

## **Kailax / Nir (Max) Levy**

### **De magische hand van de Israëlische inlichtingendienst**

**De Kailax *Unlocker* is illustratief voor de geheimzinnigheid en ondoorzichtigheid van de handel in digitale wapens. De *Unlocker* is een tool waarmee een inbreker zich toegang kan verschaffen tot een Windows computer, zonder dat de eigenaar dit in de gaten heeft.**

Over de *Unlocker* en het producerende bedrijf Kailax is nauwelijks openbare informatie beschikbaar. De website [www.kailax.com](http://www.kailax.com) bevat alleen de adresgegevens van het bedrijf (een adres in Singapore), maar geen verdere informatie. Uit openbare bronnen kan alleen worden opgemaakt dat het in Berlijn gevestigde bedrijf 2beuropa als tussenhandelaar voor Kailax fungeert.

Pas met de openbaar making van de Wikileaks documenten over Hacking Team in 2015 is er meer inzicht gekomen over het bestaan van de Kailax *Unlocker* en de handel in deze tool. De Kailax *Unlocker*, soms aangeduid als *Unlocker/U-cap* blijkt een gewild digitaal wapen. Volgens de producent, die zich in e-mails afwisselend Max en Nir Levy noemt, levert Kailax de *Unlocker* aan zeventig landen.

Of dit waar is, valt niet te controleren. Wat wel duidelijk wordt uit de Wikileaks documenten is dat het Italiaanse computerbedrijf Hacking Team interesse heeft om de *Unlocker* aan haar assortiment toe te voegen. Het belandt hiervoor bij het Britse bedrijf Providence, dat als tussenhandelaar de *Unlocker* blijkt aan te bieden.

De Kailax *Unlocker* is illustratief voor de geheimzinnigheid en ondoorzichtigheid van de handel in digitale wapens. De herkomst van digitale wapens is vaak onduidelijk, hetgeen de vraag oplevert of overheden en veiligheidsdiensten wel weten wat voor product ze kopen en met welk bedrijf ze in zee gaan. De bemoeienis van een tussenhandelaar als Providence draagt bij aan de ondoorzichtigheid en onveiligheid.

Buro Jansen & Janssen deed een digitale zoektocht naar de herkomst van de *Unlocker*. Deze leidt naar Israël. De Kailax *Unlocker* blijkt van

Israëlische afkomst te zijn, voormalig leden van de Israëlische veiligheidsdienst zijn betrokken.

## Hacking Team en Kailax

Uit de in 2015 gepubliceerde Wikileaks documenten wordt duidelijk dat het Italiaanse bedrijf Hacking Team begin 2015 interesse heeft om de Kailax *Unlocker* aan te schaffen. Met deze *Unlocker* verschaft een inbreker zich toegang tot een Windows computer zonder in te loggen en zonder dat de eigenaar dit in de gaten heeft. Het gaat hierbij om Windows Vista/7/8/8.1 Server 2008/Server 2012- 32/64 bit.

Hacking Team gebruikt eenzelfde soort techniek voor zijn Tactical Network Injector (TNI) voor Firewire. In een 'Statement of Work' schrijft Nir Levy (Max) van het producerende bedrijf Kailax dat het product '*a handheld unit is that once plugged into any USB port of locked windows PC, will automatically execute at system rights a propriety payload on the target PC.*' Het laat volgens Kailax weinig sporen achter op de computer van het slachtoffer.

De Italianen beschouwen de *Unlocker* als een aanwinst voor hun digitale inbrekerskit. Het is misschien een optie om de tool zelf te ontwikkelen, maar zonder een prototype lijkt dit voor de Italianen een stap te ver. Hacking Team probeert de tool eerst te verkrijgen via het kantoor van Kailax in Singapore, maar er volgt geen antwoord op het verzoek.

Op 23 januari 2015 vraagt Walter Furlan in een interne mail aan enkele werknemers van Hacking Team of zij de Kailax *Unlocker* kennen. Een Zwitserse klant van de Italianen, de Kantonspolizei Zürich heeft de *Unlocker* gekocht van 2beuropa. Ook een andere klant, de Raggruppamento Operativo Speciale (ROS, Special Operations Group) van de Italiaanse militaire politie, heeft de *Unlocker* aangeschaft bij 2beuropa.

Giancarlo Russo van Hacking Team neemt hierop contact op met Rami Zoltak van 2beuropa. Dit in Berlijn gevestigde bedrijf opereert als distributeur van Kailax. Zoltak antwoordt echter dat 2beuropa alleen met overheden handelt: '*We are working only with governmental offices, we are unfortunately unable to assist.*'

De Italianen blijven echter aanhouden. Russo bluft dat een 'LEA client' (Law Enforcement Agency) interesse heeft in de *Unlocker*.

Uiteindelijk reageert Max, die in de eerste mails nog ondertekent met Kailax Sales. Max zegt dat de klant van Hacking Team enkel een USB *Unlocker* kan aanschaffen via de officiële dealer van Kailax. Hij vermeldt er echter niet bij wie deze dealer is.

Russo probeert Max nog een keer te overtuigen maar Kailax blijft weigeren. Er komt wel steeds meer informatieve over de tool vrij: *'The Unlocker is a self-contained sealed and secure hand held unit that does one thing and one thing only, bypasses windows passwords and gives system rights on the locked live PC.'* Volgens Max is de *Unlocker* aan ruim zeventig landen verkocht.

Max geeft Hacking Team één optie, namelijk dat Hacking Team de *Unlocker* op haar systeem installeert voor waarmee de tool onbeperkt kan worden gebruikt. Hij vraagt Russo om de garantie dat niemand anders toegang krijgt tot het IP-adres van Kailax: *'you also have to convince and assure us that no one else but you will have access to our IP.'* Max ondertekent nu als Nir Levy (Max)

De Italiaan en Max mailen nog een tijdje met elkaar, maar veel schot lijkt er niet te komen in de zaak. Max houdt de boot af: *'We are both manufacturer suppliers of technology we are in essence competitors'*, schrijft hij. *'As you must know we are in same niche market that is usually based on trust.'*

Max stelt nog wel een tussenoplossing voor. Hacking Team kan als een soort onderaannemer fungeren, die uitsluitend een zwarte doos aan haar klanten kan verkopen: *'Option 1 is feasible only if you are prepared to supply to customers as a sub distributor black box technology which you do not own, have no deal understanding of the IP or maintain.'*

De Italianen zien het niet zitten en besluiten om enkele van hun eigen klanten te vragen een Kailax *Unlocker* voor Hacking Team aan te schaffen. Russo benadert daarvoor probeert het nu via de Zwitserse politie, de Kantonspolizei Zürich. De Zwitsers reageren niet dus proberen de Italianen het bij een Italiaanse klant, de Raggruppamento Operativo Speciale (ROS, Special Operations Group) van de Italiaanse militaire politie. Hacking Team vraagt de ROS om twee *Unlockers* te bestellen,

maar de militaire politie lijkt niet al te happig om zich voor het karretje van Hacking Team te laten spannen.

## Providence komt in beeld

Begin maart 2015 loopt het contact tussen Hacking Team en Kailax spaak. Hierop zoeken de Italianen toenadering tot het Britse bedrijf Providence. Beide bedrijven kennen elkaar, en probeerden in de voorafgaande jaren een samenwerking in Australië en Ecuador tot stand te brengen waarbij Providence als tussenhandelaar voor producten van Hacking Team wilde fungeren

Providence claimt een eigen tool, 'de *Windows Unlocker* en *U-Cap*', in haar assortiment te hebben. Deze voorziet in eenzelfde behoefte als de Kailax *Unlocker*. De Kailax *Unlocker* wordt soms ook aangeduid als *Unlocker/U-Cap*. Op 18 maart 2015 geeft Providence tijdens de ISS World MEA in Dubai een presentatie onder de titel 'Tactical Bypass of IT Security', die door medewerkers van Hacking Team wordt bijgewoond.

Een week later schrijft Giancarlo Russo van Hacking Team aan Steve Minto van Providence dat de Italianen geïnteresseerd zijn in het bespreken van een zakenrelatie. Russo mailt op 8 april 2015: *'My colleagues visited your booth in Dubai last week and they reported me positive impression about your USB tool for launching payloads on PCs. As you might know, we are active in more than 30 countries providing IT Offensive technology exclusively to many LEA/Intelligence agencies and we think that your USB might be useful for many of our countries.'*

Nog dezelfde dag antwoordt Peter Stolwerk van Providence dat hij zeer geïnteresseerd is in een mogelijke samenwerking met Hacking Team ten aanzien van de *'Windows Unlocker and U-Cap (the special add-on for the Unlocker).'* Providence maakt in dit stadium van de onderhandelingen nog niet duidelijk dat het de *'Windows Unlocker en U-Cap'* niet zelf heeft ontwikkeld.

Stolwerk reist af naar Milaan voor een presentatie. Deze verloopt echter niet vlekkeloos. De Italianen merken op dat de *Unlocker* sporen achter laat: *'Regarding the product I would like to have a feedback regarding the behavior we experienced during the demo (pop-ups on unlocked PC).'*

Russo een schrijft verslag van de bijeenkomst en stuurt dit Stolwerk op. Russo en Stolwerk hebben het tijdens hun overleg gehad over *'Partnership on Training programs for HT Clients. Social Engineering and how to get increasing benefit from HT technologies in real case operations.'*

Uit het verslag blijkt dat Hacking Team Providence een deal wil aanbieden. Het accepteert Providence als een soort distributeur, in ruil voor de USB *Unlocker*: *'The U-cap + Unlocker product to be added to Hacking Team's solution for its customers needing an additional tool to deliver payload during Physical infection.'*

Providence mag als tussenhandelaar producten van Hacking Team verkopen en klanten trainen het beste uit de cyberwapens te halen: *'Providence Group can offer and provide training, workshops and assistance to Hacking Team's end-users in order to help them maximize the efficiency of their attacks, to be either physical (covert installation, intrusion), tactical through WIFI (close to target training, mimicry) or remote (Social Engineering).'* Ook mag Providence softwareproducten van Hacking Team aan haar klanten aanbieden: *'Providence would play more the role of an agent/consultant, rather than a distributor'*.

Bij de *'Unlocker + U-cap'* willen de Italianen echter Providence omzeilen en het liefst alle mogelijkheden in handen hebben om het product aan hun assortiment toe te kunnen voegen. *'Regarding the cooperation we feel that the first, easiest and fastest, way to cooperate is to include the USB Unlocker into our portfolio'*, laat Russo aan Stolwerk weten.

Tijdens de bijeenkomst in Milaan wordt echter langzamerhand duidelijk dat Providence niets te zeggen heeft over de USB *Unlocker*. Stolwerk moet steeds terug keren naar de producent die hij slechts één keer bij naam noemt: 'Max'. Russo van Hacking Team schrijft na de bijeenkomst in Milaan, waar Max blijkbaar ter sprake is gekomen: *'I expect you and Max to elaborate more on which cooperation options you consider viable'*. Stolwerk zegt dat hij Max gesproken heeft: *'Agreed, I spoke to Max and he is positive that we will together find a solution on this.'*

Hacking Team heeft begin 2015 ook al direct contact gehad met Max over de mogelijke aanschaf van de *Unlocker*. Opvallend genoeg blijkt uit

de correspondentie in de Wikileaks documenten niet of de Italianen zich dit beseffen, of dat zij Providence hiervan op de hoogte stellen.

## **Werving nieuwe klanten**

Hacking Team wordt uitgenodigd om het kantoor van Providence in Hereford in mei 2015 te bezoeken en de samenwerking verder te bespreken. Het Engelse bedrijf is gretig en vraagt Hacking Team onder meer of het bereid is om een defensieve cyberoorlog training te geven aan twintig mensen uit het Midden-Oosten. Het lijkt erop dat Providence nog niet helemaal door heeft wat de Italianen nu eigenlijk doen. Een telefonisch onderhoud moet de Engelsen vervolgens duidelijk maken dat Hacking Team uitsluitend digitale wapens verkoopt.

De Italianen zijn, naast de acquisitie van de 'U-cap + *Unlocker*', ook geïnteresseerd om via Providence nieuwe klanten te werven: *'We should go to Hereford and take advantage to visit them and also perform a demo for their sales team'*, schrijft Vinci van Hacking Team.

Vinci suggereert ook een bijeenkomst te organiseren met het Britse Ministerie van Defensie: *'There is a big MOD field camp in Hereford. We can try to organize a meeting with MOD (Ministry of Defence)'*. Hacking Team hoopt dat Providence iets kan betekenen richting het Britse Ministerie. Er zijn echter ook andere potentiële tussenhandelaren zoals Bob Quick van BlueLight Global Solutions. Naast het Ministry of Defence zijn er ook andere potentiële klanten zoals de National Crime Agency en BAE Systems, een grote militaire wapenproducent.

Het cursus- en trainingsaanbod van Providence is voor de Italianen minder interessant. Vinci mailt: *'a training on how to enter into a home and defeat an alarm :-), can be certainly useful for our customers to do physical infections, (...) but we won't put this training in our catalogue.'*

De Italianen houden erg de boot af en Providence als tussenhandelaar lijkt nog een lange weg: *'I suggest that you provide us with 1 or 2 'low hanging fruit' we could start the collaboration on and add more accounts as we progress. Benelux would be a nice test for our cooperation in addition to the MOD intelligence in the UK for example.'*

De Italianen stellen Providence voor dat, wanneer zij distributeur willen worden voor Hacking Team, zij om te beginnen een aantal gemakkelijke

klanten moeten aanleveren. Wanneer Providence echter zelf op jacht wil gaan naar klanten dient zij de gegevens door te geven aan Hacking Team, dat vervolgens bepaalt of de Engelsen mogen handelen. De ervaring leert namelijk dat sommige klanten al bezet zijn door een andere tussenhandelaar. Dit was bijvoorbeeld het geval in Ecuador, waar Providence met een bedrijf kwam, terwijl Hacking Team al via een ander bedrijf (Robotec) zaken deed in het land.

## **Beet of toch niet**

Op 8 mei 2015 wordt de verhouding tussen Max en Providence duidelijk. Stolwerk: *'The manufacture will only allow you to purchase the Unlocker & u-cap via his regional distributors. We cover a large part of the world but for parts that we don't cover you have to make arrangements with the regional distributor that covers that area.'*

Providence heeft Max kennelijk weten te overtuigen. Volgens Stolwerk is Providence de distributeur van *Unlocker* voor een groot deel van de wereld. Hij maakt echter niet duidelijk voor welke van de zeventig landen, waarvan Max beweert dat de Kailax USB stick aan wordt geleverd, Providence als tussenhandelaar opereert. Het andere deel verloopt via lokale distributeurs zoals 2beuropa.

Kailax is bereid om voor Hacking Team een speciale versie van de *'Unlocker/U-cap combination'* te maken. De ontwikkeling hiervan komt voor rekening van de Italianen. Eigenlijk kan een succesvolle bijeenkomst in Hereford niets meer in de weg staan. De Italianen presenteren daar hun pronkstuk de Galileo RCS (Remote Controle System) en willen graag het volledige repertoire van de Engelsen zien, *'in particular the training and workshop around cyber, covert entry, installation, surveillance, getting close to the targets, etc.'*

De communicatie tussen Hacking Team en Providence, met name Peter Stolwerk, gaat de hierop volgende maanden vooral over de *Unlocker*. De Italianen zeggen een klant te hebben voor de Kailax USB stick en willen weten hoe zij die tevreden kunnen stellen. Giancarlo Russo van Hacking Team zegt dat het om een Italiaanse opsporingsdienst gaat en dat Max de dienst al kent.

Stolwerk wil de Italianen ook graag behouden als mogelijke partner en schrijft dat er in Nederland interesse bestaat voor de producten van

Hacking Team: *'I will speak to the guys here as I have some good news about the Netherlands for your products.'*

De Italianen lijken echter nog niet volledig overtuigd van de kwaliteiten van Providence. Eind mei 2015 schrijft een Hacking Team medewerker, na het bestuderen van de presentaties van de Engelsen: *'Still have to read all documents carefully, but all of them have been written on January 2015 (versions 1.0), so it seems they're recently organizing contents. P.S. All their e-mail addresses on the last pages are wrong.'* Bij Providence zijn ze kennelijk begin 2015 begonnen met het opstellen van hun trainingen, bestaan dus net en hun e-mail adressen kloppen niet.

Providence en Hacking Team zijn dichtbij een overeenkomst. De Italianen worden zelfs uitgenodigd voor een exclusieve bijeenkomst van Providence op 26 augustus 2015. Op het terrein in Hereford is een kleine markt met workshops en een barbecue georganiseerd. Naast Hacking Team zijn Tac Up (van Providence), Claresys Covert Video Surveillance (van het Britse Ministerie van Defensie), en nog twintig andere bedrijven, uitgenodigd waaronder Cobham, Eomax, Sentinor. Allemaal 'vrienden' van Providence.

Uit de Wikileaks documenten wordt niet duidelijk of Hacking Team de *Unlocker* uiteindelijk aan haar assortiment heeft toegevoegd. In juli 2015 wordt Hacking Team getroffen door een hack en worden interne documenten over het bedrijf gepubliceerd door WikiLeaks. Ook komt het Italiaanse bedrijf onder vuur te liggen vanwege de levering van digitale wapens aan repressieve regimes en verliest het haar exportvergunningen voor handel buiten de Europese Unie.

## **Kailax - Mhyli**

De correspondentie tussen Hacking Team en Providence geeft een onthullend inzicht in de wereld van de tussenhandel in digitale wapens. De Kailax *Unlocker* is illustratief voor de geheimzinnigheid en ondoorzichtigheid van de handel in digitale wapens. De herkomst van digitale wapens is vaak onduidelijk, hetgeen de vraag oplevert of overheden en veiligheidsdiensten wel weten wat voor product ze kopen en met welk bedrijf ze in zee gaan. De bemoeienis van een tussenhandelaar als Providence draagt bij aan de ondoorzichtigheid.

Over het bedrijf Kailax is nauwelijks openbare informatie bekend. Het



bedrijf heeft een website ([www.kailax.com](http://www.kailax.com)). Volgens welke het bedrijf is gevestigd onder de naam Kailax in Singapore: Kailax PTE LTD op 129 Lower Delta Rd. #09-03 Cendex Center. Op de website zijn twee zinnen te lezen, 'We provide solutions in the cyber security domain' en 'For details please contact us at [info@kailax.com](mailto:info@kailax.com)'. Verder staat er op de website geen informatie over producten, expertise, omzet, investeerders, klanten, etc.

Kailax is zelf nooit aanwezig op de verschillende beurzen voor digitale wapens of ISS World. Het verkoopt via het bedrijf 2beuropa. Het bedrijf 2beuropa wordt gerund door Rami Zoltak en is gevestigd in Berlijn aan de Mittenwalder Strasse. Zoltak komt uit de vastgoedwereld en handelt in allerlei producten waaronder digitale wapens zoals ook van Kailax.

Op de website van 2beuropa staat dat het bedrijf handelt in 'taktischen Überwachung beste High-End-Hardware- und Softwareprodukte.' Het gaat om surveillance, tactische surveillance en hoogwaardige hardware en software producten. Bij producten gaat het echter ook om een veiligheidskoffer voor een VIP, drugs testen, stinkende spray als openbare orde middel, containers voor de vervoer van explosieven

Op de website van 2beuropa wordt Kailax als partner genoemd sinds de nieuwe website in 2014 online is gegaan.

De website maakt echter niet duidelijk wat voor producten Kailax te bieden heeft. Wat opvalt is dat de winkel van Rami Zoltak uitsluitend Israëlische producten aanbiedt. Alle partners zijn Israëlische bedrijven die verbonden zijn aan de IDF, het Israëlische leger. 2beuropa geeft op haar website aan dat haar partners de volgende bedrijven zijn: Towersec, Karil International, Touch&Know, iDenta, Septier, ITP Novex, Memtex, Prosecs, ODF Optronics, ODI-X en Pro4tech. Kailax staat daar tussen en het is aannemelijk dat het een Israëlisch bedrijf is.

## **Max – Nir Levy - Mhyli**

Namens Kailax wordt gecorrespondeerd door Max. Ook gebruikt Max in de correspondentie met Hacking Team de naam Nir Levy, maar het is niet bekend of dit zijn echte naam is. De Kailax website bevat geen verdere informatie over Max en/of Nir Levy. Uit de Wikileaks documenten ontstaat de indruk dat Max / Nir Levy de belangrijkste persoon is binnen Kailax.

Buro Jansen & Janssen heeft getracht informatie te achterhalen over Max / Nir Levy. Het lijkt hier om één persoon te gaan. Hij gebruikt het e-mailadres [max@kailax.com](mailto:max@kailax.com).

Aan dit adres is nog een aantal domeinen gekoppeld. Het gaat hierbij om: s-mic.com, k-mic.info, *Unlocker-u.com* en toplucktrading.com. Deze sites werken allemaal niet, behalve de *Unlocker-u.com* die verwijst naar kailax.com. Toplucktrading houdt geen kantoor in Singapore, maar in Hong Kong, op het adres: Unit 1203 12F CEO Tower, Admin Street: 77 Wing Hong St Cheung Sha Wan, Kowloon.

Een digitale zoektocht naar Max en Nir Levy levert niet veel informatie op. Een uitdraai van de domeinnamen op naam van Nir Levy levert wel een interessant pallet op. Er zijn meerdere vele Nir Levy's: de meesten zijn Israëli, een enkeling woont in de Verenigde Staten. Bij de bovenstaande domeinen, zoals *Unlocker-u.com*, wordt Nir Levy als onderdeel vermeld van Kailax, met het e-mail adres max@kailax.com. Er bestaan echter andere domeinnamen op naam van deze Nir Levy, die gelinkt zijn aan een voormalig medewerker van de Israëliëse geheime dienst.

## Domeinnamen

Van alle Nir Levy's die domeinen hebben geregistreerd, zijn er maar twee die (net als [max@kailax.com](mailto:max@kailax.com)) de naam Max gebruiken. Het betreft een Nir Levy met het e-mail adres [max@mknowlegde.com](mailto:max@mknowlegde.com), en een Nir Levy met het adres max@mhyli.com.

Beide Maxen blijken betrekking te hebben op dezelfde Nir Levy, die als adres opgeeft: 7 shamir, hod hasharon in Israel, telefoonnummer +972.97480608. Deze gegevens hebben betrekking op de volgende websites: mknowledge-demo.com en mknowledge.com (gekoppeld aan het e-mail adres max@mknowledge.com) en mknowledge.info, smthid.com en mhyli.com (gekoppeld aan het e-mail adres max@mhyli.com).

Max van Kailax en de Max van 'mknowlegde' en 'mhyli' zijn dus dezelfde persoon. Er zijn geen andere Nir Levy's die de naam Max gebruiken. Daarnaast zijn de mknowlegde-websites even ontoegankelijk als de websites van Kailax.

Opvallend is de kleine presentatie van Max op de website van Mhyli. Hij vermeldt hier dat hij tevens directeur is van Pro4Tech, een producent van tactische video-observatie oplossingen. (Pro4Tech is ook aangesloten bij het bedrijf 2beuropa, dat ook als tussenhandelaar voor Kailax optreedt) Ook schrijft Max op de Mhyli website dat hij CEO is van EDM, een bedrijf dat informatie van het internet geautomatiseerd vergaart. Volgens de Mhyli website: *'Nir also holds the position of Director at Pro4Tech, a company manufacturing innovative Tactical Surveillance Video solutions. Nir is also founder and C.E.O. in EDM, a company dealing in automation of internet information gathering.'*

De reden waarom Nir Levy (Max) zo geheimzinnig doet over zijn achtergrond, heeft te maken met zijn carrière voordat hij in het bedrijfsleven stapte. Max heeft namelijk 25 jaar voor de Israëliëse inlichtingendienst gewerkt. De Mhyli website vermeldt: *'Before founding Mhyli, Nir served for 25 years in the Israeli Intelligence Community. During his time there, Nir commanded a variety of teams and projects, in his last post Nir headed a division specializing in computing and communications.'*

Dit is zeer opvallend. Op de website van Kailax ontbreekt enige achtergrondinformatie over Max of Nir, maar op de Mhyli website is hij een stuk openhartiger over zijn achtergrond: *'He also completed various managerial technical and command courses in the Prime Ministers Office, including the Senior Commander course.'*

Ook zijn collega bij Mhyli, Daniel Kario, blijkt een verleden te hebben bij het Israelische leger. Volgens de website heeft hij gewerkt als *'group leader in a leading technological unit of IDF.'* (Israëliëse Defense Forces)

Het valt niet vast te stellen of Kailax een zelfstandig bedrijf is en alleen door Nir Levy wordt gerund. De website van Kailax bevat hierover geen enkele informatie. De website maakt evenmin duidelijk of Nir Levy en Daniel Kario gespecialiseerde IT-ontwikkelaars zijn en die de tool zelf in elkaar hebben gezet.

Dat de Max van Kailax en de Max van Mhyli dezelfde persoon zijn, is met het oog op de geheimzinnigheid rond Kailax meer dan logisch. Wie wil er nu een digitaal wapen kopen van een voormalig medewerker van de Israëliëse inlichtingendienst? In sommige landen zal er grote twijfel ontstaan bij het in zee gaan met Kailax, zodra bekend is dat het hier een

Israëliisch bedrijf betreft, en al helemaal als daarbij contacten met de Israëliische inlichtingenwereld een rol spelen.

### **Geen zicht op afkomst *Unlocker***

Buro Jansen & Janssen concludeerde in 2011 in een onderzoek naar de relatie van Nederland met de Israëliische veiligheidsindustrie dat de Israëliërs op allerlei manieren proberen voet aan de grond te krijgen in Nederland en Europa. Hierbij gebruiken zij de oorlog in de bezette gebieden als ervaringsbewijs in de reclame voor hun producten. Tegelijkertijd proberen zij hun relatie met Israël te verdoezelen door het opzetten van buitenlandse zuster- of dochterondernemingen die de handel met bepaalde landen op zich nemen.

Het bedrijf Kailax past in dit profiel. Het is aannemelijk dat Kailax aan aan vergelijkbare landen / klanten levert als Hacking Team en Gamma Group/Finfisher, al dan niet met Providence als tussenhandelaar. Het is sterk de vraag of de afnemers van de Kailax *Unlocker* de achtergrond van het bedrijf, haar werknemers, investeerders en klanten kennen.

Deze vraag is ook relevant met betrekking tot Nederland. In antwoord op het WOB verzoek van Buro Jansen & Janssen maakt de Nationale Politie bekend dat het 39 producten of diensten van Providence heeft afgenomen. De politie maakt echter niet openbaar wat het precies van Providence heeft gekocht. Het is aannemelijk dat de Kailax *Unlocker* is aangeschaft.

Providence is een jonge speler op de veiligheidsmarkt. Het Britse bedrijf biedt trainingen, accommodatie en apparatuur aan. De Nederlandse politie kan voor trainingen gebruik maken van eigen trainers en trainingscentra. Veel apparatuur wordt door de politie ingekocht bij reguliere leveranciers als Cellebrite, Nice-Systems en andere bedrijven, vraag is of Providence met haar aanbod iets beters in handen heeft.

De Nationale Politie verklaart in antwoord op het WOB verzoek dat het belang van opsporing geschaad zou worden door meer informatie over Providence openbaar te maken. Deze redenering is moeilijk toepasbaar op het reguliere Providence aanbod aan trainingen en apparatuur, omdat deze niet zozeer voor opsporingsdoeleinden zijn bedoeld. Het argument over het schaden van het belang van de opsporing is wel van toepassing op digitale wapens.

In de afwijzing van het verzoek staat expliciet vermeld dat het bij Providence op individuele basis iets wordt afgenomen. 'Dit betekent dat zij worden afgenomen op het moment dat de desbetreffende afdeling een bepaald middel nodig heeft voor de politie- en/of opsporingswerkzaamheden,' staat in het antwoord van de politie. Dit lijkt op geen enkele manier van toepassing op de trainingen en apparatuur uit het Providence aanbod, maar wel op de Kailax Unlocker.

Met de Kailax *Unlocker* kunnen computers ontgrendeld worden waarbij gebruik wordt gemaakt van een internet verbinding. Max / Nir Levy geeft in de correspondentie met Hacking Team aan dat hij ze een zwarte doos aanbiedt waarbij de techniek en het IP adres van de server van de *Unlocker* worden verhuld. *'Option 1 is feasible only if you are prepared to supply to customers as a sub distributor black box technology which you do not own, have no deal understanding of the IP or maintain.'*

Als de Nederlandse politie de Kailax *Unlocker* gebruikt zou Nederland wel eens een tweede Israëlische zwarte doos in huis hebben gehaald. Die nog ondoorzichtiger is dan de afliuistercentrales van Nice Systems die Nederland eerder heeft aangekocht. En waarvan de minister van Veiligheid en Justitie in februari 2016 heeft aangegeven dat er meer duidelijkheid over het functioneren van de apparatuur moet komen. 'Bij de vele telefoontaps die de politie uitvoert, is de leverancier van de afliuisterapparatuur nauw betrokken. Maar essentiële informatie over de taps, wordt door diezelfde leverancier niet gedeeld. 'Er is geen garantie dat de politie volledig zicht heeft op alle storingsen in het tapsysteem' (NOS, 12 februari 2016).'

[Besluit Nationale politie op Wob verzoek over onder andere Kailax](#)

[Boeven vangen met dubieuze software van dubieuze bedrijven](#)

[Providence en de politie; Ketenaansprakelijkheid via een ex-agent](#)

[Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens](#)

[Providence en de politie; Ketenaansprakelijkheid via een ex-agent \(pdf\)](#)

[Bedrijfsprofiel Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens \(pdf\)](#)

[Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven \(pdf\)](#)

[Security Industry: links between Israel and the Netherlands? an inventory](#)

[Wikileaks Hacking Team documenten](#)

[Enkele e-mails uit HackingTeam gegevens over 2beuropa](#)

[Enkele e-mails uit Hacking Team over Kailax](#)

[Statement of Work Hacking Team en Kailax](#)