De Nederlandse politie en Hacking Team
Flirten met de tools van de dictator

Uit de in 2015 gepubliceerde Wikileaks documenten over Hacking Team blijkt dat de Nederlandse politie sinds 2012 contacten onderhoudt met het omstreden Italiaanse computerbedrijf Hacking Team. In antwoord op het WOB verzoek van Buro Jansen & Janssen antwoordt de Nationale Politie echter dat er geen documenten zijn die betrekking hebben op Hacking Team.

Het Italiaanse computerbedrijf Hacking Team verkoopt software aan politie- en veiligheidsdiensten, waarmee versleuteld digitaal dataverkeer kan worden ontcijferd en afgeluisterd. Het bekendste digitale wapen van Hacking Team is Remote Control System (RCS) - eerst onder de naam DaVinci later Galileo RCS. Hiermee kan worden ingebroken op telefoons en computers en toegang worden verkregen tot alle aanwezige programma's en accounts, zoals Skype of Facebook.

In 2015 werd Hacking Team zelf gehackt. De gepubliceerde Wikileaks documenten bevatten veel informatie over de contacten tussen de Nederlandse politie en Hacking Team. Het blijkt dat Nederlandse politiefunctionarissen sinds 2013 presentaties van Hacking Team hebben bijgewoond en verregaande interesse hadden in de aanschaf van de Galileo software.

Op grond van de Wet Openbaarheid van Bestuur (WOB) heeft Buro Jansen & Janssen bij de Nationale Politie documenten opgevraagd met betrekking tot contacten met (onder andere) Hacking Team. De politie antwoordt als volgt: '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 Hacking Team en/of vergelijkbare namen'.

Dat de politie geen contract heeft met Hacking Team, dat kan kloppen. Ook de Wikileaks documenten bevatten geen bewijs dat Nederland software van Hacking Team heeft aangeschaft. Dat de politie in het geheel geen documenten heeft betreffende Hacking Team, kan echter ten minste merkwaardig genoemd worden. Handelden de politiefunctionarissen die contact onderhielden met Hacking Team

dermate op eigen initiatief dat dit op geen enkele manier binnen de centrale politieorganisatie is vastgelegd?

Mailinglijst Hacking Team

Buro Jansen & Janssen heeft de politiefunctionarissen die op een of andere manier contact hadden met Hacking Team in kaart gebracht. En gereconstrueerd wanneer en op welke wijze verschillende functionarissen contact hadden met Hacking Team. Men zou verwachten dat hierover iets schriftelijk is vastgelegd.

In de Wikileaks documenten van Hacking Team komen diverse e-mail adressen en e-mails voor van Nederlandse politiefunctionarissen. Deze stonden allemaal of op een mailinglijst van het bedrijf, of hadden/hebben direct contact met een van de werknemers van de firma. Zo vraagt David Vincenzetti, baas van Hacking Team, op 15 januari 2015 aan Raymond van Bergem welk van de adressen hij moet verwijderen van de mailinglijst van het bedrijf.

Vincenzetti schijft dat er tien politie.nl adressen op de lijst staan namelijk: @rijnmond.politie.nl, @flevoland.politie.nl, @limburg-zuid.politie.nl, @klpd.politie.nl, @haaglanden.politie.nl, @rijnmond.politie.nl, @haaglanden.politie.nl, @klpd.politie.nl, @limburg-zuid.politie.nl, @ssc-noord.politie.nl. De documenten bevatten de namen van 22 politiefunctionarissen, mailadressen die verwijzen naar 'nl' of 'politie'.

Van de landelijke politie-eenheid stonden Henry Willering (Hoofd van de afdeling technologie en expertise ontwikkeling), Jan Noordam (Dienst Specialistische Recherche Toepassingen), Marco van Berkel (Hoofd product ontwikkeling), Felix Nijpels (Dienst Landelijke Operationele Samenwerking (DLOS) Afdeling Technologische Ontwikkeling & Expertise (ATOE)), Chris Oornick (Interceptie Specialist), Fred Wemeijer en Wilbert Paulissen (chef van de Nationale Recherche) op de mailinglijst.

Ook de naam van Joost van Slobbe (voorheen programmaleider Nationale Politie en nu Hoofd Opsporingsinformatie Inspectie Sociale Zaken en Werkgelegenheid) stond op de lijst toen hij in dienst was bij de politie, alsmede zijn toekomstige collega’s digitale expertise bij de SIOD, thans Inspectie Sociale Zaken en Werkgelegenheid, Stefan Timmermans en Jelle Oorebeek.

Verdere bestudering van de WikiLeaks-documenten maakt duidelijk welke agenten zich nog meer hadden aangemeld voor de mailinglijst van Hacking Team. Van de Haagse eenheid komen Christophe Ruijs (IT-onderzoeker), Martin Beekink en Tim Mizee (Operationeel Specialist A, Contra Terrorisme en Radicalisering, Regionaal Informatie Knooppunt Den Haag) voor tussen de stukken. Van de Rotterdamse eenheid Frans Nab (Regionaal InformatieCentrum), Paul Spek en de al eerder genoemde Raymond van Bergem. De Amsterdamse eenheid was vertegenwoordigd door Manon den Dunnen (voorheen Team Digitale Expertise politie Amsterdam nu Nationale Politie).

Limburg is vertegenwoordigd door Jan Immeker en Hans Musters en Midden Nederland via Bert Aben (digitaal rechercheur). Van de eenheid Oost Nederland Jos van den Oetelaar (in de jaren '90 Regionale Criminele Inlichtingen Dienst (RCID) Noord- en Oost-Gelderland chef informatieverwerking, vervolgens Digitale Recherche van de Bovenregionale Recherche Zuid-Nederland, daarna Technische expert technische surveillance en ondersteuning Noord- en Oost-Gelderland Criminele Inlichtingen Eenheid en nu operationeel specialist A bij Digitale Opsporing Oost-Brabant) en Martijn Hekster (Eenheid Oost, Dienst Regionale Recherche, Digitale Expertise voorheen Politie Gelderland-Zuid, Divsie Centrale Operationele).

Noord Nederland (Friesland, Groningen en Drenthe) hebben Peter Silk (Shared Service Center Noord Nederland) op de lijst staan. Noord-Holland, Zeeland en West-Brabant zijn niet vertegenwoordigd maar wel de overzeese gebiedsdelen via Paul Wessels van de eenheid op de Nederlandse Antillen (Recherche SamenwerkingsTeam).

De mailinglijst waar de politiefunctionarissen op geabonneerd waren, voorziet in krantenartikelen uit bijvoorbeeld de Britse *Financial Times* en de Amerikaanse *Wall Street Journal*. Onderwerpen waren niet alleen spionage ('*Berlin Says U.S. May Be Spying on Merkel's Phone*') maar ook het geopolitieke machtsspel tussen verschillende grootmachten ('*Washington fears losing Greece to Moscow*') en de economische crisis ('*Greece asks eurozone for third bailout*').

De nieuwsservice lijkt op die van andere ondernemingen uit de private inlichtingenwereld zoals Stratfor en Global Info. Stratfor werd in 2011 gehackt door onder anderen Jeremy Hammond die daarvoor een celstraf van tien jaar uitzit. De documenten van Stratfor maken duidelijk dat

vooral actiegroepen en de oppositie in diverse landen in de gaten worden gehouden door dit soort bedrijven. Ditzelfde geldt voor Hacking Team dat zich niet alleen richt op het verspreiden van informatie, maar ook op het offensieve werk, zoals het inbreken in computers en telefoons van mensen.

Correspondentie HT met Nationale Politie

Het contact tussen Hacking Team en Nederlandse politiefunctionarissen betrof echter niet enkel aanmelding voor de mailinglijst of nieuwsbrief. Uit de Wikileaks documenten wordt duidelijk dat Nederlandse politiefunctionarissen serieuze interesse hadden in de aanschaf van digitale wapens van Hacking Team, met name de RCS Galileo.

Op 5 november 2014 beantwoordt Massimiliano Luppi van Hacking Team een e-mail van de Nederlandse politiefunctionaris Henry Willering, hoofd van de afdeling technologie en expertise ontwikkeling van de landelijke eenheid Nationale Politie. Willering bezocht samen met enkele collega's van 20 tot en met 22 oktober 2014 de Milipol Qatar. Op deze 'Homeland Security' beurs namen zij onder meer een kijkje bij de infokraam van Hacking Team en kregen hier een demonstratie voorgeschoteld.

Luppi stuurt Willering naar aanleiding van de show in Qatar een reclameboodschap via e-mail: '*Since you showed interest in our product, I take the occasion to send you some information related to the latest version of Remote Control System, codenamed Galileo. Galileo is designed to attack, infect and monitor target PCs and Smartphones, in a stealth way. It allows you to covertly collect data from the most common desktop operating systems*.'

Willering antwoordt op 5 november 2014: '*We of course do remember your demonstration and explanation of Galileo in Qatar very well!'*. Hij deelt zijn mail aan Luppi met Marco van Berkel, hoofd productontwikkeling bij de landelijke eenheid, en Jan Noordam van de Dienst Specialistische Recherche Toepassingen. De heren reageren enthousiast aan Hacking Team: '*We are discussing your 'product' and your offer to visit us with the people in our department responsible for the deployment of solutions like Galileo. We need a couple of days to do that and to respond to you. So I guess we will be in touch with you next week*.'

Luppi antwoordt Willering op 12 november 2014, en krijgt meteen antwoord: *'Ben afwezig tot vrijdag 14 november.'* De WikiLeaks documenten bevatten geen verdere mailwisselingen meer tussen Hacking Tea en Henry Willering.

Providence als tussenpersoon

In 2015 is er opnieuw contact tussen de politie en Hacking Team. Uit de Wikileaks documenten wordt duidelijk dat het bedrijf Providence hierbij als intermediair optreedt en een afspraak probeert te regelen tussen de Nationale Politie en Hacking Team.

Providence is een Brits security bedrijf dat trainingen aanbiedt en apparatuur verkoopt. Het is zelf geen producent van digitale wapens. Uit de Wikileaks documenten wordt duidelijk dat het bedrijf tevens als tussenhandelaar in digitale wapens actief is. Providence heeft ook een duidelijke Nederlandse connectie in de persoon van Peter Stolwerk, een voormalig politieman die sinds 2012 de Nederlandse vestiging van Providence (Providence BNLX) leidt. Stolwerk heeft al eerder geprobeerd om een samenwerking tussen Providence en Hacking Team tot stand te brengen in onder meer Australië en Ecuador.

Stolwerk probeert in 2015 een bijeenkomst te organiseren met Hacking Team en de Nationale Politie. Stolwerk heeft hiervoor zijn contacten binnen de politie- en inlichtingendienst aangeboord. Na afloop van de ISS World Europe beurs in Praag neemt Stolwerk op 8 juni 2015 contact op met Philippe Vinci van Hacking Team om een afspraak met de Nationale Politie te plannen.

Vinci wil zo snel mogelijk de data voor de afspraak weten, omdat hij een specialist moet meenemen voor de presentatie. Veel medewerkers van Hacking Team houden zich bezig met de acquisitie, slechts enkelen kunnen de software daadwerkelijk bedienen. '*Regarding the trip to the Netherlands and the presentation/demo to National Police (ex KLPD) and Netherland Intelligence, let me know which are the best dates/alternatives so that we can book the week and the presence of a Field Application Engineer.*', antwoordt Vinci nog op dezelfde dag.

Stolwerk beweert vervolgens dat de politie hem enkele uren later heeft geantwoord: '*The police just came back to us that they would like to have a demonstration in the first two weeks of july (that is when their*

main technician will be present)'. Vinci laat Stolwerk weten dat de voorkeur van Hacking Team uitgaat naar de tweede week van juli 2015. Vinci schrijft tevens dat hij de namen van de twee Nederlandse agenten zal opzoeken die eerder interesse voor de software van de Italianen toonden: '*I will also send you tomorrow the names of the 2 persons from KLPD that visited our booth in UK Security & Policy (Farnborough), so that you could check if they are in the same organization*.'

Stolwerk, Van de Oetelaar, Wemeijer

Het betreft hier de agenten Jos van den Oetelaar, in 2015 werkzaam bij de eenheid Oost Nederland en het jaar daarop operationeel specialist A bij Digitale Opsporing Oost-Brabant, en Fred Wemeijer van de landelijke eenheid. Van den Oetelaar en Wemeijer bezochten begin maart 2015 de Security & Policing beurs van het Britse Ministerie van Binnenlandse Zaken in Farnborough en kregen een presentatie over RCS Galileo.

Vinci schrijft op 16 juni 2015 aan Stolwerk: '*Jos visited our booth during the Security & Policing UK conference in Farnborough. He stayed quite long with us, almost 50 minutes, during which we did a very complete demonstration of Galileo. So he was able to see different infections (PC and mobiles) and have a look at the evidence that were collected*.'

Jos van den Oetelaar kent Hacking Team al geruime tijd. Uit de Wikileaks documenten blijkt dat hij al in 2013 tijdens een bezoek aan een beurs interesse had getoond in de software van Hacking Team. Van den Oetelaar en Hacking Team correspondeerden in deze periode al met elkaar. Zo tutoyeerde Van den Oetelaar op 2 september 2013 David Vincenzetti, de baas van Hacking Team: '*Hi David and a very good afternoon from The Netherlands. I temporary have another position within the National Police organisation. (…) When I'am back in my orginal job and office I let you know! Jos van den Oetelaar, Specialist Technical Surveillance and Support*.' Een maand later benaderde Emad Shehata van Hacking Team van den Oetelaar: '*I found that you visited our booth at Security & Policing 2013 and on behalf of Hacking Team I would like to thank you again*.'

Stolwerk kent Van de Oetelaar klaarblijkelijk ook. Stolwerk meldt op 15 juni 2015 dat Van den Oetelaar niet op de bijeenkomst van de Nederlandse politie met Hacking Team aanwezig zal zijn: '*Yes I know those Police Officers really well. Especially Jos van de Oetelaar. He is*

actually promoted as a chief of the National Technical Support unit. I don't believe they will be present at this meeting as you will meet the cyber and digital forensics department', aldus Stolwerk.

Stolwerk beweert in zijn e-mail van 15 juni 2015 een bijeenkomst te hebben georganiseerd met de landelijke politie-eenheid op 6 juli 2015: '*meeting confirmed on the 6th (after lunchtime) for the presentation. They arranged a secure facility with the necessary requirements*.' Volgens Stolwerk doen de agenten nogal geheimzinnig over de locatie: '*They are a bit secretive about it*.'

Geen openbaarheid

Uit de Wikileaks documenten wordt niet duidelijk of de op 6 juli 2015 geplande presentatie daadwerkelijk heeft plaatsgevonden. Hacking Team werd in deze periode zelf gehackt, waarna interne bedrijfsgegevens via Wikileaks op straat kwamen te liggen.

De Kamerleden Oosenburg (PvdA) en Verhoeven (D66) stellen in 2015 Kamervragen naar aanleiding van de hack van Hacking Team, onder meer over de presentatie: "Klopt het dat het bedrijf Hacking Team een productpresentatie zou houden voor de NP over hun producten? Is deze presentatie doorgegaan, na de ingrijpende inbraak bij het bedrijf?". Het Ministerie van Veiligheid en Justitie gaat in haar beantwoording echter niet in op deze vraag.

In antwoord op het WOB verzoek van Buro Jansen & Janssen geeft de Nationale Politie geen enkele informatie over de contacten met Hacking Team, ook niet over de presentatie van 6 juli 2015, de inhoud van deze presentatie, en welke personen hier aanwezig zouden zijn. Evenmin maakt de politie duidelijk of er sindsdien verdere contacten met Hacking Team hebben plaats gevonden en er wellicht een nieuwe presentatie is gepland.

Het gebrek aan openbaarheid roept vraagtekens op. Handelen de politiefunctionarissen die contact onderhielden met Hacking Team dermate op eigen initiatief dat dit op geen enkele manier binnen de centrale politieorganisatie is vastgelegd ?

En hoe zit het met het ethische aspect van zaken doen met Hacking Team? Onder de klanten van Hacking Team bevinden zich veel

repressieve staten die het niet zo nauw nemen met de naleving van de mensenrechten, en die de digitale wapens van Hacking Team onder meer inzetten tegen oppositieleden, journalisten en mensenrechtenactivisten.

Dit is al enige jaren bekend. Zo werd in 2012 bekend dat de Marokkaanse geheime dienst digitale wapens van Hacking Team inzette tegen journalisten van *Mamfakinch*, en dat activisten in de Verenigde Arabische Emiraten slachtoffer van werden van overheidsspionage door middel van Hacking Team software. In 2014 publiceerde CitizenLab een onderzoek naar de digitale infiltratie van Ethiopische journalisten door het Ethiopische regime met behulp van software van Hacking Team. In april 2014 vroegen verschillende NGO's waaronder Amnesty International en Human Rights Watch, verenigd in de coalitie CAUSE(Coalition Against Unlawful Surveillance Exports) aandacht voor de export van surveillance apparatuur of software. Hacking Team werd in de documenten van CAUSE expliciet genoemd.

De Nationale Politie onderhoudt sinds 2013 uitvoerig contacten met Hacking Team. Uit niets blijkt dat de mensenrechtenreputatie een rol heeft gespeeld bij de overweging om met het bedrijf zaken te doen. Volgens het Nationaal Actieplan Beleidsleven en Mensenrechten verlangt de Nederlandse overheid van de aan hen leverende bedrijven dat ze de mensenrechten respecteren en dat de overheid de stakeholdersdialoog bevordert. Uit niets blijkt of en hoe de Nationale Politie hier in haar contacten met Hacking Team invulling aan heeft gegeven.

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

Boeven vangen met dubieuze software van dubieuze bedrijven

Hacking Team/David Vincenzetti; Italiaanse staatsnerds in dienst van dictators

Bedrijfsprofiel Hacking Team/David Vincenzetti; Italiaanse staatsnerds in dienst van dictators (pdf)

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

Gehele Observant #69 Politie Mercenaries

Wikileaks Hacking Team documenten

CitizenLab onderzoek naar Hacking Team

CitizenLab diverse artikelen over Hacking Team

Enkele e-mails uit Hacking Team met de politie

Kamervragen Hacking Team

Adressen e-maillijst van Hacking Team