that provided the file exchange functionality were first placed on these servers in the early hours of June 17, 2011.

After compromising the web servers in DMZ-ext-net, the intruder used the Microsoft SQL service running on the BAPI-db server to execute files utilizing the BAPI-db server in the Office-net.

Tools were found that had been created by the intruder to provide network tunnels. Most of the investigated tunnels were used to set up a remote desktop connection with systems that were not directly connected to the Internet using the stepping stones. The IP addresses in these tools were used to tunnel traffic between the intruder (AttIP1 and AttIP2) and servers in the DMZ-ext-net (Docproof2) and subsequently between the DMZ-ext-net (eHerkenning-AD and Pass-web) and servers in the Office-net (BAPI-db and Source-build).

The investigation showed that the first found activity by the intruder in Secure-net took place on July 1, 2011 at 22:14:31 on the Taxi-CA server. The intruder first used the administrator rights for the domain `DNPRODUCTIE` on July 1, 2011 at 23:48:43 (on the Qualified-CA server). Although this date was the first date seen in the investigation, it does not mean that the rights were not utilized earlier. All CA servers in Secure-net were included in this domain.

Traces of tools and attempts to brute force password hashes were found. Furthermore, traces of attempts were found to create certificates with the user interface of the CA management software. Moreover, XUDA scripts and other traces were found that indicated that the programming interface of the CA software was abused.

Results of the initial investigation by DigiNotar indicated that an automatic process was in place to transfer files to the stepping stone.

The presence of cached pages of the file exchange HTML-pages from the stepping stone indicated that the servers containing these cached pages had been compromised by the intruder. Additionally, found

tools, logs and other traces marked or confirmed all the investigated servers as having been compromised on the basis of the results of this part of the investigation:

Network	Server
Secure-net	Qualified-CA
	Taxi-CA
	Relation-CA
	Public-CA
	Root-CA
	CCV-CA
Office-net	Office-file server
	BAPI-db
DMZ-ext-net	Main-web
	Docproof2

Based on the investigation of tools found, the following external AttIP addresses are likely to been utilized by the attacker (see also Appendix II):

Intruder IP	Remark
AttIP1	Malware found on Docproof2 (troj65.exe)
AttIP2	Malware found on Docproof2 (95.exe)

8 Remaining investigation

During the investigation, a limited number of assorted sources were examined. The results of these examinations are combined in this chapter.

8.1 netHSM

DigiNotar used nCipher netHSM 500s. The systems have limited logging facilities. It is recommended by the vendor to store the logs on a separate log server, but this was not done at DigiNotar. The logs were stored on the netHSM for a short period of time and were deleted every time the system was turned off. This had already occurred when the investigation was started by Fox-IT. No useful log files could be retrieved.

8.2 Load balancer

The network traffic was load balanced by a Coyotepoint Equalizer e550SL appliance. The logs from this appliance were stored on a central syslog server. An investigation of the logs from the load balancer and those that were present in the appliance itself showed no information that was relevant for the investigation.

8.3 External server at AttIP2

During the investigation a tool was found that connected back to the external IP address AttIP2 (see paragraph 7.2.3). On September 13, 2011, an official request for assistance to the authorities in the country where the server was located was issued. A copy of this server was investigated.

The web server log files from the server on AttIP2 showed interesting entries of GET requests from AttIP3. These log entries showed that the file `mails.rar` was downloaded several times on July 19, 2011 between 16:35:51 and 19:42:17. This file was only downloaded by AttIP3, except for the first occurrence when it was downloaded by AttIP5.

9 Investigative summary

The primary aims of the investigation that Fox-IT performed at the request of the ministry BZK were to determine how DigiNotar's network had been breached, to what extent it had been breached, which Certificate Authorities had been compromised and if evidence could be safeguarded that could lead to a potential criminal indictment of the intruder. For these purposes, various sources of information were gathered and examined, including the log files from the web servers, firewall and the various CA servers. Additionally, the images of relevant systems in DigiNotar's network were analyzed.

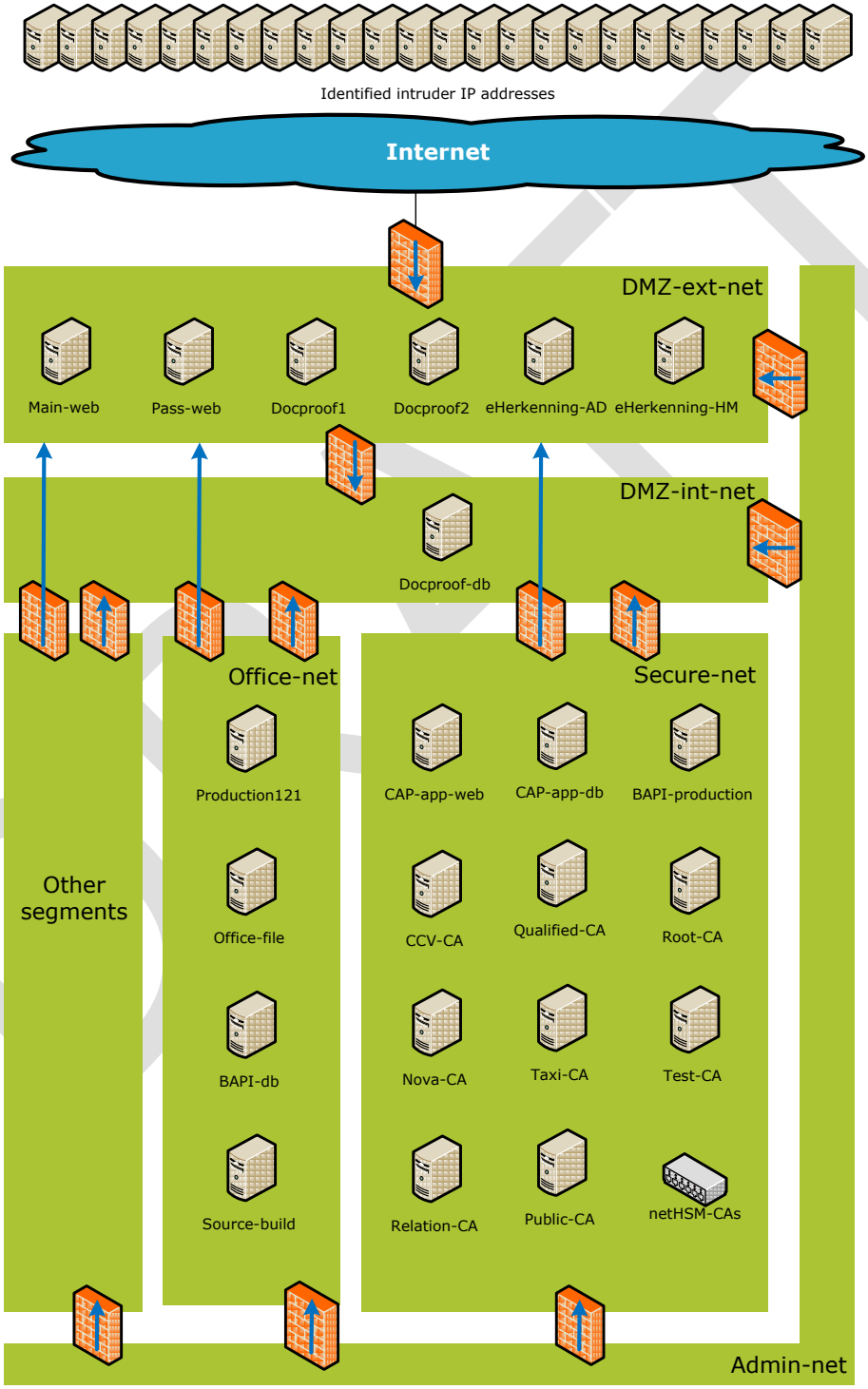


Figure 5 Referenced systems

9.1 First point of entry and stepping stones

The web servers on the outskirts of DigiNotar's network (DMZ-ext-net) served as the first point of entry for the intruder. Both the Main-web and the Docproof2 web servers were running an outdated version of DotNetNuke that suffered from known security vulnerabilities and were compromised on June 17, 2011. Log files that had been deleted on Main-web server were recovered and showed that scripts named `settings.aspx` and `up.aspx` in the directory `/beurs` had been used as rudimentary file managers and that the server acted as a stepping stone to other systems in the network. A similar script was identified on the Docproof2 server, but was used less frequently.

The log entries from the web servers that referenced the `/beurs` directory could be used to generate a list of both internal and external systems that had connected to these systems in order to use them as stepping stones. Internal systems that had connected to the `/beurs` directory could be flagged as having been compromised, while external systems that had connected to these scripts had been abused by the intruder. In total, 12 internal and 21 external suspicious IP addresses connected to the `/beurs` directory during the period that the security of DigiNotar's network was breached and 125 unique file names could be identified as having been copied to or from these stepping stones.

9.2 Compromised systems and Certificate Authorities

Based on the investigations of web server log files and the hard disks, the following internal systems could be identified as having been compromised:

Network Segment	Server
DMZ-ext-net	Main-web
	Pass-web
	Docproof1
	Docproof2
	eHerkenning-AD
	eHerkenning-HM
DMZ-int-net	Docproof-db
Office-net	BAPI-db
	Office-file
	Production121
	Source-build
Secure-net	CAP-app-db
	CAP-app-web
	Public-CA
	Qualified-CA
	Relation-CA
	Root-CA
	CCV-CA
	Taxi-CA
	BAPI-production

In addition to these systems, the attacker had the opportunity to compromise many more systems. No complete survey has been made to identify all the compromised systems due to limited time of the investigation.

The investigation showed that database records of the software managing the Certificate Authorities had been deleted or otherwise manipulated. The log files of the CA management software were stored on the same CA servers that had been compromised. Consequently, suspicious entries in the log files can only be used to make inconclusive observations regarding unauthorized actions that took place, but the absence of suspicious entries cannot be used to infer that no unauthorized actions took place.

However, in order to successfully issue rogue certificates, compromising a system that managed a Certificate Authority was not sufficient, as it also required the use of an active private key in a netHSM. This meant that the unauthorized actions that might have taken place could not have included the issuing of rogue certificates if the corresponding private key had not been active during the period in which the

intrusion took place. No records could be provided by DigiNotar if and when smartcards had been used to activate private keys in the netHSM, except that the smartcard for the CCV Certificate Authority had reportedly been in a vault for the entire period of the intrusion.

A Certificate Revocation List (CRL) generation process was identified for many Certificate Authorities on several CA servers. The identification of the regular automatic generation of CRLs showed that private keys in the netHSM for a number of Certificate Authorities were active and potentially provided an opportunity for the intruder to abuse these private keys. The combination of a compromised server, the automatic CRL generation, and the fact that logs had been or could have been tampered with, meant that the possibility could not be excluded that Certificate Authorities had been abused to issue rogue certificates. Even if no CRL generation process was active, the possibility could not be excluded that a compromised CA server had been instructed to issue rogue certificates once the corresponding private key was activated for its intended purpose.

Furthermore, it was found that the number of issued rogue certificates in the log files exceeded the number of rogue certificates in the CA management application. Additionally, serial numbers of certificates were identified that could not be matched with any certificate that DigiNotar had intentionally or unintentionally issued. These unknown serial numbers included the rogue wildcard Google.com certificate that was abused in the massive MITM attack primarily on Iranian users. The identification of unknown serials on a CA server therefore meant that the possibility could not be excluded that the Certificate Authority may have issued rogue certificates. Unknown serial numbers were identified to have been issued by certificate authorities hosted on the Public-CA, Qualified-CA, Root-CA and Taxi-CA servers.

Recovered log files from the Relation-CA server showed that the first extraordinary activity on the server occurred on July 2, 2011 and that the first rogue certificate was issued on the server on July 10, 2011. Recovered traces showed that the Remote Desktop Protocol had been used to gain access using a graphical user interface to at least seven servers: BAPI-db, Taxi-CA, Qualified-CA, Root-CA, Relation-CA, Public-CA and Qualified-CA. These connections were made through network tunnels bypassing the firewall.

It was evident that rogue certificates had been issued by Certificate Authorities managed on the Public-CA and Relation-CA servers, identifiable on the basis of their Common Name, that had to be revoked. Additionally, all unknown serial numbers had to be revoked as a number of these serials were known to correspond with rogue certificates. Given the fact that all DigiNotar's servers managing Certificate Authorities had been compromised and that relevant logging occurred on the same systems, all Certificate Authorities may have been abused in ways that are not reflected in (recoverable) log files. The way in which the Certificate Authorities may have been abused could not have included the issuing of rogue certificates, unless the corresponding private key was active in the netHSM at some point during the intrusion. Only the CCV Certificate Authority could be excluded from the list of Certificate Authorities that may have issued rogue certificates on this basis.

9.3 Information about the intrusion and the intruder

The intruder first gained unauthorized access to DigiNotar's network on June 17, 2011 and connections to AttIPs that were abused by the intruder were initiated from internal systems up to July 22, 2011. From the DMZ-ext-net, the intruder gained access to servers in the Office-net using a MSSQL server in that network. The first unauthorized connection that was identified from Office-net to DMZ-ext-net occurred on June 29, 2011. The first suspicious activity found in the Secure-net was on July 1, 2011 and connections appeared from Secure-net to DMZ-ext-net starting on July 2, 2011. Traces from the intruder were found in DMZ-ext-net up to Jul 24, 2011.

Unauthorized customized tools were used by the intruder to tunnel traffic intended for port 3389 (generally used for Remote Desktop Protocol) through port 443 (generally used for HTTPS). These tunnels allowed the intruder to connect to systems in the Office-net and Secure-net network segments, using the Remote Desktop Protocol in order to operate using a graphical user interface. This finding was confirmed by the presence of cached versions of the rudimentary file manager `settings.aspx` in the Temporary Internet Files on the hard disks of systems in these segments. These traces proved that Internet Explorer had been used in a graphical environment by the intruder.

The vast majority of the external IP addresses that were identified during the investigation were probably used as proxies to obscure the identity of the intruder. The true IP address of the intruder may have been revealed by error however, when the intruder erroneously connected to the Main-web server without using the proxy on AttIP4. This IP address AttIP3 was also identified in other parts of the investigation. More specifically, during the investigation a tool was identified that connected back to AttIP2. When this external system was examined, after an official request for assistance to the proper foreign authorities, its log files also showed connections from AttIP3. Furthermore, eight requests were made by AttIP3 when the DigiNotar's OCSP responses were tested for a rogue Yahoo certificate. AttIP3 resolved to a DSL user in the Islamic Republic of Iran. The first three OCSP requests of the wildcard Google.com certificate used for the MITM attack came from AttIP6 that also connected to the stepping stone on the Main-web server. The IP addresses AttIP6 and AttIP3 are from the same class-a network together with AttIP12, AttIP13 and AttIP14. A complete list of all the identified AttIPs has been handed over to the Dutch police (KLPD).

9.4 Timeline of the intrusion

Date	Notes
17-Jun-2011	Both the Main-web and the Docproof2 web server were compromised. File exchange functionality in DMZ-ext-net was in place. The first attempts to connect to the MSSQL server (BAPI-db) occurred from DMX-ext-net to Office-net. Later that day the first suspicious activity on the BAPI-db server in the Office-net occurred using the `MSSQLusr` user account.
18-Jun-2011	The first traffic was initiated by internal servers to IP addresses known to have been abused by the intruder (connect back functionality).
29-Jun-2011	Various scanning attempts were made to increase the foothold in other network segments (see Appendix III). The fact that scanning attempts were apparently necessary indicated that the intruder was still restricted to Office-net. The first tunneled connections over port 443 occurred from Office-net to DMZ-ext.
1-Jul-2011	The first scanning activity occurred in Secure-net. The stepping stone web page was accessed on CA servers in the Secure-net.
2-Jul-2011	The first successful connection was made from Secure-net to the stepping stone in DMZ-ext. Date of the first traces of experiments with the CA management software web interface and XUDA scripts on the Root-CA and Relation-CA servers.
3-Jul-2011	Modification time of a XUDA script with a personal message from the intruder on the Public-CA server and the first extraordinary activity in the CA software logs on the Public-CA server.
4-Jul-2011	Tools were setup to automatically transfer files from the Public-CA server to the stepping stone.
10-Jul-2011	The first rogue certificate was successfully created on the Relation-CA server. Subsequently, another 85 rogue certificates were created on the Relation-CA server. Another 198 rogue certificates were created on the Public-CA server. OCSP requests for rogue certificates started arriving at DigiNotar's OCSP responder from an DSL subscriber in Iran.
18-Jul-2011	Log files showed a burst of 124 rogue certificates that were created on the Public-CA server.
20-Jul-2011	Log files showed another burst of 124 rogue certificates were created on the Public-CA server. This is the last known date of the creation of rogue certificates.
22-Jul-2011	The last traffic was initiated from within DigiNotar's network to known intruders' IP addresses based on the investigation of the firewall logs.
24-Jul-2011	Last known date for traces of the intruder in DMZ-ext-net.

10 MITM attack

The investigation that was performed on the servers of DigiNotar as described in the previous chapters clearly showed that a large number of rogue certificates were issued by the intruder. The goal of the intrusion at DigiNotar appeared to have been to get a Certificate Authority to sign certificates. Most of the Certificate Authorities that were managed by DigiNotar were on trust lists of popular software products. Consequently, most operating systems, web browsers and document viewers instantly trusted the certificates that had been issued by DigiNotar.

The investigation showed that even though a large number of rogue certificates were identified, it could not be excluded that many more existed nor could it be excluded that these certificates could have had any content. This resulted in a situation where the intruder created certificates that could contain whatever content he desired and that these certificates would be trusted by all the most commonly used software products. Since most users trust their software, the chain of trust effectively meant that users trusted an unknown and ill-intended party.

The fact that the chain of trust of PKI had been broken by the intrusion at DigiNotar did not just result in a hypothetical threat, but a rogue certificate was abused in practice to mislead users on a large scale. The following paragraphs detail insights that resulted from Fox-IT's investigation of the breach of DigiNotar as well as of the MITM attack that subsequently took place using the issued rogue certificates.

10.1 Identified rogue certificates

The investigation identified certificates that were issued during the intrusion of DigiNotar's CA servers. Some of these certificates that were issued during this timeframe were intentionally created by DigiNotar and matched the administration in DigiNotar's back office. Certificates that were issued but that were unknown to the back office records generally used very noticeable common names within the certificates. Based on these noticeable names, other certificates were identified and accumulated to a list of 531 rogue certificates. It cannot be ruled out that the rogue certificates that were created during the period within which the intruder was active may also have contained ordinary common names. However, only the certificates with unusual common names could be flagged as rogue and further examined, since the serial numbers of certificates were not logged when they were issued.

When examining the distinguished names (DN) of the 531 certificates that were marked as rogue, only 140 unique distinguished names were encountered. Part of the distinguished names is a common name (CN). Most applications that use certificates only take note of the common name. Of the 531 certificates, only 53 unique common names were found. For example, when looking at the following distinguished names one unique common name can be identified, that is `*.google.com`.

```
CN=*.google.com, SN=google, OU=Knowledge Department, L=US, O=Google Inc, C=US
CN=*.google.com, TITLE=Google, SN=PK0002292001, L=Mountain View, O=Google Inc, C=US
```

The list below shows the common names of the identified certificates that were flagged as rogue, including the number of certificates that were issued using the common name. Of these common names, 46 contained a DNS domain name and the other 7 CNs contained names of Certificates Authorities.

Common name	Number Issued
..com	1
..org	1
*.10million.org	2
*.android.com	1
*.aol.com	1
*.azadegi.com	2
*.balatarin.com	3
*.comodo.com	3
*.digicert.com	2
*.globalsign.com	7
*.google.com	26
*.JanamFadayeRahbar.com	1
*.logmein.com	1

Common name	Number Issued
*.microsoft.com	3
*.mossad.gov.il	2
*.mozilla.org	1
*.RamzShekaneBozorg.com	1
*.SahebeDonyayeDigital.com	1
*.skype.com	22
*.startssl.com	1
*.thawte.com	6
*.torproject.org	14
*.walla.co.il	2
*.windowsupdate.com	3
*.wordpress.com	14
addons.mozilla.org	17

Common name	Number Issued
azadegi.com	16
friends.walla.co.il	8
GlobalSign Root CA	20
login.live.com	17
login.yahoo.com	19
my.screenname.aol.com	1
secure.logmein.com	17
twitter.com	18
wordpress.com	12
www.10million.org	8
www.balatarin.com	16
www.cia.gov	25
www.cybertrust.com	1
www.Equifax.com	1

Common name	Number Issued
www.facebook.com	14
www.globalsign.com	1
www.google.com	12
www.hamdami.com	1
www.mossad.gov.il	5
www.sis.gov.uk	10
www.update.microsoft.com	4
Comodo Root CA	20
CyberTrust Root CA	20
DigiCert Root CA	21
Equifax Root CA	40
Thawte Root CA	45
VeriSign Root CA	21

Some of these common names can be considered a signature from the intruder:

- CN=*.SahebeDonyayeDigital.com, SN=PK000229200006592, OU=Elme Bikaran, L=Tehran, O=Daneshmande Bi nazir, C=IR
- CN=*.RamzShekaneBozorg.com, SN=PK000229200006593, OU=Sare Toro Ham Mishkanam, L=Tehran, O=Hameye Ramzaro Mishkanam, C=IR
- CN=*.JanamFadayeRahbar.com, SN=PK000229200006594, OU=Sarbaze Gomnam, L=Tehran, O=Ke Jano Janan Toyi, C=IR

Reportedly, RamzShekaneBozorg (.com) translates to "great cracker" in Farsi, "Hameyeh Ramzaro Mishkanam" translates to "I will crack all encryption" and "Sare Toro Ham Mishkanam" translates to "I hate/break your head."

Anyone in possession of these rogue certificates could host a website that corresponded with the common name of a rogue certificate and mislead people to trust the website as the original site. By hosting a fraudulent website and redirecting the requests that are made by users to the original website, an attacker can monitor the interaction between the original website and the user without the knowledge of the user. This kind of attack is called a man-in-the-middle (MITM) attack. During the large-scale MITM attack that was perpetrated against primarily Iranian Internet users, the attack was compounded with a form of redirection, where users who tried to reach legitimate websites that were hosted by Google were redirected to fraudulent websites that used a certificate with *.google.com as its common name. The traffic which was meant for Google and that was intercepted was not necessarily forwarded to Google, as users may have been presented with a page specifically intended to phish for their credentials.

10.2 Investigation of OCSP responder log files

There are standards that prescribe how certificates should be created, be formatted, how they can be used, et cetera. All the systems involved in the creation and maintenance of certificates together form a Public Key Infrastructure (PKI). The standards also prescribe that software using certificates must verify the status of the certificate. It must be verified if the certificate that is presented has been revoked. The most commonly used way to do this is by verifying the status online in real time at the issuing Certificate Authority. This is done using the Online Certificate Status Protocol (OCSP). An OCSP responder was present at DigiNotar.

The log files of the OCSP responder were an interesting source for information because, when a rogue certificate was used to mislead users, the software that was utilized by the users verified the validity of the certificate at the OCSP responder. This provided a possibility to detect what rogue certificates were being abused and what IP addresses were affected. Profiling the OCSP responder logs could provide further insight into the MITM attack that was perpetrated using rogue certificates originating from DigiNotar. The question was posed what the greatest common divisors were in the abuse of the rogue certificates in the MITM attack.

A difficulty with this investigation was that an OCSP request that is made to the OCSP responder only consists of a serial number. Additionally, more rogue certificates could have been issued by DigiNotar than that could be identified on the basis of the evidence that could be recovered. These rogue

certificates could have any content and serial number. Therefore, it would not always be possible to determine what the common name or URL of the certificate was for the serial that the user was verifying.

Before August 29, 2011, all the OSCP verification requests of unknown serials resulted in the response of GOOD or UNKNOWN, as this is the standard prescribed response in such a case.

The content of a rogue certificate that was issued by DigiNotar, but which could only be identified as an unknown serial number in a deleted file on the CA server at DigiNotar, became public when a `*.google.com` certificate was posted by a concerned user on a forum.[35] Once the news reached DigiNotar, the serial number was revoked effectively on August 29, 2011 at 19:09:05 (CEST). This certificate became known because of an additional check on the validity of the used certificate that was performed by Google Chrome.

Between August 29, 2011 and September 1, 2011, unknown serials were manually revoked by DigiNotar. On the advice of Fox-IT, a precautionary measure was taken, namely that any serial number query that was presented to the OCSP responder which did not match with the records in the back office of DigiNotar was presumed to be rogue. In such a case, the OCSP responder was set to answer that the serial number had been revoked. This white-list based OCSP response was fully functional on September 1, 2011.

10.2.1 Sources

Log files of the OCSP verification requests from May 1, 2011 at 0:00 to August 30, 2011 at 1:56 were examined. During this period, approximately 27 million requests were made averaging at 300,000 requests per day. This log was enriched with localization fields using GeoIP from MaxMind, making it possible to determine where IP addresses are located.[36] The log files contained the following information:

- Timestamp of the request (in CEST)
- The identifier for the certificate authority receiving the request
- Serial number of the certificate that is being verified (additionally marked normal or rogue)
- IP address of the requesting client, including
    - Its country name and code
    - Its registered Autonomous System (AS) name and number[37]

10.2.2 Yahoo certificate

Fox-IT's investigation showed that remarkable OCSP requests were made for a rogue certificate with the common name `login.yahoo.com`. The first request for this rogue certificate occurred only one hour and 50 minutes after the certificate was presumably generated. Furthermore, the request originated from an IP address that was identified during the investigation of the DigiNotar intrusion (namely AttIP3).

OCSP requests Yahoo certificate	
Serial	`3612f911f611984191fc310e74645d16`
Issuer	Koninklijke Notariele Beroepsorganisatie CA
Common Name	`login.yahoo.com`
Validity	Not before 10-Jul-2011 16:22:26 (UTC) Not after 9-Jul-2013 16:22:26 (UTC)
Revoked	27-Jul-2011 12:01:41 (UTC)
Total usage	10-Jul-2011 20:12:11 to 29-Jul-2011 11:52:40 (CEST) 8 requests from AttIP3 0 status GOOD responses

This led to the assumption that the DigiNotar intruder created the rogue certificate for `login.yahoo.com` and later attempted to verify the status of the certificate.

[35] Google Groups, "Is This MITM Attack to Gmail's SSL?" at http://groups.google.com/a/googleproductforums.com/d/topic/gmail/3J3r2JqFNTw/discussion
[36] Within an reasonable margin of error.
[37] Identifying the registered network operator, usually an Internet Service Provider (ISP).

10.2.3 Google certificate

The serial number of the Google.com certificate that was found by a Gmail user was encountered many times in the OCSP logs. Between the first request and the moment that the certificate was revocated, the OCSP responder had responded to approximately 300,000 unique IP addresses that it was valid.

OCSP requests Google certificate	
Serial	05e2e6a4cd09ea54d665b075fe22a256
Issuer	DigiNotar Public CA 2025
Common Name	*.google.com
Validity	Not before 10-Jul-2011 19:06:30 (UTC) Not after 9-Jul-2013 19:06:30 (UTC)
Revoked	29-Aug-2011 16:58:47 (UTC)
OCSP requests	654.313 status GOOD responses from 298.140 unique IP addresses between 30-Jul-2011 09:11:47 and 2011-08-29 19:09:05 (CEST)

The amount of unique IP addresses that made OCSP requests can only be regarded as a very rough approximation of the amount of users who were affected. Multiple users can be masqueraded behind a single external IP address, while a single user can also make requests from multiple IP addresses. Moreover, relatively old software such as Internet Explorer 6 does not support OCSP requests and these users are not included in the aforementioned number. In conclusion, it can be said that users behind these IP addresses that made OCSP requests were the victims of a MITM attack and were redirected to a fraudulent version of a Google.com website.

When examining OCSP requests, it was noticed that the first three requests were made within one hour on July 30, 2011 from an IP address that was also discovered in the examination of the DigiNotar intrusion (AttIP6). The next requests were made starting August 4, 2011 at 03:05:40 (CEST) and showed a sudden increase and diversity. The other IP addresses found in the DigiNotar intrusion were not encountered to be validating the Google.com certificate.

10.2.4 Unknown serials for verified certificates

While the investigation focused on the rogue wildcard Google certificate, a limited number of OCSP requests for other serial numbers were also identified. Below is a list of OCSP requests for unknown serial numbers for which the OCSP responder answered with "GOOD," indicating that the certificate was valid. The amount of requests for the *.google.com certificate clearly outnumber all other requests.

Serial number[38]	Response	Number of reqs.	First request (CEST)	Last request (CEST)
0B41ABEE6F4168D3CDE5A7D223B58BC1*	GOOD	214	10-Jul-2011 20:34:16	30-Jul-2011 06:28:33
009D06313F21A4EDF734C324FFBCB9E2B5*	GOOD	2	13-Jul-2011 13:19:52	16-Jul-2011 10:11:51
44231633DEE9C328362FADC029C33B	GOOD	63	17-Jul-2011 10:32:45	26-Aug-2011 09:04:51
7C7529653431664F443A3F6C74EB9996	GOOD	231	17-Jul-2011 10:30:16	31-Aug-2011 13:54:17
417EA223198A83712618F185387463	GOOD	16	18-Jul-2011 12:21:48	27-Aug-2011 11:07:15
6AD8A1F4EBD649345320AEC182CFC2	GOOD	10	18-Jul-2011 07:57:34	25-Aug-2011 11:51:04
00E1253D04A17AB8E47F4A5916B9BF9D23*	GOOD	8	23-Jul-2011 10:21:08	30-Jul-2011 09:51:08
7A61A7778842E502E2291166C4574485*	GOOD	1	23-Jul-2011 11:32:03	23-Jul-2011 11:32:03

[38] The serial numbers marked with an asterisk were present in a serial_no.dbh database (see Chapter 6).

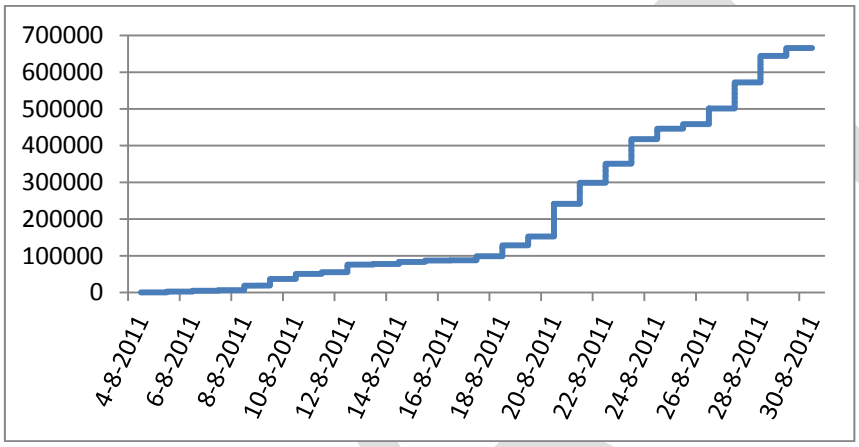
Serial number[38]	Response	Number of reqs.	First request (CEST)	Last request (CEST)
05E2E6A4CD09EA54D665B075FE22A256* (*.google.com)	GOOD	654313	30-Jul-2011 09:11:47	29-Aug-2011 19:09:04

OCSP responses to verification requests of unknown serial numbers

For the other serial numbers in this list, no matching certificate could be found. These unknown serials may have been used for small scale MITM attacks or for testing by the attacker.

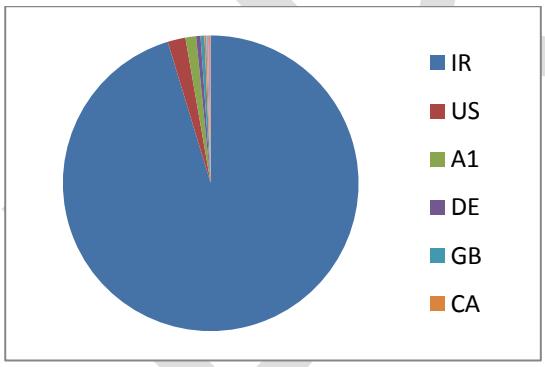
10.2.5 Targets of the MITM attack

The accumulated affected IP addresses were plotted to provide an insight into how the MITM attack developed over time. It was noted that the number of affected IP addresses seemed to have grown fast from August 4, 2011 onwards.

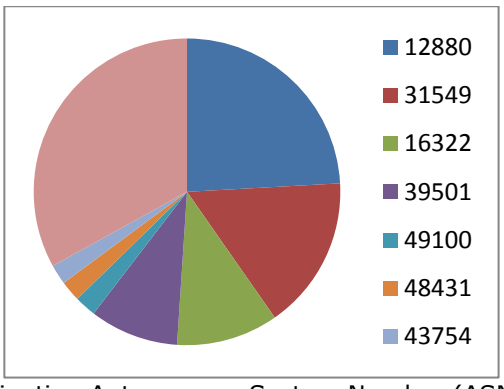


Cumulative number of originating IP addresses

The location information showed that 95% of the OCSP requests for the *.google.com certificate originated from Iran (634,665 out of the 665,974 OCSP requests). A1 in the figure below refers to 'Anonymous Proxy' according to the GeoIP results.



Originating country OCSP requests for the Google.com certificate



Originating Autonomous System Number (ASN) of the requests

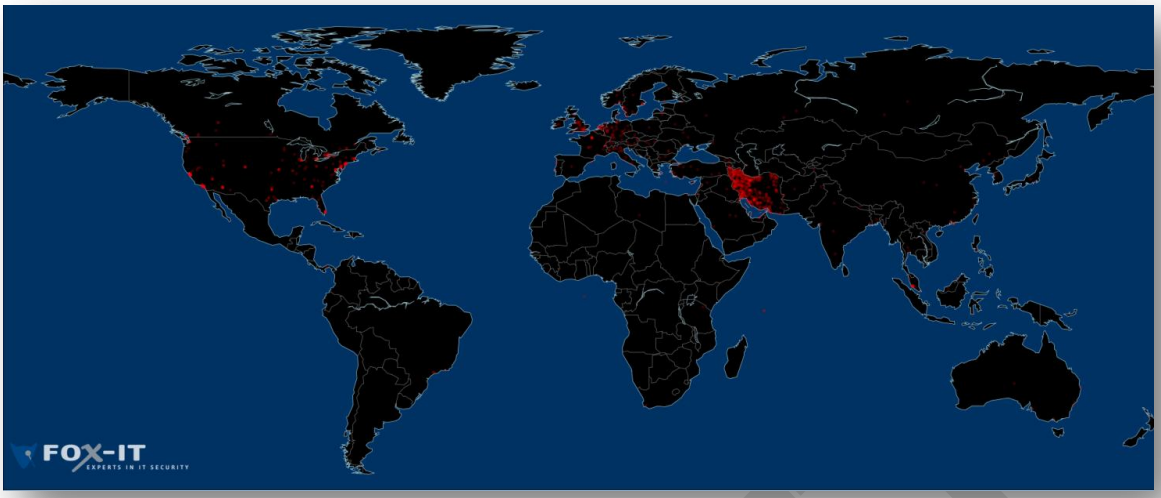


Figure 6 OCSP requests for the rogue `*.google.com` certificate[39]

In total the requests originated from 143 different ASes, while 60% of the requests originated from only 4 Iranian ASes. The spread amongst the other ASes was very broad. The top 7 of rogue requests per Iranian AS are listed below.

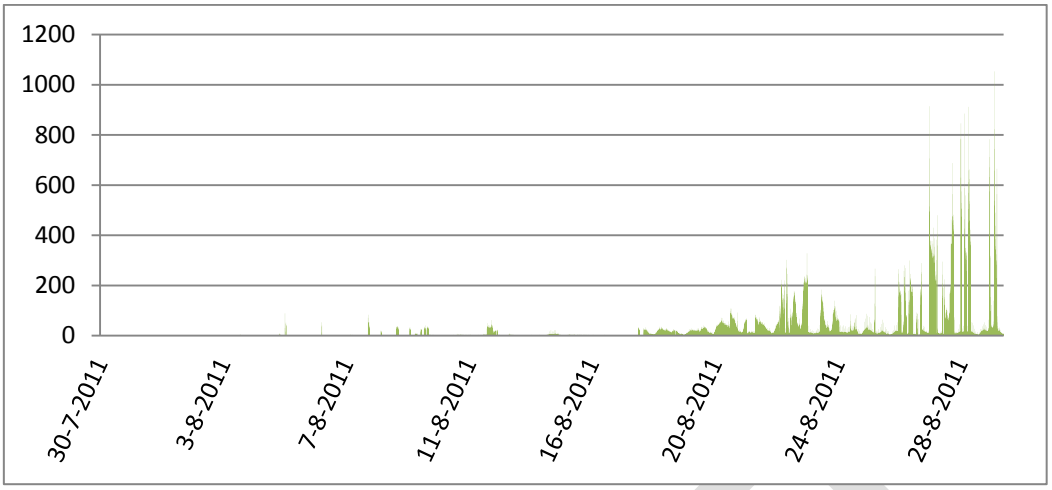
ASN	AS name		Number of requests
AS12880	DCI-AS	Information Technology Company (ITC)	160633
AS31549	RASANA	Aria Rasana Tadbir	107761
AS16322	PARSONLINE	PARSONLINE Autonomous System	71520
AS39501	NGSAS	Neda Gostar Saba Data Transfer Company Private Joint	62492
AS49100	IR-THR-PTE	Pishgaman Tose Ertebatat	15110
AS48431	MAXNET-AS	Bozorg Net-e Aria	14652
AS43754	ASIATECH-AS	AsiaTech Inc.	13998

The identification of 5% of the IP addresses outside of the Islamic Republic of Iran could partially have been caused by the inaccuracies of the GeoIP location information that was used. A sample of the IPs located outside of the Islamic Republic of Iran was inspected. Mainly Tor-exit nodes, proxies and VPN servers were identified. On this basis, it can be concluded that the MITM attacks were specifically and almost exclusively targeted at users that were located in the Islamic Republic of Iran.

10.2.6 Modus operandi for the MITM attack

In order to perpetrate a MITM attack in which SSL is used, traffic must be rerouted from the browser of the legitimate website to a fraudulent website, in addition to presenting a certificate that can be validated. Three modi operandi can be identified that could plausibly have been used to redirect users from the legitimate to the fraudulent version of a specific website.

[39] This static image shows all the IP addresses that were detected. A video at http://www.youtube.com/watch?v=wZsWoSxxwVY shows a timeline of the MITM attack on Google users taking place.



Number of requests per minute

One way in which users can be redirected to a fraudulent website is using a "transparent" MITM attack. Such an attack relies on the fact that one has access to a system that handles the traffic upstream, where specialized hardware can be used to distinguish between traffic or to perform a MITM attack on SSL for a specific domain. A press statement regarding Tor[40] suggests that Deep Packet Inspection (DPI) Intrusion Prevention Systems (IPS) are used for censorship purposes and implies that specialized hardware may be in place within the Iranian Internet infrastructure, that could provide such functionality.

However, approximately 6000 IP addresses were identified that originated outside of the Islamic Republic of Iran that correspond mainly with dedicated proxies, Tor and VPN exit nodes. Connections to these servers occur over secured lines and should remain unaffected by a "transparent" MITM attack. While rogue certificates were issued for Tor during the intrusion in DigiNotar's network, it is highly unlikely that rogue certificates could have been used to reroute traffic that went through all the identified foreign VPNs. Furthermore, the peak-like behavior that could be identified in the OCSP requests for rogue certificates does not correspond with a "transparent" MITM attack.

Another way in which traffic may be redirected is by making changes directly in a DNS server that is operated at a high level of the infrastructure. Even if services such as Tor or VPN are used, DNS queries will by default be made to the local DNS server. Therefore, a modus operandi where DNS was abused to redirect traffic could accommodate for the fact that traffic that went through proxies, Tor or VPN was also redirected. However, the hypothesis that changes were made directly to a DNS server that operated at a high level in the infrastructure does not correspond with the peak-like behavior that was identified in the amount of OCSP requests for rogue certificates. If traffic had been redirected in this way, one would expect that the amount of OCSP requests would have grown during the attack without the occurrence of repeated and sudden declines.

The most likely modus operandi to have been used during the MITM attack, based on the accumulated OCSP data, is that of DNS cache poisoning. A DNS cache poisoning attack relies on the fact that DNS servers cache the response of DNS servers at a higher level in the infrastructure. By flooding a DNS server with forged responses for a particular domain, as if it had received the response from a higher DNS server, it is possible to "poison" the entries in the DNS server and thus its responses to clients at a lower level in the infrastructure. The poisoned entries are valid for as long as the Time To Live (TTL) allows, after which these entries expire and another DNS request would be made to a higher DNS server for the domain if it is requested by a client. This methodology would explain why traffic that went through proxies, Tor and VPN was also affected by the MITM attack and also corresponds with the peak-like behavior and the occurrence of repeated and sudden declines in OCSP requests for rogue certificates.

[40] Tor project blog, "Iran blocks Tor; Tor releases same-day fix" at http://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix

10.3 Conclusion

Most of the identified rogue certificates contain a DNS domain name in the common name, indicating that they were intended to be used for a website. From 1 September 2011 onwards, all OCSP requests for unknown certificate serial numbers were answered as if they had been revoked. Before this date, all requests for unknown serial numbers were answered by the OCSP responder as if the corresponding certificates were valid. This was the prescribed standard response for an OCSP responder to unknown serial numbers.

The OCSP request logs showed that one serial that was used in a certificate for the URL `*.google.com` was abused on a massive scale in a MITM attack on the people of the Islamic Republic of Iran. This conclusion was supported by the fact that 95% of OCSP requests for the abused certificate originated from the Islamic Republic of Iran and that the remaining 5% of the requests originated from systems that were generally used as a proxy, VPN or Tor exit node.

The number of unique IP addresses that made OCSP requests for the rogue certificate was still growing when the certificate was revoked. The attack had covered 143 Iranian ASes (often ISPs) and 298,140 unique IP addresses. The amount of IP addresses was only a very rough approximation for the amount of affected users, as users may share an IP address, use multiple IP addresses or use software that does not support OCSP requests.

The broad scope of 143 ASNs and 298,140 unique IP addresses does not reveal a well-defined, narrow target. The maximum coverage of the attack's unique IP addresses may have been intentional. Without detailed knowledge about the Iranian infrastructure, it is impossible to conclusively determine how the MITM attack was perpetrated, but the OCSP data implies that DNS cache poisoning is the most likely modus operandi to have been used.

In addition to the rogue `*.google.com` certificate, validation requests were made for serial numbers that correspond with known rogue certificates as well as for unknown serial numbers. Initially these requests were answered by the OCSP responder as if they were valid. This makes it plausible that other rogue and unknown certificates may have been used for other MITM attacks on a much smaller scale. An attempt was made to verify a certificate with the common name `login.yahoo.com` by AttIP3, an IP address that had previously been identified in the context of the investigation of the DigiNotar intrusion.

10.3.1 Consequences

A large number of citizens of the Islamic Republic of Iran became victims of a MITM attack. All services of Google.com could have been the object of attack. Most likely the confidentiality of Gmail accounts was compromised and their credentials, the login cookie and the contents of their e-mails could have been intercepted. Using the credentials or the login cookie, an attacker may be able to log in directly to the Gmail mailbox of the victim and read their stored e-mails. Additionally, the MITM attacker may have been able to log into all other services that Google offers to users, such as stored location information from Latitude or documents in GoogleDocs. Once an attacker is able to receive his targets' e-mails, he is also able to reset passwords of others services such as Facebook and Twitter using the lost password functionality.

10.3.2 Timeline of the MITM attack

Date	Notes
27-Jul-2011	First OCSP request at DigiNotar for the rogue wildcard Google certificate.
28-Jul-2011	DigiNotar found evidence that attempts were made to verify the rogue `login.yahoo.com` certificate by IP addresses originating from the Islamic Republic of Iran.
04-Aug-2011	The beginning of massive activity on the OCSP responder for a rogue `*.google.com` certificate originating from the Islamic Republic of Iran.
28-Aug-2011	On the Google support forums, a customer of the Iranian ISP ParsOnline posted details about a certificate warning that was presented to him by Google Chrome for a rogue `*.google.com` certificate.

Date	Notes
29-Aug-2011	Google received multiple reports in regard to an attempted SSL MITM attack and articles about a rogue `*.google.com` certificate appeared on the blogs of, among others, Mozilla, Google and Microsoft. On the same day, the rogue `*.google.com` certificate was revoked. Additionally, GOVCERT.NL was notified by Cert-Bund.
30-Aug-2011	Fox-IT was asked by DigiNotar to initiate an investigation into the intrusion of DigiNotar and placed an incident response sensor in the network of DigiNotar.
31-Aug-2011	Google Chrome blacklisted a list of known rogue serial numbers.
01-Sep-2011	The behavior of the OCSP responder was changed to function based on a white list, effectively revoking all unknown serial numbers and therefore all remaining rogue certificates.

11 Lessons learned

Fox-IT was specifically asked by the ministry BZK to address the lessons that can be learned from an incident such as the intrusion of DigiNotar's network. The described lessons that can be learned from such an incident do not necessarily imply that DigiNotar failed to implement the following measures.

Average users and businesses will have a very limited capacity to protect themselves properly against attacks such as those against Trusted Third Parties in the Public Key Infrastructure. In general, the best way for average users to protect themselves on public networks is to keep their software up to date, to use an antivirus product and to be wary of content from untrusted sources. The MITM attack on users that was perpetrated in the aftermath of the intrusion of DigiNotar's network was only detected by Google when users of the Google Chrome browser reported abnormal behaviour while using Google services.

Since users have a very limited ability to protect themselves from attacks that abuse the Public Key Infrastructure, they need to be able to trust the security of all the parties that make up the Public Key Infrastructure in order for the system as a whole to operate securely. Given the impact that a breach in the security of a Certificate Authority has on the Public Key Infrastructure as a whole and the Internet in general, ensuring the security of every Certificate Authority is paramount to the trust in PKI and its role in providing security for a diverse range of activities on the Internet. While the approach to protecting the potential targets from this type of intrusion does not differ significantly from other threats, the range of scenarios that need to be taken into account is rapidly expanding.

More generally users and businesses including Certificate Service Providers (CSPs) can protect themselves against a wide range of security threats. Various security books, articles, courses and standards can provide detailed information about taking appropriate security measures. In addition to implementing a formal information security management system (such as ISO-27001), we would like to note a number of basic practical requirements for critical environments such as those on which CSPs rely.

As with any organization, it is important for CSPs to complement prevention with detection. There is no such thing as an absolute guarantee that preventive measures will be sufficient to prevent an attack. When complemented with measures aimed at the detection of attempts to intrude a secured infrastructure however, it is possible minimize the chances of a successful intrusion. Furthermore, detection can prevent that critical parts of the infrastructure can be targeted, even in the case of a breach of a specific segment.

It is also important to enforce a strict separation in the tasks with competing aims that employees perform, insofar as these tasks may affect the security of the organization or its infrastructure. For example, a person that is responsible for system administration should not be the same person that sets up and maintains the firewall or other security components of the infrastructure. A system administrator may aim to provide users with a pleasant working environment, while the operator of a firewall will aim to create an optimally secure setup of the firewall and the interaction between the segments that it segregates and regulates. The framework within which the operator of the firewall performs his tasks should be defined by a security officer, who is specifically tasked with defining and enforcing a security policy tailored to your organization.

Additional measures, point by point:

- Air gap vital systems as much as possible, to make sure that they are physically separated on a network level from untrusted networks such as the Internet.
- Update all software products on all systems with the latest patches as often as possible. Subscribe to relevant mailing lists or use dedicated patch management software to support this process.
- Harden all systems. Do not rely on default settings. Make sure that the most critical systems are only being used for the critical processes that they are intended for. By limiting the amount of services on any given system, the attack surface for an attacker is limited.
- Regularly have the security of your infrastructure and systems therein tested by penetration testers. Do not always use the same team to perform penetration tests.
- Monitor your systems and network and make sure that anomalies trigger notifications to the appropriate employee(s).

- Use data that can be accumulated by the OCSP responder to check if unknown serials are being validated.
- Separate vital logging services from the systems that perform other vital functions. In an infrastructure where secure logging is vital, a logging server can be placed behind a unidirectional security gateway.
- Ensure forensic readiness so that, for example, all events that are relevant for an incident response team are logged, that events from multiple systems can be correlated, that a balance is found in advance between business continuity and potential evidence gathering, that roles and reporting structures are defined for and communicated to all employees and external parties that take part in incident response before an incident takes place and that a feedback loop is created to learn from incidents in the past.

12 Potential follow-up investigation

The scope and goal of the investigation regarding the intrusion at DigiNotar that was performed by Fox-IT changed over time. At first, the focus was on controlling the incident by mitigating the intrusion and regaining trust in the systems. Later the focus changed to identifying evidence that could lead to the location and identity of the intruder and safeguarding evidence. As time progressed, the need for detailed information about the intrusion and its aftermath diminished for the main stakeholder, the ministry BZK, who commissioned the continued investigation. Therefore, not all questions were answered and a number of traces were not fully investigated. Consequently, the information that was uncovered during the investigation can be used as the basis for further research in regard to several additional questions.

12.1 Intruder's steps

As the results of the investigation presented in the previous chapters show, some steps made by the intruder in his path through the network were not detailed. More specifically, some questions remain unanswered, such as:

- Were the database credentials on the BAPI-db discovered by the intruder in the `web.config`?
- How did the intruder gain access to the Secure-net? Examination of the BAPI production workstation may provide a conclusive answer to this.
- What was the exact behavior of the CA management software?
    - How were log and database files of the CA management software normally created, were log files manipulated and if so in what way?
    - Are vulnerabilities present in the software and were they abused by the intruder?
- What information was stored in the CAP database? Were private keys or passwords stored in this database?

12.2 Network infrastructure

Paragraph 3.3 describes the normal operation of the network segments and firewall based on interviews with the administrators. The exact firewall rules have not been examined to confirm their statements in this regard.

12.3 Investigation of CA servers

Chapter 6 contains the results of the investigations of the CA servers. Additionally, more research is possible into the following questions:

- The exact behavior of the used CA management software could be analyzed.
    - Did the intruder use the option in the CA software to perform a complete backup of the databases? What traces did this leave on the system?
    - What extensions were installed that provided functionality that could have aided the intruder in issuing rogue certificates?
    - Further investigation could be performed to explain the duplicate certificates that were found in the database files.
    - Was the CA software and netHSM setup able to startup unattended? Was it possible to restart CA servers or services and activate private keys on the netHSM? What configuration options are there for an unattended setup? Were attempts made by the intruder to change these settings?
    - Can the CA management software detect deleted log files? Is it possible to establish with absolute certainty if log files may have been tampered with?
    - Why could private keys found in `id2entry.dbh` not be matched with the certificates extracted from the databases?
- The CA web server log files (`enrol-cipher.log`) of the Public-CA server could contain interesting entries outside office hours that could be examined further.
- The CA servers could be searched for any further remains of deleted (log) files.
- How were the private keys in the netHSM activated exactly? Was it possible to activate more than one key with a smartcard?
- Were the certificates of the keys used in the netHSM in the internal DMZ for the *Parelsnoer* service on the trust lists of operating systems? The servers that hosted the *Parelsnoer* service were not investigated. If their certificates or root certificates were also on trust lists, it would be interesting to determine if these servers were utilized by the intruder.

12.4 Systems

Chapter 7 contains the results of the investigations of systems access and tools. Additionally, the following questions could be researched:

- The CA servers, netHSM, firewall and other equipment at the co-location were not investigated thoroughly, which could provide additional results. Some suspicious connections have been identified as originating from one of the co-located servers.
- The system event logs of most of the servers were exported and retained. This was done in August 2011. The log files of some of these systems have not been examined.
- Further research is possible on the extensive firewall logs including their integrity.
- The backup tapes could be investigated for traces of the intrusion and may contain deleted tools.
- Some of the servers in the DMZ-ext-net were not investigated, namely those that were used for various services that DigiNotar provided. Investigating these servers might provide insights regarding potential misuse of these DigiNotar services.
- Examination of all executables that were transported through the stepping stones might reveal additional insights on the methods used by the intruder.

12.5 Aftermath

Chapter 10 contains the results of the investigation of the large-scale MITM attack where one of the rogue certificates was abused. Additionally, the following questions could be researched:

- The OCSP data could be used to examine the limited set of IP addresses outside of the Islamic Republic of Iran that were targeted in the MITM attack further, to determine if they can all be identified as proxies, Tor-exit nodes and VPN providers.
- If additional data from Google could be obtained, it would be possible to determine if login data that could have been obtained during the MITM attack was abused in practice.
- Data regarding OCSP requests for valid certificates from other Certificate Authorities could be used to determine if a "round robin" algorithm was used and thus provide more information about the capabilities of the attacker and the infrastructure that was used.
- Zooming in on the targets and the underlying infrastructure in the Islamic Republic of Iran could reveal information about the identity and aim of the MITM attacker.
- The CRL requests could be examined to reveal additional abuse of rogue certificates.

13 Terminology

Term	Meaning
AS	Autonomous System
ASN	Within the Internet, an Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet. A unique AS Number (ASN) is allocated to each AS for use in (Border Gateway Patrol) routing.
ASN.1	Abstract System Notation One is a standard for the notation of data in networking.
ASPX	Web pages that are based on the ASP.NET web application framework by Microsoft.
BAPI	Belastingdienst Advanced Program Integration (Dutch tax administration)
CA	Certificate Authority, an issuer of certificates.
CAP	Control Application for the back office administration.
Certificate	A digital file used among others to authenticate a website and to encrypt network traffic. The validity of a certificate is generally verified with the issuer (CA).
CEST	Central European Summer Time (UTC+2).
CN	Common Name of a certificate.
CRL	Certificate Revocation List.
CSP	Certificate Service Provider.
CSR	Certificate Signing Request.
DARPI	DigiNotar "Abonnementen Registratie" (Subscription Registration) Production Interface.
DER	Distinguished Encoding Rules is a standard that is used to encode an ASN.1 value.
DMZ	Demilitarized Zone. Its purpose it to add an additional layer of security to an organization's local area network.
DN	Distinguished Name of a certificate.
DNS	Domain Name System is a hierarchical distributed naming system for systems connected to a network that translates domain names to IP addresses.
GET	A GET request is a HTTP request to receive a file that is specified using an URL.
HTM/HTML	HyperText Markup Language is a standard and file format that is used for web pages.
HTTPS	HyperText Transfer Protocol Secure is a combination of HTTP with SSL/TLS.
ISP	Internet Service Provider.
IPS	Intrusion Prevention System.
IP	Internet Protocol. An IP address is used to identify a specific system within a network.
MD5	Message Digest algorithm is a cryptographic hash function that can be used to check data integrity.
MITM	Man-in-the-Middle. In this type of attack an attacker places himself between two parties in order to intercept the traffic that occurs between these parties.
Mscache	A hash for cached credentials for user on a Windows domain.
MSSQL	Microsoft SQL Server is a database management system that was developed by Microsoft.
netHSM	Hardware security module that is accessible over the network that contains private keys.
OCSP	Online Certificate Status Protocol, a protocol that is used to obtain the revocation status of certificates as described in RFC 2560.
PEM	Privacy Enhanced Mail is a proposed standard for securing e-mail using public key cryptography.
PIN mailer	Sends a Personal Identification Number.
PKI	Public Key Infrastructure.
Port	A 16 bit number that is used to refer to a communications endpoint.
RDP	Remote Desktop Protocol is a proprietary protocol by Microsoft to provide a user with a graphical interface to another computer.
RFC	Request For Comments describe the specifications, protocols, procedures and events that are related to the Internet and Internet-connected systems.
SMTP	Simple Mail Transfer Protocol is used to send e-mail across IP networks.
SSL	Secure Sockets Layer and the subsequent Transport Layer Security are cryptographic protocols to provide secure communication of a public telecommunication network.
SVO	Evidentiary item ("Stuk Van Overtuiging").
Tor	The onion router. Initiative of the Tor project. Intended to enable online anonymity.
TTP	Trusted Third Party.
Tunnel	An Internet Protocol communications channel between systems.

Term	Meaning
UTC	Coordinated Universal Time.
VPN	Virtual Private Networks are used to secure data that is transferred over a public telecommunication infrastructure.
XUDA	Xcert Universal Database API.

Appendix I: References to equipment

The servers, workstations and network equipment referenced in this report are listed in the following table. The names used in this report are characteristic of each item's usage. For cross reference, the server ID used by DigiNotar and the related exhibit number are included in table. Also, the IP address and network segment are shown.

When a server is referenced in the report and it has more than one IP address assigned to it, the specific IP address is included in the reference. If no IP address is included in the reference, the bold-marked IP address at the top of the line entry applies.

Name[41]	Server Id[42]	SVO number[43]	IP-address	Network segment	Remarks
CA servers					
Root-CA	winsvr167	SVO1	172.18.20.247	Secure-net	
Qualified-CA	winsvr022	SVO2	172.18.20.249	Secure-net	
CCV-CA	winsvr057	SVO3	172.18.20.246	Secure-net	
Nova-CA	winsvr021	SVO4	172.18.20.252	Secure-net	Also called 'Orde-CA'.
Taxi-CA	winsvr053	SVO5	172.18.20.251	Secure-net	
Test-CA	winsvr054	SVO7	172.18.20.250	Secure-net	
Relation-CA	winsvr055	SVO12 DD.055	172.18.20.244	Secure-net	
Public-CA	winsvr056	SVO13 DD.056	172.18.20.245	Secure-net	
DNTest-CA	winvm012	SVO149	10.10.240.39	Test-net	
DNAcceptance-CA	winvm032	SVO114	10.10.230.39	Acceptance-net	
Public-CA-Colo	winsvruw07	SVO342	172.27.20.19	Secure-colo-net	
Qualified-CA-Colo	winsvruw08	n/a	172.27.20.20	Secure-colo-net	
Relation-CA-Colo	winsvruw09	SVO325	172.27.20.17	Secure-colo-net	
Root-CA-Colo	winsvruw10	n/a	172.27.20.15	Secure-colo-net	
Nova-CA-Colo	winsvruw11	n/a	172.27.20.16	Secure-colo-net	Also called 'Orde-CA'.
CCV-CA-Colo	winsvruw18	n/a	172.27.20.23	Secure-colo-net	
Taxi-CA-Colo	winsvruw19	n/a	172.27.20.26	Secure-colo-net	
netHSMs					
NetHSM-CAs	dnhsm01	n/a	172.18.20.254	Secure-net	
NetHSM-web	dnhsm02	n/a	10.10.200.254	DMZ-int-net	
NetHSM-test	dnhsm04	n/a	10.10.240.254	Test-net	Also called "Stichting continuïteit hsm"
NetHSM-CAs-Colo	dnhsmuw01	n/a	172.27.20.254	Secure-colo-net	
HSM-connector	winvm024	SVO179 SVO180	10.10.240.35	Test-net	
Web servers					
Main-web	winsvr101	SVO8	**10.10.20.41** 10.10.20.11 10.10.20.14 10.10.20.28 10.10.20.46 10.10.20.58 10.10.20.61 10.10.20.69 10.10.20.73 10.10.20.97	DMZ-ext-net	
Docproof2	winsvr119	DD.119 SVO328	10.10.20.65	DMZ-ext-net	
Docproof1	winsvr118	SVO11	10.10.20.37	DMZ-ext-net	

[41] Server name as it is used in this report.
[42] Server Id as it is used by DigiNotar.
[43] This is an internal code for a piece of evidence (such as a disk image).

Name[41]	Server Id[42]	SVO number[43]	IP-address	Network segment	Remarks
Pass-web	winsvr108	SVO35 SVO36	**10.10.20.16** 10.10.20.40 10.10.20.35 143.177.11.3 143.177.11.12	DMZ-ext-net	Hosting the website auth.pass.nl
Soap-signing	Winsvr109	SVO46	10.10.20.98 10.10.20.129 10.10.20.42 10.10.20.92 10.10.20.84 10.10.20.85 10.10.20.86 10.10.20.137 10.10.20.87 10.10.20.88 10.10.20.89 10.10.20.130 10.10.20.90 10.10.20.91 10.10.20.99 10.10.20.93	DMZ-ext-net	
Main-web-new	winvm045	SVO55 SVO56 SVO57	**10.10.20.158** 10.10.20.172 10.10.20.164 10.10.20.165 10.10.20.182 10.10.20.173 10.10.20.167 10.10.20.174 10.10.20.169 10.10.20.183 10.10.20.175 10.10.20.184 10.10.20.181 10.10.20.176	DMZ-ext-net	Main-web was replaced by WINVM045. The first firewall entries of 10.10.20.158 from WINVM045 appeared on 18-Jul-2011. See also chapter 4.
Other in DMZ					
eHerkenning-AD	winsvr155	SVO51	**10.10.20.134** 62.58.44.101	DMZ-ext-net	
eHerkenning-HM	winsvr157	SVO28 SVO29 SVO31	**10.10.20.139** 143.177.3.40	DMZ-ext-net	
Docproof-db	Winsvr066	SVO312 SVO313 SVO314	10.10.200.20	DMZ-int-net	
Production-notification	winsvr009	SVO34	**10.10.200.18** 62.58.44.120	DMZ-int-net	
Workstations					
Production121	digiws121	SVO371	172.17.20.59	Office-net	
BAPI-production	digiws146	n/a	172.18.20.230	Secure-net	
Develop182	digiws182	n/a	172.17.20.114	Office-net	
AdminWS164	digiws164	SVO10	10.10.210.32	Admin-net	
Other					
BAPI-db	winsvr007	SVO75 SVO76	172.17.20.4	Office-net	Internally called Bapi Database New.
Source-build	winsvr003	SVO374	172.17.20.25	Office-net	
Source-build-new	winsvr010	SVO100	172.17.20.21	Office-net	
Office-file	winsvr065	SVO77 SVO78	172.17.20.8	Office-net	
Exchange-mail	winsvr126	SVO21 SVO22 SVO95	172.17.20.5	Office-net	Exchange mail server.

Name[41]	Server Id[42]	SVO number[43]	IP-address	Network segment	Remarks
CAP-app-web	winsvr130	SVO317	172.18.20.10	Secure-net	Part of the CAP application (Control Application)
CAP-app-db	winsvr131	SVO321 SVO322 SVO323	172.18.20.11	Secure-net	Part of the CAP application (Control Application)
CAP-web	winsvr125	SVO340 SVO341	172.18.20.12	Secure-net	Part of the CAP application (Control Application)
CAP-CCDB	winvm048	SVO225 SVO226	10.10.240.25	Test-net	
Admin-DNS	winsvruw05	n/a	**172.27.20.21** 193.173.36.37	Secure-colo-net	
AntiVirus	winsvr008	SVO14 SVO26	10.10.210.14	Admin-net	
Network equipment					
Load-balancer-1	dnlb01	n/a	10.10.20.8	DMZ-ext-net	
Load-balancer-2	dnlb02	n/a	10.10.20.9	DMZ-ext-net	
Squid-proxy	dlx001	SVO283	172.17.20.7	Office-net	
Syslog	dlx131	SVO288 SVO289	10.10.210.35	Admin-net	
Cluster addresses					
Cluster-prodpass		n/a	**10.10.20.18** 62.58.44.107	DMZ-ext-net	Cluster production Pass

Appendix II: List of suspected intruders IP-addresses

The IP addresses that were found leading to the location or identification of the intruder are not included in this report due to the ongoing investigation. These IP addresses are referred to as *AttIP* in this report.

Reference	Country	Source	Remark
AttIP1	United Kingdom	Malware on Docproof2	`troj65.exe` was probably used for tunneling RDP.
		Firewall logs	Successful connections initiated from DMZ-ext-net (tunnels). Blocked attempts from Secure-net.
AttIP2	United Kingdom	Malware on Docproof2	`95.exe`
		Other	Server was confiscated by the Dutch police (KLPD).
		Firewall logs	Successful connections initiated from DMZ-ext-net.
AttIP3	Islamic Republic of Iran	Access to /beurs on Main-web	Probably revealed by error in proxy chain (see paragraph 4.3.4).
		OCSP log	OCSP request test run for a rogue `login.yahoo.com` certificate. Resolved to an DSL user in Iran.
		Other	Made connections to server running at AttIP2.
AttIP4	Netherlands	Access to /beurs on Main-web	Suspicious. Much activity.
AttIP5	Russian Federation	Access to /beurs on Main-web	Suspicious. Much activity.
		Other	Server was confiscated by the Dutch police (KLPD).
		Other	Made connections to server running at AttIP2.
AttIP6	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. One log entry for a post to `settings.aspx`.
		OCSP log	First 3 requests of the `*.google.com` certificate used in the MITM attack.
AttIP7	United States	Access to /beurs on Main-web	Suspicious. One log entry for a post to `settings.aspx`.
AttIP8	United States	Access to /beurs on Main-web	Suspicious. Many file downloads.
AttIP9	Germany	Access to /beurs on Main-web	Suspicious. Downloaded some files.
AttIP10	United States	IIS logs on Docproof2	Unknown.
AttIP11	United States	Access to /beurs on Main-web	Suspicious. One file downloaded.
AttIP12	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. Many file downloads.
AttIP13	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. Many file downloads.
		Firewall logs	Dropped connections initiated from DMZ-ext-net.
AttIP14	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. Downloaded files.
AttIP15	Germany	Access to /beurs on Main-web	Suspicious.
AttIP16	United States	Access to /beurs on Main-web	Suspicious. Downloaded a file.

Reference	Country	Source	Remark
AttIP17	Islamic Republic of Iran	Access to /beurs on Main-web	Suspicious. Downloaded the file `jobsdone.zip`.
AttIP18	Australia	Access to /beurs on Main-web	Suspicious. Posts and gets to `settings.aspx`. Downloaded the file `jobsdone.zip`.
AttIP19	United States	Access to /beurs on Main-web	Suspicious. Downloaded files.
		Firewall logs	Successful connections initiated from DMZ-ext-net.
AttIP20	Israel	Access to /beurs on Main-web	Suspicious. Uses `settings.aspx` very often.
AttIP21	United States	Access to /beurs on Main-web	Suspicious. Downloaded files.
AttIP22	United Kingdom	Access to /beurs on Main-web	Suspicious. Downloaded files.
		Firewall logs	Successful connections initiated from internal IPs.
AttIP23	Finland	Access to /beurs on Main-web	Suspicious. Posts and gets to `settings.aspx`.
N/A	United States	Access to /beurs on Main-web	Not suspicious. Gets `default.aspx`. IP resolves to Googlebot web crawler.
N/A	Netherlands	Access to /beurs on Main-web	Not suspicious. Probably used for internal incident response activities, since it was only seen on July 27, 2011.
N/A	Belgium	Access to /beurs on Main-web	Not suspicious. Probably used for internal incident response activities, since it was only seen on July 24, 2011.
N/A	Belgium	Access to /beurs on Main-web	Not suspicious. Probably used for internal incident response activities, since it was only seen on July 23, 2011.
N/A	Netherlands	Access to /beurs on Main-web	Not suspicious. Probably used for internal incident response activities, since it was only seen on July 28, 2011.

The IP addresses AttIP3, AttIP6, AttIP12, AttIP13 and AttIP14 are in a close range together and share the same class A network (/24).

Appendix III: Timeline of noteworthy traffic

This appendix shows the timeline of noticeable traffic as it was found when examining the firewall logs.

Time start	Time end	Notes	Source server	Destination server	Destination port
2011-06-17					
13:06:57	13:07:00	RDP attempts[44] from office net to admin net	Develop182	AntiVirus	3389
2011-06-28					
14:24:42	14:24:51	Port 139/ 445 attempts[45] from secure to colo-secure net	Taxi-CA	Admin-DNS	139/445
2011-06-29					
11:56:15	11:56:24	RDP attempts from DMZ ext to Office net	Main-web	Source-build	3389
13:13:33	13:14:40	Network discovery from DMZ ext to Test net	Main-web	HSM-connector 10.10.240.48	80,137
13:17:42	13:18:45	Network discovery from DMZ ext to DMZ int	Main-web	NetHSM-web	80,137, 443
13:20:52	13:21:05	Network discovery from DMZ ext to secure net	Main-web	NetHSM-CAs	137, 443
13:21:38	13:21:54	Network discovery from DMZ ext to Colo-Secure net	Main-web	NetHSM-CAs-Colo	137, 443
13:22:26	13:22:40	Network discovery from DMZ ext to Test net	Main-web	NetHSM-test	137, 443
13:26:06	13:26:23	Connection attempts from Office to Secure net	BAPI-db	CAP-app-web	80, 3389
13:26:22	13:26:35	Network discovery from DMZ ext to Secure	Main-web	CAP-app-web	80, 137
13:27:14	13:29:25	Connection attempts from Office to Secure net	BAPI-db	CAP-app-web CAP-app-db	21, 1433, 135, 137
13:29:39	13:29:52	Network discovery from DMZ ext to Secure net	Main-web	CAP-app-db	137, 1433
13:29:50	13:30:03	Connection attempts from Office to Secure net	BAPI-db	CAP-app-db	80, 137
13:31:06	13:31:19	Network discovery from DMZ ext to Test net	Main-web	CAP-CCDB	80, 137
13:33:32	13:34:08	Network discovery from DMZ ext to DMZ old	Main-web	10.10.0.12	80, 137, 443
13:40:40	13:40:44	Connection attempts from DMZ ext to Office	Main-web	172.17.20.164	137, 443
15:11:13	15:11:25		Office-file	BAPI-production	139->4461
2011-06-30					
00:08:21	00:08:24	Some more attempts	eHerkenning-AD	BAPI-db	137
00:16:34		Connect back home	eHerkenning-AD	AttIP2	443
00:36:46	00:41:37	Connection attempts from DMZ-ext-net to Office-net	Main-web	BAPI-db	21, 80, 137
02:22:26	02:22:35	Failed RDP attempts	BAPI-db	CAP-app-web	3389
02:22:56	02:23:38	Successful HTTP/HTTPS connections	BAPI-db Squid-proxy	CAP-app-web	80, 443
02:24:18	02:24:19	Connect back from Office db server to drop server @DMZ	BAPI-db	eHerkenning-AD	443
02:25:10	02:26:59	Failed RDP/SQL attempts from the Office net	Source-build BAPI-db	CAP-app-web CAP-app-db	80, 137, 1433, 3389
02:28:31	02:28:40		eHerkenning-AD	CAP-CCDB	443
10:39:59	10:40:29	Failed attempts	Pass-web	BAPI-db	139, 445, 1433
13:22:05	13:22:15	FTP from the DMZ (could be legal activity)	Main-web (10.10.20.46)	Source-build-new	21
23:54:04	23:56:36	Unknown dropped activity.	Office-file:139	BAPI-production	
2011-07-01					

[44] Probably not relevant for this attack.
[45] Probably not relevant for this attack since no traces on Taxi-CA server were found before 01-Jul-2011.

Time start	Time end	Notes	Source server	Destination server	Destination port
01:15:30	01:15:38[46]	Dropped activity from another host.	172.17.20.22:139	BAPI-production	2400
01:16:15	01:17:16	Port scan on local segment.[47]	BAPI-production	Firewall (172.18.20.2)	
01:17:22	01:19:49	Connect back attempts to the admin-net.	172.17.20.59 BAPI-production	AntiVirus	80, 139, 445
01:23:52	01:24:46		BAPI-db:139	BAPI-production	
18:00:56	18:02:26	Failed attempts.	BAPI-db	172.18.20.239	135, 319, 389
20:23:52	20:24:05	And again sometime later.	BAPI-db	Taxi-CA	80,137
21:21:54	21:22:24		BAPI-db:139	BAPI-production	
22:52:47	23:40:45	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
2011-07-02					
00:14:14	00:47:07	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
01:48:42	01:48:42	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
02:10:01	02:10:01	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
02:10:01		First occurrence of many SMTP connections.	CAP-app-web	172.17.20.5	25
02:18:36	02:18:36	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
02:26:54	02:27:02	Strange port combinations	Admin-DNS:445	CAP-app-web:1433	
03:36:15	03:44:19	Unsuccessful connections to public stepping stone.	Root-CA [ICMP]	AttIP1	8/0
04:40:06	04:40:06	Successful connections to DMZ stepping stone.	Root-CA	Main-web	80
05:37:05	05:48:56	Successful connections to DMZ stepping stone.	Root-CA	Main-web	80
21:57:55	22:35:20	Successful connections to DMZ stepping stone.	Root-CA	Main-web	80
23:33:40	23:34:56	Admin possibly working late.	AdminWS164	CAP-app-db	1056, 1433
23:35:57	23:35:57	Admin possibly working late.	AdminWS164	CAP-app-db	1433, 3389
2011-07-03					
00:14:48	00:14:48	Successful connections to DMZ stepping stone.	Qualified-CA	Main-web	80
13:03:02	13:15:51	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
16:51:36	16:54:06	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
2011-07-04					
00:48:43	21:09:36	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
2011-07-05					
00:15:40	00:18:26	Admin possibly working late.	AdminWS164	CAP-app-web	3389
15:09:35	21:09:36	Successful connections to DMZ stepping stone at regular intervals. Automation could be in place.	Public-CA	Main-web	80
2011-07-06					
15:09:36	21:09:36	Successful connections to DMZ stepping stone at regular intervals. Automation could be in place.	Public-CA	Main-web	80
2011-07-07					

[46] From here on outgoing traffic exists originating from Secure-net.
[47] Only the IP-address of firewall itself is logged.

Time start	Time end	Notes	Source server	Destination server	Destination port
15:09:36	21:09:36	Successful connections to DMZ stepping stone at regular intervals. Automation could be in place.	Public-CA	Main-web	80
22:58:18	22:58:27		BAPI-production	NetHSM-web	80
2011-07-08					
01:09:36	07:09:36	Successful connections to DMZ stepping stone. Other interval.	Public-CA	Main-web	80
2011-07-09					
01:09:36	07:09:36	Successful connections to DMZ stepping stone.	Public-CA CAP-app-web	Main-web	80
10:05:32	10:06:03		CAP-app-web	Main-web	80
10:06:07	23:34:59	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
2011-07-10					
00:00:14	00:26:24	Continued.	CAP-app-web	Main-web	80
01:09:36	01:09:37	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
01:24:36	01:24:36	Switching host.	CAP-app-web	Main-web	80
04:09:36	04:11:36	Successful connections to DMZ stepping stone.	Public-CA CAP-app-web	Main-web	80
07:09:36	07:09:36	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80
10:01:04	23:57:55	Successful connections to DMZ stepping stone.	CAP-app-web	Main-web	80
2011-07-11					
00:46:58	00:51:43	Successful connections to DMZ stepping stone.	Public-CA	Main-web	80

From here on there are connections from Public-CA port 1385 to Main-web port 80 at regular intervals at 01:09:36, 01:33:33, 04:09:36, 04:09:37, 07:09:43 and 07:09:44 each day from 11-07-2011 up until 20-07-2011.

Time start	Time end	Notes	Source server	Destination server	Destination port
2011-07-20					
16:46:50	16:47:30	Dropped connections. May be caused by incident response actions.	BAPI-production	Office-file	80
16:57:33	16:57:33	Successful connections to DMZ drop. May be caused by incident response actions.	BAPI-production	Office-file	80
2011-07-25					
18:50:52	19:10:08	Few days later. Successful connections to DMZ drop. May be caused by incident response actions.	Public-CA	Main-web	80
19:10:37	19:13:05	Dropped connections to DMZ drop. Firewall adjusted.	Public-CA	Main-web	80
2011-07-26					
09:09:14	09:09:23	Dropped connection. May be caused by incident response actions.	CAP-app-web	62.58.36.117	80
09:10:46	09:10:47	Accepted connections. May be caused by incident response actions.	172.18.20.25	62.58.36.117	80

All timestamps are in CEST.

Appendix IV: Certificate Authorities generating CRLs

The Certificate Authorities that automatically generated CRLs based on repetitive log entries in the CA management software.

Server	CA nickname
Nova-CA	Nederlandse Orde van Advocaten
	Orde van Advocaten SubCA Administrative CA
	Orde van Advocaten SubCA System CA
Public-CA	DigiNotar Cyber CA
	DigiNotar Extended Validation CA
	DigiNotar Private CA
	DigiNotar Public CA - G2
	DigiNotar Public CA 2025 Administrative CA
	DigiNotar Public CA 2025 System CA
	DigiNotar Public CA 2025
	DigiNotar Services 1024 CA
	DigiNotar Services CA
	CertiID Enterprise Certificate Authority
Root-CA	DigiNotar Root CA Administrative CA
	DigiNotar Root CA G2
	DigiNotar Root CA System CA
	DigiNotar Root CA
	MinIenM Organisatie CA - G2
	MinIenM SIMULATOR NL Organisatie CA-G2
Qualified-CA	DigiNotar PKIoverheid CA Organisatie - G2
	DigiNotar PKIoverheid CA Overheid en Bedrijven
	DigiNotar Qualified CA - G2
	DigiNotar Qualified CA Administrative CA
	DigiNotar Qualified CA System CA
	DigiNotar Qualified CA
	TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2-1
	TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
Test-CA	AA Interfinance Test CA
	DigiNotar HSM RSA Test CA Administrative CA
	DigiNotar HSM RSA Test CA System CA
	DigiNotar RSA Test Root 4096 G2
	DigiNotar RSA Test Root 4096
	Hypotrust CA
	TEST Key Recovery CA
	Test DigiNotar Company CA
	Test DigiNotar Extended Validation CA
	Test DigiNotar PKIOverheid CA Overheid en bedrijven
	Test DigiNotar PKIoverheid CA Organisatie - G2
	Test DigiNotar Private CA
	Test DigiNotar Public Subroot G2
	Test DigiNotar Public Subroot
	Test DigiNotar Qualified CA
	Test DigiNotar Services CA
	Test EASEE- gas CA
	Test KNB CA
	Test Ministerie van Justitie CA 2
	Test Nederlandse Orde van Advocaten - Dutch Bar Association
	Test Renault Nissan Nederland CA
	Test SHOCK CA
	Test SNG CA 2048
	Test SSL 3 Client Root CA 2010
	Test SSL 3 Server Root CA 2010

Server	CA nickname
	Test Stichting TTP Infos CA
	Test TU Delft CA
Relation-CA	Algemene Relatie Services Administrative CA
	Algemene Relatie Services System CA
	EASEE-gas CA
	KNB CA 2
	Ministerie van Justitie CA
	SNG CA
	Stichting TTP Infos CA
	TU Delft CA

Appendix V: Certificate Authorities

Based on the investigations of the database files of the CA management software, the issuing CAs were determined. The validity period has not been taken into account.

Root-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Root-CA server.

Root-CA: Issuer	#
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA	2
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA	32
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	24
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2	3

Certificates with the basic constraints attribute set found in the database files on the Root-CA server.

Root-CA: Basic constraints = TRUE
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA

Self-signed root certificates found in the database files on the Root-CA server.

Root-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr020
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2

Qualified-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Qualified-CA server.

Qualified-CA: Issuer	#
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2	142
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2	1
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2	1560
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven	5358
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA	5
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA	33
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr022	1
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl	16515
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	2
/C=NL/O=PKIoverheid TEST/CN=TRIAL PKIoverheid Organisatie TEST CA - G2	1
/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Organisatie CA - G2	1
/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Overheid CA	1

Certificates with the basic constraints attribute set found in the database files on the Qualified-CA server.

Qualified-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

Self-signed root certificates found in the database files on the Qualified-CA server.

Qualified-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr022
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

CCV-CA server

Issuers and numbers of occurrences of certificates found in the database files on the CCV-CA server.

CCV-CA: Issuer	#
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010	1
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010	2
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010	1
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010	1
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010	1
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010	14
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA	1
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA	14
/C=NL/O=DigiNotar B.V./OU=IT/CN=winsvr057.DNproductie	2

Certificates with the basic constraints attribute set found in the database files on the CCV-CA server.

CCV-CA: Basic constraints = TRUE
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=CCV-CH-TMS 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-110-364
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-160-364
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-179-095
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-237-323
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-300-362
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-310-362

CCV-CA: Basic constraints = TRUE
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-399-095
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-507-524
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-537-524
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-569-094
/C=NL/O=CCV Services B.V./CN=USPP-Perso Certificate ST4000 260-659-094
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA

Self-signed root certificates found in the database files on the CCV-CA server.

CCV-CA: Self signed
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=winsvr057.DNproductie

Nova-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Nova-CA server.

Nova-CA: Issuer	#
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA	4
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA	31
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr021	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	2
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association	37830

Certificates with the basic constraints attribute set found in the database files on the Nova-CA server.

Nova-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association

Self-signed root certificates found in the database files on the Nova-CA server.

Nova-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr021
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

Taxi-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Taxi-CA server.

Taxi-CA: Issuer	#
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA	4
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA	15
/C=NL/O=DigiNotar/OU=IT/CN=Winsvr053.DNproductie	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2	1
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2	3
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA	13
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2	1
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2	639
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2	230
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2	3
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Root CA - G2	2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2	420
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2	7

Taxi-CA: Issuer	#
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA	5

Certificates with the basic constraints attribute set found in the database files on the Taxi-CA server.

Taxi-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA

Self-signed root certificates found in the database files on the Taxi-CA server.

Taxi-CA: Self signed
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=DigiNotar/OU=IT/CN=Winsvr053.DNproductie
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA

Test-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Test-CA server.

Test-CA: Issuer	#
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010	8
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA	25
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl	2
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010	4
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010	4
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010	1
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA	91
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2	1
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Overheid en bedrijven	562
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA	3
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA	20
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl	5
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl	1
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl	606
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl	1134
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl	47
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA	6
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA	42
/C=NL/O=DigiNotar/OU=IT/CN=RSATESTCA	1
/C=NL/O=Hypotrust/CN=Hypotrust CA	87
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.	1
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA	29
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association	97
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA	11
/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA	16
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA	52
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA	174
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL	30
/CN=Test Renault Nissan Nederland CA/O=Renault Nissan Nederland N.V./C=NL	42
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/OU=TEST/CN=TEST Key Recovery CA	1

Certificates with the basic constraints attribute set found in the database files on the Test-CA server.

Test-CA: Basic constraints = TRUE
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-219-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-269-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-429-072
/C=DE/O=CCV Deutschland GmbH/CN=USPP-Perso Certificate ST4000 260-439-072
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=CCV Group/CN=oltp.ccvpay.nl
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Group/CN=Test.SSL3.certificate.erwin.nl
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Overheid en bedrijven
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Schuberg Philis/CN=Schuberg Philis Class 1 Issuing CA
/C=NL/O=Schuberg Philis/CN=Schuberg Philis Class 2 Issuing CA
/C=NL/O=Schuberg Philis/CN=Test Schuberg Philis Class 1 Issuing CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA
/CN=oltp.ccvpay.nl/OU=DMT/O=CCV Group/L=Arnhem/ST=Gelderland/C=NL
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL
/CN=Test.SSL3.certificate.erwin.nl/OU=Systems/O=CCV Group/L=Arnhem/ST=Gelderland/C=NL
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA

Self-signed root certificates found in the database files on the Test-CA server.

Test-CA: Self signed
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA
/C=NL/O=DigiNotar/OU=IT/CN=RSATESTCA

Relation-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Relation-CA server.

Relation-CA: Issuer	#
/C=FR/O=EASEE-gas/CN=EASEE-gas CA	47
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA	5
/C=NL/O=Delft University of Technology/CN=TU Delft CA	274
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA	3
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA	31
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr055	1
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	11

Relation-CA: Issuer	#
/C=NL/O=Hypotrust/CN=Hypotrust CA	977
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA	1
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA	1192
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA	6139
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA	155
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA	379
/C=NL/O=Stichting SHOCK/CN=SHOCK CA	1
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA	2320
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011	135

Certificates with the basic constraints attribute set found in the database files on the Relation-CA server.

Relation-CA: Basic constraints = TRUE
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011

Self signed root certificates found in the database files on the Relation-CA server.

Relation-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=winsvr055
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011

Public-CA server

Issuers and numbers of occurrences of certificates found in the database files on the Public-CA server.

Public-CA: Issuer	#
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl	124
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl	226
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl	54
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl	45002
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl	2
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl	6
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl	564
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl	86
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA	4
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA	29
/C=NL/O=DigiNotar/OU=IT/CN=winsvr056	1
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root	1

Certificates with the basic constraints attribute set found in the database files on the Public-CA server.

Public-CA: Basic constraints = TRUE
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl

Self-signed root certificates found in the database files on the Public-CA server.

Public-CA: Self signed
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA
/C=NL/O=DigiNotar/OU=IT/CN=winsvr056

Appendix VI: References to private keys

This appendix contains lists of private keys that were present in the databases of the CA servers. The validity period has not been taken into account. The entries *No Certificate found* mean that a private key entry was found in the database but that no corresponding certificate or name was found.

Root-CA keys
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Root CA System CA
/C=NL/O=DigiNotar/CN=DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM SIMULATOR NL Root CA - G2

Qualified-CA keys
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA G2
/C=NL/O=DigiNotar B.V. TEST/CN=TRIAL DigiNotar PKIoverheid Organisatie TEST CA - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=DigiNotar PKIoverheid CA Overheid en Bedrijven
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=DigiNotar Qualified CA System CA
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Qualified CA/emailAddress=info@diginotar.nl

CCV-CA keys
/C=BE/O=CCV Belgium NV/SA/CN=Prod UpLoad Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Client Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod SSL3 Server Root CA 2010
/C=CH/O=CCV Jeronimo S.A./CN=Prod UpLoad Root CA 2010
/C=DE/O=CCV Deutschland GmbH/CN=Prod UpLoad Root CA 2010
/C=NL/O=CCV Services B.V./CN=Prod UpLoad Root CA 2010
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA Administrative CA
/C=NL/O=DigiNotar B.V./OU=IT/CN=CCV Group CA System CA
No Certificate found
No Certificate found

Nova-CA keys
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA Administrative CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Orde van Advocaten SubCA System CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Nederlandse Orde van Advocaten - Dutch Bar Association

Taxi-CA keys
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Taxi CA System CA
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Root CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Organisatie CA - G2
/C=NL/O=Inspectie Verkeer en Waterstaat/OU=Test CA/CN=IVW SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Productieomgeving/CN=BCT Infrastructuur AP CA
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Referentie CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Organisatie CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Systeemkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM Taxi CA Boordcomputerkaarten - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Test CA/CN=MinIenM SIMULATOR NL Autonome Apparaten CA - G2
/C=NL/O=Ministerie van Infrastructuur en Milieu/OU=Testomgeving/CN=BCT Infrastructuur OT CA
No certificate found
No certificate found

Test-CA keys
/C=DE/O=CCV Deutschland GmbH/CN=Test UpLoad Root CA 2010
/C=FR/O=EASEE-gas/CN=Test EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=AA Interfinance B.V./CN=Test AA Interfinance CA/emailAddress=info@diginotar.nl
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Client Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Group/CN=Test SSL3 Server Root CA 2010
/C=NL/O=CCV Services B.V./CN=Test UpLoad Root CA 2010
/C=NL/O=Delft University of Technology/CN=Test TU Delft CA
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Organisatie - G2
/C=NL/O=DigiNotar B.V./CN=Test DigiNotar PKIoverheid CA Overheid en bedrijven
/C=NL/O=DigiNotar/CN=Test DigiNotar Company CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation CA
/C=NL/O=DigiNotar/CN=Test DigiNotar Extended Validation Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025 G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Qualified CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Root CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=Test DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar HSM RSA Test CA System CA
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Interbank N.V./CN=Test Interbank N.V.
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Test Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie CA
/C=NL/O=Nederlandse Orde van Advocaten/CN=Test Nederlandse Orde van Advocaten - Dutch Bar Association
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=Test SNG CA
/C=NL/O=Stichting SHOCK/CN=Test SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Test Stichting TTP Infos CA
/C=NL/O=Test Ministerie van Justitie/CN=Test Ministerie van Justitie CA
/CN=Test AA Interfinance CA/O=AA Interfinance B.V./C=NL
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/CN=Test DigiNotar Public CA
/emailAddress=info@diginotar.nl/C=NL/O=DigiNotar/OU=TEST/CN=TEST Key Recovery CA
No certificate found
No certificate found
No certificate found
No certificate found

Relation-CA keys
/C=FR/O=EASEE-gas/CN=EASEE-gas CA
/C=NL/O=AA Interfinance B.V./CN=AA Interfinance CA
/C=NL/O=Delft University of Technology/CN=TU Delft CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services System CA
/C=NL/O=DigiNotar B.V./OU=Operations/CN=Algemene Relatie Services Administrative CA
/C=NL/O=Hypotrust/CN=Hypotrust CA
/C=NL/O=Koninklijk Notariele Beroepsorganisatie/CN=Koninklijk Notariele Beroepsorganisatie CA
/C=NL/O=Koninklijke Notariele Beroepsorganisatie/CN=Koninklijke Notariele Beroepsorganisatie CA
/C=NL/O=Ministerie van Justitie/CN=Ministerie van Justitie JEP1 CA
/C=NL/O=Renault Nissan Nederland N.V./CN=Renault Nissan Nederland CA
/C=NL/O=Stichting Netwerk Gerechtsdeurwaarders/CN=SNG CA
/C=NL/O=Stichting SHOCK/CN=SHOCK CA
/C=NL/O=Stichting TTP Infos/CN=Stichting TTP Infos CA
/C=NL/O=TenneT TSO BV/CN=TenneT CA 2011
No certificate found

Public-CA keys
/C=NL/O=DigiNotar/CN=CertiID Enterprise Certificate Authority/emailAddress=info@diginotar.com
/C=NL/O=DigiNotar/CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Extended Validation CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Private CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA - G2/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Public CA 2025/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/CN=DigiNotar Services CA/emailAddress=info@diginotar.nl
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 Administrative CA
/C=NL/O=DigiNotar/OU=IT/CN=DigiNotar Public CA 2025 System CA

Appendix VII: Unknown serial numbers

The following serial numbers were encountered in the `serial_no.dbh` database on servers managing the Certificate Authorities, but could not be related to any identified certificates.

Root-CA

```
83120A023016C9E1A59CC7D146619617
68E32B2FE117DFE89C905B1CCBE22AB7
711CE18C0423218425510EF51513B7B8
B7ABEFC8A1F844207B774C782E5385B3
6E0088D11C7E4E98CC9E0694D32A0F6B
80C990D339F177CA9FDAC258105882AB
7F73EC0A14C4BA065BECFAD69DC5A61D
```

Qualified-CA

```
C6E2E63E7CA99BBA1361E4FB7245493C
863DE266FB30C5C489BF53F6553088C4
```

Taxi-CA

```
25B6CA311C52F0E4F72A1BD53774B5B3
A0CF459D0D1EA9A946861A0A02783D88
71A10FA4C491D3A72D18D33E3CCF576C
FE456B099700A6C428A193FE5968C9FD
E7E2B46B8C9AA64679E03841F88CA5A0
AEC9F2324D80020B6E2B2A1103D6A4E8
CB20C25F14583AFC86465F14E621FBC1
947FF1DB66A41D809A9BC7E7344E342A
90BCA541B4DF5E77FB1349684F84A930
AB4967CE8B94FCF8DA7691922E6FD59C
BA479991C9103C005726FAB83088A8D6
363E9AAF4DAC7085F31B89B2AC49059A
8A63042B8A8FA256035773BC9417435A
963CCB2601B15C73DCA821F4BC4C7458
6B7057D5DE0170842C372821D3F17DB2
C391438C15FF31BD89544A7F68DDF3B3
7278CB2A8270A3E66A021A7CD75F1211
F401D4C50FCA9161A70ED9D91D40E684
6C396359C423417E20C54CFC6690F3FF
9916C8350225BB607857375A02B6DC72
0F48A14121370B5CF4828EF826749FBC
DB43E2CE6110750785FCBBE9A8EAE061
C641E4B7F19B63C4FF1EA6D3833FC874
D8B771F90BC01C9ED1333C23EF24CFC1
```

Public-CA

```
79C03FE0C81A3022DBF8143B27E40223  BC01852405D3F4E22C48600266655026  E3E120935934CBD77E1DA7F00431F745
FCCF53CB3D0A71494AF9664690FFCF84  9F7DDFE3CAAD224EC6BD68B60DE78550  0A6DFACFDEAE74A816031534BE90B75A
82BC18B1AA5D59C61D0EFDBEA7664C08  A67C22A6E1F9D87799548EBFC7D5527E  9AD82BE2FED538B10BDFBD229A8A5AEA
5D4352671C39616670B2F34C173A1F63  11661878CCE9DC337CEEBB16E30F9A3A  C0F216CA8197AD00F0D98927EAE29E64
6FA3C48173B3B289943F113A8CD9DB8C  6BF3BEB26AFF31116200B14F4378C33B  DE76B17BFB1B6D6D6634C8C104A6E59F
CFAF9BE4E5BD0F5A75F628E45E0178C9  7A61A7778842E502E2291166C4574485  A90F1BB43E9DB5EDFC60C15FB897C593
4ADA28D281D3D14D19FB782D64086D0C  82C42F0EDC18BD751727BE5C54413EF7  8625B32398C2722D96E7B972580A0238
0B41ABEE6F4168D3CDE5A7D223B58BC1  03124C25849D9E49BC2A2FAD3E10C8A4  D1FDE3A78C9D2E80C2303CC4E3E92A4C
13548FC160BC5C9F315AE28CDB490E36  EFF0DD4B4927DF64232C5D2FF280C1E4  B355E909FD55C5E9EF1A6E67E9C18203
5D8D0D43611275982E6A5490E7F87BD7  9EDCB5E1FE1255A2F1D7FC52C4AFA3B1  ADB59A303C6260DBE466F0149AB11A4A
C880AE4D7927E6A8FA7D456CB03E9763  3A32AAA9DFE2CA7F9E003885E316944B  5CEBD524469A075FB6B42D06C9BF27AD
82072FC8F8DD7E6C0ECE9B47185F0521  4455B43B9173CBAE4E247272EE2573D5  0E0886EEAA119CF14F1C54387060929A
90DB656E273476CC836778255582FA8B  B95F62E86194734C9F68D4BF8B200C49  B4F9299F05A327E60543C4CDE3277FC0
171A8599EDE711A3315BC7D694CEBEC6  FE873B742B230B22AE540E840490A2F4  E4B2F09505726306314DF05B734FD9D0
E9EB8075F7FE3683B431552C2D962CB0  8779917563EC38B7746B8ECAFE239BE6  4DD0497CBAABBA058574A611B26151BA
E6F9E095464F64448840A832FB3443DB  72CBC4824C6215B139FDE6BA10DAC6AD  7073C6C01DEE4E158F554555F697F7D9
C83D16E9CB29DCF35F3B351CB942FE0D  8D09D4B98DE67C9E9C7C18CB72AD2418  EB72415ECD0B4AACBDEEA3734F4349BF
39B5DD0ECC85C3F62A72391DC055F561  07BC72A463D4DE33B2BE733D6FAC991D  BED90D98FA3A1E0A5BD78AD54E55774D
DF3FD6AFBBFBC30C9AD80BF764A102DB  D3E2205C3B899FC99D77FE802985283F  3CDCD81930F91AC0B990664931E5412E
327B9A443C49018D7B0A97B6EC2254B8  A5029D6A057D50D20ECFE0E528EDA067  763B0C2A7B83066A9D995C8C4FD9E35E
8B0EABAF922D4C6E6917FCBE365DD64A  C8B2487ADFAF969E34306029AC934406  720DF591261D710ADC73127C1BC4303D
4FC2D72D6427CABBE3E859453865F43B  5F3C1BDC7A2BCD47ABAF0C8E62D9F757  C06C12DBBC7055FE40950803238EC104
53B53BF2F74997EBEB2577D63DA692B7  601315BB085FECF29538DA3F9B7BA1CE  62BF5A170CC779ADE7EF0090F395D5E6
ABB21F43553F2695031A1C85355D7F1C  30170F15A240446E6B482E0A364E3CCA  61BF9A0FF2CE9D55D86BC063839F72F4
5563605FDC2DC865E2A1C32995B5A086  0590B310AEFC7A3EDC03ECA2A6F6624F  B5D7A148CA6C1F9693A2C16ACDD66226
5DD6A72747D90C018B63F959DFE7C976  FDEB145AAC81B8CD29B8DA018E71456F  35FBDCDF923F99B5E1C5FF4423B715B8
CAB736FFE7DCB2C47ED2FF88842888E7  C3F9F45F19E334C8303F44288856D843  F1EBE73557546DC8B21E0A2DE5E3A33E
9C79C9FE16727BAC407B4AA21B153A54  028CF7556F8BE27026800448FA6AA527  EBE7561CA573DA5DBB8EFAA250A40FD3
2D711C9CB79EC15445747BFE3F8BC92F  E93B28B47C34B243EBA62E58FE2FF46F  6BACB6C5B74FA747A3CF375EC3095035
752A2D0325A3D34D9F5198C2F5C92A6C  F89F5DE575755A3B4C0DECC6EDA7C804  6C1950AA83F4663F1BA063B5275C25EC
39936336286F843756FC4BC296D7A8E0  5D8F8D78B0C19EF4479F744DECBD84BC  56EF1EE54D65EF7B39AF541E95BB45A9
4A6D90618A5CA6797C768C03C860C4F8  EAACDC2F46D4A86F39B035B793F4A94F  2B1EA767EC59E46364BC2DF9B1F30B97
0954E1AB9141ED7E8B640FE681046451  9D06313F21A4EDF734C324FFBCB9E2B5  3913B1E1C35BDDF02CE03C916E8AA638
8259C3E1DB6C2C9B7FCD6A305EADEFE4  35C54E845AE855F818504C8C189F52C7  AFA2F7E964280B36DB0D714B86256F54
```

Public-CA		
022E35B1ACD40F040C444DF32A7B8DE6	D0BA58BA609CC1A001F612987A822BEF	9A3A951BE27E0729726FD8B80060E7E1
170370B60D515F164119BE54FD55E1ED	6B339433956F1505104BB231314A153E	6410577C738133297472F6C22C2BB397
CBFE437C9B62805C4353516699E44649	C1366C7246041A3089E1C244C5DC42E7	C8C06B0C6B7FE7CA66BCFE617AB6C4E6
5FFA79AB76CE359089A2F729A1D44B31	61D11B35765ECB85890D5349786D9FCA	58C18B290620E18B8C78AC1912E5DCD7
5298BCBD11B3952E3FDDC6FDD6711F5C	44C287C1C3697367B0E6CB78A78C1DF5	2F5ABFDCCAB1A2927E54283296F19FB8
1836289F75F74A0BA5E769561DE3E7CD	DAACF72BC91FB6DA90A804933CB72E23	A07CB7881E35C91FD9C5D20F6102572C
DEB427AC9F1E8A0D0237049C80DF7E7F	2ACBA14BB6F65F7BD0A485BFCB6D023F	05E2E6A4CD09EA54D665B075FE22A256
FD8FE350325318C893AFE03F9DFC7096	84BE5D762F37E9018D623C8E91F4D924	8BA800DDDD865B6BF3A85ADEC4C29730
A8031D608F6549941879981764674DD7	1A89324D6D3E6DE6726C688BFF225DDD	07B546E8E002FC5854651BE31802F96D
DDAD29B8B1215191E7EB5AAEE0219338	F5FA42A5B421705E4803DA93C4F7E099	DF2AD7F766E2EEFAF0FD1FB5C6883AB4
3F8A5EA1756DDF4A6B6F2645B4911486	A869B96BCDF1D474C0714763AA34A8C9	1C6EA2DA6ECED5C5C761BCA9CA4C5308
30DF96D87EEC8CA77A135ECCAB1AD25E	3EA0F90DE57187FC7E1AC45AE44D16C6	A640A29E706AF38557B86619EAF45E7A
7DD8E0E1906C1754E11E901927CCABBD	F7DE638B76C3958AA3413A9785A19900	F88885670C3D55EBA52096A65310DACA
DAC51C3D23B163601305AF99DF129689	3F8C9CDAACBB533AE94F47456819FA0E	B85E7BB83667097F15D8A3DEAAA1B198
D77EC92400AE0D9FA57DEF4DD8CFA4D4	209920C169512D3EB4A1ED7CAD17D033	A5F6F149B468683318DC178F4208E237
09369288E36D7AFFEE94EA81998FA316	B2F57BD01BAAF7AF01EF442910CEBBA0	04841B82A9D81E44CB4F2D98CFE7C374
EEBE188553223432891919 13F6D769EB	C0766829AA4D2E1A5D97213A4E4A654E	A81686CEFDEFFCE82B8DBF100E1395F1
C00132DA154BDEE361EDEE727226D0F5	FC9993EA7A4E761B6CB79ABE2BD3CDE1	9952073595776A3D7A8101664A56AB96
6580BE22A0566352B9622777BFCB7164	4D556B338FAA020979A740B4C3AEE28C	A076DA72A8C8E2137F05FE3FA59870EB
7352C61297D6B04E874EDAD12480F78E	8ED896B9A622FF24559A3429E5888E0A	121378A6DE0A13DDB295106E912A4E14
F658C0D52B3EEF71DDE6C284E7E1B337	8CF1F45323EC5AB449451E7A9476CFDC	65A925E578098658FADA30E9FB67B5E4
E1253D04A17AB8E47F4A5916B9BF9D23	D1718E9BD91257D2169C81197D508A67	5B8E5202EC6769F2389605D33DC245B2
8922A9A23BE960FFE9707A0B3F4D75BD	E4A691D60266784968DF971D6BF473AF	EA71F746BD17D1B05450329818572F2E
EAE97F465015E49A14F3B23403ACFA11	B3B64F1925F759A2E145190333D1D6D2	DD8C315D2CA61870CBCF9D56ED7474E2
13A757022817C0514A5C142FE9BF143A	ED4C2EBC14B85F46A9A75F159DF8BEB3	F346A1E62FED476F472560C6DDE0CADC
5132F0FCB3F8DCAA501C620575D33FEE	CDBC0441C10DB5ABA43120E63A048425	CBBCB9E06F9FC92C533B2F2A5284BA22
39953BF6383A00D29BEB377568E3DE7A	DC1665266A0198728861AC99ED368928	79DCFDA2700E06F8EAA640BA9B827810
67887932934DFF086153CA905E7DE9EE	706BBC770C62D41DD799721ABD1868AB	17CF5474D5A8B4E735E69E017CEC2F37
DCD1072719692871126E4159D80EFDA8	B2205D8CBDDFE49D7C5F0F95D506718F	7034FBF641CEB257FC109A6819D19DA0
C6741E3D08C0FFD4617B94E654DD89F1	901F30DB86EEB1666F5A8CAE1C7BD08B	6E6D052B5ABC015C779EA3500FA11A28
8CC74931E64061491652CC169C8BAAB3	C731140FAA7690918BABF17BECB7938D	0370390E48A7F26AA62188A79E612DC3
4157D99E46A3E45E6130A95645410DAC	8C605DFAA0EC88CDB7D12F7250C9F53A	
E34C4FC7488C4DFEF0EA475A17AF2C7B	68F252CD36F2798A2182F6406A31A5A2	
59F8BDDA3F56D8026FAB6E3130F5D843	BD7CB0D124DFDE784CD5B9EF288C304E	
FAB79682C8EAE556F11ECF6DAD7121BA	3D2BC95A85EF539A68DAC84542A1AE7A	

Appendix VIII: Rogue certificates

Of the 531 encountered rogue certificates, 140 unique distinguished names and 53 unique common names were identified.

Common Name	Number issued
..com	1
..org	1
*.10million.org	2
*.android.com	1
*.aol.com	1
*.azadegi.com	2
*.balatarin.com	3
*.comodo.com	3
*.digicert.com	2
*.globalsign.com	7
*.google.com	26
*.JanamFadayeRahbar.com	1
*.logmein.com	1
*.microsoft.com	3
*.mossad.gov.il	2
*.mozilla.org	1
*.RamzShekaneBozorg.com	1
*.SahebeDonyayeDigital.com	1
*.skype.com	22
*.startssl.com	1
*.thawte.com	6
*.torproject.org	14
*.walla.co.il	2
*.windowsupdate.com	3
*.wordpress.com	14
addons.mozilla.org	17
azadegi.com	16
Comodo Root CA	20
CyberTrust Root CA	20
DigiCert Root CA	21
Equifax Root CA	40
friends.walla.co.il	8
GlobalSign Root CA	20
login.live.com	17
login.yahoo.com	19
my.screenname.aol.com	1
secure.logmein.com	17
Thawte Root CA	45
twitter.com	18
VeriSign Root CA	21
wordpress.com	12
www.10million.org	8
www.balatarin.com	16
www.cia.gov	25
www.cybertrust.com	1
www.Equifax.com	1
www.facebook.com	14
www.globalsign.com	1
www.google.com	12
www.hamdami.com	1
www.mossad.gov.il	5
www.sis.gov.uk	10
www.update.microsoft.com	4

Appendix IX: Suspicious files

Suspicious files were encountered on the following servers:

Network	Server
Secure-net	Qualified-CA
	Taxi-CA
	Relation-CA
	Public-CA
	Root-CA
	BAPI-db
	CCV-CA
Office-net	Office-file server
	BAPI-db
DMZ-ext-net	Main-web
	Docproof2

Temporary Internet files

A non-exhaustive list of suspicious files found in the temporary Internet files directory:

Server	File name	User	Size	Create Date	Create time
BAPI-db	kir[1].txt	MSSQLusr	9	17-Jun-2011	16:15:49
BAPI-db	libeay32[1].dll	MSSQLusr	1017344	17-Jun-2011	16:18:44
BAPI-db	PwDump7[1].exe	MSSQLusr	77824	17-Jun-2011	16:19:21
BAPI-db	PwDump[1].exe	MSSQLusr	393216	17-Jun-2011	18:56:01
BAPI-db	7za[1].exe	MSSQLusr	264704	17-Jun-2011	19:33:55
BAPI-db	mswinsck[1].ocx	MSSQLusr	127808	17-Jun-2011	19:41:31
BAPI-db	base64[1].exe	MSSQLusr	45056	18-Jun-2011	0:34:05
BAPI-db	test[1].zip	MSSQLusr	2666	18-Jun-2011	5:11:53
BAPI-db	mstsc[1].exe	MSSQLusr	407552	18-Jun-2011	14:46:46
BAPI-db	mstscax[1].dll	MSSQLusr	655360	18-Jun-2011	14:47:28
BAPI-db	clxtshar[1].dll	MSSQLusr	69632	18-Jun-2011	14:47:51
BAPI-db	tclient[1].dll	MSSQLusr	68096	18-Jun-2011	14:48:29
BAPI-db	test2[1].zip	MSSQLusr	2666	18-Jun-2011	14:53:55
BAPI-db	nc[1].exe	MSSQLusr	65028	20-Jun-2011	10:34:15
BAPI-db	demineur[1].dll	MSSQLusr	151552	20-Jun-2011	11:14:09
BAPI-db	klock[1].dll	MSSQLusr	153600	20-Jun-2011	11:14:27
BAPI-db	mimikatz[1].exe	MSSQLusr	368128	20-Jun-2011	11:15:40
BAPI-db	sekurlsa[1].dll	MSSQLusr	200704	20-Jun-2011	11:15:51
BAPI-db	cachedump[1].exe	MSSQLusr	45056	21-Jun-2011	12:50:00
BAPI-db	PwDump[1].exe	MSSQLusr	393216	21-Jun-2011	13:09:47
BAPI-db	mswinsck[2].ocx	MSSQLusr	127808	21-Jun-2011	13:46:33
BAPI-db	uploader[2].exe	MSSQLusr	28672	21-Jun-2011	14:18:15
BAPI-db	uploader[1].exe	MSSQLusr	28672	21-Jun-2011	15:07:23
BAPI-db	up3[1].exe	MSSQLusr	28672	21-Jun-2011	15:21:03
BAPI-db	sfk[1].exe	MSSQLusr	1155072	21-Jun-2011	19:53:15
BAPI-db	ReadF[1].exe	MSSQLusr	8192	22-Jun-2011	8:41:06
BAPI-db	Read1[1].exe	MSSQLusr	9728	22-Jun-2011	10:26:02
BAPI-db	Read2[1].exe	MSSQLusr	9728	22-Jun-2011	10:46:20
BAPI-db	Read3[1].exe	MSSQLusr	9728	22-Jun-2011	12:17:29
BAPI-db	Read4[1].exe	MSSQLusr	9728	22-Jun-2011	12:20:09
BAPI-db	Read5[1].exe	MSSQLusr	10240	22-Jun-2011	12:34:28
BAPI-db	PortQry[1].exe	MSSQLusr	143360	29-Jun-2011	9:44:53
BAPI-db	troj172[1].exe	MSSQLusr	61440	29-Jun-2011	22:13:34
BAPI-db	troj172[1].exe	MSSQLusr	61440	29-Jun-2011	22:13:34
BAPI-db	troj134[1].exe	MSSQLusr	61440	29-Jun-2011	22:18:17
BAPI-db	troj134[1].exe	MSSQLusr	61440	29-Jun-2011	22:18:17
BAPI-db	134[1].exe	MSSQLusr	37888	29-Jun-2011	22:30:33
BAPI-db	RunAs[1].exe	MSSQLusr	24576	29-Jun-2011	22:52:25
BAPI-db	RDP[1].exe	MSSQLusr	553472	29-Jun-2011	23:01:49
BAPI-db	13480[1].exe	MSSQLusr	37888	29-Jun-2011	23:19:32

Server	File name	User	Size	Create Date	Create time
BAPI-db	Troj25[1].exe	MSSQLusr	61440	1-Jul-2011	13:45:18
BAPI-db	psexec[1].exe	MSSQLusr	381816	1-Jul-2011	19:12:25
BAPI-db	mimi[1].zip	MSSQLusr	477545	1-Jul-2011	22:15:25
Taxi-CA	mimi[1].zip	Administrator	477545	1-Jul-2011	22:15:49
Qualified-CA	172.18.20[1].htm	Administrator.DNPRODUCTIE	4867	1-Jul-2011	23:20:51
Taxi-CA	winsvr130[1].htm	Administrator.DNPRODUCTIE	476	2-Jul-2011	0:53:44
Root-CA	corner[2].gif	administrator.DNPRODUCTIE	3196	2-Jul-2011	1:00:58
Root-CA	enrollbg[4].gif	administrator.DNPRODUCTIE	558	2-Jul-2011	1:00:58
Root-CA	icontrol[1].vbs	administrator.DNPRODUCTIE	35007	2-Jul-2011	1:08:45
Root-CA	up[1]	administrator.DNPRODUCTIE	3415	2-Jul-2011	1:24:31
Root-CA	favicon[1].ico	administrator.DNPRODUCTIE	3878	2-Jul-2011	2:40:06
BAPI-db	ldap[1].msi	MSSQLusr	14297088	2-Jul-2011	18:41:27
Relation-CA	get[1].htm	Administrator.DNPRODUCTIE	323	2-Jul-2011	20:57:35
Relation-CA	banner[1].htm	Administrator.DNPRODUCTIE	6143	2-Jul-2011	21:55:49
Relation-CA	172.18.20[1].htm	Administrator.DNPRODUCTIE	5291	2-Jul-2011	21:59:01
Relation-CA	172.18.20[1]	Administrator.DNPRODUCTIE	5692	2-Jul-2011	21:59:34
BAPI-db	direct[1].exe	MSSQLusr	37888	3-Jul-2011	23:40:23
BAPI-db	direct[1].zip	MSSQLusr	19702	4-Jul-2011	1:06:00
Taxi-CA	direct[1].zip	Administrator.DNPRODUCTIE	19702	4-Jul-2011	4:18:39

Recent files

A non-exhaustive list of suspicious files and other unspecified pages found in the recent files directory:

Server	File name	User	Create date	Create time
Main-web	Nieuw - Tekstdocument.txt.lnk	Administrator	20-Jun-2011	2:15:43
BAPI-db	pki.zip.lnk	Administrator	1-Jul-2011	14:58:07
BAPI-db	DARPI.lnk	Administrator	1-Jul-2011	16:13:07
Taxi-CA	Desktop.ini	Administrator	1-Jul-2011	22:32:39
Taxi-CA	Recent	Administrator	1-Jul-2011	22:32:39
Qualified-CA	certs.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:29:57
Qualified-CA	ssl.crt.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:29:57
Qualified-CA	root.crt.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:31:45
Qualified-CA	cas.crt.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:32:06
Qualified-CA	a.crt.lnk	Administrator.DNPRODUCTIE	1-Jul-2011	23:35:35
Qualified-CA	qualifiedData.zip.lnk	Administrator.DNPRODUCTIE	2-Jul-2011	0:09:57
Qualified-CA	qualifiedData.zip.lnk	Administrator.DNPRODUCTIE	2-Jul-2011	0:09:57
Root-CA	MinIenM Organisatie CA - G2.p7b.lnk	administrator.DNPRODUCTIE	2-Jul-2011	1:12:54
Root-CA	httpd.conf.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:13:05
Root-CA	dist.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:27:17
Root-CA	schema.conf.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:27:49
Root-CA	iXudad.conf.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:29:19
Root-CA	xudad.oc.conf.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:30:43
Root-CA	origrsa.zip.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:40:26
Root-CA	CertiID Enterprise Certificate Authority.crt.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:48:45
Root-CA	muh.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:48:45
Root-CA	USPP-Perso Certificate ST4000 260-160-364.crt.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:50:20
Root-CA	certs.lnk	administrator.DNPRODUCTIE	2-Jul-2011	2:50:20
Relation-CA	dbpub.zip.lnk	Administrator.DNPRODUCTIE	2-Jul-2011	20:35:41
Qualified-CA	m.zip.lnk	Administrator.DNPRODUCTIE	2-Jul-2011	22:15:28
Public-CA	Desktop.ini	Admin1[48]	4-Jul-2011	0:05:17

[48] The real username is replaced by a pseudonym to protect the privacy of the personnel of DigiNotar.

Other local settings files

A non-exhaustive list of other suspicious files found in the local settings directory:

Server	Full path	Size	Create date	Create time
BAPI-db	Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-2196791791-1123517030-1950105499-500\	256	30-Jan-2006	11:44:01
Public-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\$I30	4096	20-Jul-2010	12:55:21
Public-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\	56	20-Jul-2010	12:55:21
Public-CA	Documents and Settings\Admin1\Local Settings\Application Data\	472	17-Jun-2011	14:05:22
BAPI-db	Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-2196791791-1123517030-1950105499-500\Credentials	346	1-Jul-2011	14:46:46
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\index.dat	49152	2-Jul-2011	0:53:44
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\	152	2-Jul-2011	0:53:44
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\index.dat	32768	2-Jul-2011	1:00:58
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070220110703\index.dat	32768	2-Jul-2011	1:00:58
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011061320110620\	152	2-Jul-2011	1:00:58
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070220110703\	152	2-Jul-2011	1:00:58
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\	264	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\	264	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\drwtsn32.log	203258	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\drwtsn32.log	203258	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\user.dmp	90852	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Dr Watson\user.dmp	90852	2-Jul-2011	2:18:56
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Last Active\{51503BD7-A456-11E0-941C-D48564505644}.dat	70144	2-Jul-2011	2:52:26
Relation-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\Application Data\Softerra\LDAP Browser 4\UserImages.bmp	9014	2-Jul-2011	21:46:30
Public-CA	Documents and Settings\administrator.DNPRODUCTIE\Local Settings\Application Data\Microsoft\Terminal Server Client\	144	4-Jul-2011	4:11:29
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011062720110704\index.dat	32768	4-Jul-2011	4:19:23
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070420110705\index.dat	32768	4-Jul-2011	4:19:23
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011062720110704\	152	4-Jul-2011	4:19:23
Taxi-CA	Documents and Settings\Administrator.DNPRODUCTIE\Local Settings\History\History.IE5\MSHist012011070420110705\	152	4-Jul-2011	4:19:23

Other files

A non-exhaustive list of remaining suspicious files:

Server	Full path	Size
BAPI-db	WINDOWS\system32\drivers\etc\hosts	792
BAPI-db	Program Files\Symantec AntiVirus\savrt.dat	3220
BAPI-db	Program Files\Symantec AntiVirus\SRTSEXCL.DAT	76
BAPI-db	WINDOWS\system32\config\default	262144
BAPI-db	WINDOWS\system32\config\SAM	262144
BAPI-db	WINDOWS\system32\config\SECURITY	262144
BAPI-db	WINDOWS\Tasks\SchedLgU.Txt	10364
BAPI-db	WINDOWS\system32\ipconfig.exe	63488
BAPI-db	Program Files\Symantec AntiVirus\$I30	12288
BAPI-db	Program Files\Symantec AntiVirus\	288
BAPI-db	Documents and Settings\All Users\Application Data\Symantec\Common Client\settings.dat	20204
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBConfig.log	3676
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBDebug.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBDetect.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBNotify.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBRefr.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetCfg.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetDev.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetLoc.log	2108
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBSetUsr.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBStHash.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBStMSI.log	7576
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\BBValid.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPPolicy.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPStart.log	64
BAPI-db	Program Files\Common Files\Symantec Shared\SPBBC\LOGS\SPStop.log	64
BAPI-db	Partition 5\Log [NTFS]\[root]\MSSQL\Log\finance01_Log.LDF	1048576
BAPI-db	Partition 5\Log [NTFS]\[root]\MSSQL\Log\Applog01_Log.LDF	2359296
BAPI-db	Documents and Settings\Admin3\Bureaublad\WebRAOBeheer02\Web.config	7415
Main-web	Partition 3\Data [NTFS]\[root]\Websites\Bapiviewer\BapiViewer\web.config	5471
Public-CA	WINDOWS\system32\wbem\Logs\mofcomp.log	14664
BAPI-db	Partition 5\Log [NTFS]\[root]\MSSQL\Log\wietse_log.ldf	3145728
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\js\b.aspx	72689
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\RunAs.exe	24576
BAPI-db	Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\06172011.Log	262
BAPI-db	Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs\06172011.Log	262
BAPI-db	WINDOWS\system32\archive.zip	198024801
BAPI-db	WINDOWS\system32\mswinsck.ocx	127808
Main-web	Partition 3\Data [NTFS]\[orphan]\demineur.dll	151552
Main-web	Partition 3\Data [NTFS]\[orphan]\klock.dll	153600
Main-web	Partition 3\Data [NTFS]\[orphan]\mimikatz.exe	368128
Main-web	Partition 3\Data [NTFS]\[orphan]\sekurlsa.dll	200704
Main-web	Documents and Settings\Administrator\Recent\Nieuw - Tekstdocument.txt.lnk	872
BAPI-db	WINDOWS\system32\BAPI-DB_MS IIS DCOM Server.pvk	332
BAPI-db	WINDOWS\system32\BAPI-DB_SELFSIGN_DEFAULT_CONTAINER.pvk	620
BAPI-db	WINDOWS\system32\BAPI-DB_Microsoft Internet Information Server.pvk	332
BAPI-db	WINDOWS\system32\BAPI-DB_tmpHydraLSKeyContainer.pvk	332
BAPI-db	WINDOWS\system32\BAPI-DB_0_BAPI-db.diginotar.nl.pfx	1737
BAPI-db	WINDOWS\system32\Documents.7z	1015873568
BAPI-db	WINDOWS\system32\bsqweyec.dll	65536
BAPI-db	WINDOWS\system32\xjegjvhr.exe	53760
BAPI-db	WINDOWS\system32\uploader\	48
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\94.exe	37888
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\Troj65.exe	61440
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\PwDump.exe	393216
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\cachedump.exe	45056
Docproof2	Partition 3\Data [NTFS]\[root]\Websites\Docproof\Docproof01\demo\test.txt	127
BAPI-db	Documents and Settings\Administrator\Desktop\rdp.exe	553472

Server	Full path	Size
BAPI-db	Documents and Settings\Administrator\Desktop\rdp.exe	553472
BAPI-db	Documents and Settings\Administrator\Desktop\Default.rdp	2458
Office-file	Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	141
Office-file	Documents and Settings\Administrator\Desktop\sfk.exe\	1155072
Office-file	WINDOWS\system32\sfk.exe\	1155072
BAPI-db	Documents and Settings\Administrator\Desktop\13480.exe	37888
BAPI-db	Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	141
BAPI-db	Documents and Settings\Administrator\Recent\pki.zip.lnk	424
BAPI-db	Documents and Settings\Administrator\Recent\DARPI.lnk	941
Taxi-CA	Documents and Settings\Administrator\Cookies\administrator@10.10.20[1].txt	139
Taxi-CA	WINDOWS\system32\Microsoft\Crypto\	136
Taxi-CA	WINDOWS\system32\Microsoft\Crypto\RSA\MachineKeys\	48
Taxi-CA	WINDOWS\system32\Microsoft\Crypto\RSA\	256
Taxi-CA	Documents and Settings\Administrator\Recent\Desktop.ini	150
Taxi-CA	Documents and Settings\Administrator\Recent\	152
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\certs.lnk	598
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\ssl.crt.lnk	720
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\root.crt.lnk	725
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\cas.crt.lnk	720
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\a.crt.lnk	736
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	141
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\qualifiedData.zip.lnk	448
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\qualifiedData.zip.lnk	448
Qualified-CA	WINDOWS\system32\Microsoft\Protect\S-1-5-18\User\457718b9-fa34-41e3-8d9d-3ecf7391929c	388
Qualified-CA	WINDOWS\system32\nfmodexp.dll	742680
Qualified-CA	WINDOWS\system32\nfmodexp.dll	742680
Qualified-CA	WINDOWS\system32\ncspmess.dll	357656
Qualified-CA	WINDOWS\system32\ncspmess.dll	357656
Qualified-CA	WINDOWS\system32\ncsp.dll	1041688
Qualified-CA	WINDOWS\system32\ncsp.dll	1041688
Qualified-CA	WINDOWS\system32\ncspdd.dll	1041688
Qualified-CA	WINDOWS\system32\ncspdd.dll	1041688
Qualified-CA	WINDOWS\system32\ncspsigdd.dll	1033496
Qualified-CA	WINDOWS\system32\ncspsigdd.dll	1033496
Root-CA	WINDOWS\SchCache\DNproductie.sch	370536
Root-CA	WINDOWS\SchCache\	272
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\Crypto\RSA\S-1-5-21-4190788878-266275749-1156481715-500\9cb4f8bdfaa302f85333ef07fa3fb192_60643e52-42b0-4d55-aea2-38a5b64b11ec	2073
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\Certificates\40F1C4C24E802122FBC4DB5061CADF1DDCEB33DD	858
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\Certificates\	320
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\CRLs\	48
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\CTLs\	48
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Application Data\Microsoft\SystemCertificates\Request\	456
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\MinIenM Organisatie CA - G2.p7b.lnk	560
Root-CA	Documents and Settings\All Users\Application Data\nCipher\Log Files\keysafe.log	566
Root-CA	Documents and Settings\All Users\Application Data\nCipher\Log Files\cmdadp.log	388
Root-CA	Documents and Settings\All Users\Application Data\nCipher\Log Files\cmdadp-debug.log	0
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\httpd.conf.lnk	696
Root-CA	WINDOWS\PCHealth\ErrorRep\	256
Root-CA	WINDOWS\PCHealth\ErrorRep\	256
Root-CA	WINDOWS\PCHealth\ErrorRep\UserDumps\	576
Root-CA	WINDOWS\PCHealth\ErrorRep\UserDumps\	576
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\dist.lnk	531
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\schema.conf.lnk	677

Server	Full path	Size
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\iXudad.conf.lnk	677
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\xudad.oc.conf.lnk	683
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	140
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Cookies\administrator@10.10.20[1].txt	140
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\origrsa.zip.lnk	416
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\CertiID Enterprise Certificate Authority.crt.lnk	804
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\	256
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\	256
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\Desktop.ini	75
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\Desktop.ini	75
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\muh.lnk	571
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\target.lnk	463
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\NetHood\d$ on CCV-CA\target.lnk	463
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\USPP-Perso Certificate ST4000 260-160-364.crt.lnk	879
Root-CA	Documents and Settings\administrator.DNPRODUCTIE\Recent\certs.lnk	631
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\Qualified-CA.txt	461
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\Root-CA.txt	272
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\kcavkfsc.dll	65536
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\njnypgqa.exe	53760
CCV-CA	Documents and Settings\administrator.DNPRODUCTIE\Desktop\Public-CA.txt	458
Relation-CA	Partition 2\Data [NTFS]\[root]\Progs\rsa_cm_68\Web server\enroll-server\ca\get.xuda	254
Relation-CA	Documents and Settings\Administrator.DNPRODUCTIE\Desktop\dbpub.zip	59545925
Relation-CA	Documents and Settings\Admin2\Desktop\administrator@10.10.20[1].txt	141
Relation-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\dbpub.zip.lnk	404
Qualified-CA	Documents and Settings\Administrator.DNPRODUCTIE\Recent\m.zip.lnk	380
Public-CA	Partition 5\NONAME [NTFS]\[orphan]\add-pkcs10-request[16].htm	96617
Public-CA	WINDOWS\system\osvchost.exe	36864
Public-CA	Documents and Settings\Admin1\Recent\Desktop.ini	150
Public-CA	WINDOWS\system32\wbem\AutoRecover\C8463ECBE33BC240263A0B094E46D510.mof	2826402
Public-CA	WINDOWS\system32\wbem\AutoRecover\23BDE61F1F4FACE17E9B0C01F2A1FD9B.mof	36574
Public-CA	Partition 5\NONAME [NTFS]\[orphan]\Settings[2].htm	3097
Public-CA	Partition 5\NONAME [NTFS]\[orphan]\direct83[1].exe	37888
Public-CA	WINDOWS\system32\csrsss.exe\	37888
Public-CA	WINDOWS\system32\csrsss.exe\Zone.Identifier	26
Public-CA	Partition 5\NONAME [NTFS]\[orphan]\139[1].exe	37888
Public-CA	WINDOWS\system32\svhost.exe\	37888
Public-CA	WINDOWS\system32\svhost.exe\Zone.Identifier	26
Taxi-CA	WINDOWS\system\svchost.exe\	19702
Taxi-CA	WINDOWS\system\svchost.exe\Zone.Identifier	26
Relation-CA	Documents and Settings\Administrator.DNPRODUCTIE\My Documents\Default.rdp	1214
Public-CA	Partition 2\NONAME [NTFS]\[orphan]\x-select-settings.xuda	28875

Van: [redacted] (Fox-IT) [redacted]@fox-it.com]
Verzonden: maandag 13 augustus 2012 18:04
Aan: [redacted]
CC:
Onderwerp: FW: Definitieve versie DigiNotar rapport
Bijlagen: REP_MinBZK_PR-110202_Operation_Black_Tulip_Update_1.0.pdf

Heren,

Bij deze het rapport zoals het gedistribueerd kan worden.

Mocht de bedoeling zijn dat het wegzakt tussen andere interessante hackaangelegenheden dan is morgen een goede dag.

Met vriendelijke groet,

[redacted]