Gamma Group en de politie
FinFisher trojan in de Nationale politie

Uit in 2014 gepubliceerde Wikileaks documenten over Gamma Group wordt duidelijk dat de Nederlandse politie sinds september 2012 zestien licenties heeft aangeschaft voor het digitale wapen FinSpy en FinMobile. De Nationale Politie maakt in antwoord op het WOB verzoek van Buro Jansen & Janssen echter geen verdere informatie openbaar.

Gamma Group is een van oorsprong Brits bedrijf met takken en dochterondernemingen over de gehele wereld. Sinds 2008 biedt Gamma Group het digitale wapen FinFisher aan. Met de software FinFisher of FinSpy kan via een USB of vanaf afstand via wifi of een netwerk inbreken op computers, laptops, tablets en smartphones.

Bevestigen noch ontkennen

Op grond van de Wet Openbaarheid van Bestuur (WOB) heeft Buro Jansen & Janssen bij de Nationale Politie documenten opgevraagd met betrekking tot contacten met Gamma Group. In antwoord op het WOB verzoek beweert de Nationale Politie over geen informatie te beschikken over de Gamma Group: 'Na onderzoek is gebleken dat met geen van de door u genoemde bedrijven de politie een contract heeft. Ook zijn bij de politie geen documenten aangetroffen betreffende de bedrijven Gamma Group en/of Gamma International en/of vergelijkbare namen.'

De Nationale Politie zegt dus geen contract te hebben met Gamma Group of een bedrijf met een vergelijkbare naam. Dit kan zijn. Gamma Group bestaat uit een netwerk van verschillende bedrijven. De FinFisher software wordt te koop aangeboden door een aantal Duitse bedrijven die tot het netwerk behoren namelijk Elaman GmbH de Duitse dochterondernemingen van Gamma Group die sinds 2013 de naam FinFisher in de naamvoering hanteren (FinFisher GmbH, FinFisher Labs, FinFisher Holding).

Buro Jansen & Janssen heeft ook een WOB verzoek ingediend naar de contacten met FinFisher. De Nationale Politie antwoordt hierop dat het niet kan bevestigen noch ontkennen dat zij informatie bezit over

FinFisher: 'Indien zoals in het onderhavige geval, uw verzoek om informatie ziet op het openbaar maken c.q. verstrekken van informatie over met name genoemde bedrijven waarmee de politie overeenkomsten c.a. zou kunnen hebben, vormt dit een onaanvaardbaar risico voor die overeenkomsten c.a..'

De politie hanteert hier een moeilijk te doorgronden formulering (‘bedrijven waarmee de politie overeenkomsten zou kunnen hebben’). Dit roept vraagtekens op. Indien de politie geen overeenkomst heeft met een FinFisher bedrijf, dan zou men dat kunnen zeggen. Zo antwoordt de politie in antwoord op het WOB verzoek inzake de relaties met Hacking Team ook dat er geen contract is met Hacking Team. In de beantwoording van het WOB verzoek ontkent noch bevestigt de Nationale Politie dus dat er een contract is met FinFisher.

Het valt ook moeilijk te ontkennen. Uit de in 2014 gepubliceerde Wikileaks documenten over Gamma Group wordt immers duidelijk dat de politie de FinFisher heeft aangeschaft.

Jochem van der Wal

De Wikileaks documenten over Gamma Group bevatten een overzicht van de klantgegevens van het bedrijf, en een overzicht van hulpvragen die door gebruikers van Gamma software aan het bedrijf zijn gesteld. Uit de documenten blijkt dat het Korps Landelijke Politiediensten (KLPD), tegenwoordig de landelijke eenheid van de Nationale Politie, sinds 2012 een klant is van Gamma Group. De Wikileaks documenten bevatten een overzicht van zestien licenties die het KLPD heeft aangeschaft.

Het KLPD wordt aangemerkt als klant '20FEC907'. Dit is een code, die is gekoppeld aan een naam: het KLPD uit Nederland. Nader onderzoek toont aan dat een Nederlandse politiefunctionaris de contactpersoon is met het bedrijf: Jochem van der Wal. Deze persoon werd aan zijn PGP-Key identiteit herkend door Twitter persoonlijkheid '@DrWhax', Jurre van Bergen.

Wie is Jochem van der Wal? Van der Wal wordt in 2007 en 2008 regelmatig in de media aangehaald. Emerce.nl noemt van der Wal in relatie tot een congres op 14 juni 2007 over de politie en SPSS (Data collectie, voorspellende analyses en netwerken met collegae – De politie als getuige). Hij zal als KLPD politiefunctionaris op het congres spreken

over 'digitaal forensische analyse onder handbereik van het tactische onderzoekstraject door toepassing van de Digitale Wasstraat.' *Predictive policing*, een net woord voor *profiling*, is toch iets anders dan digitaal inbreken, maar Van der Wal werkt dan al voor het KLPD.

Techzine wijdt in september 2008 een artikel aan SPSS (Statistical Package for the Social Science). SPSS is software die in de sociale wetenschappen voor statistieken wordt gebruikt, en wordt ontwikkeld door het gelijknamige bedrijf. In het artikel (SPSS helpt politie bij voorspellen van misdaad) wordt Van der Wal aangehaald als ICT-specialist bij het KLPD.

Ook in het buitenland wordt het werk van Van der Wal opgemerkt. *Hendon Publishing* publiceert in december 2008 een artikel '*Police departments fighting crime with predictive analytics software.'*, waarin van der Wal wordt omschreven als '*technical engineer at KLPD*.' In een interview met *Hendon Publishing* zegt Van der Wal: '*After implementing text-mining software and deploying it to a crime case, we found an essential connection within just five minutes—which we couldn't have found in the past three months of investigations*.' Hij heeft het over de digitale wasstraat die is ontwikkeld door het KLPD. Hij noemt het 'Open Computer Forensic Architecture (OCFA), the '*digital washing machine', which creates an automated index out of the unstructured contents of a PC's hard drive, enabling investigators to perform keyword searches for evidence.*'

Copyright op OFCA zou liggen bij het KLPD met als contactadres ocfa@dnpa.nl. Dnpa.nl werd 4 april 2005 geregistreerd door het KLPD. DNPA staat voor Dutch National Police Agency en de afkorting wordt bijvoorbeeld gebruikt op github.com en andere websites. Van der Wal hanteert het al in 2002 voor een artikel in de bundel '*Dealing with the data flood, mining data, tekst and multimedia*.' Hij is dan al werkzaam voor het KLPD: '*J. van der Wal, Msc. Duch National Police, Criminal Investigation Department. Research and Development, Driebergen – Rijsenburg, the Netherlands.*'

Van der Wal is anno 2016 nog steeds werkzaam bij de landelijke eenheid (voorheen KLPD). Dit blijkt uit de *acknowledgement*-pagina van Tim Cocx, die in 2016 zijn Phd afrondde aan de Universiteit van Leiden. Cocx bedankt enkele medewerkers van de landelijke eenheid van de Nationale politie voor hun steun aan zijn onderzoek, waaronder Jochem van der Wal.

Daarnaast worden ook Ton Holslag (Dienst Specialistische Recherche Toepassingen), Wil van Tilburg (Coördinator informatieverzoeken), Leen Prins (adviseur expertise bij de Dienst Internationale Politie Informatie (IPOL) van het KLPD) en Henry Willering genoemd. Deze laatste komt ook naar voren in de in 2015 openbaar gemaakte Wikileaks documenten over Hacking Team. Willering is hoofd van de afdeling technologie en expertise ontwikkeling (Research and Development) van de nationale eenheid en de baas van Jochem van der Wal.

Inzet van FinSpy en FinSpy Mobile

Uit de Wikileaks documenten blijkt dat de Nederlandse politie, gedurende de vier jaar dat het met Gamma Group heeft samengewerkt, zestien licenties voor het gebruik van FinSpy / Fin Mobile heeft afgenomen. Sommige licenties eindigen na 2014 (het jaar waarin Gamma Group is gehackt). In totaal zou het gaan om 58 doelen, waarmee naar alle waarschijnlijkheid wordt gedoeld op computers, smartphones en andere digitale hulpmiddelen (en niet op individuen).

De Nationale Politie geeft, in antwoord op het WOB verzoek van Buro Jansen & Janssen, geen enkele informatie over de inzet van FinFisher. Er zijn echter aanwijzingen die wijzen op het gebruik van FinFisher door de Nederlandse politie.

Computerworld meldt op 8 augustus 2014 (naar aanleiding van de publicatie van de Wikileaks documenten over Gamma Group) dat het al eerder duidelijk was dat de politie digitale wapens inzette: *'Dat de Nederlandse politie wel dergelijke software gebruikt, werd duidelijk in het begin van dit jaar, bij de geslaagde operatie om een zedenverdachte op te pakken. Op diens PC in een vakantiebungalow werd spionagesoftware geplaatst. Welke software is verder nooit bekend gemaakt en ook nu doen politie en justitie geen mededelingen over welke type software zij gebruiken voor opsporingsdoeleinden.'*
Het is overigens niet duidelijk of deze operatie is geslaagd, de rechtszaak tegen de verdachte loopt nog.

Volgens de politie werden bij deze zaak van begin december 2013 tot en met half januari 2014 keyloggers ingezet. Het ging om zogenaamde doelen (digitale hulpmiddelen) die werden besmet, waarvan er één mislukte. Er zouden twee computers als doelwit zijn uitgekozen.

Dit kan overeenkomen met een van de hulpvragen die door de Nederlandse politie aan Gamma Group/FinFisher zijn gesteld en die gaan over het feit dat het digitale wapen FinSpy door het anti-virus programma AVG werd ontdekt. Een hulpvraag meldt: '*Some functionality of the agent/system do not work when the AVG AV tool is active. For example the keylogger module.*' In een andere hulpvraag wordt gewag gemaakt van dezelfde foutmelding: '*AVG anti virus tool detects generated infection on agent.*'

De Wikileaks documenten bevatten in totaal negen hulpvragen van de Nederlandse politie aan Gamma Group. Enkele hulpvragen gaan over '*non encrypted audio traffic between mobile target and server*' en '*non encrypted SMS traffic between mobile target and system*.' Dit kan betekenen dat een derde partij de gegevens kan onderscheppen.

Een andere hulpvraag gaat over een '*Android bug easy to reverse engineer and easy to find in target.*' Dit kan betekenen dat het doel waartegen de politie het digitale wapen inzet, door het slachtoffer zelf of door anderen gemakkelijk kan worden opgespoord.

Uit de Wikileaks documenten wordt niet duidelijk of de geconstateerde gebreken aan de software zijn verholpen. Evenmin is duidelijk of de politie naar aanleiding van de ondervonden problemen heeft besloten om het verkregen bewijsmateriaal voor de inbraken niet te gebruiken. Ook in de beantwoording van het WOB verzoek verstrekt de Nationale Politie hier geen informatie over.

Andere vraagtekens

Er kunnen ook andere vraagtekens gezet worden bij de aanschaf van FinFisher en bij de handel met Gamma Group.

Nederland bevindt zich als FinFisher gebruiker in een dubieus gezelschap. Gamma Group heeft het digitale wapen ook verkocht aan een reeks repressieve regimes die het hebben ingezet tegen onder meer oppositieleden, journalisten en mensenrechtenactivisten. Met de publicatie van de Wikileaks documenten in 2014 en de gehackte gegevens van Gamma Group zijn de details over de klantenkring van Gamma Group in de volle openbaarheid gekomen. Maar ook daarvoor was er al het nodige bekend. In 2011 ontdekten activisten tijdens de

Arabische Lente dat dictator Moebarak voor meer dan drie ton aan FinFisher spyware had aangeschaft. In 2012 volgden onthullingen over de inzet van FinFisher in Bahrein.

Ook bij de financiële integriteit van het bedrijf kunnen vraagtekens geplaatst worden. De wijze waarop de Gamma Group is georganiseerd, maakt het tot een perfecte constructie om gelden weg te sluizen naar belastingparadijzen, al dan niet via andere bedrijven. Verschillende bedrijven van de Gamma Group zijn nooit veel geld waard geweest. Gamma Group, zoals het bedrijf zich presenteert op beurzen, is gevestigd in het belastingparadijs Britse Maagdeneilanden, op naam van Gamma Group International Ltd. Daarnaast heeft Gamma Group vestigingen in Libanon (Gamma Group International Sal), Cyprus en Singapore, landen die bekend staan als belastingparadijzen.

Politie nog geheimzinniger dan AIVD

De Nationale Politie heeft de beschikking over de FinFisher, maar wenst geen verder informatie te geven. Geheimzinnigheid is troef. Een grondige bestudering van de beantwoording van het WOB verzoek leert dat de Nationale Politie ten aanzien van FinFisher nog geheimzinniger doet dan het normaliter doet bij de beantwoording van WOB verzoeken.

De beantwoording is nog ondoorgrondelijker dan de gebruikelijke beantwoording van inlichtingendiensten in het kader van de WIV (Wet op de Inlichtingen- en Veiligheidsdiensten). Bij inzageverzoeken in het kader van de WIV wordt vaak gesteld dat 'met betrekking tot aangelegenheden die voor de taakuitvoering van de AIVD nog wel actueel zijn, uitdrukkelijk geen mededeling worden gedaan, ook niet ten aanzien van de vraag of dergelijke gegevens wel of niet aanwezig zijn.'

De Nationale Politie antwoordt ten aanzien van FinFisher: 'Indien zoals in het onderhavige geval, uw verzoek om informatie ziet op het openbaar maken c.q. verstrekken van informatie over met name genoemde bedrijven waarmee de politie overeenkomsten c.a. zou kunnen hebben, vormt dit een onaanvaardbaar risico voor die overeenkomsten c.a..'

Het is opmerkelijk dat hier gesproken wordt over onaanvaardbaar risico voor de overeenkomst. In 2014 weigerde het Ministerie van Veiligheid en Justitie namelijk nog om informatie te verstrekken vanwege de risico’s ten aanzien van de inzetbaarheid van het middel. Op 8 augustus 2014

stelde woordvoerster Sentina van der Meer van het ministerie in *Computerworld*: *'Het verstrekken van informatie over welke specifieke software opsporingsdiensten beschikken een onaanvaardbaar risico vormt voor de inzetbaarheid van die middelen. Mede om die reden hebben de verwervingstrajecten van deze middelen onder geheimhoudingsverklaring plaatsgevonden.'*

Plaatsvervangend Politiechef/Hoofd Operatie Landelijke Eenheid Theo van der Plas struikelt in de beantwoording van het WOB verzoek dan ook bijna over zijn woorden: 'Onder meer dit gegeven c.q. deze omstandigheid verhindert dat wordt meegedeeld dat er geen gegevens bij een bestuursorgaan berusten die op uw verzoek om informatie zien en eveneens moet worden geheimgehouden dat er wel gegevens bij een bestuursorgaan berusten. Daarom kan ik geen mededeling doen of de gevraagde informatie in documenten is vastgelegd, dan wel al dan niet bij een bestuursorgaan berusten.'

In gewoon Nederland: de politie kan geen mededeling doen of dergelijke gegevens wel of niet aanwezig zijn. In de beantwoording van het WOB verzoek ontbreekt zelfs een motivering: 'Een nadere motivering van dit oordeel is uit de aard van de aangelegenheid dan wel de aard en/of inhoud van de gevraagde informatie niet te geven, zonder zicht te bieden op de al dan niet aanwezigheid van de door u gevraagde informatie.'

De Nationale Politie is hiermee nog ondoorgrondelijker dan de AIVD normaliter is in reactie op verzoeken op grond van de WIV. Hoewel inlichtingendiensten in het kader van de geheimhouding vaak ook gebruik maken van onnavolgbare redeneringen, verwijzen inlichtingendiensten meestal naar wetsartikelen die in ieder geval de wettelijke basis voor de weigering verduidelijken. Bij de AIVD gaat het dan om niet verstrekking in verband met 'het actueel kennisniveau van de AIVD (WIV artikel 53, lid 1); bronnen van de AIVD en/of zijn rechtsvoorgangers (WIV artikel 55, lid 1 onder b, in samenhang met artikel 15, aanhef en onder b); werkwijze van de AIVD en/of zijn rechtsvoorgangers (WIV artikel 55, lid 1 onder b).'

De Nationale Politie bedient zich van een vergelijkbaar ondoorgrondelijk jargon als Louthean Nelson en zijn bedrijf Gamma Group. Bij het bedrijf zelf is nauwelijks te doorgronden wie de ontwikkelaars van FinFisher en wie de partners en/of tussenhandelaren van Gamma Group zijn. De Nationale politie is onderdeel geworden van het spiegelpaleis van Louthean Nelson.

Besluit Nationale politie op Wob verzoek over Hacking Team, Gamma Group en Providence

Boeven vangen met dubieuze software van dubieuze bedrijven

Gamma Group/Louthean Nelson; Wapenhandelaars pur sang

Bedrijfsprofiel Gamma Group/Louthean Nelson; wapenhandelaars pur sang (pdf)

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

Gehele Observant #69 Politie Mercenaries

Door Wikileaks openbaar gemaakte stukken over Gamma Group/FinFisher

CitizenLab over FinFisher

CitizenLab diverse artikelen over FinFisher

gebruik FinFisher Nederlandse politie

gebruik FinFisher Nederlandse politie support

Kamervragen FinFisher/Gamma Group