Hacking Team/David Vincenzetti
Italiaanse staatsnerds in dienst van dictators

Het in 2003 opgerichte Italiaanse computerbedrijf Hacking Team heeft zich in dertien jaar tijd ontwikkeld van een handelaar in beveiligingssoftware waarmee bedrijven zich kunnen weren tegen digitale inbraak, tot aan een specialist in offensieve wapens om documenten op internet aangesloten apparatuur in te zien en af te luisteren.

In 2006 presenteerde Hacking Team de eerste versie van haar digitale wapen Remote Control System (RCS) onder de naam DaVinci uit. Later verandert de naam in 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.

De digitale wapens van Hacking Team zijn gewild. Het bedrijf heeft een bedenkelijke reputatie. Onder meer vanwege het leveren van offensieve software aan autoritaire regeringen die ze hebben ingezet tegen oppositieleden, journalisten en mensenrechtenactivisten. De volle omvang werd duidelijk met de hack van Hacking Team in juli 2015 waarmee 400 GB aan interne data van het bedrijf (waaronder klantgegevens en emailcorrespondentie) in de openbaarheid kwamen.

Terug in de tijd

De Italianen David Vincenzetti en Valeriano Bedeschi richten in 2003 Hacking Team op. Beiden zijn nog altijd werkzaam bij het bedrijf: Bedeschi op de achtergrond, Vincenzetti altijd op de voorgrond.

David Vincenzetti is technisch onderlegd. Hij werkt van 1989 tot 1992 voor Hewlett Packard Italia als training course instructor. Vervolgens is hij tot 1996 werkzaam bij de Universiteit van Milaan als medewerker op de afdeling '*Dipartimento di Scienze dell'Informazione*'. Als '*Assunto ex. Art. 26*' is hij verantwoordelijk voor '*network & security laboratori siLAB*'.

Vincenzetti houdt zich in het begin van de jaren '90 vooral bezig met de beveiliging van computersystemen en de inzet van defensieve digitale wapens op het internet. In mei 1995 geeft hij bijvoorbeeld samen met

Stefano Taino, collega op de universiteit, twee lezingen tijdens een Italiaanse Unix bijeenkomst. Unix is een open source besturingsprogramma waar een gemeenschap gezamenlijk aan werkt om die te ontwikkelen. De lezingen gaan over Unix system & Network security en internet Firewall.

Een maand later spreken Vincenzetti, Taino en Fabio Bolognesi (eveneens werkzaam op de Universiteit van Milaan) op een bijeenkomst over computerbeveiliging in Salt Lake City in de Verenigde Staten. De drie Italianen presenteren zich hier als het 'Computer Emergency Resource Team Italy (CERT-IT)' van de informatie technologie faculteit van de Universiteit van Milaan. Ter introductie van hun presentatie schrijven zij: '*Eavesdropping is becoming rampant on the Internet. We, as CERT_IT, have recorded a great number of sniffing attacks in the Italian community. In fact, sniffing is the most popular hacker's attack technique all over the Internet (juni 1995)*.'

In hun presentatie stellen zij dat er vooral door overheden veel wordt afgeluisterd op het internet. Zij omschrijven dit als een soort sniffen, het rondneuzen in computersystemen. In hun presentatie claimen zij een beveiligd systeem hebben ontwikkeld om dat sniffen te verhinderen: '*This paper presents a secure telnet implementation which has been designed by the Italian CERT, to make eavesdropping ineffective to remote terminal sessions. It is not to be considered as a definitive solution but rather as a 'bandaid' solution, to deal with one of the most serious security threats of the moment.*'

Tijdens zijn werkzaamheden voor de Universiteit van Milaan is Vincenzetti tevens betrokken bij twee bedrijven. Van 1992 tot 1995 is hij voor de helft eigenaar van het bedrijf ISAC Snc (Information Security And Cryptography) en heeft hij in dit bedrijf ook een management functie. Ook neemt Vincenzetti van 1995 tot 1997 voor 33 procent deel aan CryptoNet Spa. Beide bedrijven, maar vooral CryptoNet, houden zich bezig met defensieve middelen op het internet. CryptoNet levert oplossingen voor antimalware, anti-DDos en anti-defacement, antimalvertising en security awareness. Vincenzetti's voormalige collega op de universiteit Stefano Taino is momenteel nog steeds werkzaam voor CryptoNet als directeur en informaticus.

Interesse voor offensieve strategieën

Vincenzetti houdt zich in de jaren 90 hoofdzakelijk bezig met defensieve

software, maar hij is in het begin van de jaren 90 al wel geïnteresseerd in offensieve software. Kennis die hij later te gelde zal maken voor Hacking Team.

De website *Ars Technica* publiceert op 8 juli 2015 enkele oude bijdragen van Vincenzetti op internetfora. In november 1991 schreef hij bijvoorbeeld over het stelen van wachtwoorden als methode om computersystemen over te nemen: '(…) *written a program that spies pseudo terminals when they are first used by rlogin or telnet or similar programs. I can steal the root password on most unixes in hours, or even minutes. The bug lies on the fact that the idle unallocated ptys are by default mode 666, and so readable and writeable by everyone. The login phase is virtually simulated, the user cannot get aware of what is happening, unless it effectively enters the password, and at that time it is too late. The bug is simple and evident: it's a just a matter of programming skill*.'

In 1992 schreef Vincenzetti op een Usenet forum: '*I have written ATP (Anti Tampering Program), a program that system administrators and `paranoia-users' will find useful. It is a program to make file tampering and nasty-hacking ineffective. ATP snapshots the critical files and you can examine them later, to discover if SOMETHING has changed. There are many options and the program is quite flexible. I cannot explain it here. Just get a copy at ftp site ghost.dsi.unimi.it, under the pub/crypt directory.*' Hij stelde computer beveiligingsprogramma's beschikbaar via de servers van de universiteit. Het is ook de tijd dat hij PGP gaat gebruiken, versleutelde email berichten.

Stefano Zanero, voormalig klasgenoot en momenteel professor op de Universiteit van Milaan, zegt over Vincenzetti: '*He was one [of the] geeks that were beginning to understand how the Internet worked (Foreign Policy 26 april 2016).*' Volgens Zanero dacht Vincenzetti tijdens zijn studietijd al na over de ontwikkeling van digitale wapens: '*The security industry was dominated by companies focused on defending businesses and governments against hackers. But, he wondered, what would happen if hackers were instead unleashed as a mode of security?*'

Keerpunt in Vincenzetti's carrière

Het jaar 1997 vormt een keerpunt in de carrière van Vincenzetti. Hij verlaat de Universiteit van Milaan en stapt in het bedrijf Intesis SpA In minder dan drie jaar tijd werkt het bedrijf zich op tot een bedrijf

gespecialiseerd in oplossingen voor digitale infrastructuur, netwerken en computerbeveiliging. Intesis SpA wordt in 2000 verkocht aan Finmatica Spa, een Italiaanse software onderneming van de succesvolle zakenman Pierluigi Cruel. Vincenzetti bezat 14 procent van Intesis SpA en maakt voor de eerste keer in zijn loopbaan een flinke winst. Hij zal het geld investeren in de oprichting van Hacking Team.

Vincenzetti gaat de commerciële markt op, net als veel van zijn vroegere universitaire collega's van de Universiteit van Milaan. Zo wordt Fabio Bolognesi, met wie Vincenzetti en Taino samenwerkte op de Universiteit van Milaan, Network Security Manager bij het Italiaanse I.Net, een Italiaanse provider. I.Net wordt in 2001 overgenomen door BT, het voormalige British Telecom.

Een andere medestudent en ontwikkelaar van software van de Universiteit van Milaan is Massimo Cotrozzi. Hij bezocht samen met Vincenzetti in oktober 1993 het vierde Unix security Symposium om een voordracht te geven over een door hen ontwikkeld programma, het ATP - Anti-Tampering Program. Ook Cotrozzi maakt na de universiteit carrière in de commerciële sector en werkt twee jaar als adjunct-directeur bij Ernst & Young (EY) in Londen en drie jaar bij KCS Group (Knightsbridge Company Services). KCS Group wordt geleid door een voormalig medewerker van MI6 en is een private inlichtingendienst die ook aan risico management doet. Te vergelijken met Stratfor, Global Info, The Inkerman Group en andere private inlichtingendiensten. Op dit moment is Cotrozzi Director Cyber Security - Cyber Engineering bij Deloitte UK.

Cotrozzi kent de wereld van de private inlichtingendienst en onderhoudt contact met Vincenzetti. In 2012, als Massimo Cotrozzi bij KCS Group werkzaam is, regelt hij een ontmoeting tussen zijn oude vriend Vincenzetti en de baas van KCS. Cotrozzi en Vincenzetti delen sinds 2012 geregeld informatie uit over potentiële klanten.

Zo mailt Cotrozzi op 3 juni 2015, hij werkt dan voor EY in London, dat het hoofd van het Amerikaanse National Cyber Security Program van de FBI, Peter Trahon, en de commandant van Special Investigations van de Amerikaanse luchtmacht, Kevin J. Jacobsen, in Rome zijn. Het gaat om 'classified' informatie die door de Italianen wordt gedeeld: '*I due individui saranno a roma dal 22 al 25 :)*.' De Amerikanen reageren niet.

De beginjaren van Hacking Team

In 2003 richt Vincenzetti, samen met Valeriano Bedeschi, Hacking Team (HT) op. Vincenzetti wordt voor twee derde eigenaar van Hacking Team en Bedeschi voor een derde.

Bedeschi en Vincenzetti kennen elkaar al heel lang. Bedeschi werkte in het verleden (net als Vincenzetti) voor CryptoNet, ISAC en (als technisch directeur) voor Intesis SpA Bedeschi leidt bij Hacking Team de afdelingen voor defensieve software en digitale wapens. In 2004 treedt een andere oude bekende van CryptoNet in dienst bij Hacking Team. Marco Bettini, voormalig collega op de universiteit van Milaan, wordt sales manager van het jonge IT bedrijf.

In de beginjaren van Hacking Team vormen digitale wapens zeker niet het belangrijkste product van het bedrijf. Volgens Alberto Pelliccione, die van 2007 tot 2014 in dienst was bij het bedrijf, was Hacking Team in 2007 een klein bedrijf, waar slechts vier mensen actief werkten aan het produceren van digitale wapens: *”At the time (2007), the company was a small brand that dealt with consulting for other companies, such as large banks who wanted to protect themselves. The year before, the company had begun to work on some offensive hacking solutions, such as the application which is then known as DaVinci, the first version of RCS*'', aldus Pelliccione in een interview met Motherboard (2 november 2015).

Volgens Pelliccione had het bedrijf in 2007 een beperkte ontwikkelafdeling met weinig financiële middelen. In *Ars Technica* van 20 juli 2015 zegt hij: ,,*[When I joined], they were only doing [penetration testing], they were only a defensive unit—the offensive unit had only existed for three months, it was brand new*.''

Remote Control System RCS

De komst van Marco Valleri naar Hacking Team in 2004 speelt een belangrijke rol in de ontwikkeling van digitale wapens door het bedrijf. Valleri werkte eerder voor Intesis SpA (het bedrijf waar Vincenzetti in 2001 vertrok). Valleri vertrekt ook begin deze eeuw bij Intesis en ontwikkelt daarna samen met Alberto Ornaghi (ALoR) de software Ettercap (Ettercap-Graphical).

Ettercap is een van de eerste ‘*man in the middle*’ (MITM) software

applicaties. ‘*Man in the middle*’ is een programma waarmee ingebroken kan worden op datastromen om zo digitale communicatie af te kunnen luisteren, wachtwoorden te stelen en iemands computer van afstand te manipuleren. Inbreken op dataverbindingen behelst een geheel andere techniek dan inbreken in een programma op een computer. In korte tijd werd Ettercap zeer veel gebruikt, zowel door mensen die de veiligheid van hun netwerken wilden controleren als door hackers om op systemen in te breken. Ook de Italiaanse politie bleek al snel geïnteresseerd in Ettercap. *The Verge* schrijft in een artikel van 13 september 2013 dat de Milanese politie rond 2001 al geïnteresseerd bleek in Ettercap en Valleri benaderde met de vraag of zij Ettercap konden aanpassen voor het afluisteren van Skype gesprekken op Windows computers.

In 2006 brengt Hacking Team de eerste versie van het digitale wapen Remote Controle System (RCS) onder de naam DaVinci uit. DaVinci en de opvolger Galileo RCS worden de pronkstukken van Hacking Team en het bedrijf gaat zich uiteindelijk volledig richten op digitale wapens. In 2007 wordt Alberto Pelliccione aangetrokken om de toepasbaarheid van het digitale wapen verder te ontwikkelen. Hij ontwikkelde in het verleden Ettercap en deed onderzoek naar robots en kunstmatige intelligentie. In 2008 trekt Hacking Team ook de andere ontwikkelaar van Ettercap, Alberto Ornaghi ('ALoR'), aan. Zo breidt het bedrijf langzamerhand zijn ontwikkelafdeling uit.

Vincenzetti beschrijft de allereerste versie van RCS in *Foreign Policy* als volgt: '*Think of it as a criminal dossier: A tab marked 'Targets' calls up a profile photo, which a spy must snap surreptitiously using the camera inside the subject’s hacked device. Beside the picture, a menu of technologies (laptop, phone, tablet, etc.) offers an agent the ability to scroll through the person’s data, including email, Facebook, Skype, online aliases, contacts, favorite websites, and geographical location. Over time, the software enables government spooks to build a deep, sprawling portfolio of intelligence.*'

Na het inbreken, neemt het programma de telefoon of de computer van de verdachte over en heeft zo toegang tot alle programma’s en accounts, bijvoorbeeld Skype en Facebook, van de betreffende persoon. Dat inbreken is in het begin nog niet zo eenvoudig. '*Spies must get it into technology quickly and secretly — say, in the seconds a phone passes through security at a border checkpoint. Moreover, each device a target uses must be infected separately. Yet there are myriad options for delivery: a USB, DVD, public Wi-Fi network, or even a QR code disguised*

as something enticing (such as an ad for an escort service)', aldus Vincenzetti.

Eigenlijk is er in de loop der jaren niet veel veranderd aan de tool, al is deze natuurlijk wel verbeterd. Het inbreken, blijft echter een probleem. Dit moet ofwel fysiek met een USB stick of DVD, maar kan ook online via wifi of een netwerk.

De Italiaanse overheid als klant

Hacking Team groeit na de oprichting in 2003 gestaag. Het jaar 2007 is financieel een belangrijk jaar. Het bedrijf haalt twee miljoen euro aan investeringen binnen van twee grote Italiaanse fondsen: 'Next' van Finlombarda SGR S.p.a. en 'Innogest Capital' van Innogest SGR SpA. Het bedrijf groeit gestaag verder. In 2008 werken er 24 mensen voor het bedrijf en dit stijgt naar 26 in 2009, 30 in 2010, en 33 in 2011.

Tot de eerste afnemers van de digitale wapens van Hacking Team in 2004 behoort de Milanese Polizia postale e delle comunicazioni, de Italiaanse digitale recherche die regionaal is georganiseerd. Vincenzetti verklaart in een artikel in Foreign Policy van 26 april 2016 dat de Milanese recherche al in 2003 een eerste prototype van RCS gebruikte. De Spaanse geheime dienst (Centro Nacional de Inteligencia) wordt in 2006 overtuigd door Hacking Team dat met de RCS de Spanjaarden terroristen kunnen vangen.

Het duurt tot 2009 voordat Hacking Team andere Italiaanse klanten werft. In 2009 kan Vincenzetti de Italiaanse Presidenza del Consiglio dei Ministri (PCM, president van de ministerraad) bijschrijven. De PCM is een coördinatie orgaan voor de Italiaanse inlichtingendiensten.

Daarnaast verkoopt Hacking Team haar digitale wapens aan SIO SpA, een privaat bedrijf dat afluistercentrales voor telefoon- en internetverkeer beheert voor bijvoorbeeld het Italiaanse Openbaar Ministerie. Het is een private onderneming die grotendeels afhankelijk is van de Italiaanse staat, maar ook de commerciële markt op mag. SIO SpA heeft samen met Area SpA en Research Control Systems de Italiaanse markt voor afluistercentrales in handen. Er is niet veel openbare informatie bekend over de commerciële klanten van deze drie bedrijven.

In de jaren die volgden sleept Vincenzetti nog een aantal andere belangrijke Italiaanse spelers de opsporings- en inlichtingenwereld binnen. In 2010 bestelt de ROS (Raggruppamiento Operativo Speciale), een speciale eenheid van de Italiaanse politie, voor een half miljoen digitale wapens bij Hacking Team. In 2012 bestelt SIO S.p.a. opnieuw en werd door Vincenzetti bestempeld als een 'vaste' klant. De Italiaanse FIOD, de Guardia di Finanza, sluit zich in 2013 zich bij de andere diensten aan en betaalt Hacking Team vier ton.

Als laatste bekende Italiaanse klant koopt de concurrent van SIO SpA, Area SpA, in 2014 voor ruim vier ton digitale wapens in. Sinds eind 2016 loopt er een justitieel onderzoek in Italië naar illegale export naar Syrië door Area SpA. Het was echter al eerder bekend dat Area SpA samen werkte met het regime van Bashar al-Assad in Syrië.

De Italiaanse overheid als financier

Vincenzetti heeft zich binnen enkele jaren tijd genesteld in de top van de Italiaanse opsporings- en inlichtingenwereld. Met zijn contacten binnen zit hij aan tafel met de hoogste bazen van de inlichtingendiensten.

De verwevenheid tussen Hacking Team en de Italiaanse staat neemt verder toe door de financiële injectie in 2007 door het regionale overheidsfonds 'Next' van Finlombarda SGR SpA en het private fonds 'Innogest Capital' van Innogest SGR SpA dat ook geld van de Italiaanse overheid ontvangt. Beide fondsen hebben een kwart van Hacking Team in handen. 'Next' is een fonds van de regionale overheid waar de regio's Milaan en Lombardije onder vallen. 'Innogest Capital' is een privaat investeringsfonds, maar uitsluitend geïnteresseerd in het Italiaanse bedrijfsleven, vooral startups in de zorg en de digitale sector. Tien procent van het 'Innogest Capital' is in handen van een voormalig Amerikaanse ambassadeur in Italië: Ronald Spogli. Hij is tevens een van de oprichters van het fonds.

De Amerikaanse betrokkenheid bij dit investeringsfonds, en bij de ontwikkeling van Hacking Team, lijkt zelfs verder te gaan. In een interview met het Italiaanse *Panorama* noemt Fernando Napolitano, partner van Innogest SGR, nog een andere Amerikaan die betrokken is bij het fonds: "*Mike McCollough, a Booz&Co. partner and former head of the National Security Agency*".

Waarschijnlijk betreft het hier Michael McCullough die al twee decennia werkt voor Booz Allen & Hamilton, het bedrijf waarvoor ook Edward Snowden werkzaam was. Booz Allen & Hamilton is een bedrijf dat onder andere voor de NSA werkt.

Volgens Napolitano heeft McCullough een rol gespeeld bij het verkrijgen van toegang tot de Amerikaanse markt voor Hacking Team. ,,*It was McCollough himself who met with the young members of the Milan-based Hacking Team, specialists in eavesdropping software used by police forces, the purpose of the meeting being to help them break into the tough US market*", noteert *Panorama* op 8 november 2011. In 2011 en 2012 mocht Hacking Team de FBI (Federal Bureau of Investigation), Department of Defense (Amerikaanse Ministerie van Defensie) en Drug Enforcement Administration (DEA) bijschrijven als klant voor ruim een miljoen euro.

Klanten stromen binnen

Hacking Team groeit vanaf 2007. Het digitale wapen RCS blijkt een zeer gewild product dat kennelijk in behoeften voldoet.

De klantenkring van Hacking Team breidt zich snel uit. Onder de klanten bevinden zich dus Italiaanse overheidsdiensten, veel diensten uit Europese landen (Albanië, Cyprus, Hongarije, Luxemburg, Polen, Spanje, Tsjechië, Zwitserland), maar ook 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.

De omvang van, en de details over, de klantenkring worden pas in juli 2015 in volle omvang duidelijk met de publicatie van de Wikileaks documenten.

Tot de eerste klanten van Hacking Team behoren in 2008 de inlichtingendiensten Infocomm Development Authority of Singapore en Information Office uit Hongarije en in 2009 de Malaysian Anti Corruption Commission. In 2009 wordt ook een andere Hongaarse inlichtingendienst, de Special Service of National Security (SSNS), klant van Hacking Team. Hongarije wordt onder de autoritaire leiding van Viktor Orbán een vaste klant en zal uiteindelijk miljoenen besteden aan digitale wapens. Vanaf 2010 is ook Mexico een grote klant.

Nog voor de Wikileaks in 2015 vinden er echter verschillende onthullingen plaats over controversiële klanten van Hacking Team. Onder meer door onderzoek van het Canadese Citizen Lab (Universiteit van Toronto).

In 2012 gebruikt de Marokkaanse geheime dienst de CSDN digitale wapens van Hacking Team tegen journalisten van *Mamfakinch*. Dit komt in oktober 2012 in de openbaarheid in een onderzoek van Citizen Lab over de inzet van DaVinci van Hacking Team tegen het Marokkaanse journalistencollectief.

Op 10 oktober 2012 publiceert Citizen Lab een rapport over een activist uit de Verenigde Arabische Emiraten: dhr. Mansoor. Hij werd het slachtoffer van overheidsspionage en vervolgens gearresteerd vanwege zijn politieke activiteiten. Mansoor en vier van zijn mede-activisten (de UAE5) werden in 2011 tot drie jaar gevangenisstraf veroordeeld. De president verleende Mansoor gratie, maar zijn veroordeling blijft staan, en zijn toekomst lijkt onzeker. Onderzoek van Citizen Lab toont aan dat Hacking Team achter de spionage van de activisten zat: "Some of the *backdoor* programming code in the *Mamfakinch* infection alluded to a user named "Guido" and the software has been identified as a variant of a commercial spyware marketed by Hacking Team, a Milan company, the report says."

Citizen Lab komt op 12 februari 2014 met een nieuw onderzoek, naar de digitale infiltratie van Ethiopische journalisten door het Ethiopische regime met behulp van software van Hacking Team. Citizen Lab schrijft: "In this report, we identified three instances where Ethiopian journalist group ESAT was targeted with spyware in the space of two hours by a single attacker. In each case the spyware appeared to be RCS (Remote Control System), programmed and sold exclusively to governments by Milan-based Hacking Team."

Begin april 2014 vragen 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 wordt in de documenten van CAUSE expliciet genoemd.

Ondanks de negatieve publiciteit over de controversiële leveranties van Hacking Team, blijft het aantal klanten van het bedrijf stijgen. Het lijkt

welhaast of de negatieve publiciteit als gratis reclame voor het digitale wapen RCS DaVinci en haar opvolger Galileo RCS werkt. In 2009 en 2010 had Hacking Team nog maar vijf klanten per jaar in 2011 stijgt dit tot acht en in 2012 tot vijftien, en in 2013 ook (getallen zijn een benadering van de gegevens van Hacking Team).

Tussenhandel

De lijst van leveranties van digitale wapens door Hacking Team aan repressieve regimes is lang, en wordt in de loop der jaren steeds langer. Soms vindt de handel plaats met behulp van een tussenhandelaar.

Nice Systems (Nice Intelligence Solutions of Nice Ltd), een Israëlisch bedrijf dat handelt in tapcentrales, is een belangrijke tussenhandelaar voor Hacking Team. Privacy International maakt in een onderzoek van november 2014 al duidelijk dat Israëlische bedrijven in Centraal-Azië surveillance software leveren aan repressieve regimes. De tussenhandel van digitale wapens past daar mooi bij: Hacking Team en Nice Systems hebben elkaar iets te bieden. Het onderzoek maakt duidelijk dat Nice Systems Italiaanse digitale wapens levert aan Azerbeidzjan, een land met een bedenkelijke reputatie op het gebied van de mensenrechten. Of de software van Hacking Team tegen journalisten, ngo's of de oppositie werd ingezet, is niet vastgesteld. Ook bemiddelt Nice Systems tussen het repressieve regime in Oezbekistan en Hacking Team over de aanschaf van digitale wapens. Ook andere landen in Centraal-Azië, waaronder Kazachstan, staan op het lijstje van beide bedrijven.

De Italianen en de Israëliërs zijn erg close. Marco Bettini van Hacking Team geeft in een mail toe dat zij de Russische inlichtingendienst als klant hebben. '*Dear Adam. Thank you very much for this opportunity! Please let me be very open to you with regard to FBS. We got in touch with FSB in September 2010 through a Russian Governmental R&D Institution which is acting as a local partner. They visited us last week and they confirmed their interest in our solution. We have provided them with a demo version of our product and they are presently testing it. They are looking forward to setting up a large pilot project in order to test our product in real-life investigation scenarios with multiple targets*', aldus Bettini in een mail aan Adam Weinberg van Nice Systems.

Nice Systems en Hacking Team hebben ook samengewerkt in de leverantie van digitale wapens naar Oeganda. Dit wordt blootgelegd in

een artikel van *Buzzfeed* op 24 augustus 2015: 'Emails Reveal Israeli and Italian Companies Role In Government Spying'. Uit de openbaar gemaakte Wikileaks documenten blijkt dat het Nice Systems als tussenhandelaar voor Hacking Team aan de Oegandese politie heeft geleverd. De Israëliërs en Italianen hebben de Oegandezen geen belemmeringen opgelegd ten aanzien van het gebruik van de geleverde digitale wapens. De digitale wapens zijn ingezet in 2014 tegen LHBT-activisten (lesbisch, homo, bi en trans).

De Oegandese LHBT-activisten zijn het slachtoffer geworden van de zogenoemde Zeus malware, die al eerder door Hacking Team is gebruikt in haar digitale wapens. Een medewerker van Hacking Team, Alberto Ornaghi, grapt over Zeus en het feit dat de activisten niet hebben ontdekt dat Hacking Team erachter zat: '*They think we are a new Zeus*.'

Robotec fungeert als tussenhandelaar voor Hacking Team in Latijns Amerika. Robotec is een privaat Colombiaans bedrijf onder leiding van Hugo Fernando Ardila en Jamie Caicedo. Het bedrijf heeft verschillende deals voor Hacking Team afgesloten, onder meer met de anti-drugs en inlichtingendienst in Colombia, en met Panama, waar de digitale wapens zijn ingezet tegen de oppositie.

In 2013 schaft de Ecuadoraanse inlichtingendienst Senain met bemiddeling van Robotec software van Hacking Team. De Senain heeft een dubieuze reputatie. In 2015 publiceerde de website Ecuador Transparente een rapportage over de Senain die tussen 2012 en 2014 de oppositie, de media en mensenrechtenactivisten systematisch had bespioneerd. Amnesty International en Human Rights Watch schreven in dezelfde periode over de schendingen van de rechten van de inheemse volken in dat land door de Ecuadoraanse overheid en haar veiligheidsapparaat. Ook rapporteerden de mensenrechtenorganisaties over bedreigingen en de moord op mensenrechtenactivisten, de straffeloosheid van de politie en zorgen over de vrijheid van meningsuiting.

Uittocht van ontevreden medewerkers

Niet iedereen bij Hacking Team is gelukkig met de klantenkring van het bedrijf. Binnen het bedrijf zijn verschillende ontwikkelaars ongelukkig met de verkoop van digitale wapens aan repressieve regimes.

Al na de onthulling van Citizen Lab in 2012 over de inzet van de digitale wapens door de Marokkaanse overheid tegen journalisten, breekt er een discussie uit binnen het bedrijf. In 2014, na de onthullingen over de inzet van Hacking Team's digitale wapens tegen Ethiopische journalisten, wordt de onvrede nog duidelijker. Alberto Pelliccione neemt ontslag, en in de maanden die volgen houden meerdere werknemers het voor gezien.

Het antwoord van Vincenzetti op de interne discussie was de verschillende afdelingen van elkaar te scheiden zodat de ontwikkelafdeling geen zicht had op de verkoop, maar ook niet op de 'exploit afdeling', de afdeling die de documenten bewerkt om de apparatuur van mensen te infecteren. Deze documenten kunnen Word-documenten, pdf's of andere digitale bestanden zijn.

De technici van het bedrijf stellen dan ook dat zij niet wisten wie de klanten waren. De mensen van de 'exploit afdeling' zijn echter wel op de hoogte van de afnemers. Als Hacking Team zijn digitale wapens verkoopt aan Marokko, Ethiopië of Soedan, zijn deze landen immers van deze afdeling afhankelijk om documenten te prepareren waarmee het slachtoffer kan worden geïnfecteerd. De inhoud van die documenten verraadt allerlei aspecten van het doelwit.

De onthullingen van Citizen Lab toonden aan dat de digitale wapens van Hacking Team niet meer onzichtbaar zijn. Vincenzetti en zijn managers willen dat de ontwikkelaars zich inspannen om de software meer te verhullen, zodat ze niet meer te herleiden zijn tot Hacking Team. Na het vertrek van Pelliccione in 2014 vertrekken ook andere ontwikkelaars. Vincenzetti spreekt de vrees uit dat het onmogelijk zal zijn om het digitale wapen in de toekomst onzichtbaar en *up to date* te houden. Er lijkt sprake van een lichte vorm van paranoia binnen het bedrijf. De baas van Hacking Team is bang dat alle werknemers naar de concurrentie overlopen en hun kennis meenemen.

Vincenzetti is 'not amused' over de ontstane commotie over zijn bedrijf en over het vertrek van zijn medewerkers. Als Guido Landi krijgt hij de woede van de grote baas over zich heen. Landi is de voormalige rechterhand van de CTO (Chief Technology Officier). Landi is een van de belangrijkste ontwikkelaars die Hacking Team in 2014 verlaten.

Vincenzetti is woedend over het vertrek van de ontwikkelaar. Landi zal in de maanden die volgen ontdekken dat Vincenzetti goed is ingevoerd in de top van de Italiaanse opsporings- en inlichtingenwereld. De baas van

Hacking Team schrijft na het vertrek van Landi dat hij dit op het hoogste niveau bij de Italiaanse overheid zal aankaarten. Vervolgens krijgt Landi bezoek van twee hooggeplaatste functionarissen van de Italiaanse geheime dienst: kolonel Riccardo Russi en generaal Antonello Vitale. Later wordt Landi flink aangepakt door de openbare aanklager, die de hack van Hacking Team in 2015 onderzoekt. Landi is niet aangeklaagd, maar het onderzoek naar de hack loopt nog.

Vincenzetti en ethiek

Hacking Team ligt de afgelopen jaren regelmatig onder vuur vanwege de dubieuze leveranties van digitale wapens aan repressieve regimes. De reactie van Vincenzetti hierop is niet overtuigend. Eerst ontkende Vincenzetti de handel met omstreden regimes. Vervolgens claimde hij dat zijn bedrijf geen invloed had op de wijze waarop de wapens door haar klanten werden gebruikt. Vincenzetti beweerde ook regelmatig dat Hacking Team normaliter zorgvuldig naar de achtergrond van haar klanten kijkt, maar wat hier mee bedoelde maakte hij niet duidelijk.

Het overtuigt niet. Hacking Team heeft namelijk vanaf het begin geen problemen gehad om digitale wapens te verkopen aan klanten die een twijfelachtige reputatie hebben. Zo was Mexico vanaf het begin een van de grootste klanten van Hacking Team. Een land waar veel twijfels zijn over relaties tussen opsporings- en inlichtingendiensten en criminele organisaties, en waarbij men zich dus kan afvragen in welke handen de digitale wapens van Hacking Team terecht komen. Voor Mexico kochten Singapore, Marokko, Saoedi-Arabië digitale wapens bij de Italianen.

Uiteindelijk stelde Vincenzetti een ethische commissie, onder leiding van het advocatenkantoor Bird & Bird, in die moest toezien of de afnemers van Hacking Team wel door de beugel konden. Het is niet duidelijk met hoeveel zaken de commissie zich heeft bezig gehouden en hoe ze deze heeft beoordeeld.

Het werk van de ethische commissie kan echter weinig om het lijf hebben gehad en er lijkt eerder sprake te zijn van window dressing. Illustratief is dat in 2014, toen de ethische commissie al werkzaam was, Hacking Team digitale wapens leverde aan Soedan en hiervoor door de Verenigde Naties werd getikt vanwege het schenden van een embargo.

Hacking Team en Vincenzetti hebben ethiek niet hoog in het vaandel

staan. In maart 2013 velt Reporters Without Borders in haar jaarlijkse rapport *Enemies of the Internet* een hard oordeel over het bedrijf. Vincenzetti en zijn oude vrienden die allen een geschiedenis hadden in defensief beveiligingswerk op het internet waren in een periode van twintig jaar van vrienden tot vijanden van het internet verworden. Hun woorden uit de tijd van CryptoNet, toen het nog over het beschermen van de vrijheid van meningsuiting ging, blijken leeg. Zij zijn uiteindelijk voornamelijk geïnteresseerd in geld verdienen door middel van digitale offensieve wapens.

Het is dan ook een schok voor Hacking Team als twintig actievoerders in 2013 de voorruit van het kantoor van het bedrijf kapot slaan en binnenstormen. Vincenzetti is daar drie jaar later nog verontwaardigd over. Als *Foreign Policy* naar de bestorming vraagt, zegt hij: "*It was a full assault*." Bij het protest namen de actievoerders documenten, notities, zo'n beetje alles wat er te pakken viel, mee.

Een voormalig collega van Vincenzetti, Salvatore Sanfilippo die met hem samenwerkte bij Intesis SpA, wordt door *Ars Technica* geïnterviewd. Hij zegt niet verbaasd te zijn dat Vincenzetti de commerciële weg is ingeslagen en digitale wapens is gaan produceren, maar wel over de gebrekkige beveiliging van Hacking Team als gevolg waarvan het bedrijf in 2015 werd gehackt: "*I don't have the details, but if this is the case, it's a big mismatch to the experience I had with Vincenzetti and [Hacking Team Managing Director Valeriano] Bedeschi. They are both top-class hackers, and when I used to work with them in 1998, security was a top concern.*"

Volgens Sanfilippo was Vincenzetti wel een groot voorstander van de vrijheid van meningsuiting en encryptie. Toch vindt Sanfilippo het logisch dat Vincenzetti de markt van digitale wapens en de verkoop aan repressieve regimes is opgegaan: "*I'm not surprised about Hacking Team creation since probably this was seen as an effective way to monetize on security products.*"

Financiële motieven zullen dan ook een belangrijke reden voor het opzetten van Hacking Team zijn geweest. De *Daily Dot* stelt op 7 juli 2015 dat Vincenzetti zijn collega's uit de jaren 90, zoals Massimo Cotrozzi en Fabio Bolognesi, zag vertrekken naar de commerciële sector en daar veel geld gingen verdienen: '*In his 20s, Vincenzetti watched from afar as security colleagues became big-time businessmen who traded with the world's top banks, a path he'd eventually follow.*'

Financiële motieven lijken doorslaggevend voor Vincenzetti. Dit komt misschien wel het beste tot uitdrukking op zijn LinkedIn account waarin hij verklaart: '*My main non-professional interest is finance*.'

Exportvergunning

In 2014, twee jaar na de ontdekking van de inzet van digitale wapens van Hacking Team tegen Marokkaanse journalisten, wordt de Italiaanse overheid wakker. Vanwege de export van digitale wapens naar landen als Marokko, Ethiopië en Soedan vergelijkt de Italiaanse overheid de digitale wapens van Hacking Team met oorlogstuig. Dit betekent dat er in principe tevens een exportvergunning voor moeten worden aangevraagd bij het Italiaanse Ministerie van Economische Zaken.

Hacking Team had dit in het verleden nooit eerder gedaan uit angst voor het 'dual use' argument tegen de export: de digitale wapens kunnen voor opsporing worden gebruikt, maar ook om dissidenten, journalisten en politieke oppositieleden mee aan te vallen. Deze mogelijkheid kan na de onthullingen over onder meer Marokko in 2012 en Ethiopië in 2013 echter niet meer worden genegeerd.

Het Italiaanse Ministerie van Economische Zaken komt inmiddels tot een zelfde conclusie. Het ministerie stelt dat zij informatie heeft dat de digitale wapens van Hacking Team worden ingezet voor repressieve doeleinden waarbij de mensenrechten worden geschonden, en schrijft op 30 oktober 2014: '*Questa amministrazione è in possesso di elementi di informazione relativamente ad operazioni di esportazione da parte della Società in oggetto, che potrebbero configurarsi come connesse con possibili utilizzazioni attinenti alla repressione interna ed alla violazione dei diritti umani.*'

Het ministerie eist van klanten van Hacking Team dat zij een zwart-op-wit verklaring overhandigen waarin gesteld wordt dat de digitale wapens niet tegen de eigen bevolking worden ingezet.

Vincenzetti ziet meteen in dat dit misschien het einde van de lucratieve export voor Hacking Team betekent. Van de vijf landen die het meest besteden aan digitale wapens zijn er in ieder geval al twee (Marokko en Saoedi-Arabië) die de wapens niet gebruiken voor opsporingsdoeleinden. Ook met betrekking tot Mexico leven er grote twijfels, en kunnen de

wapens bovendien in handen komen van criminele kartels. Wanneer alleen de Europese Unie overblijft als handelsgebied, is het de vraag of Hacking Team financieel zal kunnen overleven.

Vincenzetti ziet het gevaar in en schrijft al zijn Italiaanse klanten aan met de mededeling dat het bedrijf mogelijk zijn handel moet opgeven. Via een van die klanten, de PCM, is Vincenzetti in staat om de president en de ministerraad van Italië te bereiken. Dit heeft resultaat. Er volgt een gesprek op het Ministerie van Economische Zaken waarbij ook enkele topambtenaren aanwezig zijn.

Het Ministerie van Economische Zaken zit zelf namelijk ook met een probleem. Zij is niet alleen controleur van Hacking Team, maar ook een klant van het bedrijf. Sinds 2013 gebruikt ook de Italiaanse FIOD (Guarda di Finanza) immers de digitale wapens van het bedrijf.

Vincenzetti wint deze slag, Hacking Team mag blijven exporteren. Begin 2015 wordt er een oplossing gevonden. Hacking Team vraagt een exportlicentie aan voor de gehele wereld om de uitvoer van spionagesystemen die niets met wapens of oorlog te maken hebben mogelijk te maken.

Een paar maanden later, in juli 2015, ligt de administratie van het Italiaanse bedrijf op straat en blijkt op welke schaal Hacking Team heeft samengewerkt met repressieve regimes. Dit heeft nog niet direct gevolgen voor de wereldwijde exportlicentie. De Italiaanse overheid wacht met het intrekken van die exportvergunning tot april 2016. In april 2016 trekt de Italiaanse overheid de vergunning voor de export naar landen buiten de Europese Unie in. Voor export naar landen buiten de EU moet Hacking Team per klant elke keer een aparte vergunning aanvragen. Hacking Team verliest daardoor in eerste instantie het grootste deel van zijn klanten. Slechts Zeven van de ongeveer 46 klanten van het bedrijf komen uit de Europese Unie.

De *backdoor* lekt uit

Voor de Italiaanse overheid dient zich naast de export vraagstukken vervolgens nog een ander probleem aan.

In hoeverre is het bewijs dat wordt verkregen met behulp van de inzet van digitale wapens van Hacking Team rechtsgeldig? Vincenzetti heeft

regelmatig gezegd dat zijn digitale wapens door Italiaanse opsporingsdiensten worden gebruikt om grote misdrijven mee op te lossen, zoals rond maffiabazen en moordenaars. Concreet bewijs hiervoor is echter nooit geleverd door Hacking Team noch door de Italiaanse overheid. Net als in Nederland is in Italië het inbreken op smartphones, laptops en andere digitale hulpmiddelen een grijs gebied waar binnen veel mogelijk is.

Er is echter nog een groter probleem. Informatie over de werking van de software die Hacking Team voor zijn digitale wapens gebruikt, is ook openbaar geworden. Verschillende publicisten, zoals internet veiligheidsdeskundige Bruce Schneier, verwijst naar openbaar gemaakte documenten waarin een *backdoor* (achterdeur) in de digitale wapens van Hacking Team wordt beschreven. Middels die *backdoor* kan het bedrijf het wapen in ieder geval op afstand uitzetten zonder dat de klant daar weet van heeft.

De klanten van Hacking Team zijn niet geïnformeerd over die achterdeur. De *backdoor* geeft echter niet alleen Hacking Team toegang tot de geïnfecteerde smartphones, laptops, computers. In theorie kunnen anderen zich daardoor ook toegang verschaffen en gegevens manipuleren. Dat maakt de bruikbaarheid van het bewijs dat verkregen is met behulp van digitale wapens minder aannemelijk.

Naast vragen ten aanzien van de afwezigheid van exportvergunningen, zelfs naar landen waar een VN embargo voor geldt en repressieve regimes, en de mogelijke aanwezigheid van een *backdoor* is er ook nog de handel in *zero-days* van Hacking Team. *Zero-days* (nul dagen) zijn veiligheidslekken in software die nog niet bekend zijn bij de makers van de software waarbij dei lekken zijn vastgesteld. Die *onbekende* veiligheidslekken worden door Hacking Team gebruikt om met hun digitale wapens in te breken op smartphones, tablets, etc. De handel in *zero-days* is een zwarte markt waar veel geld in omgaat.

De mensen die *zero-days* verkopen, kunnen werkzaam zijn bij een bedrijf als het Franse VUPEN security, Coseinc uit Singapore, het Amerikaanse Netragard and Vulnerabilities Brokerage International, maar individuen kunnen veiligheidslekken aanbieden. De bedrijven die beweren dat ze alleen overheden veiligheidslekken aanbieden dus niet aan de producenten van de software die lek is. De openbare data van Hacking Team maakt echter duidelijk dat het voor private partijen niet al te moeilijk is om *zero-days* aan te schaffen, zowel van bedrijven als

Vupen en Coseinc als van individuen.

Wie die individuele handelaren zijn blijft duister. Zo schaft Hacking Team veiligheidslekken aan van een Rus met de naam ‘Vitaliy Toropov’. Hij biedt lekken aan in de browser Safari van Apple, in Flash van Adobe en Silverlight browser plug-in van Microsoft. De Italianen kopen uiteindelijk de lekken in Flash van de Rus maar hebben geen exclusiviteit. De Rus kan ze ook aan andere bieders aanbieden, zowel overheden, bedrijven als individuen. De Italiaanse overheid gebruikt dus digitale wapens die gebruik maken van veiligheidslekken die verhandeld worden op een zwarte markt waarbij onduidelijk is wie ze allemaal in handen krijgen.

Hacking Team heeft enkele Flash *zero-days* gekocht welke waarschijnlijk zijn gebruikt om in te breken op een smartphone, tablet, computer van een verdachte. Er is geen garantie dat Hacking Team de enige partij is die op de hoogte was van die veiligheidslekken in Flash en dat niemand anders dus bij de data van verdachten heeft kunnen komen. Hoe wijd verspreid de kennis van dit specifieke lek was, is moeilijk te achterhalen omdat ook criminele organisaties en inlichtingendiensten deze *zero-days* aanschaffen.

Hacking Team heeft dan wel een digitaal wapen ontwikkeld om mee in te breken, maar kan nooit garanderen dat iemand anders ook al aan het inbreken is. Het feit dat het Italiaanse technologiebedrijf zelf het slachtoffer is geworden van een digitale inbraak, maakt duidelijk dat digitale wapens misschien eerder digitale boemerangs zijn dan technische hulpmiddelen voor opsporings- en inlichtingeninstanties.

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

Boeven vangen met dubieuze software van dubieuze bedrijven

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

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

Presentatie van Hacking Team RCS

Presentatie Man in the Middle hack uit 2003

Despite Hacking Team's poor opsec, CEO came from early days of PGP

Fear This Man; To spies, David Vincenzetti is a salesman. To tyrants, he is a savior. How the Italian mogul built a hacking empire.

The Hacking Team Defectors

Hacking Team goes to war against former employees, suspects some helped hackers

Let me show you the America that counts

Bruce Schneier over de Hacking Team *backdoor*

Hacker 'Phineas Fisher' Speaks on Camera for the First Time—Through a Puppet

Naar inhoudsopgave Observant #69