Cyber Security Perspectives 2013

kpn

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

POLITIE

TNO innovation for life

Quotes
contributing partners

JAYA BALOO,
CISO KPN

Philip of Macedon, the father of Alexander the Great said that the way to get into an impenetrable fortress was to send a donkey carrying gold. Victory is not only to those who use brute force but deceit and cleverness as well. Treachery and cunning are nothing new and the digital realm is just as fraught with danger as the real world. Vigilance and rapid response are therefore necessary today to make a difference in the cyberarena, and WE are all gladiators.

WILBERT PAULISSEN, *DIENSTHOOFD DIENST LANDELIJKE RECHECHE, LANDELIJKE EENHEID, NATIONALE POLITIE*

Notorious bank robber Willy Sutton was alleged to have explained why he robbed banks by saying: 'Because that is were the money is.' Since banking is getting more and more digitized, banking-related crime is doing the same. Not only banking-related crime but all sorts of crime becomes digitized. Team High Tech Crime fights these new forms of crime. But we can not do this alone; we need our partners in both the public and private domain. Together we're the efficient answer to cyber crime. Expect us.

HENK GEVEKE,
MANAGING DIRECTOR DEFENCE, SAFETY AND SECURITY, TNO

Socrates once said "the more you know, the more you realize you know nothing". This certainly applies to the field of cyber security. Recent revelations, for instance regarding cyber espionage, have again shown the magnitude and complexity of the risks that we are facing. This is why TNO will keep collaborating with its many partners to jointly develop innovative solutions for a secure and reliable cyberspace.

WIL VAN GEMERT,
DIRECTOR CYBER SECURITY, NCTV

Famed for many wise words, Albert Einstein said: 'Life is like riding a bicycle. To keep your balance, you must keep moving.' For cyber security this is the case as well, and I would like to add that to keep moving, we must also keep our balance. In the second National Cyber Security Strategy, we have signaled the ongoing and dynamic balancing act between security, freedom and social-economic benefits in cyber space. It requires a joint effort involving all stakeholders in society to constantly find that right balance. Therefore, the coming years in cyber security will revolve around building the coalitions to ensure we achieve this.

Foreword

Dear Reader,

In front of you is the first edition of what we all hope to become a yearly tradition: a report on cyber security seen from different perspectives. Four parties, working in the Netherlands, have contributed to this report on security issues we feel are interesting and important for 2013. We hope to give you a peek into the dark side of Cyberspace.

By giving you a glimpse behind the scenes of what is happening in the Dutch security field we would like to show the threats that so often go unnoticed to the general public and share some worries that keep us awake at night. We hope that these experiences and insights can help you to develop your own defenses against the quickly changing threat landscape. 2013 has been a busy year in the field of cyber security, as is shown in the diversity of the subjects of the articles that range from specialist attacks against GSM networks to ransomware on common desktop systems.

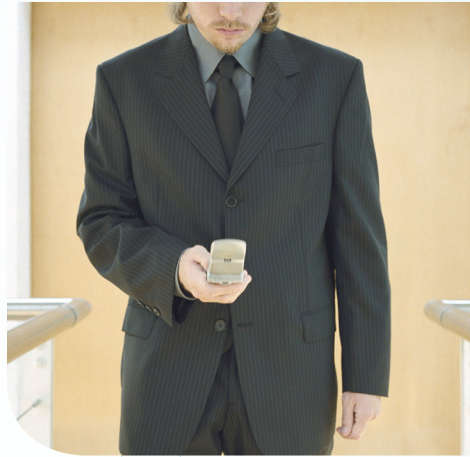*We wish you a safe and enjoyable read.*
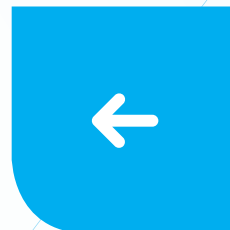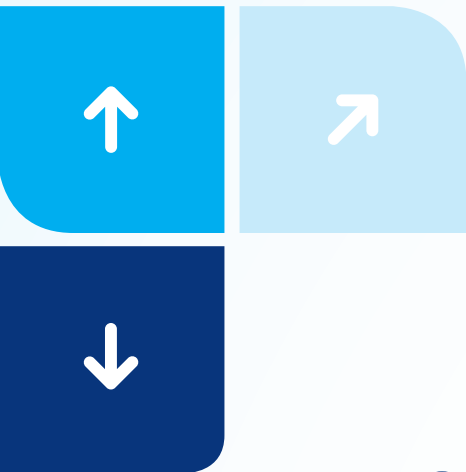
Overview contributing partners

> The National High Tech Crime Unit of the Dutch national police focuses on combating the most innovative and complex forms of cybercrime, with a high impact on society. Since 2007, this specialized unit has been able to solve a number of world-renowned cases, thanks to the close and kind co-operation of national and international partners, both from the public and private sectors. In 2013, the NHTCU expanded to a staff of 90 personnel, and was able to handle 15 heavy cases of high tech crime, besides being the 24/7 contact point for all 41 countries who have ratified the Budapest Convention on Cybercrime. In early 2013, the NHTCU proclaimed that, with partners, it would like to make The Netherlands the safest cyber country in the world.

> KPN is the largest telecom and IT service provider in the Netherlands. Our network is Dutch to the core. We have a clear mission – to help the Netherlands move forward through that network.We believe in a society in which communication technology makes life richer, easier and fuller. KPN wants to be the unifier of that society, for people and companies. At home, at work and on the move. We have the resources, and the technology and the reliable fixed and mobile networks.

> The 3800 TNO professionals put their knowledge and experience to work in creating smart solutions to complex issues. These innovations help to sustainably strengthen industrial com-petitiveness and social wellbeing. We are partnered by some 3000 companies and organisations, including SMEs, in the Netherlands and around the world.

> For more information about TNO and the seven societal themes that are the focus of our work, go to www.tno.nl.

> The National Cyber Security Centre (NCSC) is a government organization with its foundations in public-private cooperation. The NCSC strives to gradually encourage more and more private parties to become actively involved with the NCSC on many different subjects. One of which is the annual Dutch Cyber Security Report (Cyber Security Beeld Nederland) where the NCSC in co-operation with its partners describes the current state of affairs in cyber crime and digital security in the Netherlands. The NCSC contributed to the Cyber Security Perspectives 2013 in the form of the article 'Denial of Service within the mobile network'.

Content Cyber Security
Perspectives 2013

Cyber security events 2013

09-01-2013

Leak in development platform Ruby on Rails forces Dutch government to take authentication service DigiD off-line

31-01-2013

New York Times digitally infiltrated by Chinese hackers following an article on hidden riches for the families of Chinese leaders

01-02-2013

KPN recieves a responsible disclosure report on vulnerabilities in Zyxel modems from independent security researchers

02-02-2013

Large hacking attempt forces Twitter to reset the account passwords of 250.000 users

19-02-2013

Apple attacked by hackers infecting the Macintosh computers of employees with malware

21-02-2013

Security breach at Bit9, a supplier of digital certificates, remains unnoticed for 6 months. Perpetrators used malware with "exceptionally clever mechanisms"

04-03-2013

Two Dutch teenagers expelled from school after infecting the notebooks of their teachers with spyware

14-03-2013

Malware infection causes US National Vulnerabilty Database (NVD) maintained by NIST to go off-line for several days

27-03-2013

Anti-SPAM organisation Spamhaus hit by one of largest DDoS attacks of all time. The attack also affects some of Europe's major ISPs and internet exchanges

05-04-2013

Start of large scale DDoS attack on Dutch banks, causing disruptions in on-line banking portals and payment services such as iDeal

13-04-2013

Massive attack on Wordpress sites in an attempt to establish a server based botnet, thus acquiring substantial network capacity

02-05-2013

US Defense contractor Qinetiq turns out to have been infiltrated by Chinese spies on several occasions since 2007

05-06-2013

The Guardian a secret court order showing that US government had forced telecoms provider Verizon to hand over millions of phone records

06-06-2013

The Washington Post reveals the PRISM program, a secret espionage operation that allows the NSA access to data held by Google, Facebook, Apple and other US internet companies

07-06-2013

Pirate Bay co-founder Goffrid Svartholm Warg convicted to 2 years in prison for hacking IT company Logica and a Swedisch bank.

09-06-2013

The Guardian and Washington Post disclose Edward Snowden, a contractor at the NSA, as their source for espionage related leaks

18-06-2013

Criminal organization exposed for stealing sea containers with the help of hacking techniques such as malware, phishing and keyloggers

21-06-2013

The Guardian reports that British intelligence agency GCHQ collects and stores vast quantities of global e-mail messages, Facebook posts, internet histories and calls and shares these with the NSA

20-09-2013

Snowden documents published in German magazine Der Spiegel suggest that UK intelligence agency GCHQ is responsible for the espionage incident at Belgacom

25-06-2013

KPN recieves a responsible disclosure report on vulnerabilities in the KPN access network that give access to the management network of KPN

30-09-2013

Second National Cyber Security Research Agenda (NCSRA-II) for the Netherlands is published

23-10-2013

German government states strong suspicion that private cellphone of chancellor Merkel was eavesdropped by the NSA

27-06-2013

Hackers steal a digital certificate from browser manufacturer Opera and use this to push banking trojan Zeus to thousands of Opera users

04-10-2013

Adobe reveals that hackers broke into its network and stole the source code for several of its software products

02-11-2013

Dutch Defence organization reveals that it will recruit 150 cyber security reservists that can be called to action in case of an urgent digital threat

21-07-2013

Apple reveals that its on-line Development Center has been compromised by hackers. The website is taken off-line and will fully be rebuilt to avoid further security breaches

13-10-2013

According to the Duch government, there are no indications of Dutch telecom providers being hacked by the NSA

11-11-2013

Eurocommissioner Kroes calls for action against cyber espionage and warns that simply making espionage illegal will not suffice

22-07-2013

Renowned German code-breaker Karsten Nohl, uncovers a design flaw in around 750 million SIM cards around the world leaving them vulnerable to hack attacks

18-10-2013

Belgacom subsidiary BICS discovers that the software on some of its routers has been infected with malware

04-12-2013

Belgian newspapers report that Belgacom is still having trouble removing espionage malware from its routers

12-09-2013

Telelcoms giant Vodafone Germany reveals that cyber criminals have stolen personal data from 2 million of its customers and states that the attack involved substantial effort and insider knowledge

28-10-2013

Dutch government publishes its new National Cyber Security Strategy

05-12-2013

Facebook is forced to reset 318.000 accounts after discovering a large scale of password theft. The information was stolen through malware controlled by a botnet structure

16-09-2013

Belgian telco Belgacom issues press release about a digital breach of its internal infrastructure. Media suggest a sophisticated case of state sponsored cyber espionage
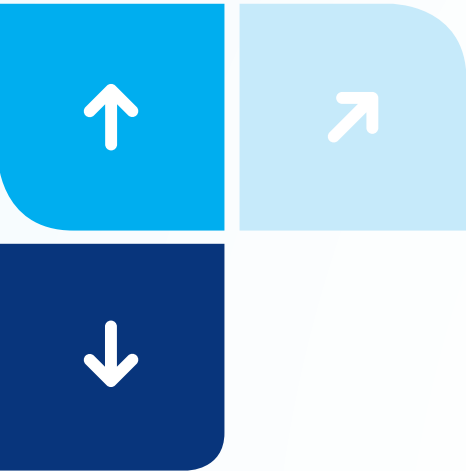
13-12-2013

Detectives of the Rotterdam Police arrest an 18 year old resident of Rotterdam on the suspicion of having hacked thousands of computers of home users.

Security Trends
to Watch in 2014

Authors: Richard Kerkdijk, Frank Fransen and Reinder Wolthuis, TNO

From the perspective of (cyber) security, 2013 has been a rather eventful year. This is illustrated by the overview of cyber security events presented in this report. The interesting question is of course which trends this vast amount of threats, incidents and otherwise troubling affairs represents. In this article we highlight five (cyber) security trends that we believe will continue to impact Dutch or even global society in 2014 and beyond.

Trend #1: Mainstream cyber attacks increasingly become available to the masses

Conducting cyber attacks no longer requires any technical skills and is steadily becoming more 'user friendly'. Hacking services can be bought as an online service, including online support if there are any questions. All major credit cards accepted. Ready to use hacking toolboxes, even available as plug & play USB sticks, are available and will do the job for you. All these easily available tools and services will cause a dramatic change in the hacker profile and increase the number of attacks. An example could be a small company that buys a DDoS attack (available for 10 dollars per hour) to bring down the website of its competitor. This could be cheaper than placing advertisements in the local newspaper. Of course

the example is illegal and one might get caught. Some perpetrators will try to reduce the chance of getting caught by utilizing an anonymous web service such as Tor (www.torproject. org). The issue is that the barrier to launch a simple cyber attack, which until recently was quite high due to necessary knowledge and skills, is rapidly becoming lower. This means more people will be able to launch cyber attacks and more damage will be done.

Trend #2: Targeted and sophisticated attacks occur closer to home

As described above, mainstream cyber attack techniques have become widely available as automated tools and services. The good news is that defense against most of these attacks has also become common; many providers of tools and services that will protect against these simple attacks are available. Many medium and large companies have implemented these measures, although improvement is still required (see trend #05). On the other end of the spectrum, however, we find highly skilled professionals that are rapidly progressing in knowledge and degree of organisation. In the past year, we have again seen an increase of complex, targeted attacks on ICT systems and infrastructures that are

very difficult to detect and mitigate.

In cyber espionage (targeted at capturing confidential data of the victim) we have seen that attack types known as "Advanced Persistent Threats" (APTs) now occur closer to home. Such attacks combine different hacking techniques that utilize several channels, vulnerabilities and methods, e.g. social engineering, malware infection, zero day exploits, poorly patched systems, weak passwords and insufficiently secured websites. Determined attackers can use these techniques to increase their impact. What makes things worse is that attackers try to avoid detection and mitigation by applying techniques such as stealth and self-replication. We also see a shift from attacks on generic platforms (such as windows platforms) towards specific operating systems of dedicated devices (such as routers). A recent incident at Belgian carrier BICS has shown an example of malware targeted at these specific operating systems. Common defensive security measures are unlikely to prevent this kind of attacks. As described in another article in this report, security monitoring of systems and infrastructure is essential in order to detect and mitigate any intrusions as early as possible.

DDoS attacks are also becoming more sophisticated and harder to mitigate. In the Netherlands, 39 large DDoS attacks were registered between January and

September 2013 by the NCSC. Common attacks that are aimed at saturating resources on network or protocol level can be detected and mitigated relatively easy. Usually DDoS traffic is diverted to another destination after detection, thus ensuring the proper operation of the targeted website. One thing to take into account here is to make sure that the DDoS service provider that mitigates the DDoS attack has sufficient capacity during the attacks.

Because common DDoS attacks do not provide large impact anymore, DDoS attackers now launch application layer attacks that crash the webserver. Such attacks are gradually getting more sophisticated. One example seen (http://www.incapsula.com/the-incapsula-blog/item/811-funded-persistent-multi-vector-ddos-attack) was a 100Gbps Network DDoS attack involving

specialized techniques and in-depth knowledge of how the company's website operated. These attacks typically are designed in such a way that separation between valid web traffic and DDoS traffic is nearly impossible. DDoS attacks will probably evolve further in the near future and new defense mechanisms to mitigate the attacks will have to be designed.

Trend #3: Cyber espionage is out of the shadows

Cyber espionage has been a hot subject of debate throughout 2013. Already in February, US incident response firm Mandiant released its APT1 report that outlined professional cyber espionage activities funded by the Chinese government. The report linked the APT1 group to more than 140 attacks in an endeavor to acquire intellectual property from US businesses.

In June the Washington Post revealed the existence of PRISM, a secret cyber espionage programme that allows the NSA access to data held by Google, Facebook, Apple and other US internet companies. And in August, Belgian telecoms provider Belgacom revealed that its infrastructure had been hit by sophisticated cyber espionage operations. German magazine Der Spiegel later published details about this attack, indicating that it was conducted by UK intelligence service GCHQ in an operation codenamed Op Socialist.

Much of the information on UK and US cyber espionage activities was put forward by a whistleblower called Edward Snowden. Among other things he revealed the existence of the GENIE programme, through which US intelligence allegedly placed some 85.000 "implants" in strategically selected computers across the globe. One might thus argue that the aforementioned Belgacom case is only the tip of the iceberg when it comes to US and UK cyber espionage operations.

Many nations of course spy on their rivals for military, political and industrial interests. This year's developments, however, have revealed that such espionage is conducted through internet (and related) channels at an enormous scale. What's more, such cyber espionage is apparently also taking place among partnering states. This

has raised some serious issues of trust, both among nations and in the reliability of (US or Chinese built) internet infrastructure.

It is likely that we will see more revelations about state sponsored cyber espionage in the coming years, among other things because whistleblower Snowden has only released a small fraction of its documentation on US espionage activity. A new trend that might emerge is the concept of "espionage for hire", analogous to trend #01. Some vendors of IT security products have already reported the existence of criminal organisations offering such services.

Trend #4 The individual becomes increasingly vulnerable

The number of connected pieces of equipment, in use by consumers, grows rapidly. Desk top computers, laptops, tablets and smartphones are very widely used today. But also equipment such as settop boxes, NAS equipment, media players, photo cameras, surveillance cameras, cars and smart watches increasingly are in use and connected to the Internet. In the coming years to be followed by fridges, washing machines, and other household appliances. An average household nowadays typically connects to the Internet with 10-30 pieces of equipment, each having an IP address. All this equipment

holds data, either locally or in the cloud. And it is not only meant for private use. A growing number of companies allows their staff to bring their own devices, offering more freedom to their staff and in addition save costs.

People are depending on the proper functioning of all this equipment and correctness and availability of the data. But most people are not experts in security and will make mistakes such as using the same password for several services. Moreover, they are not interested and only see security as an obstacle.

Meanwhile, service providers are looking for ways to utilize the broad range of available equipment as additional and possibly cheaper channels to offer their services. A striking example in this respect is the financial world, where paper transactions almost completely have been transformed into electronic transactions utilizing computers, tablets and smartphones. Of course, the use of multiple channels will increase the attack surface.

Some service providers are moving to a model where they put part of the responsibility of any damage on their users. The Dutch banks e.g., jointly have decided that they will no longer fully compensate damage resulting from attacks if consumers do not have secured their equipment sufficiently (http://www.nvb.nl/nieuws/2013/2365/

regels-voor-veilig-internetbankieren-bij-alle-banken-gelijk.html) . Other service providers have implemented additional security measures, as seen some time ago with the credit card companies, that have introduced additional passwords for online payments.

Increased use of electronic channels and electronic equipment also presents the service providers with the opportunity to automatically collect vast amounts of data. Data of users and data concerning user behavior . Of course most service providers seize this opportunity, because information represents value. The effect being that some service providers (e.g. Google: http://articles.washingtonpost.com/2012-01-24/business/35440035_1_google-web-sites-privacy-policies) gain very detailed knowledge about their users. Such information, when falling in the wrong hands, will present big opportunities to be misused for example in identity theft.

All of the aspects described above lead to the conclusion that the individual is becoming increasingly vulnerable. The dependency on personal electronic equipment grows, the attack surface grows because he or she utilizes more channels and equipment, the damage of incidents will become (partly) his or her responsibility, the need to manage a multitude of accounts will probably result in

a reduction of password strength and all information collected and stored present an inherent risk. It is clear we have to look for new ways of managing these challenges and protect the individual.

Trend #5: Investment in cyber security is not decreasing susceptibility to attacks

Both businesses and governmental agencies are devoting strong attention to cyber security. ICT intensive organisations such as telecoms providers and financial institutions are gradually enhancing their cyber defences and seeking collaboration with other organisations. Cyber security is also starting to penetrate the level of corporate boardrooms, although often only after a severe cyber incident has occurred. Dutch government has taken action as well, among other things by launching a new National Cyber Security Strategy (NCSS2) and a variety of awareness campaigns for the public. What's more, the Dutch National Cyber Security Center (NCSC) has (among other things) been extending its capabilities with respect to security monitoring. Much is therefore being done to improve the country's overall resilience to cyber attacks.

Having stated the above, we also see that the number of registered vulnerabilities in ICT is growing at
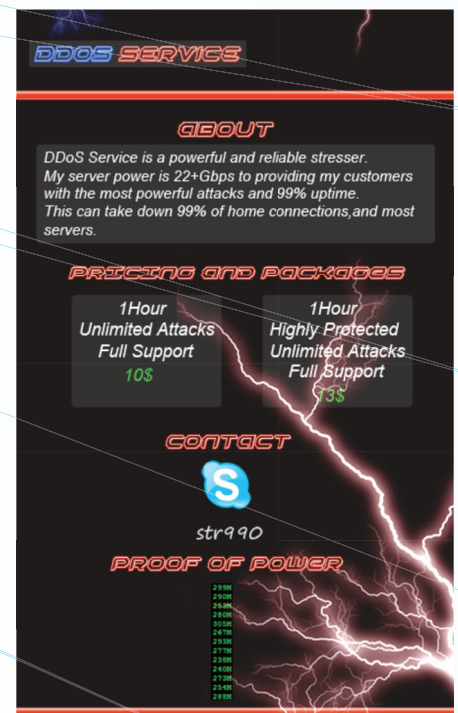
great pace and that such vulnerabilities are increasingly qualified as "severe". Moreover, the NCSC recently reported that many organisations still fall short when it comes to basic provisions such as patching and updating ICT systems and maintaining a solid password policy. Meanwhile the attackers are quickly enhancing their capabilities, thus amplifying the threat of cyber attacks. The latter is illustrated by some of the aforementioned trends.

All in all, present investments in cyber security barely suffice to remain at the same level of resilience. In the coming years, keeping pace with the attackers will continue to pose a challenge.

Ransomware: holding your data hostage

Author: Roeland van Zeijst, Team High Tech Crime, KLPD

In 2013, Dutch police put a lot of effort in the fight against ransomware. The National High Tech Crime Unit ran a major investigation against the criminals, while citizens and corporations assisted in combating the phenomenon together.

What is ransomware?

Ransomware is a program that blocks the computer (or data on it) and then asks the user for money to unblock it. Instead of starting up, the computer displays a warning, often showing a logo from the police or another law enforcement agency.

The blocking screen states that the user has been found guilty of a criminal offense, such as downloading illegal content, and therefore a fine has to be paid. Obviously, this is a false message and paying the fine will not unblock the computer.

The police are familiar with dozens of types of ransomware. The psychological impact of this malware increases. Whereas previous versions displayed a plain-text warning, newer adaptations will show the user on screen by means of their own webcam, or will play an audio clip where a male voice warns the user.

Developments in 2013

In October of 2013, the National High Tech Crime Unit discovered hundreds of Dutch infections in one month, for just one new variety of ransomware. Dozens of varieties are known and their numbers are growing. Antivirus companies estimate that the Netherlands is amongst the most severely hit countries in Europe.
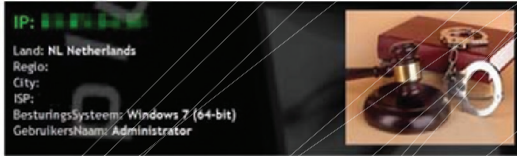
In 2013, the Dutch police asked the audience to assist in identifying the person behind the voice used in a specific type of ransomware. A national television broadcast led to dozens of tips and a heightened

POLITIE
Korps Landelijke Politiediensten
Openbaar Ministerie
CYBERCRIME POLITIE NEDERLAND

Nog beschikbare tijd: 47:59:52

paysafecard **Ukash**

IP:
Land: NL Netherlands
Regio:
City:
ISP:
BesturingsSysteem: Windows 7 (64-bit)
GebruikersNaam: Administrator

PIN-Code   Waarde
[ ]   [100 ▼]

1 2 3 4 5 6 7 8 9 0

Betalen PaySafeCard   Betalen Ukash

ATTENTIE! Uw persoonlijke computer wordt geblokkeerd om veiligheidsoverwegingen wegens de hieronder aangegeven redenen.

U wordt beschuldigd van het gebruik/opslaan en/of verspreiden van de pornografische productie wier inhoud wettelijk verboden is (kinderporno/zoöfilie/verkrachting etc.). Hiermee heeft u de voorwaarden van de internationale Declaratie over de bestrijding van kinderporno geschonden en daardoor wordt u beschuldigd van het plegen van een strafbaar feit waarvan artikel 161 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden van toepassing is.

De misdrijven van deze aard worden volgens artikel 161 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden gestraft met de vrijheidsontneming voor de duur van 5 tot 11 jaar.

Daarnaast wordt u ook verdacht van het schenden van de "Wet inzake het auteursrecht en naburige rechten" (het illegale downloaden van muziek, video, het gebruik van ongelicenseerde software) en van het gebruik maken van en/of verspreiden van de content waarop het auteursrecht rust. Daardoor wordt u verdacht van schenden van artikel 148 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden.

Volgens artikel 148 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden worden de misdrijven van deze aard gestraft met het opleggen van de geldboete ter waarde van 150 tot 550 van de basiswaarde of met de vrijheidsontneming voor de duur van 3 tot 7 jaar.

Vanuit uw computer werd er via internet een illegitieme toegang gekregen tot de voor het publiek gesloten informatie en staatsgeheimen.

U kon de illegitieme toegang opzettelijk uit hebzucht plegen of kon de illegitieme toegang zonder uw geweten en toestemming worden gemaakt omdat uw computer besmet is door de schadelijke software. Totdat er een onderzoek naar uw zaak afgerond is, wordt u verdacht van de onopzettelijke schending van artikel 215 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden (de "Wet over een zorgloos en nalatig gebruik van computertechniek/persoonlijke computer").

Volgens artikel 215 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden worden de misdrijven van deze aard gestraft met het opleggen van geldboete ter waarde tot €100.000 en/of met de vrijheidsontneming voor de duur van 5 tot 8 jaar.

Evenals bij de analyse van de in uw computer opgeslagen informatie is het vastgesteld dat er vanuit uw persoonlijke computer regelmatig spam e-mails worden rondgestuurd die u opzettelijk uit hebzucht heeft gepleegd of die zonder uw geweten en toestemming plaatsvinden omdat uw computer met schadelijke virussen is besmet. Deze spam e-mails verspreiden schadelijke software of illegaal pornografisch materiaal. Totdat er een onderzoek naar uw zaak afgerond is, wordt u verdacht in de onopzettelijke schending van artikel 301 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden (de "Wet over de bestrijding van spam e-mails en het verspreiden van schadelijke software (computervirussen)").

De misdrijven van deze aard worden volgens artikel 301 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden gestraft met het opleggen van geldboete ter waarde tot €250.000 en door de vrijheidsontneming voor de duur tot 5 jaar.

Wij maken u erop attent dat uw persoonlijke gegevens en verblijfplaats geïdentificeerd zijn en dat er tegen u binnen 96 uur een proces-verbaal kan worden aangespannen op grond van de bovengenoemde artikels van het Wetboek van Strafrecht. Daarna wordt de strafzaak naar de rechter overgedragen.

Conform de wijzigingen aangebracht aan het Wetboek van Strafrecht van het Koninkrijk der Nederlanden d.d. 10 juli 2013 en de Declaratie van de Rechten van de Mens kunnen de door u gepleegde schendingen echter als 'onopzettelijk' worden gekwalificeerd (als u deze schendingen voor de eerste keer heeft gepleegd) en dan wordt u niet strafrechtelijk vervolgd. Om aan deze regel in aanmerking te komen dient u een boete aan de Staat te betalen (die bedoeld is ter ondersteuning van bescherming van de internet cyberruimte).

Deze boete moet u binnen 48 uur voldoen vanaf het moment van het plegen van een strafbaar feit. Nadat deze termijn van 48 uur afgelopen is, wordt u gedurende de volgende periode van 48 uur informatie over uw persoon verzameld, en dan wordt er een strafzaak tegen u aangespannen.

Uw boete bedraagt €100.
U kunt hem met behulp van vouchers PaySafeCard of Ukash voldoen.

Alleen nadat u deze boete heeft betaald en het bedrag op de rekening van de Staat wordt bijgeschreven, wordt uw computer binnen 24 uur gedeblokkeerd.

Daarna bent u verplicht binnen 7 dagen alle schendingen die via uw computer zijn gemaakt, op te heffen. Hebt u aan deze voorwaarde niet voldaan, dan wordt uw computer weer geblokkeerd en er wordt een strafzaak tegen u aangespannen (deze keer zonder de mogelijkheid de boete te betalen).

We maken u erop attent dat u bij de betaling van de boete de juiste codes van de geldvouchers moet aangeven en evenals niet proberen de vouchers na de betaling in geld te verzilveren. Als u verkeerde codes invoert of probeert uw geldvouchers na de betaling te annuleren, wordt u -behalve hierboven genoemde overtredingen - nog in het plegen van fraude beschuldigd (artikel 377 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden; volgens dit artikel wordt er een vrijheidsontneming voor de duur van 1 tot 3 jaar voorzien) en er zal een strafzaak tegen u worden aangespannen.
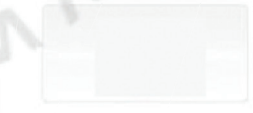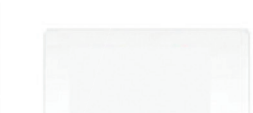
Waar kan ik een geldvoucher PaySafeCard aanschaffen?

PaySafeCards zijn vast en zeker dichtbij verkrijgbaar, in Nederland bijvoorbeeld bij veel tankstations (benzinestations), kiosken, supermarkten en sigarenwinkels. Overzicht verkooppartners: Trekpleister, HEMA, VIDEOLAND, T-Mobile, SuperCoop, TAMOIL, PostKantoor (www.Post.nl), KijkShop (www.KijkShop.nl), Gulf, Totaal Gemak, Primera, Coop Compact, Coop, Argos, AKO, Narvesen, Free Record Shop, Total, Texaco, Spar, Shell, Q8, Esso, BP, Avia.

Waar kan ik een geldvoucher Ukash aanschaffen?

U kunt Ukash ontvangen op honderdduizenden locaties wereldwijd, online, via portefeuilles, kiosken en bankautomaten. E-VA, MaxRetail,

ca | copyright alliance

INTERNET POLICE DEPARTMENT · EXTRA OMNES

ICSPA International Cyber Security Protection Alliance

CYBER CRIME UNIT

® Gecontroleerd door het Ministerie van Binnenlandse Zaken, Interpol, Copyright Alliance, International Cyber Security Protection Alliance.

national awareness. The underlying investigation lead to an arrest of a person involved in spreading ransomware.

To further increase pressure on their victims, the criminals behind ransomware have resorted for the first time to actually displaying child abuse material on screen, followed by the blocking message popping up. This led to the police sending out a national warning, which was broadcasted in all news bulletins. Fortunately, the police are able to verify if illegal contents were downloaded by a user or by malware.

Police forces worldwide co-operate in the fight against this phenomenon. In 2013, several gangs of ransomware criminals were arrested.

What can I do against it?

Ransomware infections are usually contracted through surfing the internet. There malware can be hidden in malicious (sex) advertisements but also in regular sites that had been hacked. Therefore, an infection does not indicate anything about the user's surfing habits.

Measures you can take:
- Optimize your backup cycle.
- Keep your operating system and applications up-to-date.
- Never surf the web without a firewall, antivirus and/or anti

malware. You should also consider using a pop-up blocker or advertisement filter.
- Never open unexpected e-mail attachments.
- Be alert whilst downloading software, music, movies, or television shows.
- If your system is equipped to read PDF files, display Flash sites, or execute Java applications, the risk increases. This can be partly mitigated by keeping Adobe (PDF/Flash) and Oracle (Java) software up to date.

A recent development, feared to grow further in 2014, is cryptoware. This kind of malware encrypts user files on their computer. Just removing the malware has no effect. You'll have to pay to get the key, although this still doesn't always solve your problem. The best way to tackle cryptoware is to, again, always make backups of your important and well-loved files.

How can we attack these criminals?

Like any extortionist, these cyber criminals too are driven by a quest for money. As long as computer users are willing to pay after having become a ransomware victim, the problem will continue to exist. The criminals behind the malware play into people's sense of shame (for instance when they have been on a pornographic site) to get them to pay

up quickly and not tell the police.

To not be traceable, the criminals demand that their victims pay using anonymous payment vouchers. These can be bought at most gas stations, post offices and convenience stores. After paying an amount of money, a voucher code is obtained which the victim has to enter into the blocking screen of his computer.

Subsequently, the computer generally does not get unlocked.

It has been estimated that in 2012 ten percent of Dutch ransomware victims paid. This was mostly in amounts of 50 or 100 euro. Through 2013, the percentage of paying victims dropped significantly (2,7%) after the major resellers of anonymous payment vouchers joined the police campaign against ransomware. Another success factor was increasing public awareness on how to remove ransomware using free tools.

Interested? Look at the ransomware-site to read more about it: www.politie.nl/politievirus

De politie waarschuwt:

COMPUTER GEBLOKKEERD? BETALEN HELPT NIET!
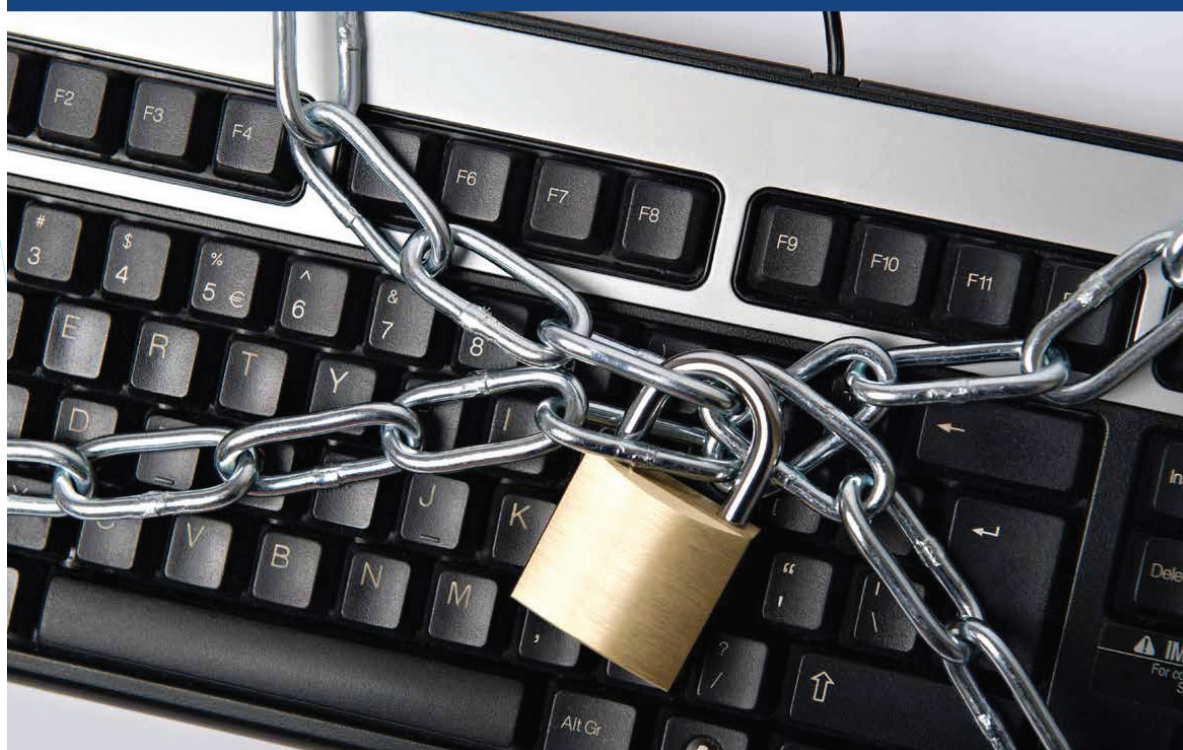
Het 'politievirus' blokkeert uw computer en vraagt om geld, vaak namens de politie. Betaal nooit, de blokkade gaat daarmee niet weg! De politie doet internationaal onderzoek naar de criminelen achter dit virus.

Virus verwijderen? Kijk op www.politie.nl/politievirus

NP-131016

《 waakzaam en dienstbaar 》

POLITIE

Engaging with the security community at large – Lessons from Responsible Disclosure

Author: Rob Kuiters, KPN CISO

25th of June, on the incident response handler's workstation, pops up an incoming chat message. "Hi, does the IP address 10.171.23.7 makes sense in your network? I have a notification from somebody who claims he can get to your system".

A little troubled the handler starts to investigate because private IP addresses are normally not known to the outside world. Pin-pointing an IP address within a large internal network can be a time consuming job. To speed up the identification of the system, he requested more information from the notifier. But the original notifier was not the one who had this information, the actual notifier made a call to the National Cyber Security Centre (NCSC) and wanted to stay anonymous because he was afraid of repercussions from the company.

This was how one of the responsible disclosure cases started a significant security improvement process at KPN.

Where there is light

Up to this point in time the current known information was not sufficient enough to directly take the appropriate actions to classify the incident. A request was made to the NCSC to get in contact with the original notifier of the findings. After a few e-mails, phone numbers were exchanged and more information was shared.

The original notification was brought up to the attention of the NCSC by a person with the nickname CrossWire. Being a member of a hackerspace community he was asked to look for the best way to get a working Internet connection in the abandoned school facility were the hackerspace got room for their community gatherings. CrossWire hooked up his equipment to a fiber optic internet connection cable and found that it still carried a signal. This roused his curiosity and to find out more about this connection he decided to investigate a little bit further. With some additional network equipment he discovered not only which operator the cable belonged to, but also noticed that he was able to see more technical network information than he ought to as 'just' a regular customer.

As he looked even deeper, he discovered that he could see other traffic streams that he definitely should not be seeing. In this case, he was able to observe management traffic from network equipment towards what looked like end user devices. Following this trail, he found an open FTP server where he could gain access to with an anonymous account. On this server he discovered all kinds of files containing potentially sensitive network equipment configuration details. At this point in time he realized that he had access to something which he probably should not have as a customer. The result of his probing led not merely to an usable internet connection, but also gave access to a part of the management network of KPN.

The follow-up

He decided to contact the NCSC because he was not sure about the reaction of the company involved and wanted an intermediary body to provide legal protection if necessary. The NCSC introduced CrossWire to KPN and in this first contact, CrossWire explained to the KPN incident response team the details of the vulnerability he discovered. Just to begin mitigating this particular incident, the response team notified the departments involved and the fiber optic connection at the abandoned school facility was terminated. The KPN incident response team met CrossWire at the site of the vulnerability discovery. After a short introduction, the two parties worked together to gather more details and technical information. This was then packaged to be handed over to the KPN's network resolution team so they could investigate further and take the necessary actions to mitigate the current risks CrossWire brought to their attention. Enhancements were made to the network level and the network support systems.

At this point in time the noticeable actions had been taken and for the outside world this case seem to be closed, however in reality the real long term resolution still needed to be implemented. A team of technical specialists directly started working on the issues to be resolved. For this operation, portions of the infrastructure had to be rebuilt and new procedures needed to be implemented and these needed to be communicated throughout the company. This seemingly harmless unterminated fiber optic connection resulted in countless hours of additional work to resolve the discovered issues and to ensure that such an incident cannot occur again in the future. For KPN, the effort was not only worth it, it was also absolutely necessary to bring this service back to the required level of security.

Importance of information

This responsible disclosure should be seen in the light of the trend that, more than ever, digital information has become an indispensable and valuable asset to our society. Most of us utilize information technology seemingly all of the time. Not only do we express our feelings, beliefs and state of mind across whatever social media is available. We also use our network to quickly gather information on topics relevant to us in our professional as well as personal lives.

Supporting this everyday need of millions of people is a brain like network which connects almost every part of this globe. What we nowadays call the Internet is a

mixture of networks and servers carrying our information across the globe. This highly sophisticated network is like a black box to most of us. Under the hood there are many programs running on different types of computers which transport and convert the information back and forth so that it is useful to us. Sometimes a glitch in 'the matrix' is discovered by the end users. Glitches that are not supposed to be there.

These malfunctions often result in headline news for the companies who are deliver internet and communication services. Companies over the years have become more and more aware of how important information security is for their customers. Security teams within companies are relatively small when compared to the operational networking teams and often do not have the required resources to address all the security issues that arise.

Relevance of Responsible Disclosure

Security researchers have been reporting security vulnerabilities to vendors and companies for some time now. However, they have not always met with a positive response. Traditionally, companies have reacted to these type of disclosures with threats of legal prosecution. The fear of becoming headline news in main stream media for the wrong reasons was a public relation nightmare that no one wanted. Furthermore, handled irresponsibly, disclosure of application and system vulnerabilities can end up jeopardizing the information security

of users utilising the service. The costs in terms of implementation and on-going efforts required in maintaining a responsible disclosure program is not insignificant. However, when compared to the event of being compromised due to not having such a channel for disclosure, then the effort does not seem so considerable.

For these reasons, an increasing number of companies have now introduced a responsible disclosure program into their organisation where security related vulnerabilities can be reported to without the risk of legal prosecution. This is the case as long as the notifier has not "actively misused" the information he or she had access to and he has given the company the required information and time to resolve the findings.

Other items to be agreed upon are the timelines and details of what is to be published externally. This can be a new area of discussion to some companies. Whilst openness is a good thing, care must also be taken to protect their intellectual property and customer data.

Therefore, describing in some detail what was discovered but, ensuring that this is done in a responsible manner, diminishes negative impact to the service or customers data. Openly discussing security vulnerabilities that exist may be uncomfortable but it will give an enterprises customers and partners the message that security is taken seriously.

Still work in progress

There is however also a down side to the whole responsible disclosure movement. Although the industry encourages people to bring up vulnerabilities they find on the services they use, the law considers this as a criminal act and the notifier may still face the consequences of the law.

This could discourage the members of the security researcher community from coming forward. For them it would be safer to disclose using the media as an intermediary and be granted the lawful anonymity of sources protection that journalist can provide.

As part of the Telecommunication industry, we definitely see the benefit of a responsible disclosure program but agree that current legal legislation governing this area can be discouraging and potentially leave the responsible disclosure notifier exposed. The fact that our industry is taking responsible disclosure seriously and seeing the benefit of it, should encourage lawmakers and politicians to alter the law so that adequate protection are given to the security community members who notify responsibly like CrossWire did to KPN. The saying "A journey begins with a first step" holds true here. The first step has now been taken, so let us continue and follow the road to make this a more secure industry for us all.

Denial of Service within the mobile network

Author: Bart Roos, National Cyber Security Center

In October of this year, RTL news went public with the fact that SIM cards of Vodafone can easily be blocked by a call to the customer service line. Result was effectively a Denial of Service (DoS) on the victims phone services. RTL news tested this with the telephone number of Ronald Plasterk, the Dutch Minister of Internal Affairs, causing this to become a national news item. While this vulnerability was easy to mitigate, this cannot be said of all DoS vulnerabilities known in mobile networks.

Within GSM networks there exists a protocol flaw that was already described over ten years ago, the so called "IMSI detach attack ". An "IMSI detach" is normally send by a GSM phone when it wants to deregister from the network, for example when its battery is about to go flat. It has been found that in the GSM protocol these detach messages are not authenticated and thus any malignant person could spoof these messages and make random phones unavailable. If the perpetrator would want to aim his attack at a specific GSM user he would require the IMSI of his victim. The IMSI is the unique identifier for each SIM card on the mobile network. To be able to do this the attacker would require equipment to inject the spoofed messages into the victims provider network.

1. http://www.blackhat.com/presentations/bh-asia-01/gadiax.ppt
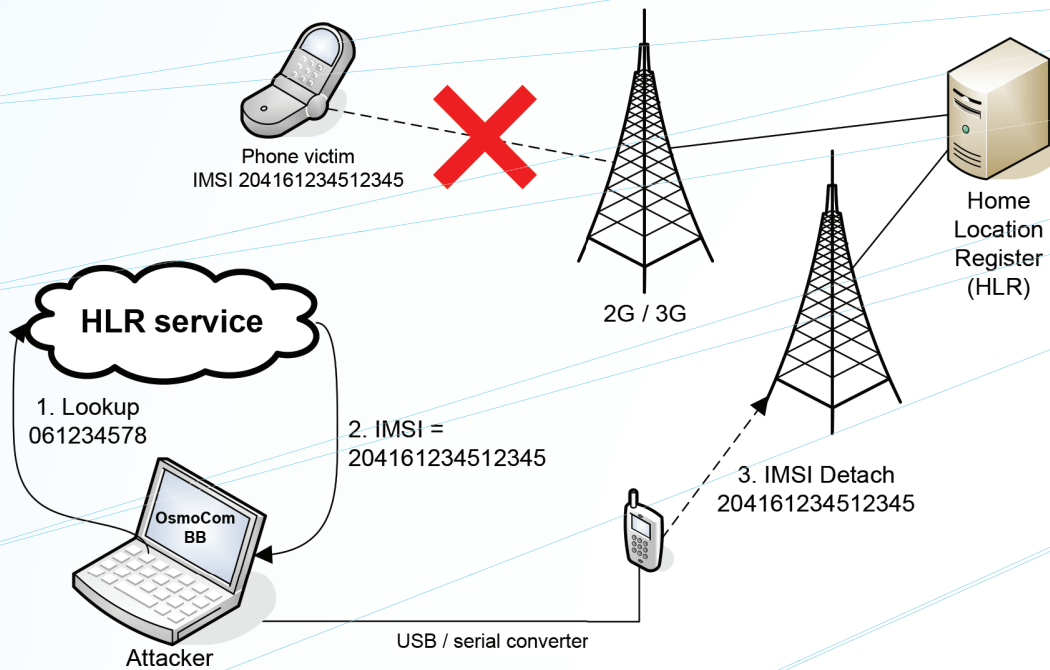
2. http://osmocom.org/
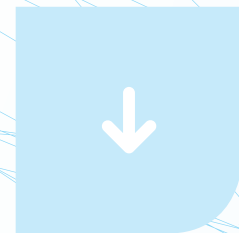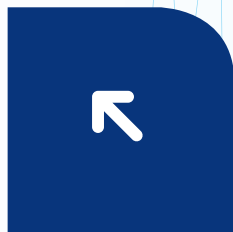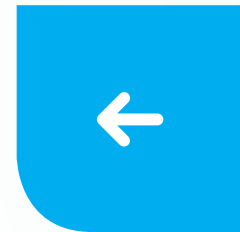
Figure 1 Schematic of an IMSI-detach attack.

It turns out that the tools enabling this attack have become more accessible to the public over the last year. There are several web services that provide an interface into the worldwide signalling network of mobile operators. This interface can be used to do an HLR query. The HLR is the central user database of each mobile network. Using a query like this it is possible to not only get information on the global location of the phone, but also on the victim's IMSI that is required for a targeted attack. The next required tool in the attacker's toolbox is a way to communicate with the GSM network. The open source project OsmocomBB offers this capability. Using a laptop, an USB cable and an ancient Motorola phone the hacker can now go ahead. Currently the OsmocomBB software has no built in capability to perform this attack but it seems only a matter of time until standard tools that do have an easy to use attack feature will become available. Additionally most mobile network operators combine the HLR for their 2G (GSM) and 3G (UMTS) networks into one database. This means that even users that have switched their phone to 3G-only mode are still potential victims of this attack.

Large scale attacks

A slightly different technique can be used to conduct a large scale attack. In this attack the evildoer listens to the paging request messages send out by the GSM network each time a call or SMS message needs to be delivered to a mobile phone. These messages will be addressed by the network to a temporary IMSI (TMSI), but it is often also possible to detach phones from the network based on this TMSI. The paging requests containing the TMSI are broadcasted within one so-called 'Location Area', meaning every device in that location area is able to receive these requests. Generally location areas are the size of a single town. By sending IMSI detach requests immediately after intercepting a paging request an attacker can, in theory, block an entire location area for all incoming calls and messages. Although it remains to be seen how much equipment is required to actually perform this attack in a busy area this scenario is certainly feasible.

Paging Request
TMSI 123456
TMSI 987654
TMSI 147885

1. Sniff Paging
Requests

OsmoCom
BB

Attacker

USB / serial converter

2. IMSI Detach
TMSI 123456
TMSI 987654
TMSI 147885
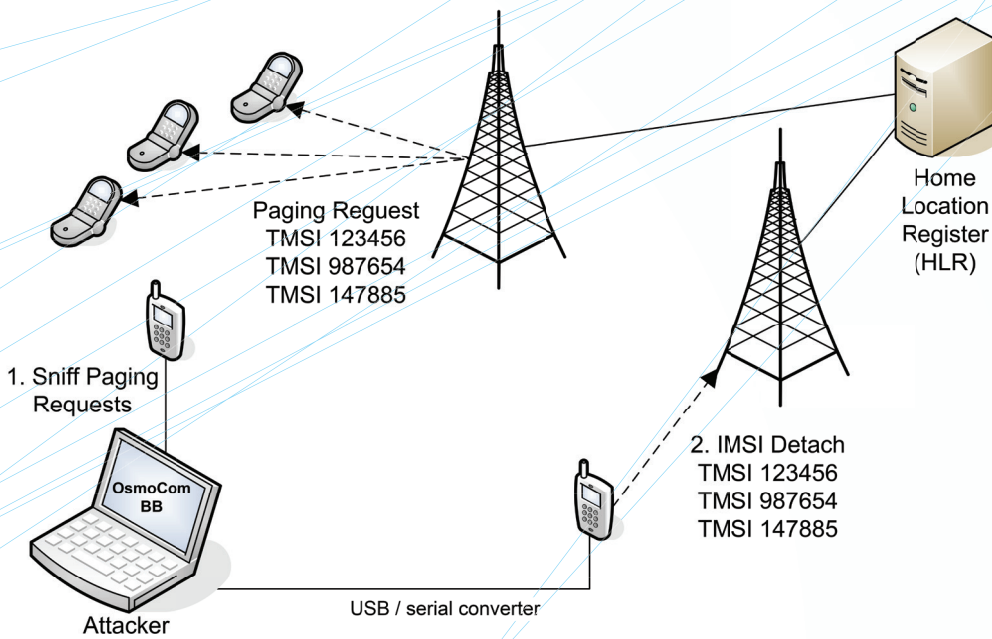
Home
Location
Register
(HLR)

Figure 2 Schematic of a large scale attack.

This attack effectively makes the users in the location area unreachable for any mobile terminated service like receiving calls or texts. The end-user is still able to initiate calls and send messages and thus does not notice the attack. Switching the phone off and on will negate the effect of the attack as this causes the phone to reattach itself to the network until the attacker sends out a new detach request.

Solutions

An end user can't prevent to become a victim of these attacks. Solutions for these issues should come from the providers, but they also have limited options.

Solutions can be:
- A strict separation of 2G and 3G networks can protect users who only use the 3G network.
- The provider can monitor suspicious messages or filter suspicious detach requests in the back-end systems.

There is however no simple solution to solve this issue.

To conclude we can state that tools to attack GSM networks are becoming more usable and accessible. It only seems to be a matter of time before ready to run toolkits will become available and GSM DoS will start to be a serious issue.

- Note by the editor: The attacks explained above do not apply to 4G services. However since 4G services are currently always delivered together with 2G/3G subscriptions for voice traffic this attack remains effective against current 4G subscriptions.

Snowden files

Author: Johan Romkes, KPN CISO

The most alarming news of last year has been the revelations from the US National Security Agency (NSA) delivered by Edward Snowden. This gave the general public an insight into the information the NSA is collecting, the methods used to obtain this information and the main information requirements of this agency.

The 2012 annual report of the AIVD (Dutch General Intelligence and Security Service) states: "Foreign intelligence services deploy very advanced digital attacks. These are so complex that they can exist in ICT systems for years without being detected by normal security software. This allows sensitive information to be siphoned off over a long period and on a large scale."

So we were warned, but without the information Snowden provided, it was not concrete enough for most of us. Most people or companies are not aware of what information they own or process that could be valuable to foreign intelligence services. Therefore it is hard to comprehend what the actual impact of espionage is on a personal or on a corporate level. With the leaked information regarding the NSA, we got a peek into the cyber espionage capabilities of the modern world.

What did we learn so far?

At the time of writing, 570 pages of NSA material have already been made public through selected media channels. It is hard to draw definite conclusions about the internal workings of the NSA based on a couple of slides and partly censored documents, but some of the information is very explicit. A list of leaked files can be found on www.eff.org/nsa-spying/nsadocs.

Here is a quick overview:
The NSA collects vast amount of data from the worlds telecommunication backbones and satellite connections. Next to intercepting data in transit, the NSA had deployed over 50,000 instances of malware worldwide to provide access to computers or other devices. They refer to this as Quantum Inserts (QI). The size of this data extraction network is comparable to a medium size botnet. With these QIs, they even gained access to smartphones of world leaders.

The NSA has also a more specific collections system, which they call PRISM. PRISM is a system that collects metadata from large cloud services of companies such as Microsoft, Google, Yahoo, Apple. Whether this is done with or without their knowledge is not known. It could be that they extract the data directly from fiber optic cables they have access to without involving the companies.

In the enormous amount of data that the NSA collects, it can be difficult to find the relevant and interesting data for the intelligence service. Therefor they created tooling to query this collected SIGINT(Signal Intelligence) data using Big Data technology. Xkeystore and BOUNDLESS INFORMANT are examples of this, which are mentioned in the leaked documents.

Another problem to tackle for the NSA is encryption. As the use of encryption has become more common nowadays, the collected data is not always directly usable for the NSA. For example, Google and Facebook switched to secured channels using HTTPS, thus making the NSA's lives harder. To get around this problem, the NSA invested in countering this encryption problem. They already have some capabilities against common encryption protocols like Secure Sockets Layer (SSL). The NSA also attempted to

modify cryptographic protocols to make it exploitable or does this by influencing policies, standards and specifications. Specifics about these programs are not known.

Another example of overcoming encryption to try and identify users of the The Onion Router (TOR) network. TOR is a free piece software that encrypt network data and hides the sender information of the data. The NSA is searching for exploitable vulnerabilities in the TOR software and is already capable of de-anonymising a small fraction of the TOR users by hand.

This list of capabilities of the NSA is overwhelming. There are a lot of people and journalists trying to interpret this information and form an opinion. For a corporate telecom provider, it is difficult to translate these capabilities into possible risk scenarios which could impact our business. The revelations of the Belgacom case made this much more concrete.

The Belgacom case

A telecom provider can be used to gain access to data stream of their customers. The AIVD describes this threat in their publication "Kwetsbaarheidsanalyse Spionage": "Through access into telecom providers networks, a foreign service is able to gain access to all their

core interests" (freely translated). In the same publication, the AIVD states that telecom providers probably are not the primary goal in espionage, but a means to get access to third party information. "As the society depends heavily on the infrastructure provided by the telecom sector, by attacking these telecom networks, the national security is almost immediately at stake."

This statement became reality for our southern neighbors when Belgacom discovered that they were hacked by a very capable opponent. Not long after Belgacom reported the hack of their infrastructure to the world, the German newspaper "Der Spiegel" released a presentation about "Operation Socialist". It then became clear that the Britain's Government Communications Headquarters (GCHQ) intelligence service, a close partner of the NSA, was the opponent who had access to the Belgacom network. The released slides show that the NAC (internal department of GCHG) has gained access to the Belgacom network and is trying to get a better foothold. The documents are probably created in 2010 according "Der Spiegel". This means that GCHQ had access to the Belgacom network for over a period of at least two to three years.

As the first step into Belgacom, GCHQ targeted employees

TOP SECRET STRAP 2
Key BELGACOM staff

- Identify Belgacom employees
  - NOC staff
  - In areas related to maintenance or security
- Selectors to enable QUANTUM targeting
  - Use of LinkedIn noted
  - Use of Slashdot.org noted
- MUTANT BROTH used to identify TDI/Selectors coming from identified range/proxy
- QI capability enhanced to allow shots on LinkedIn
- QI capability enhanced to allow 'white listing' when shooting on proxy

One of the slides of the presentation of the Britain's Government Communications Headquarters (GCHQ) intelligence service

(engineers and system administrators) with access to the network infrastructure. They used altered websites of Linked-In and Slashdot to deploy their Quantum Inserts. Employees within a telecom provider should be particularly aware of their value to foreign intelligence services.

From the slides it becomes clear that access to the Belgacom network is only a first step to a bigger plan. The main focus is enabling CNE (Computer Network Exploitation) access to Belgacom International Carrier Services (BICS), Belgacom' GRX network. GRX stands for GPRS (General Packet Radio Service) Roaming eXchange, where mobile internet data is being transported for roaming purposes. Belgacom is the owner of one of the largest international carrier services which provides GRX service to many telecom providers. The BICS' network stretches out to countries that are of interest to GCHQ and the NSA in the Middle East, Asia and Africa. A foothold in the BICS GRX network will give the NSA and GCHQ access to mobile data of users that are roaming. In the slides, it says that they getting close to the GRX core routers. When this objective is achieved, GCHQ wants to undertake MitM (Man in the Middle) attacks against specific targets.

So the whole purpose of the hack is to use a telecom provider to get access to data of specific customers. This could include spying on politicians in Brussels or those visiting Brussels and eavesdropping on other individuals of interest that make use of to the BICS infrastructure.

With the news of the hack on Belgacom, it became clear that organisations like GCHQ and NSA will go through a lot of trouble to obtain their required information and that they do not shun hacking targets in befriended nations. Even if the goal of the Anglo-Saxon partners was to only obtain access to communication of terrorist, this behavior is not acceptable.

View and actions of KPN

Is the control of the NSA and its close partner, GCHQ, a good thing or a bad thing?

Western Secret Services state that they expand their activities in the interest of their citizens. Supporters of open and free information see the activities as an unwanted state surveillance. KPN do not have a judgment on how far a secret service may go to protect their national interest. But we draw the line here:

We do not tolerate secret access to our information or the information of our customers. This is a no-go area for anyone, NSA or other party. The data of our customers and the integrity of the KPN networks is of the outmost importance to KPN.

After the Belgacom hack became public and based upon the identifiers of compromise, KPN checked their own networks. Sweeping for traces of what was known at that point in time, KPN researched several systems for every possible identifier. Nothing which relate to the Belgacom hack was found. This does not mean the investigation comes to a complete stop however. On the contrary, gradually the complete network will be inspected and not only will KPN look for known identifiers, but also look for anomalies in server behavior or suspicious network related events which could lead to unknown pieces of malware on our systems.

With almost unlimited resources that an organization like the NSA has access to, it becomes a difficult opponent to tackle. So with the knowledge provided by Snowden, it is almost impossible to state that the NSA or another organization with the same capabilities has no access to KPN information. But KPN is dedicated to bringing security up to the highest level and to make sure it becomes too difficult even for

these kinds of organisations to get in. At this time there is no indication that the NSA has access to the infrastructure of KPN. But if they are already in, we will find them.

What the Snowden files taught us so far, is that every individual and company should be aware of the possibility of eavesdropping on or penetration into their network by a foreign nation. With the information that Snowden provided to the world, the NSA is the bad guy for now. But do not forget: every nation spies and there is more that we are not aware of that is occurring in the spy underworld, than that we have heard of till now. If the alleged number of documents stolen by Edward Snowden is correct, there are still a lot of revelations to come in the coming months.

Whatever happens or is published, KPN will continue to take the foreign espionage threat seriously.

Side information

The NSA stands for the National Security Agency and is tasked with the global monitoring, collection, decoding, translation and analysis of information and data for foreign intelligence and counterintelligence purposes. The NSA is also called Signal Intelligence (SIGINT) agency. Next to this, the agency is also responsible for the protection of U.S. government communications and information systems.

The Government Communications Headquarters (GCHQ) is a British intelligence agency responsible for providing signals intelligence (SIGINT) and information assurance to the British government and armed forces. NAC (Network Analysis Center) is a department within GCHQ.

Worldwide wave of security concerns

Author: Jesse Helder, KPN CISO

Sometimes you feel yourself drawn into an argument you really do not want be part of. This happened to KPN when a U.S. house of representatives committee brought out a report on the 8th of October 2012. The report was titled: "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE".

This report contained heavy accusations, blaming the named companies of being vessels for Chinese espionage, but was found light on evidence by most security analysts. However, it was presented with such drama and drumroll, the impact caused a large shockwave across the world of telecommunications. It even caused a ripple to cross the big pond and wash up on Dutch shores, where the Dutch

parliament was happy to surf along on the worldwide wave of security concerns.

Before the report surfaced there already were multiple accusations of vendors being actively involved in cyber-espionage. In some cases these accusations led to a ban of Huawei or ZTE from certain projects like the Australian Broadband network. But now with this report in hand questions were starting to be asked in the Dutch parliament. And since KPN partners with Huawei in multiple large projects, like delivery of a Business Support System, mobile core network and DWDM networks, KPN felt it had to work on answers to these questions to alleviate the worries and provide clarity to its customers and the Dutch citizens.

Huawei has always vigorously denied any involvement in espionage, even getting their CEO to break a 25 year silence to the press to state "Huawei has no connection to the cybersecurity issues the US has encountered in the

past, current and future." . So it did not take long to convince Huawei to participate in a project to provide KPN positive assurance regarding the security of their products.

How did KPN ride the waves??

Within KPN a program was set up on how to assure the security of KPN and KPN's customers. As part of this program, Huawei and KPN engaged in security testing one of their mobile core network products used by KPN. This network element is called the Uniform GateWay (UGW) and basically is the main element for processing all data traffic on KPN's mobile network. A device in that position would be an ideal point for gathering sensitive data or eavesdropping on data traffic of unknowing subscribers and thus a perfect test sample.

To establish the overall security of this Huawei product, KPN joined forces with the European Network for Cyber Security (ENCS) to ensure third party verification. Together a two phased approach was set up to get a thorough security assessment of the UGW.

The first step was to do a Blackbox assessment in the test network of KPN. Two highly skilled ethical hackers "tortured" the device for two weeks in January 2013 to see if and where they could crack it open. They found several flaws in how things were secured. These findings only proved that Huawei suffers from the same legacy problem all Telecommunication vendors seem to suffer, which is a lingering difficulty in adjusting to an all IP world. While telecommunication networks used to be closed off secured environments, they have now entered the internet age. And while this has many advantages, the drawback is that security standards have to be much higher as the internet is not a safely fenced world as the old telecommunications networks used to be. This requires a change in thinking on security that is hard to grasp for many telecommunications vendors.

The second step was to review the "sourcecode" of the UGW application software. Now it needs to be understood that the "sourcecode" of a product is the most valued intellectual property for a company like Huawei. This code is the product of long intensive research labour and gives them their competitive advantage over the competition. Therefore it is almost never accessible to third parties. However, Huawei agreed upon this inspection on the condition it was conducted on their premises in Shenzhen, China. So we packed our bags and prepared to dig down deep in the holy grail of Huawei.

Arriving in Shenzhen in March 2013, we were surprised by the set up Huawei had arranged for inspections just like this. There was a strictly secured Cyber Security Center at our disposal. This center was obviously a brand new set up and it was very impressive to see the effort that has been put into this. A separately secured bunker like area was set up for code inspection that made sure the code could be inspected but never could any part of it be taken off the premises. Next to that a complete lab was at our disposal to actually test possible security flaws. Huawei had brought in the development team leader and two of his engineers to assist us if we had any questions. And in case they did not know, they had a development team in Beijing available for conference calls.

For two weeks we tested over long and intensive days with the joint team. All findings were immediately discussed and clarified with the development team. This gave us a clear insight into the how and why the code was written and also

provided us a chance to deliver direct input for improvement where we thought this was required. This lead to very productive discussions in which the Huawei development team displayed a great eagerness to improve on all findings reported immediately. In our experience such close cooperation between vendor and operator is not seen very often within the telecommunications world.

The overall impression here was the same as in the first test. Yes, there was room for improvements, and yes some issues were considered serious, but nothing that one would not expect to find in any other vendor's code when you were permitted to review their "sourcecode". And although it was impossible to review the entire source code base in two weeks, we did not find any of the cloak and dagger stuff that the US report seemed to indicate.

Consequences?

In the light of the publications by Edward Snowden, it would appear the U.S. accuses other countries of using "spying" techniques and methods they themselves employ without a second thought. This should however not distract us from the concerns at hand. Espionage is a fact of life and something that has always been there. However with the enormous take-off of internet and the ubiquitous access to the internet, the focus of spying entities will be more and more in this arena.

Off course it could be a strategy of any government to build-in spyware into equipment of vendors from their country. However this would result in a significantly large number of people to have knowledge of such an operation. And the question that should be asked is: is this really an efficient way of going about it? The security implementations of most telecoms products allow for a lot cheaper and less obvious ways to get to our data. Who needs an agent inside a company when the basic building blocks like outdated versions of the Apache webservers and Linux operating systems already contain security vulnerabilities?

What to do about it?

The first thing to keep in mind is that it is impossible to protect networks and services from intruders with unlimited time and resources. However the culprit's lives gets a lot more challenging if the operators and vendors work together on the basic security process of system hardening, security patching and segmenting of their network elements and applications. There needs to be a different focus on security within the industry, in which a joint effort is required from vendors, operators and national intelligence agencies. The role of vendors is to deliver secure products through secure coding standards and first party hardware and software vetting of their products. Operators should then deploy these products in a secure architecture and with well secured configurations, while national intelligence agencies should focus on preventing foreign intelligence gathering within their jurisdiction.

It is only by close cooperation and unfaltering dedication to their responsibilities by all three parties involved that secure networks and services can be delivered.

1. http://www.theverge.com/2013/5/9/4314912/huawei-ceo-breaks-silence-denies-us-allegations-of-china-espionage

Security Monitoring and Incident Response

Authors: Richard Kerkdijk and Reinder Wolthuis, TNO

In the past few years, many organisation have sought to establish or further enhance their security monitoring and incident response capabilities. A notable trend has been the emergence of dedicated security monitoring facilities (often referred to as Security Operations Centers). This article will explore the essentials of security monitoring and incident response and reveal some lessons learned in recent projects on the matter. First and foremost, however, we will elaborate on some of the trends and developments that have made security monitoring and incident response essential in the present era.

Why prevention no longer suffices

As explained earlier in this report, attacks on ICT systems and infrastructure are becoming increasingly sophisticated and targeted. What's more, present day attacks are often conducted by well organised and highly skilled professionals, contracted by organised crime or even sponsored by national governments. It is therefore becoming increasingly difficult to avoid security incidents through preventive measures. In fact, if the adversary is sufficiently motivated and competent, averting such incidents may not be realistic at all.

In parallel to the above, vulnerabilities in ICT systems and software surface at a dazzling speed. In its most recent threat report, the NCSC revealed that the number of registered vulnerabilities in mainstream software grew by 27% in 2012 and that such vulnerabilities are increasingly qualified as "severe". Proactively remediating such vulnerabilities is time consuming and sensitive to error, especially in a large and complex ICT environment. As vulnerabilities emerge at higher rates, it will become increasingly difficult for organisations to maintain fully patched and updated infrastructures.

The above does not imply that organisations should no longer invest in preventive measures such as firewalling, access control, security patching and malware defence.
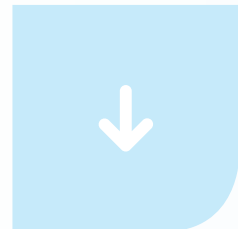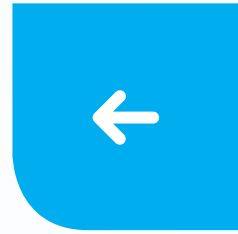
Contrary, the most recent NCSC report suggests that Dutch organisations still have much to gain when it comes to prevention. What the above developments do reveal, however, is that organisations cannot fully rely on preventive measures to avoid damage due to cyber attacks. Complementing such measures with effective security monitoring and incident response provisions has become a clear necessity.

Essential setup

Present day security monitoring encompasses two distinct activities:

1. *Security incident monitoring.*
   This refers to active and continuous monitoring of security relevant events in ICT infrastructures to promptly detect any (attempt at an) attack and initiate responsive actions that minimise subsequent damage.

2. *Vulnerability monitoring.*
   Systematically assess vulnerabilities in IT assets and initiate remediation thereof. Such activity is intended to avoid security incidents from occurring and is thus a natural extension of incident monitoring.

Organisations will usually deploy commercially purchased vulnerability scanners and Intrusion Detection Systems (IDSs) in their infrastruc-

tures to monitor for vulnerabilities and incidents, respectively. In addition, organisations might employ a so called Security Incident and Event Management (SIEM) solution, thus enabling correlation of security events from various source systems (e.g. IDS alarms and security logs).

Security monitoring operations can only be successful if the aforementioned security systems are operated by adequately skilled security analysts. Such specialists assess vulnerability reports and security alerts to determine an appropriate response. Actual execution of responsive actions usually resides with the operational teams that are responsible for managing the ICT assets. Large and mature organisations will also have a CERT1 or CSIRT2 function in place – a team of highly skilled security experts that can provide specialist support where required. In such a setup, security analysts will usually coordinate response for common (known) security occurrences whilst the CERT or CSIRT has the lead in complex (or otherwise unknown) cases.

In recent years the trend has been to unite security monitoring duties (i.e. provisions for and work conducted by the aforementioned security analysts) in a centralised security service facility, usually referred to as a Security Operations Center (SOC). Such centralisation has a

number of benefits, among which the consolidation of scarce skills and expertise in a team of substantial mass. Here we note that many organisations also incorporate other operational security duties in their SOCs such as the maintenance of firewall configurations or cryptographic key material. Unification of security monitoring capabilities is, however, usually the primary driver for establishing a SOC.

The above provisions will be most effective if incident response procedures are adequately documented and periodically exercised. Ideally, organisations maintain an incident management manual or handbook that addresses first (SOC), second (CERT/ CSIRT) and third line response to security incidents and vulnerabilities. Here, third line response refers to escalation, i.e. a procedure in which response coordination is elevated to higher levels of management as severity and impact of the incident or vulnerability increase.

Getting started

For any organisation that requires security monitoring capabilities, the first fundamental choice is whether to establish this an in-house provision or to employ a specialised service provider. Large, ICT intensive organisations that consider (cyber) security as a core competence will

1. Computer Emergency Response Team
2. Computer Security Incident Response Team

usually opt for an in-house solution. This is illustrated by the fact that SOC facilities have become quite common at telecoms providers1 (e.g. KPN), financial institutions (e.g. Rabobank and ING) and government bodies (e.g. the Dutch tax service), to name a few. For organisations that wish to avoid this capital investment, outsourcing security monitoring provisions to a third party can be a viable alternative. There are many competent providers of such services from which an organisation can choose the most suitable partner for its specific needs and context. It is important to realise, however, that external service providers will rarely acquire the in-depth knowledge of an organisation's business and infrastructure that internal specialists have. Thus, outsourcing of security monitoring capabilities often implies some concessions regarding the accuracy with which alarms are raised and prioritised.

Incident response capabilities are less easily outsourced, although providers of commercial CERT services do exist. Any organisation where cyber attacks pose a serious risk will usually establish an in-house CERT or CSIRT function. A common model is to combine a small core of dedicated CERT/ CSIRT staff with a pool of part-time specialists that offer supplementary resourcing or specific expertise.

Some other lessons learned in recent monitoring projects are as follows:

• *Start small and define gradual path for growth.* In case of large ICT infrastructures, a newly established SOC cannot immediately cover all relevant ICT assets. Fine-tuning configurations of monitoring systems requires time and dedication. If this process is not carefully played out, security analysts will end up looking at false alarms only.

• *Build relationships.* Effective security monitoring and incident response involves a variety of internal and external stakeholders. Organisations should invest in relationships and working agreements to make all entities function as one coherent team.

• *Seek easy accessible 24/7 capability.* Many organisations have the desire to monitor for security incidents on a 24/7 basis, but experience the cost of resourcing as a hindrance. The company might, however, already have 24/7 staff in place for other purposes and in some cases these might be trained to perform first line monitoring during nightly hours.

In addition to the above, it is worthwhile to inventory building blocks that are readily available in the organisation. There might, for instance, be small scale implementations of an IDS or vulnerability scanner in place that can serve as a starting point for a more elaborate and professional SOC.

Anticipated developments

Acquiring and assessing security intelligence (e.g. regarding new threats) is an important requisite for effective monitoring and response operations. The amount of security intelligence that is relevant to an organisation is steadily increasing. At present, processing such intelligence and employing it in actual operational security processes (i.e. actually putting the intelligence to work) involves much manual labour. CERT teams might for instance identify a new threat and put this forward to the SOC via e-mail, at which point it is up to the analysts in the SOC to see if and how they should incorporate this into their monitoring operations. An interesting next step would be to streamline and possibly even automate the process of exchanging cyber threat and incident information as well as (semi-) automatically translating such intelligence to actual security operations. The authors expect that organisations will devote much attention to this topic in the coming years.

3. From its yearly telco security benchmark, TNO is familiar with 9 telco SOCs across Europe, most of which were erected in the past 2-3 years.