Kailax / Nir (Max) Levy
The magic hand of Israeli intelligence

The Kailax *Unlocker* is exemplary of the secrecy and lack of transparency surrounding the trade in digital weapons. The *Unlocker* is a tool with which a burglar can gain entrance to any Windows computer, without the owner becoming aware.

There is hardly any information about the *Unlocker* and its manufacturer Kailax in the public domain. The website www.kailax.com only contains the address details of the company (an address in Singapore), but no additional information. From public sources, we can only gather that the Berlin based company 2beuropa serves as an intermediary for Kailax.

It wasn't until the publication of the Wikileaks documents about Hacking Team in 2015 that we gained any insight into the existence of the Kailax *Unlocker* and the trade in this tool. The Kailax *Unlocker*, sometimes also referred to as *Unlocker/U-cap* appears to be a desirable digital tool. According to its manufacturer, who calls himself either Max or Nir Levy in his emails, Kailax distributes the *Unlocker* to seventy countries.

There is no way to check whether this claim is true. What does become apparent from the Wikileaks files is that Italian computer company Hacking Team has expressed an interest in adding it to their selection of products. In order to do so they approach British company Providence, which appears to present itself as an intermediary offering the *Unlocker*.

The Kailax *Unlocker* is emblematic of the secrecy and the lack of transparency surrounding the trade in digital weapons. The provenance of digital weapons is often unclear, which begs the question whether governments and intelligence services have any idea about the products they're buying and the companies with which they do business. The interference of intermediaries like Providence only adds to the lack of transparency and security.

Buro Jansen & Janssen executed a digital search into the provenance of the *Unlocker*, which led to Israel. The Kailax *Unlocker* appears to be Israeli in origin, and there are former members of Israeli intelligence involved.

Hacking Team and Kailax

From the Wikileaks documents published in 2015 we can see that the Italian company Hacking Team started showing an interest in the Kailax *Unlocker* at the beginning of 2015. With the *Unlocker,* any burglar can gain entry into a Windows computer and log on without the owner becoming aware. This concerns Windows Vista/7/8/8.1 Server 2008/Server 2012- 32/64 bit.

Hacking Team uses a similar technique with its Tactical Network Injector (TNI) for Firewire. In a 'Statement of Work' Nir Levy (Max) of the manufacturing company Kailax writes that the 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.*' According to Kailax it leaves little to no trace on the computer of the victim.

The Italians consider the *Unlocker* to be an asset to their digital burglary toolkit. They might be able to develop the tool themselves, but without a prototype this seems to be beyond the capabilities of the Italians. Hacking Team tried to acquire the tool at first via Kailax's offices in Singapore, but to no avail, the request is left unanswered.

On January, 23rd, 2015 Walter Furlan asks in an internal email to some employees of Hacking Team whether they are familiar with the Kailax *Unlocker*. A Swiss client of the Italians, the Kantonspolizei Zürich, has bought the *Unlocker* from 2beuropa. Another client, the Raggruppamento Operativo Speciale (ROS, Special Operations Group) of the Italian military police, also acquired the *Unlocker* from 2beuropa.

Following this, Giancarlo Russo of Hacking Team contacts Rami Zoltak of 2beuropa. This Berlin-based company operates as intermediary for Kailax. However, Zoltak responds that 2beuropa only deals with governments: '*We are working only with governmental offices, we are unfortunately unable to assist.*'

The Italians, however, are persistent. Russo bluffs that an 'LEA client' (Law Enforcement Agency) has expressed an interest in the *Unlocker*.

Eventually, Max, who first signs as Kailax Sales, responds. He says that Hacking Team's client can only acquire a USB *Unlocker* from Kailax' offical dealer, though he doesn't mention who this dealer is supposed to be.

Russo tries to convince Max one more time, but Kailax keeps refusing. Little by little they do reveal more information about the tool: '*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.*' According to Max the *Unlocker* has been sold to over seventy countries.

Max gives Hacking Team one option: they may install the *Unlocker* on their systems, which provides unlimited use of the tool. He asks Russo to guarantee that no one else is provided access to Kailax's IP-address: '*you also have to convince and assure us that no one else but you will have access to our IP.'* In this instance Max signs as Nir Levy (Max).

The Italian and Max exchange emails for a while, but they don't seem to get much further. Max keeps him at arm's length: '*We are both manufacturer suppliers of technology we are in essence competitors*', he writes. '*As you must know we are in same niche market that is usually based on trust*.'

Max does offer an intermediate solution. Hacking Team may operate as a sort of subcontractor, who can only sell the black box to customers: '*Option 1 is feasible only if you are prepared to supply to customers as a sub distributer black box technology which you do not own, have no deal understanding of the IP or maintain.*'

The Italians aren't comfortable with this option and they decide to approach some of their clients to get them to acquire the Kailax *Unlocker* for Hacking Team. Russo approaches the Swiss police, the Kantonspolizei Zurich.

The Swiss don't respond, so the Italians try their Italian client, the Raggruppamento Operativo Speciale (ROS, Special Operations Group) of the Italian military police. Hacking Team asks the ROS to order two *Unlockers*, but the military police don't seem to be all that keen to be used by Hacking Team.

Providence enters the picture

At the beginning of March 2015 contact between Hacking Team and Kailax breaks down. Then the Italians approach the British company Providence. Both companies are familiar with one another, and have tried to forge a co-operation in Australia and Ecuador, whereby Providence proposed to act as intermediary for products of Hacking Team.

Providence claims to have their own tool, the *'Windows Unlocker'* and '*U-Cap*' in their product range. This caters to a similar need as the Kailax *Unlocker*. Sometimes the Kailax *Unlocker* is also referred to as the *Unlocker/U-Cap*. On March 18th, 2015, Providence gives a presentation at the ISS World MEA in Dubai titled 'Tactical Bypass of IT Security', which members of Hacking Team attend.

A week later Giancarlo Russo of Hacking Team writes to Steve Minto of Providence stating that the Italians are interested in discussing a business relationship. Russo mails on April 8th, 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*.'

That same day Peter Stolwerk responds that they would be very interested to develop business relations with Hacking Team regarding the *'Windows Unlocker and U-Cap* (the special add-on for the *Unlocker*)'. At this stage Providence does not yet let on that they haven't developed the *Unlocker* themselves.

Stolwerk travels to Milan to give a presentation, but this doesn’t go smoothly. The Italians notice that the *Unlocker* leaves traces: '*Regarding the product I would like to have a feedback regarding the behavior we experienced during the demo (pop-ups on unlocked PC)*.'

Russo writes a report of the meeting and sends this to Stolwerk. It seems that in their meeting Russo and Stolwerk have discussed '*Partnership on Training programs for HT Clients. Social Engineering and how to get increasing benefit from HT technologies in real case operations.*'

From this report it becomes clear that Hacking Team wants to offer Providence a deal. It will accept Providence as some kind of distributor, in exchange for the 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.*'

As intermediary for Hacking Team, Providence can sell their products and train their clients to get the most out of the cyber weapons: '*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)*.' Providence may also offer their clients Hacking Team's software products: '*Providence would play more the role of an agent/consultant, rather than a distributor*'.

Concerning the '*Unlocker + U-cap*' it appears that the Italians would rather bypass Providence altogether and obtain all options to add the product to their assortment. '*Regarding the cooperation we feel that the first, easiest and fastest, way to cooperate is to include the USB Unlocker into our portfolio*', Russo informs Stolwerk.

During the meeting in Milan, however, it slowly becomes apparent that Providence has no say in the matter of the USB *Unlocker*. Stolwerk keeps referring to the manufacturer, which he only mentions by name once: 'Max'. Russo of Hacking Team writes immediately after the meeting in Milan, in which Max apparently has been mentioned: '*I expect you and Max to elaborate more on which cooperation options you consider viable*'. Stolwerk responds after talking to Max: '*Agreed, I spoke to Max and he is positive that we will together find a solution on this.*'
Hacking Team has already been in direct contact with Max at the beginning of 2015 about the possible acquisition of the *Unlocker*.

However, it isn't clear from the Wikileaks documents whether the Italians are aware of this or whether they have informed Providence of this fact.

Acquisition of new clients

Hacking Team is invited to the offices of Providence in Hereford, UK, in May 2015 to discuss further co-operation. The English company seems keen and asks Hacking Team, amongst other things, if it would be prepared to give their defensive cyber war training to 20 people from the Middle East. It looks like Providence still does not really understand what it is the Italians actually do. A subsequent phone conversation is needed to point out to the English that Hacking Team only sells digital weapons.

Besides seeking to acquire the 'U-cap + *Unlocker'*, the Italians also appear to be interested in acquiring new clients via Providence: '*We should go to Hereford and take advantage to visit them and also perform a demo for their sales team*', writes Vinci of Hacking Team.

Vinci also suggests organising a meeting with the British Ministry of Defence: '*There is a big MOD field camp in Hereford. We can try to organize a meeting with MOD (Ministry of Defence)*'. Hacking Team hopes Providence will prove useful with regards to the British MOD. There are, however, also other potential intermediaries, like Bob Quick of BlueLight Global Solutions. Apart from the MOD, there are also other potential clients they are interested in, like the National Crime Agency and BAE Systems, a large military weapons manufacturer.

Providence's offer of courses and trainings does not really interest the Italians. Vinci mails: '*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.*'

The Italians continue to be rather evasive and Providence appears to have a long way to go to be accepted as intermediary: '*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.*'

The Italians are proposing that if Providence wants to be considered as an intermediary for Hacking Team they will first have to deliver some easy clients. If Providence wants to pursue any clients themselves, they first need to run the details past Hacking Team, who will decide whether the English may proceed or not. They know from experience that some clients are already being served by another intermediary. This was the case in Ecuador where Providence suggested a company with which Hacking Team was already doing business via another intermediary (Robotec).

Deal or no deal

On May 8th, 2015, the relation between Max and Providence finally becomes clear. Stolwerk: '*The manufacturer 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.*'

Apparently, Providence have managed to persuade Max. According to Stolwerk, Providence is the distributor of the *Unlocker* for a large part of the world. He doesn't specify for which of the seventy countries that Max alleges the Kailax USB stick is distributed to, Providence acts as an intermediary. The other parts are being serviced by local distributors like 2beuropa.

Kailax is prepared to make a special version of the *Unlocker/U-cap* combination, especially for Hacking Team. Its development will be at the cost of the Italians. It seems nothing stands in the way of a successful meeting in Hereford. The Italians will be presenting their jewel in the crown - the Galileo RCS (Remote Control System) - and would like to see the full range of the English, '*in particular the training and workshop around cyber, covert entry, installation, surveillance, getting close to the targets, etc*.'

During the following months, the communication between Hacking Team and Providence mostly concerns the *Unlocker*. The Italians claim to have a customer for the Kailax USB stick and want to know how they can satisfy them. Giancarlo Russo of Hacking Team claims it concerns an Italian crime department and that Max is already familiar with it.

Stolwerk is eager to hold onto the Italians as possible partners and writes that there is some interest from The Netherlands in the products of Hacking team: '*I will speak to the guys here as I have some good news about the Netherlands for your products.*'

And still, the Italians do not seem completely convinced by the credentials of Providence. At the end of May 2015 a Hacking Team employee, who has studied the presentations of the English, writes: '*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*.' It appears that Providence started compiling their trainings at the beginning of 2015, so they only recently came into being and their email addresses are wrong.

Providence and Hacking Team are close to an agreement. The Italians are even invited to an exclusive gathering of Providence on August 26th, 2015. On the Hereford premises some workshops and a little barbecue have been organised. Apart from Hacking Team, Tac Up (a Providence outfit), Claresys Covert Video Surveillance (part of the British Ministry of Defence), and another twenty companies are invited, among them Cobham, Eomax, Sentinor. All 'friends' of Providence.

From the Wikileaks files it isn't clear whether Hacking Team finally added the *Unlocker* to their selection. In July 2015 Hacking Team is hit by a hack and internal documents about the company are published by Wikileaks. The company is also plagued by criticism over their distribution of arms to repressive regimes and it loses its export licence to trade outside the European Union.

Kailax - Mhyli

The correspondence between Hacking Team and Providence provides a revealing insight into the world of intermediaries in digital weapons. The Kailax *Unlocker* is exemplary of the mystery and lack of transparency surrounding the trade in digital weapons. The provenance of digital weapons is often shady, which raises the question if governments and security services are fully aware of what kind of products they're buying and from what kind of companies. The interference of an intermediary like Providence only adds to the opaqueness.

There is hardly any public information available about the company called Kailax. They do have a website (www.kailax.com), according to which the company is registered under the name of Kailax in Singapore: Kailax PTE LTD op 129 Lower Delta Rd. #09-03 CendexCenter. On the website are two sentences: 'We provide solutions in the cyber security domain' and 'For details please contact us at info@kailax.com'. Apart from that, it contains no information about products, expertise, revenue, investors, clients, etc.

Kailax itself has never been present at any of the different trade fairs for digital weapons or ISS World. It handles its sales through the company 2beuropa. This company is run by Rami Zoltak and is registered in Berlin on the MittenwalderStrasse. Zoltak comes from the world of real estate and trades in all kinds of products, among which digital weapons from Kailax.

On the website of 2beuropa it says that the company deals in 'taktischen Überwachung beste High-End-Hardware- und Softwareprodukte.' This concerns surveillance, tactical surveillance and high end hardware and software products. These products also encompass VIP security cases, drugs tests, smelly sprays as a public order measure, containers for the transport of explosives. On the website of 2beuropa it mentions Kailax as partner ever since the new version went online in 2014.

However, the website does not show what kind of products Kailax offers. What does stand out is that Rami Zoltak exclusively offers Israeli products. All of its partners are Israeli companies that are linked to the IDF, the Israeli army. 2beuropa indicates on their website that their partners include: Towersec, Karil International, Touch&Know, iDenta, Septier, ITP Novex, Memtex, Prosecs, ODF Optronics, ODI-X and Pro4tech. It also mentions Kailax among them, so it is reasonable to assume Kailax is an Israeli company.

Max – Nir Levy - Mhyli

The person corresponding on behalf of Kailax is Max. He also uses the name Nir Levy in his correspondence with Hacking Team, but it is unclear whether this is his real name. The Kailax website contains no further information about Max and/or Nir Levy. From the Wikileaks files it appears that Max/Nir Levy is the most important person within Kailax.

Buro Jansen & Janssen has tried to obtain more information about Max/Nir Levy. It appears to be the same person. He uses the email address max@kailax.com

There are a number of domain names linked to this email address, these are: s-mic.com, k-mic.info, *Unlocker*-u.com and toplucktrading.com. Few of these sites are functional, with exception of the *Unlocker*-u.com, which refers to kailax.com. Toplucktrading doesn't hold office in Singapore, but in Hong Kong, at this address: Unit 1203 12F CEO Tower, Admin Street: 77 Wing Hong St Cheung Sha Wan, Kowloon.

A digital search for Max and Nir Levy does not provide much information. The transcript of domain names in Nir Levy's name does however provide an interesting pallet. There seem to be multiple Nir Levy's: most of whom are Israeli, with one or two residing in the US. Regarding the above-mentioned domain names, like *Unlocker*-u.com, Nir Levy is mentioned as part of Kailax, with the email address of max@kailax.com. However, there are other domain names in the name of Nir Levy, that are linked to a former employee of the Israeli secret service.

Domain names

Of all the Nir Levy's who have registered domain names, there are only two that use the name Max. This concerns a Nir Levy with the email address max@mknowledge.com and a Nir Levy with the address max@mhyli.com

Both Maxes appear to apply to the same Nir Levy, who gives his address as: 7 shamir, hodhasharon in Israel, phone number +972.97480608. These details are also linked to the following websites: mknowledge-demo.com and mknowledge.com (linked to the email address max@mknowledge.com) and mknowledge.info, smthid.com and mhyli.com (linked to the email address max@mhyli.com).

Max from Kailax and Max from ‘mknowledge’ and ‘mhyli’ seem to one and the same. No other Nir Levy's that use the name Max can be found. Furthermore, the websites are equally inaccessible as those of Kailax.

On the website of Mhyli there's a short but remarkable presentation by Max, where he explains that he's also director of Pro4tech, a manufacturer of tactical surveillance video solutions (Pro4tech is also

connected to 2beuropa, which also operates as intermediary for Kailax). Max also writes on the Mhyli website that he is CEO of EDM, a company that deals in automation of internet information gathering. According to the 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*.'

The reason why Nir Levy (Max) is so evasive about his background, has to do with his career before he entered the world of business. Max worked for the Israeli secret service for 25 years. The Mhyli website reveals: *'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.'*

This is truly astonishing. On Kailax' website there is no trace of background information on Max or Nir, but on the Mhyli website he seems to be much more forthcoming about his background: *'He also completed various managerial technical and command courses in the Prime Minister's Office, including the Senior Commander course.*'

His colleague at Mhyli, Daniel Kario, also appears to have a past with the Israeli army. According to the website he has worked as *'group leader in a leading technological unit of IDF'* (Israeli Defence Forces).

It's impossible to determine whether Kailax is an independent company and is solely run by Nir Levy. The Kailax website does not provide any information whatsoever, nor does it provide any insight whether Nir Levy and Daniel Kario are qualified IT-developers who designed the tool themselves.

That Kailax' Max and Mhyli's Max are one and the same makes complete sense if you consider the mystery surrounding Kailax. Who would want to buy a digital weapon from a former employee of Israeli Intelligence? In some countries there would be a certain amount of reluctance to do business with Kailax if it were to become known that the company is Israeli, and even more if their contacts involved the Israeli intelligence services.

Clueless about origin *Unlocker*

During research into the relations of The Netherlands with the Israeli security industry, Buro Jansen & Janssen concluded in 2011 that the Israeli are doing everything they can to get a foothold in The Netherlands and Europe. They use their war in the occupied territories as evidence-based advertising for their products. At the same time they are trying to obscure their ties to Israel by using proxy foreign companies that handle the trade with certain countries.

The company called Kailax fits this profile. It's quite likely that Kailax delivers to similar countries/clients as Hacking Team and Gamma Group/Finfisher, either through Providence or another intermediary. It's very doubtful whether the buyers of the Kailax *Unlocker* are aware of the background of the company, its employees, investors and clients.

This question is also relevant regarding The Netherlands. In answer to a Freedom of Information (FOI) request by Buro Jansen & Janssen, the Dutch National Police declared that they have purchased 39 products or services from Providence. The police, however, refuses to specify which items they bought from them. It is not unthinkable that they purchased the Kailax *Unlocker.*

Providence is a relative newcomer to the security market. The British company offers trainings, accommodation and equipment. For trainings the Dutch police can make use of their own trainers and training centres. Most equipment the police buys from regular suppliers like Cellebrite, Nice-Systems and other companies, which leaves the question whether Providence has anything better to offer.

In answer to the FOI request, the National Police claims that it would harm their crime detection abilities to reveal any more information about Providence. This claim can hardly be applied to the regular selection of

Providence's offer of trainings and equipment, because they don't serve crime detection purposes. The argument could make sense if it concerns digital weapons.

In the rejection of the request, the National Police does explicitly state that it made the purchase from Providence on an individual basis: '*This means that they have been acquired if and when the concerning department needed a specific tool for police and/or detection activities'*. This doesn't appear to apply in any way to the trainings and equipment in Providence's selection, but it does apply to the Kailax *Unlocker*.

With the Kailax *Unlocker* computers can be unlocked using an internet connection. Max / Nir Levy indicates in the correspondence with Hacking Team that he offers them a black box that obscures the technique and the IP address of the server of the *Unlocker*. '*Option 1 is feasible only if you are prepared to supply to customers as a sub distributer black box technology which you do not own, have no deal understanding of the IP or maintain.*'

If the Dutch police does make use of the Kailax *Unlocker*, The Netherlands just might have brought in a second Israeli black box. One that is even more obfuscated than the wiretapping switchboards of Nice Systems that were acquired earlier. The Minister for Security and Justice referred to the previous switchboards in a February 2016 statement, saying that more clarity was needed about the functioning of the equipment. 'With the many telephone taps the police executes, the supplier of the tapping equipment is closely involved. But essential information about the taps has not been shared by the same supplier'. 'There is no guarantee that the police has a full overview of all interferences on the tapping system' (NOS, February 12th, 2016).

Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence (pdf)

Kailax technical details (pdf)

Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)

Providence and the Dutch National Police Supply chain liability via a former police officer (English translation of article from Observant #69)

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