Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

Reporting and Analysis Centre for Information Assurance MELANI
www.melani.admin.ch

INFORMATION ASSURANCE

SITUATION IN SWITZERLAND AND INTERNATIONALLY

Semi-annual report 2015/II (July – December)

28 APRIL 2016
REPORTING AND ANALYSIS CENTRE FOR INFORMATION ASSURANCE MELANI
http://www.melani.admin.ch

1 Overview/content

2 Editorial

MELANI: Continuing the work undertaken and reinforcing partnerships with the private sector

Jean-Pierre Therre, Executive Vice President/ Head of Technology Risk & Business Continuity, Banque Pictet & Cie SA, Associate Fellow GCSP, Lead Lecturer UniGE.

Within the framework of the national strategy for the protection of Switzerland against cyber risks, the strategic objectives assigned to MELANI are the early identification of threats and dangers in cyberspace, the reduction of cyber risks, especially of cybercrime, cyberespionage and cyber sabotage as well as the improvement of the resilience of critical infrastructure.

In this essential context for increasing the operational resilience of all stakeholders in both the public and private sectors, the MELANI team diligently strives to attain the objectives set, despite the still limited resources. But MELANI also endeavours to support sectoral initiatives aimed at reinforcing the sharing of important information as well as structured exchanges between the stakeholders in the main economic sectors.

For example, the half-yearly meetings that bring together a large number of representatives of the banking and financial sector have become benchmarks. Experts attending these events are provided with a summary of the complete range of national and international threats.

With the same aims of exchange and collaboration in mind, MELANI organised the Swiss Cyber Risks 2015 conference at the Stade de Suisse in Bern on 2 November 2015. The event was attended by many experts from the private sector, the army as well as the political arena and enabled fruitful discussions between the public and private sectors.

These efforts help to reinforce a real public-private partnership (PPP) which is pursued by all of the professionals concerned in view of the increasing number of cyber threats and their more complex and international nature. Action in the areas of prevention, detection, response and crisis management can no longer be ensured by isolated institutions, but rather by all national stakeholders in a coordinated and structured manner. A good example of this is the partnership between MELANI and the Swiss Cyber Experts (SCE)[1] association, which enables the knowledge of various experts to be pooled for the purpose of effective diagnostics in the event of a critical cyberattack.

The MELANI team, led by Pascal Lamia, has earned recognition and gratitude from all of us for their various information-sharing initiatives and their work on cross-sectoral coordination.

[1] https://www.swiss-cyber-experts.ch/ (as at 29 February 2016)

3 Key topic: Handling security vulnerabilities

Directly or indirectly, internet users are constantly exposed to security vulnerabilities of one sort or another. In 2015, a total of 6,419 vulnerabilities worldwide were entered in the database kept by MITRE[2], a non-profit organisation that systemically records vulnerabilities. However, only a very small number of these made the headlines. It can also be assumed that some of the security vulnerabilities were not entered in this database as they were not reported to the manufacturers for whatever reasons.

In contrast, the range of devices connected to the internet which use an operating system's components and the corresponding *libraries* is steadily growing. This in turn increases the impact and scale of the individual security vulnerabilities. Furthermore, many of these systems are generally not updated automatically. Be honest: when was the last time you renewed the *firmware* on your *router* or updated your internet radio's software. Missing or unperformed updates are thus a huge problem in terms of the increasing number of security vulnerabilities each year.

3.1.1 A lack of update policies

Meanwhile automatic updates belong to the standard process in many areas. But the Stagefright security bug that was made public in July 2015 demonstrated perfectly that this is not the case everywhere. An efficient, fast update process was lacking for the Android systems. It was no surprise when a 2011 study concluded that 56% of all Android smartphones were running under an outdated operating system.[3] It often takes a long time for updates to find their way from Google to the consumer, because Google depends both on smartphone manufacturers, such as Samsung or LG, and on individual mobile providers when dispatching updates. Before being distributed, mobile providers must test and certify the updates offered to them by manufacturers. Apple, on the other hand, can distribute its updates directly to customers. Following the Stagefright incident, Google announced a monthly update cycle. Some mobile phone manufacturers want to pursue this practice and are engaged in talks with network operators. You can find further information on the Stagefright bug in section 5.6.1.

Content management systems (CMS) are another problem area. While updates are generally made available quickly for large CMSs, the motivation of operators to install them often leaves a lot to be desired. This was shown clearly in the last MELANI semi-annual report.[4]

3.1.2 The lucrative business of security vulnerabilities

Before a security vulnerability can even begin to be remedied and a *patch* produced, the manufacturer must first become aware of it. Although this might sound straightforward, it is

[2] http://www.cvedetails.com/ (as at 29 February 2016)

[3] https://www.carbonblack.com/files/info-graphic-orphan-android/ (as at 29 February 2016)

[4] See the MELANI semi-annual report I/2015, chapter 3 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-1.html (as at 29 February 2016)

not always the case. The security business market is extremely competitive and dealing with security-related information is always a balancing act. Different interests are at play, including financial ones of course.

The attack on the Italian surveillance software company Hacking Team in the summer of 2015 and the subsequent publication of confidential business data is a good case in point. In addition to surveillance software and personal emails, the stolen data also contained various *zero-day exploits* that Hacking Team had purchased. In one case, the company paid a Russian hacker USD 45,000 for a *Flash* bug.[5] It is not known who else the Russian hacker sold the bug to.

Specific businesses involving surveillance software, espionage and the operational side of national digital armament policy are not openly discussed. It is therefore difficult to estimate the extent and number of zero-day exploits that are in circulation. Chaouki Bekrar, former CEO and head hacker at VUPEN, goes against this confidentiality principle. Back in 2012, Bekrar said in an interview that not even for USD 1 million would he sell security bugs that he found to the software manufacturer, but only to his own clients, which in his specific case meant NATO partners and governments. In the meantime, Bekrar has set up the company Zerodium, which also specialises in ICT device surveillance. In 2015, he launched a one million dollar competition in the company's name so that hackers would inform him of a method of using *Jailbreak* to covertly hack into iPads and iPhones running on the latest operating system iOS 9.1.[6] His competition was a success. As this example shows, the zero-day market follows common market rules: the more exclusive the security bug, the higher the sum paid for it.

To ensure that researchers report security bugs to software manufacturers and do not sell them to the highest-bidding third-party company, rules must be defined and the corresponding incentives created. In the ICT security community, there is a large number of people who campaign for the formulation of such best-practices without gaining from it financially. On the other hand there is no consolidated approach foreseen from manufacturers to whom vulnerabilities will be reported and which should produce patches. When manufacturers fail to take the reported vulnerability seriously or, worse still, even threaten to report the person reporting the bug to the police, it is not surprising that these vulnerabilities are published unannounced or appear on the zero-day market before an update to remedy the vulnerability becomes available.

The case between the US security company FireEye and ERNW, a security research firm based in Heidelberg, illustrates just how sensitive the issue of vulnerability reporting can be. An ERNW researcher found five security bugs in FireEye's Malware Protection System and reported them to FireEye. ENRW had planned to publish the bugs after a 90-day period. What ensued was a legal dispute over the content of the advisory that ENRW had intended to publish. FireEye felt that the advisory contained too much information on the inner workings of its product, whereas ERNW argued that the information was needed to understand the vulnerabilities. Moreover, the workings of this vulnerability were due to be

[5] http://arstechnica.com/security/2015/07/how-a-russian-hacker-made-45000-selling-a-zero-day-flash-exploit-to-hacking-team/ (as at 29 February 2016)

[6] https://www.zerodium.com/ios9.html (as at 29 February 2016)

presented at the London-based 44CON security conference. However, FireEye had already obtained an injunction to ensure that only a highly censured version could be presented.

3.1.3 Responsible disclosure

Different countries and software companies have recognised that there is a lack of rules and processes, and have taken action: to ensure that security vulnerabilities are uncovered responsibly, they have developed responsible disclosure processes and have put in place initiatives, known as *bug bounty* programmes, for the identification, elimination and disclosure of software flaws. Examples of such programmes are the Microsoft bug bounty programme and the "Responsible Disclosure" programme of the Dutch government that was already described in the MELANI semi-annual report II/2014[7]. The precise steps that are to be taken after a vulnerability has been reported and what the reporter should expect are described on the website www.government.nl[8]. Other large companies such as Google, Facebook and Twitter run programmes like these too. In addition to defining rules for researchers, reporters and the companies affected to regulate the timeframe for debugging as well as financial and non-material aspects, what is also needed for successful functioning is basic trust, which first of all has to be built up.

3.1.4 Legal situation in Switzerland

Aside from the voluntary rules on conduct described above, a clear legal framework is also necessary. This must make it possible for security researchers to continue to look for bugs, because it is only in this way that program security can be improved. A solution here is to not to place the focus on the search for bugs, but instead on how the bug is used once found. Swiss criminal law takes the motivation of the researcher into consideration too: any person who "markets or makes accessible passwords, programs or other data that he knows or must assume are intended to be used to commit an offence […]"[9], or any person who "manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that he knows or must assume will be used for [causing damage to data], or provides instructions on the manufacture of such programs"[10] is liable to prosecution. Accordingly, searching for security vulnerabilities for the purpose of reporting them to the manufacturer is not a criminal offence under Swiss law. Exchanges between security researchers would also appear to be permitted. Publication, however, is a criminal offence as it must be assumed that someone will exploit the vulnerability in a criminal way. The person who publishes the information may be accused of accepting that risk and therefore acting with conditional intent. Consequently, you cannot threaten a manufacturer in Switzerland with publishing (detailed) information on a vulnerability so as to pressurise it into eliminating the vulnerability.

[7] Semi-annual report II/2014, section 5.5 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2014-2.html (as at 29 February 2016)

[8] https://www.government.nl/topics/cybercrime/contents/fighting-cybercrime-in-the-netherlands/responsible-disclosure (as at 29 February 2016)

[9] Art. 143bis para. 2 of the SCC: https://www.admin.ch/opc/en/classified-compilation/19370083/index.html (as at 29 February 2016)

[10] Art. 144bis para. 2 of the SCC: https://www.admin.ch/opc/en/classified-compilation/19370083/index.html (as at 29 February 2016)

However, researchers are free to report on the existence of an identified vulnerability in a general way and to criticise any unsatisfactory conduct of the manufacturer online.

The extent to which a reward for finding and reporting a security vulnerability can be demanded from a manufacturer has nevertheless (still) not been established and would need to be precisely defined by case law. This could possibly be deemed in particular to be "agency without authority"[11] or an obligation arising out of unjust enrichment[12], as the manufacturer receives a service. However, it is doubtful that a researcher would ever instigate this kind of legal dispute with a manufacturer, and thus give a court the opportunity to establish a decision: security researchers may feel they have "better things to do" than involve themselves in battles with courts and lawyers. In the meantime, there are still lots of security bugs to be discovered.

[11] Art. 419 et seq. of the CO: https://www.admin.ch/opc/en/classified-compilation/19110009/index.html (as at 29 February 2016)

[12] Art. 62 et seq. of the CO: https://www.admin.ch/opc/en/classified-compilation/19110009/index.html (as at 29 February 2016)

4 Situation in Switzerland

4.1 Cyber espionage

This chapter does not reveal details that would enable specific espionage targets or operations to be identified. The reason is the need to protect the anonymity of victims and sources of information. Furthermore, to safeguard the interests of the financial centre and the state, it would be counterproductive to reveal such information. Nevertheless, our overview of current cases allows us to present an assessment of the situation regarding cyber espionage in Switzerland. The main focus of the chapter is the information gathered on various active operations in Switzerland over the past six months.

Before even beginning to draw up a typology of attack targets, it is advisable to know first of all what type of information is valuable from a possible attacker's viewpoint. We will limit ourselves here to attacks benefiting a state and can therefore identify the information of interest to that state as being anything that would help it to execute its strategic objectives. Very often, these are political agendas (particularly upcoming negotiations, monitoring of political opposition abroad), security agendas (terrorism), military agendas and, for some countries, economic agendas (particularly innovation, expertise, details on business relationships) that these actions must feed into.

Switzerland is a popular choice for cyber operations precisely because a large number of organisations that possess information of interest as described above are located here. Examples include numerous foreign representations, international organisations and communities that are of political interest to many states, or entire branches of economic activity, where expertise or information on business relationships or pending offers could enable various economic players from other countries to gain a considerable competitive advantage. It is also worth noting that for many countries, this economic espionage feeds into a wider political agenda and may even sometimes be justified by security concerns.

Operations aiming to obtain this type of information target different types of victims. Attackers may opt to attack the target directly, or they may also adopt a two-phase strategy if their direct target proves too resilient. They thus try to compromise a supplier in order to subsequently access their final target. This was the approach used for infiltrating hotels in the Lake Geneva region with the aim of accessing the delegations lodged there during the negotiations on Iran's nuclear programme held in 2014 and 2015.[13] In other cases, maintenance companies with access to a company's secure area or telecommunications service providers may be targeted first. A good example of this last scenario is the attack that targeted BICS BELGACOM, which was uncovered in 2013.[14]

[13] MELANI semi-annual report I/2015, section 4.1.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-1.html (as at 29 February 2016)

[14] MELANI semi-annual report II/2013, section 4.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-1.html

In other cases, companies or individuals may be collateral victims of matters that go beyond them and do not concern them. It can happen that after a targeting error or other unintended effects, operations result in the infection of an unrelated third party. For instance, a company operating in the wine sector was infected by software as part of a cyber espionage campaign in 2015. After verification, and having established the attackers' interests, the victim could quickly be assigned to the "collateral damage" category.

Cyber espionage on Swiss interests is a reality. MELANI has highlighted various cases in its previous semi-annual reports. The FIS annual report also gives an overview of the situation. Prevention is one of most important, if not the most important, aspect fighting against espionage. For a company, however, the first essential step towards increasing awareness is recognising the existence of real, not hypothetical, danger. Numerous cases brought to the attention of MELANI are proof of this reality. If we are to effectively combat espionage, there must be a flow of information. If cases are reported, authorities are able to take measures and learn the necessary lessons with regard to legislation or policy. Moreover, if this type of information is exchanged, other organisations can detect possible intrusions in their network. Naturally, treating the entrusted data confidentially must be a top priority for the authorities.

For the past ten years, MELANI has been advocating protection against IT risks in partnership with various private entities. On its website, it offers a reporting form for notifying it of incidents:

REPORT

MELANI Reporting form:

https://www.melani.admin.ch/melani/en/home/meldeformular/form.html

With its "Prophylax" programme, the FIS is running a prevention and awareness-raising campaign on non-proliferation and industrial espionage. The programme's aim is to raise awareness among companies and educational establishments:

DOCU

Prophylax Programme:

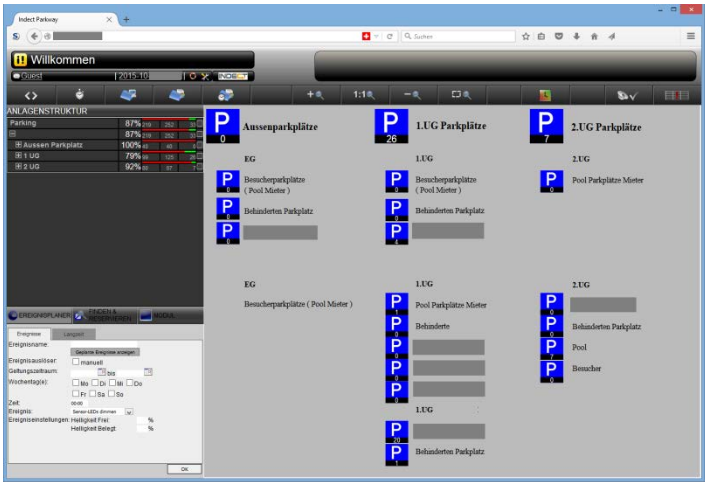
http://www.vbs.admin.ch/internet/vbs/en/home/documentation/publication/snd_publ.html

4.2 Industrial control systems

As a result of the internet of things, information and communications technology (ICT) – including networked industrial control systems (ICS) – is penetrating more and more areas of our daily lives. Cyber risks are also becoming more relevant and topical in these fields of application. In this semi-annual report, we take a look at critical systems in connection with mobility.

4.2.1 Open car-park management

Building automation is an area of control systems that most of us use on a daily basis, consciously or not. Car park management is an area in larger building complexes where industrial control systems are applied. From the straightforward networked car-park meter to the parking guidance system that encompasses the whole city, *ICS systems* are used. In October 2015, MELANI was notified of a car park management interface (Figure 1) in Switzerland that was freely accessible online. The occupancy of each individual parking space could be known by all at any time. It was thus possible, for instance, for burglars to establish when the buildings were most empty or employees were not at home.



Ereignisname:
Ereignisauslöser: □ manuell
Geltungszeitraum: bis
Wochentag(e): □ Mo □ Di □ Mi □ Do □ Fr □ Sa □ So
Zeit: 00:00
Ereignis: Sensor-LEDs dimmen
Ereigniseinstellungen: Helligkeit Frei: %
Helligkeit Belegt: %

Figure 1: Screenshot of the car-park management web interface

MELANI immediately informed the operator about the matter and the potential threat.

4.2.2 Vulnerable railway infrastructure

Industrial control systems are also used in transport systems, such as railway infrastructures that are increasingly networked using ICT, where they are used to control signals or to set switches, for instance. At the 32nd Chaos Communication Congress held in Hamburg from 27 to 30 December 2015, the Russian group *SCADA* Strangelove[15] presented all sorts of possible attacks on a wide range of railway infrastructures: in addition to the obvious information systems for rail passengers, automated signal boxes, surveillance cameras and solar stations on the railway line can also be located with little or no effort. These systems are often vulnerable, because physical access to them is insufficiently protected, the systems and the security mechanisms used are outdated or publicly known passwords are used. To raise awareness of this problem among suppliers and operators and to persuade them not to use standard passwords, the group published a list of 37 suppliers of commonly used control system components such as servers and *switches* whose standard passwords are circulated online. The list included a Swiss manufacturer of railway routers and *VPN* solutions.

[15] https://blog.kaspersky.com/train-hack/10946/ (as at 29 February 2016)

Conclusions/ Recommendations:

We use public transport to get around and order products online that are due to be delivered as early as the next day. The logistics we use and that are all around us are becoming ever more efficient. This is possible thanks to both intelligent transport systems and robot-assisted warehouse management. With the greater interconnectedness of everyday items, all forms of industrial control systems are becoming an increasingly important part of our daily lives.

This means that more and more people are affected by the risks this entails. MELANI provides a checklist of measures for the protection of industrial control systems on its website:

DOCU

Checklists and Instructions: Measures for the protection of industrial control systems

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-for-the-protection-of-industrial-control-systems--icss-.html

4.3 Website attacks: DDoS, defacement

Companies and individuals in Switzerland continue to be the targets of different types of attacks. Websites are a particularly common target for attacks. Especially for companies, which depend on a credible online presence, *DDoS attacks* and website *defacement* are particularly problematic. In the second half of 2015, an increased incidence of attacks on websites was observed as a means of subsequently spreading malware.

4.3.1 Advertising networks

Attackers are always looking for easy ways in which to infect the highest possible number of devices belonging to potential victims. In the past, their main method was emails containing links or attachments. Not a lot of technical knowledge was required for sending out these emails. However, the prospects of success have been steadily dropping, because internet users are more aware and no longer click on every attachment or link. These kinds of email campaigns also result in huge visibility, and the malware they aim to spread quickly ends up in the databases of antivirus manufacturers. For this reason, website infections, known as *drive-by infections*, are currently becoming an increasingly prevalent method for spreading malware. In order to achieve the widespread dissemination of malware, criminals prefer to hack websites with a vast reach. Newspaper websites and advertising networks are particularly popular targets for this. Advertising networks specialise in managing advertising content centrally and then sending it out to a wide range of clients, such as online newspapers. An infection on one of these central systems can therefore have serious consequences and can result in a large number of infections.

Two such cases that were notified to MELANI in the current reporting period are described below.

4.3.1.1 Website infections on daily newspaper

A first infection was reported to MELANI by a security researcher on 11 September 2015. A Swiss advertising network was leading visitors to the Niteris *exploit kit*. The advertising network is also used by a website that supplies the online editions of various daily newspapers. This meant that there was likely to be a high number of potential victims. If an internet user visited a website containing this compromised display of ads, the malware firstly determined what the language settings of the end device were. If these were French or German, the computer was examined for vulnerabilities in Internet Explorer (e.g. CVE-2014-6332), Firefox (e.g. CVE-2013-1710), Java (e.g. CVE-2013-2465) and Adobe Flash (e.g. CVE-2015-5119). Although the security vulnerabilities in the browsers dated from 2013 or 2014 and were thus relatively old, an update for the Adobe Flash vulnerabilities had been available only since 7 July 2015. Computers on which this program had not been updated were infected. The malware installed was the well-known e-banking Trojan Gozi IFSB that is run by various criminal groups and is used worldwide for attacking financial institutions. One week later, on 18 September 2015, the criminals began quite unexpectedly to remove the malware from the infected computers. There could be many reasons for this action. The group had probably noticed that the operation had been exposed and wanted to make it difficult to trace it back to them.

Conclusions:

Apart from all the advantages and cost savings made possible by the centralisation of web content, every company should also be aware of the risks associated with this. In addition to the threat of malware infections on website visitors' computers, an incident may also cause visitors to lose trust in the company.

It is imperative to define in advance the procedure to follow in the event of compromised content of third-party suppliers. Does the company have access to the third-party content, and can it influence and suppress it in emergencies? Most importantly, the contacts with the ICT security divisions of the third companies should be clarified and established in advance, so that the right people can be contacted quickly in an emergency and appropriate countermeasures can be introduced.

4.3.1.2 TV media portal also hit

Another incident of this kind involved a TV media portal. On 3 December 2015, it was discovered that the portal had a website infection that was spreading the Angler Exploit Kit. The infection was not limited to the website in this case either. The content of the manipulated website was also shared with the media partners of other online newspapers, including a free magazine. This increased the scale and the number of potential victims considerably. Fortunately, only one sub-website was affected. MELANI notified the website operators so that they could remove the malicious code.

Website infections, or drive-by infections, are now part of attackers' standard methods for infecting as many devices as possible. The Angler Exploit Kit used in this case appeared for the first time at the end of 2013 and has been an increasingly popular tool for attackers ever since. The various groups of perpetrators generally have an almost identical modus operandi: the exploit kit often checks the target device itself using JavaScript on the installed plug-ins and their versions in order to find a vulnerability and attack it with the most suitable exploit. It is interesting to observe just how quickly exploit kits find suitable exploits when new vulnerabilities appear. Not all exploit kits have the same exploits and there is a relatively large degree of variation. Furthermore, it is increasingly common to find exploit kits with 0-day exploits.

4.3.2 Defacement on lematin.ch: Virus IRAQ

Third-party supplier content made the headlines once more in another case: on 8 July 2015, the TV guide page on lematin.ch displayed an image from an Islamic group of hackers known as "Virus IRAQ".[16] What was actually hacked was not *Le Matin* itself, but the supplier Guide Loisirs that supplies website content for various clients. This was not a targeted attack, but a non-specific website defacement that occurs a thousand times a day. The "Virus IRAQ" group that claimed this attack has been active for many years. According to the zone-h.org website, which records these kinds of attacks, the group attacked over 300 websites in 2015 in this way. The targets are selected randomly. The attacked websites were located in countries such as Ukraine, the Netherlands, Germany, France and the Czech Republic, with the vast majority of them in the USA.

Conclusions:

Websites are constantly and systematically explored for security vulnerabilities. Once they are found, they are exploited. Political or religious content is often displayed in defacements. There is also competition between the different activist groups for who has carried out the highest number of attacks.

4.3.3 IP address takeover – the basics on the BGP problem

The internet is made up of tens of thousands of networks (known as *autonomous systems*, AS) that are connected up to each other and can exchange data packages. This information is exchanged using a protocol called *Border Gateway Protocol (BGP)* which tells the routers the routes via which networks can be reached. The protocol is almost as old as the internet itself and was last revised in 1991 (RFC 1269). Unfortunately, the protocol has always had its shortcomings. For instance, attacks can be launched under false identities (*spoofing* attacks). It is thus possible for any AS to believe that it is the owner of a network even when the propagated network does not belong to it at all. From a technical viewpoint, there is no way of checking if a route is legitimate or not. The AS simply trust that the speaker is propagating correct routes.

Spamhaus, one of the largest providers of blocking lists in the world, informed MELANI on two occasions last year that Swiss AS address spaces were being "taken over" and used by spammers for sending *spam* emails. The first case was reported to MELANI in June 2015 when a canton's address space was hijacked. The second case occurred in September 2015, when part of a pharmaceutical company's address space was hijacked. MELANI informed the organisation affected in both cases.

[16] http://www.tagesanzeiger.ch/digital/internet/Hacker-platzieren-SchockBilder-auf-Website-von-Le-Matin/story/27762519 (as at 29 February 2016)

Recommendations:

If you own your own public address space, we would recommend the following:

- Ensure that the website belonging to your address space is up to date with your Regional Internet Registry (RIR), e.g. RIPE, and has a valid *abuse mailbox*.
- If you own an address space that you are not currently propagating, we recommend that you propagate it even if you are not currently using it. This makes it more difficult for spammers to hijack unused address spaces.
- Use a BGP monitoring tool for your address spaces to ensure you are notified if a foreign AS propagates your address space. There are commercial companies that offer services such as these if you cannot or do not want to do this yourself.

You can find further information on the issue of BGP and IP address takeover on the GovCERT.ch blog:

INFO

GovCERT.ch Blog:

http://www.govcert.admin.ch/blog/11/cantonal-ip-space-in-switzerland-hijacked-by-spammers

4.3.4 DDoS extortion: first DD4BC, now Armada Collective

In the second half of 2015, extortion continued to be a popular practice among cybercriminals who were seeking rapid financial gain. Aside from the numerous families of encryption malware (see section 4.5.1 of this semi-annual report), *DDoS attacks* were used again to disrupt website availability and subsequently extort money from the victim. After this sort of activity, primarily from DD4BC, was observed in the middle of 2015, the group Armada Collective emerged in the second half of the year. The two groups had identical tactics. Armada Collective's attacks targeted email and hosting providers, among others. In particular, the November 2015 attack on Protonmail, a Swiss provider of encrypted email communication, also attracted attention from the international media.

DDoS attacks have been a well-known phenomenon for quite some time. In 2015, attacks that were motivated purely by financial gain became more frequent. The perpetrators selected mainly companies whose business model relies heavily on website availability and which thus have the corresponding potential to be blackmailed. Under pressure from the threat of their website being inaccessible and in the hope of finding a "quick" solution, some companies consider paying. Payments, however, provide the perpetrators with funds to strengthen their attack infrastructure and step up their attacks. Besides, there is no guarantee that the attacks will stop once the payment is made. Attackers often use *booter or stresser services*, which provide DDoS attacks as a paid service, i.e. DDoS-as-a-service attacks. The more money an attacker has available, the greater the volume of attacks (in terms of intensity as well as duration) that can be acquired from such a service provider. If no ransom payments are made, the criminals' business model falls to pieces. Paying the ransom money is thus a short-term way of treating the symptoms at best, and with no guarantee. This will not contribute to the long-term resilience of the payer's infrastructure or of online security against DDoS attacks.

Recommendations:

If a DDoS attack hits a company that is unprepared, it is often too late for rapid and efficient action to be taken. Especially for internet services with a distribution channel depending heavily on a web presence the protection of this (very) critical business process should have absolute priority. The first line of defence should therefore be developing a strategy for a DDoS-attack scenario. It is imperative to know what internal and external offices are responsible for this area and who else can take action in the event of an attack. Ideally, a company addresses the DDoS problem within the framework of general risk management at Executive Board level before an attack occurs, and establishes a certain degree of preparedness for DDoS attacks at the operational level. Any organisation can be hit by a DDoS attack. Talk to your internet provider about your needs and appropriate precautions. You can find a complete checklist and guide with measures to counter DDoS attacks on the MELANI website:

DOCU

Checklists and instructions: Measures to counter DDoS attacks

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/massnahmen-gegen-ddos-attacken.html

4.3.4.1 ProtonMail attack

The DDoS attack on the email provider ProtonMail was an exception both in terms of publicity and the approach described above. This email service developed by CERN researchers offers *end-to-end encryption*. The company was founded in 2013 as a result of the Edward Snowden revelations. It is headquartered in Geneva and is crowdfunded.[17]

On the night of 3 November 2015, ProtonMail has detected a DDoS attack on its systems. Armada Collective was suspected of being responsible for the attacks. After this, more attacks followed on a daily basis according to ProtonMail's statements. This is uncharacteristic of Armada Collective: the group usually limits itself to just one demonstration attack and hopes that the victim is intimidated immediately and pays the ransom. Nevertheless, ProtonMail presumed in the first few days that there was just one attacker. The attacks had collateral effects on other clients in the data centre. Following consultation with these companies, the decision was taken to pay the ransom. It was only when the attacks did not stop following payment and even Armada Collective distanced itself from the attacks that ProtonMail assumed there was a second attacker.[18]

Right from the start, ProtonMail communicated very openly about the events and voiced the suspicion that a state could be behind the attacks,[19] although this was never proved.

[17] https://en.wikipedia.org/wiki/ProtonMail (as at 29 February 2016)

[18] https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/ (as at 29 February 2016)

[19] https://twitter.com/ProtonMail/status/6616830548664297984 (as at 29 February 2016)

However, it seems reasonable to assume that a free-rider exploited the situation. This open communication about the DDoS attacks from the very start could have been why the free-rider learned of this attack, seized the opportunity and also wreaked havoc alongside Armada Collective.

4.3.4.2 DD4BC arrest

Many of the DDoS extortion attempts observed in 2015 were assigned to the group DD4BC (DDoS for bitcoin). On 15 and 16 December, the High-Tech Crime Department of the Republika Srpska (entity of Bosnia and Herzegovina) launched Operation "Pleiades" against DD4BC. Police officers from various European countries and Europol assisted with the operation. The action was initiated by Austria and supported by the European Cybercrime Centre (EC3). Switzerland also supported this operation, which led to the arrest of the suspected head of the group and one other person. A 32-year-old Bosnian national is suspected of having played a leading role in DD4BC.

4.3.4.3 Anonymous threat in Lausanne

The loosely formed group Anonymous gained international fame primarily in connection with large international disputes such as defence for the activities of WikiLeaks founder Julian Assange or the current fight against IS sympathisers on the internet (see also section 5.4.2 of this semi-annual report). An incident in western Switzerland that made the headlines in July 2015 clearly shows that Anonymous is not only involved in international issues. A group called Anonymous Switzerland threatened to hack Lausanne City Council's ICT systems if it did not show more consideration for the inhabitants of the high-rise building "Tour de la Sallaz". The threat was made in response to noise pollution arising from construction work which the inhabitants apparently had to suffer. A complaint was filed against the threat. Precautionary measures were also taken in order to protect the city council's ICT from attacks.

> Conclusion:
>
> As Anonymous is not a defined group, it is difficult to ascertain if the threat was actually connected to the Anonymous movement or if it came from someone who had hoped for a greater impact by using the group's name. The loose affiliation results in a series of uncoordinated, more or less spectacular announcements and attacks. Since, given its structure, Anonymous has no membership as such and there are no official speakers or other persons responsible for the whole movement, in principle anyone can publish messages in the name of Anonymous and generate media interest.

4.4 Social engineering, phishing

In addition to technical attacks, attackers are also fond of methods that exploit human weaknesses.

4.4.1 Phishing statistics

The number of *phishing*-related queries processed by MELANI in recent years has risen dramatically. In order to deal with the large amounts of phishing reports more efficiently, MELANI launched the antiphishing.ch website in 2015, which can be used for reporting phishing sites. In the first year, a total of 2,500 phishing sites were reported, with the amount varying greatly over time. There are very different reasons for this: firstly, there are fluctuations owing to holidays, as fewer phishing sites are reported during holiday periods (and even attackers take holidays). Secondly, attackers regularly move their attacks around different countries.

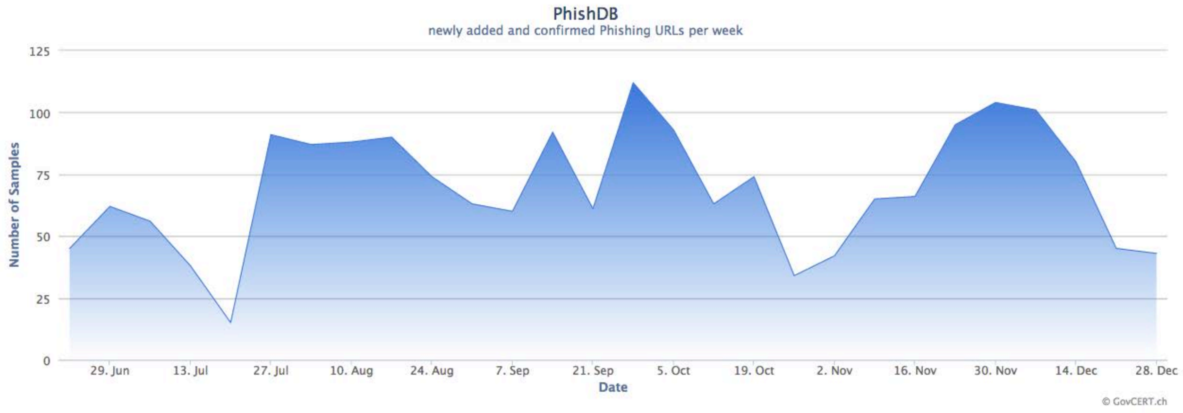


Figure 2: Phishing sites reported and confirmed on a weekly basis on antiphishing.ch

4.4.2 Federal Administration logo misused repeatedly (part 1)

The logo of the Swiss Federal Administration is very popular among fraudsters. It was used twice for phishing and once for spreading malware in attacks (see chapter 4.5.2) that did not target the Federal Administration. The improper use of the logo served the sole purpose of creating the illusion of integrity for victims.

Also in the second half of 2015, fraudsters tried once more to obtain internet users' credit card details disguised as the Swiss Federal Office of Energy (SFOE). The first of these cases were already observed in 2014. The recipients were baited with a supposed rebate to which they were entitled. To enable payment, the victims were asked to access the indicated website. The deceptively authentic-looking website requested not only the name and address of the victim, but also the credit card number including the expiry date and verification number.

In a second case, the name of the Federal Tax Administration (FTA) was misused once more at the end of September 2015. The fraudster tried to obtain taxpayers' bank account and credit card details as well as photocopies of their passports by email. The FTA was misused as the sender in this case.[20]

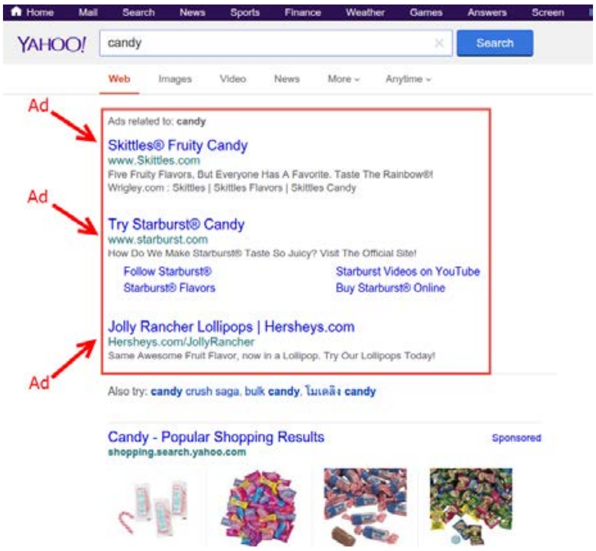
4.4.3 Phishing using ads

Since April 2015, MELANI has observed a new approach to phishing attacks on Swiss financial institutions. Hackers no longer send phishing emails, but instead place paid ads on

[20] https://www.estv.admin.ch/estv/de/home/allgemein/aktuell/warnung--phishing.html (as at 29 February 2016)

search engine operators such as Google, Yahoo and Bing. For this, the fraudsters buy keywords on the search engine operators that are connected to the attacked financial institutions: if the phishers are targeting the customers of "Bank XY", they place phishing ads for the keywords "XY" or "XY Bank".

Ads on search engines are usually displayed at the very top of the actual search results and are easily visible. Therefore, there is a high probability of a user clicking on the ad instead of the actual search result to access Bank XY's website.



Ads related to: **candy**

Skittles® Fruity Candy
www.Skittles.com
Five Fruity Flavors, But Everyone Has A Favorite. Taste The Rainbow®!
Wrigley.com : Skittles | Skittles Flavors | Skittles Candy

Try Starburst® Candy
www.starburst.com
How Do We Make Starburst® Taste So Juicy? Visit The Official Site!
Follow Starburst® | Starburst Videos on YouTube
Starburst® Flavors | Buy Starburst® Online

Jolly Rancher Lollipops | Hersheys.com
Hersheys.com/JollyRancher
Same Awesome Fruit Flavor, now in a Lollipop. Try Our Lollipops Today!

Also try: **candy** crush saga, bulk **candy**, ไมเคลิ่ง **candy**

Candy - Popular Shopping Results
shopping.search.yahoo.com

Figure 3: Example of an ad displayed on Yahoo

Fraudsters take advantage of this fact to lead unsuspecting internet users to phishing websites. However, phishing attacks using ads placed on well-known search engines offer attackers other advantages:

- It is difficult for ICT service providers and *CERTs* to identify phishing ads on search engines as such.
- The attackers do not need to worry about spam filters or reliable recipient email address lists, as emails are not used in this approach.
- At least some of the search engine operators do not screen new customers, or screen them insufficiently, which makes it possible for attackers to open a new user account on the advertising platform to place fraudulent ads.

MELANI contacted all three large search engine operators in Switzerland in order to address the problem. Two of these three operators were actually affected by the phishing attacks described in this section.

Recommendation:

You can find further information on phishing via ads on the GovCERT.ch blog:

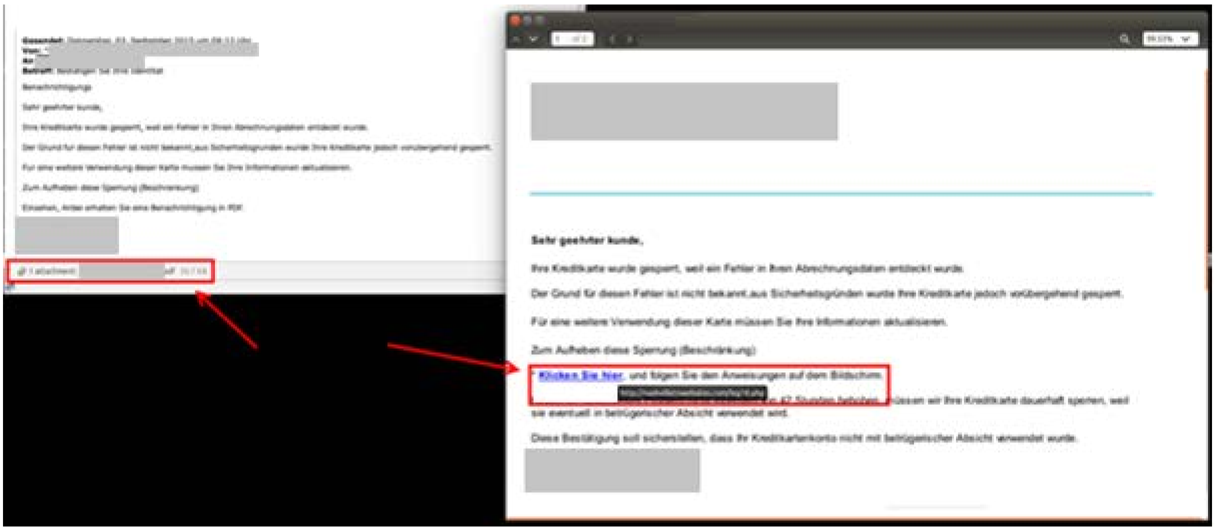
INFO

GovCERT.ch Blog

http://www.govcert.admin.ch/blog/16/ads-on-popular-search-engine-are-leading-to-phishing-sites

4.4.4 Phishing using PDF files

Another approach increasingly observed by MELANI in the second half of 2015 was phishing using PDF files. Normal phishing emails are sent out for this purpose. However, the emails contain an attachment ending in .pdf instead of a HTML link leading to the actual phishing website. The PDF file contains instructions that trick the victim into clicking on the link in it. This link then leads to the actual phishing website.



Gesendet: Donnerstag, 03. September 2015 um 08:13 Uhr
Von: [redacted]
An: [redacted]
Betreff: Bestätigen Sie Ihre Identität

Benachrichtigung

Sehr geehrter kunde,

Ihre Kreditkarte wurde gesperrt, weil ein Fehler in Ihren Abrechnungsdaten entdeckt wurde.

Der Grund für diesen Fehler ist nicht bekannt,aus Sicherheitsgründen wurde Ihre Kreditkarte jedoch vorübergehend gesperrt.

Für eine weitere Verwendung dieser Karte müssen Sie Ihre Informationen aktualisieren.

Zum Aufheben diese Sperrung (Beschränkung)

Einzelheit, Anbei erhalten Sie eine Benachrichtigung in PDF

[redacted]

1 attachment [redacted] .pdf [illegible]

[redacted]

Sehr geehrter kunde,

Ihre Kreditkarte wurde gesperrt, weil ein Fehler in Ihren Abrechnungsdaten entdeckt wurde.

Der Grund für diesen Fehler ist nicht bekannt,aus Sicherheitsgründen wurde Ihre Kreditkarte jedoch vorübergehend gesperrt.

Für eine weitere Verwendung dieser Karte müssen Sie Ihre Informationen aktualisieren.

Zum Aufheben diese Sperrung (Beschränkung)

* Klicken Sie hier, und folgen Sie den Anweisungen auf dem Bildschirm.

[illegible] 47 Stunden beheben, müssen wir Ihre Kreditkarte dauerhaft sperren, weil sie eventuell in betrügerischer Absicht verwendet wird.

Diese Bestätigung soll sicherstellen, dass Ihr Kreditkartenkonto nicht mit betrügerischer Absicht verwendet wurde.

[redacted]

Figure 4: *Example of an email with a link to an attachment ending in .pdf*

Conclusion:

Although it makes no great difference to the recipient of a phishing email if the link to the phishing website is placed directly in the email or in an attached file, this new practice involves a significant advantage for attackers: by using PDF files, the email filters that generally only check for dangerous content in the email itself are not working any more. Internet criminals appear to have realised this and are therefore using this approach more and more.

4.5 Crimeware

Crimeware is a form of malware further developed by cybercriminals which, in criminological terms, ranks as computer crime and legally comes under internet fraud. In terms of crimeware, e-banking Trojans are still very common, as the statistics below show. The majority of infected systems in Switzerland which were reported to MELANI involved e-banking Trojans such as Torpig, Dyre, Tinba, Gozi and ZeuS. While Tinba was the most widely used e-banking malware in the first half of the 2015, Gozi earned this inglorious title in the second half of the year. This is probably connected, among other things, to the dissemination methods using infected advertising networks described in section 4.3.1. However, just like in the first half of 2015, most of the infections are still using Downadup (also known as Conficker). This worm has been around for over eight years and is spread via a security vulnerability in Windows operating systems that was both discovered and eliminated in 2008.

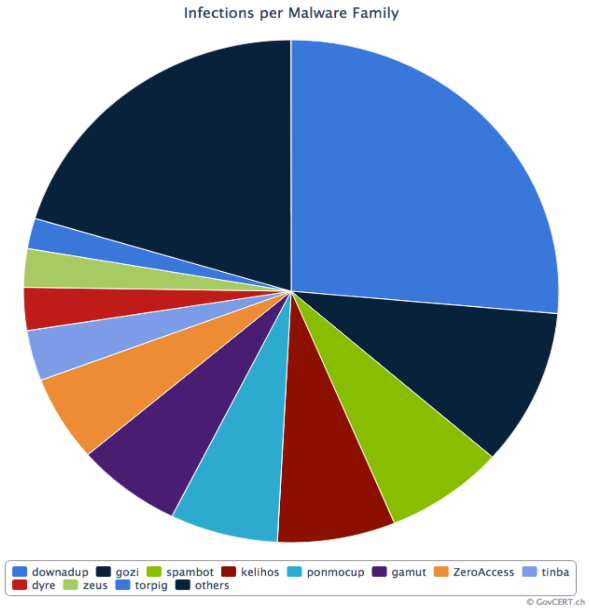


Figure 5: Breakdown of malware in Switzerland known to MELANI. The reference date is 31 December 2015. Current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/

Like in the first half of 2015, the cantons of Zurich and Valais again show a higher rate of infection than other cantons (based on the number of inhabitants). While the higher rate in Zurich may be due to a high concentration of computers, the reason for the higher rate of infection in Valais is currently not apparent.

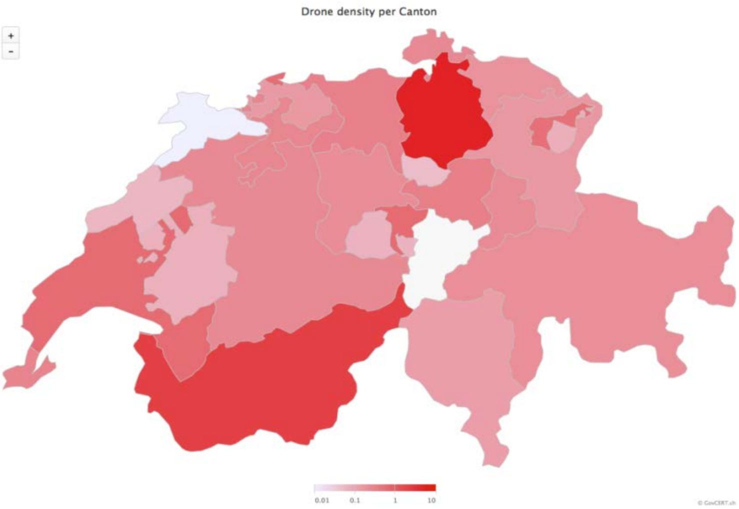


Figure 6: Number of infections per canton based on the number of inhabitants. The reference date is 31 December 2015. Current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/

4.5.1 Encryption Trojans – still very widespread

There were once again numerous reports of crypto Trojans in the second half of 2015. These primarily involved the *ransomware* Teslacrypt. However, cases were also reported to MELANI that involved other families of Trojans, such as Cryptowall. Those affected included both private individuals and companies from all sectors and of all sizes. When an attack occurs, anyone who has not previously made a backup or whose backup has not been updated loses all or at least part of their data.

Recommendation:

A *backup* copy of data saved on the computer should regularly be made on external storage devices. The devices should be connected to the computer only during the backup procedure and should be stored in a safe place.

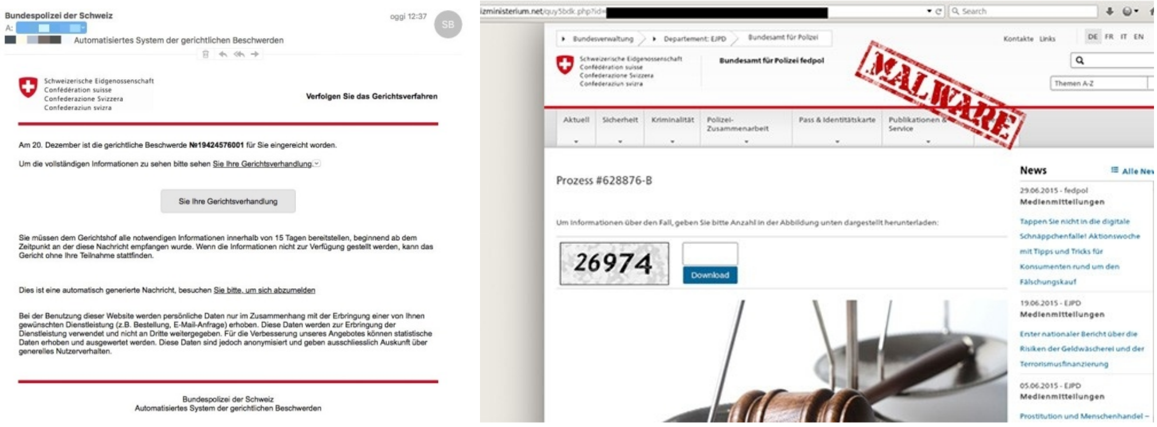
INFO

Measures against ransomware:

https://www.melani.admin.ch/melani/en/home/themen/Ransomware.html

4.5.2 Federal Administration logo misused repeatedly (part 2)

According to the Cybercrime Coordination Unit (CYCO) at the Federal Office of Police (fedpol) emails claiming to be from fedpol were circulated which instructed recipients to download documents from a fictitious court hearing on a specific website at the start of July 2015. Another wave of fraud was observed in January 2016. The wording of the email was such that it intimidated recipients and placed time constraints on them: anyone who fails to make the requested data available within 15 days, the court hearing will be held in their absence. The link led to a fake fedpol website. The user was then instructed to enter a security code (*CAPTCHA*) and download files. However, anyone who followed the instructions from the website and email unwittingly installed the encryption malware Cryptolocker on their device.



Bundespolizei der Schweiz

A: [redacted]

[redacted] Automatisiertes System der gerichtlichen Beschwerden

oggi 12:37

SB

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verfolgen Sie das Gerichtsverfahren

Am 20. Dezember ist die gerichtliche Beschwerde **№19424576001** für Sie eingereicht worden.

Um die vollständigen Informationen zu sehen bitte sehen Sie Ihre Gerichtsverhandlung.

Sie Ihre Gerichtsverhandlung

Sie müssen dem Gerichtshof alle notwendigen Informationen innerhalb von 15 Tagen bereitstellen, beginnend ab dem Zeitpunkt an der diese Nachricht empfangen wurde. Wenn die Informationen nicht zur Verfügung gestellt werden, kann das Gericht ohne Ihre Teilnahme stattfinden.

Dies ist eine automatisch generierte Nachricht, besuchen Sie bitte, um sich abzumelden

Bei der Benutzung dieser Website werden persönliche Daten nur im Zusammenhang mit der Erbringung einer von Ihnen gewünschten Dienstleistung (z.B. Bestellung, E-Mail-Anfrage) erhoben. Diese Daten werden zur Erbringung der Dienstleistung verwendet und nicht an Dritte weitergegeben. Für die Verbesserung unseres Angebotes können statistische Daten erhoben und ausgewertet werden. Diese Daten sind jedoch anonymisiert und geben ausschliesslich Auskunft über generelles Nutzerverhalten.

Bundespolizei der Schweiz
Automatisiertes System der gerichtlichen Beschwerden

izministerium.net/quy5bdk.php?id=[redacted]

Bundesverwaltung › Departement: EJPD › Bundesamt für Polizei

Kontakte Links DE FR IT EN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Polizei fedpol

Themen A-Z

Aktuell | Sicherheit | Kriminalität | Polizei-Zusammenarbeit | Pass & Identitätskarte | Publikationen & Service

Prozess #628876-B

Um Informationen über den Fall, geben Sie bitte Anzahl in der Abbildung unten dargestellt herunterladen:

26974

Download

News — Alle News

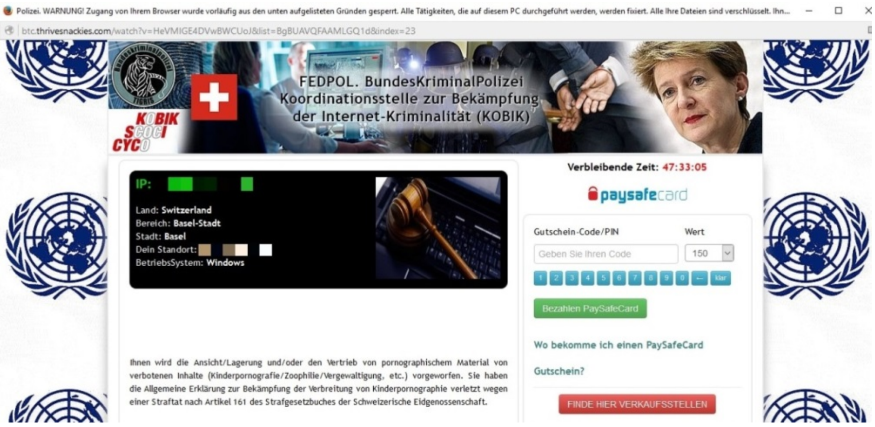
29.06.2015 - fedpol
Medienmitteilungen
Tappen Sie nicht in die digitale Schnäppchenfalle! Aktionswoche mit Tipps und Tricks für Konsumenten rund um den Fälschungskauf

19.06.2015 - EJPD
Medienmitteilungen
Erster nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung

05.06.2015 - EJPD
Medienmitteilungen
Prostitution und Menschenhandel –

Figure 7: Misuse of the Federal Office of Police website for spreading the encryption Trojan CryptoLocker. Source: CYCO/ fedpol

At the start of February 2016, the logo of the Federal Office of Police was misused in another case of fraud and the internet user's computer screen/browser was blocked. The user was accused of having committed illegal activities on the internet. If the user paid a fine, payable with a PaySafeCard, the browser would be unblocked and criminal proceedings circumvented. An increasing number of cases such as this have emerged in recent years. Unlike the aforementioned crypto Trojan, this is not a very professional type of fraud. Depending on the operating system and browser, the blocked browser window can be closed and prevented from automatically opening the recently visited pages again when relaunched (so that the process is not repeated). To do this, please consult the guidelines on the software concerned. In Windows, for instance, the browser is closed via Task Manager (Ctrl-Del-Alt). Not only desktop-computers or laptops are affected by the browser variants. It has also been observed that the attackers increasingly integrate code with the same functionality for mobile-browsers in smartphones or tablets.



Polizei. WARNUNG! Zugang von Ihrem Browser wurde vorläufig aus den unten aufgelisteten Gründen gesperrt. Alle Tätigkeiten, die auf diesem PC durchgeführt werden, werden fixiert. Alle Ihre Dateien sind verschlüsselt. Ihn...

btc.thrivesnackies.com/watch?v=HeVMIGE4DVwBWCUoJ&list=BgBUAVQFAAMLGQ1d&index=23

FEDPOL. BundesKriminalPolizei
Koordinationsstelle zur Bekämpfung
der Internet-Kriminalität (KOBIK)

IP: [redacted]

Land: Switzerland
Bereich: Basel-Stadt
Stadt: Basel
Dein Standort: [redacted]
BetriebsSystem: Windows

Ihnen wird die Ansicht/Lagerung und/oder den Vertrieb von pornographischem Material von verbotenen Inhalte (Kinderpornografie/Zoophilie/Vergewaltigung, etc.) vorgeworfen. Sie haben die Allgemeine Erklärung zur Bekämpfung der Verbreitung von Kinderpornographie verletzt wegen einer Straftat nach Artikel 161 des Strafgesetzbuches der Schweizerische Eidgenossenschaft.

Verbleibende Zeit: 47:33:05

paysafecard

Gutschein-Code/PIN: Geben Sie Ihren Code

Wert: 150

1 2 3 4 5 6 7 8 9 0 ← klar

Bezahlen PaySafeCard

Wo bekomme ich einen PaySafeCard Gutschein?

FINDE HIER VERKAUFSSTELLEN

Figure 8: Fake block page bearing the logo of the Federal Office of Polic. Source: CYCO/ fedpol

4.5.3 E-banking Trojans: Retefe and Tinba

At the end of November 2015, MELANI took the decision in consultation with its partners and the financial institutions concerned to shut down the *command and control infrastructure* used by the e-banking Trojan Retefe. MELANI also contacted the hosting providers and domain registrars responsible abroad and asked them to take down the servers and domain names used by Retefe. Over 30 servers and domain names in Europe were taken down. In the weeks that followed, MELANI did not detect any new infections or new waves of spam connected with Retefe. The takedown of this *botnet* was a success until the end of December 2015 as new waves of spam appeared that were identical to the spam observed in connection with Retefe in the months before the takedown. However, an analysis of the attachment produced surprising results: the malware used was not Retefe but another much better known e-banking Trojan called Tinba (or "Tiny Banker"). The group behind Retefe had clearly changed their tools and had been using Tinba, and thus a new command and control infrastructure, since December 2015.

These two Trojans, Retefe and Tinba, differ considerably from each other: while Retefe was apparently developed by the attackers themselves and used exclusively for e-banking fraud in Switzerland, Austria, Sweden and on occasions in Japan, Tinba was a well-known *crimeware kit* sold in underground forums. They also differ in how they work: while Retefe changes the DNS or proxy settings of the infected computer, Tinba implants itself in the system and regularly communicates with a central command and control infrastructure. This allows the perpetrators to access the victim's computer at any time and use it to commit e-banking fraud.

4.5.4 Botnet: Dridex/Bugat

In October 2015, the US Department of Justice and the FBI struck a blow against the Bugat botnet. Better known as Dridex, Bugat is an e-banking Trojan that targets the clients of dozens of financial institutions throughout the world. The US Department of Justice charged a 30-year-old Moldavian man with administrating the botnet. Despite the FBI's attempts to interfere with the Bugat botnet and arrest those involved, Bugat is still active today and attempts on a daily basis to infect the devices of unsuspecting internet users in the USA and Europe with the help of spam campaigns.

Recommendation:

MELANI recommends that internet users do not open suspicious attachments even if they come from supposedly trustworthy senders. Users should also ensure that an antivirus is installed and is kept up to date at all times.

INFO

Rules of conduct for the use of E-Mails:

https://www.melani.admin.ch/melani/en/home/schuetzen/verhaltensregeln.html

4.5.5 Raid on Droidjack buyers

Android *remote access tools* (RAT) are becoming increasingly popular in the cybercrime underground. These RATs make smartphone surveillance possible,[21] including the surveillance of data traffic, the tapping of telephone calls and background noises and control of the camera. It is even possible to determine the device's location. Instigated by the German prosecution authorities, a raid on sellers of the Droidjack RAT was launched at the end of October. House searches were conducted at the same time in the UK, the USA, France, Germany, Belgium and also Switzerland. The malware buyers stand accused of illegal data espionage and computer fraud. The tool was sold online for USD 210. It is hoped that the evidence gathered will produce findings about the authorship, which was not the focus of the raid. Some traces of the authors lead to India.

4.6 Other topics

4.6.1 Domain management as a business-critical process

Domain names are more than just addresses where websites can be reached. More often than not, they make up the second part of employee email addresses in companies and may be part of the infrastructure for employees' remote access to internal networks. Domain names are addressing resources in telecommunications and have a wide variety of applications in this respect, including in particular their function as a company brand. Given the various functions for which domain names are used in companies, their management can be a business-critical process because, for instance, the website and emails are vital for business activity or because changing the ICT infrastructure configuration to other domain names is only possible with considerable effort.

Domain names cannot be bought however – they are registered. This means that the registrant receives a temporary right of use for the corresponding addressing resource and becomes its holder. This right must be renewed regularly. If the holder forgets to do this, the website can suddenly no longer be accessed and emails are also no longer delivered – these are just the obvious technical consequences.

The allocation of Swiss domain names was reorganised in 2015.[22] The register operator's duty to allocate names from the *top-level domain* ".ch" directly to retail end-users (domain holders or registrants) was abolished. It was also decided that register operators would have to fully abandon the retail business after a transitional period. Their activity would be limited to the technical administration of the .ch domain, while domain name allocation and retail end-user administration in the sense of a complete unbundling of the domain market would only be carried out by registrars. The result was that registrants who up to that point had obtained their domain name directly from the register operator SWITCH had to look for a

[21] http://www.symantec.com/connect/blogs/droidjack-rat-tale-how-budding-entrepreneurism-can-turn-cybercrime (as at 29 February 2016)

[22] Separation of functions in the management of .ch internet addresses: http://www.bakom.admin.ch/themen/internet/00468/04167/04981/index.html?lang=en (as at 29 February 2016)

registrar that would manage domain registration for them. When selecting a registrar, the registrants needed to know what their needs were and choose a suitable service.

At the end of 2015, several registrants complained to MELANI that their registrar had not informed them about the imminent expiry of their domain registration agreement in a manner or by a date convenient to them. Their domain names were subsequently shut down, which had the aforementioned consequences for their business. Fortunately, expired .ch domain names are not released immediately for re-registration, so the (previous) registrants were able to secure their domain names again, albeit with a little bureaucracy and their registrar's help.

A company should know and be aware of how many and which domain names it has registered, what they are used for and especially when their registration has to be renewed. We recommend that you speak with your registrar about your needs and its services. Establish the processes and mechanisms for protecting your domain names from accidental or deliberate changes at the administrative and technical levels.

DOCU

Leaflet IT-Security for SMEs

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html (not available in english)

5 Situation internationally

5.1 Espionage

5.1.1 Hacking Team hacked

The Italian surveillance software manufacturer Hacking Team had a substantial amount of data stolen in a hacker attack. Over 400 gigabytes of the stolen data was published on 5 July 2015. Hacking Team produces surveillance software for prosecution authorities, intelligence services and private companies. The Zurich cantonal police are also among its clients.[23] Its product list includes surveillance software for Windows, MacOS, Linux and all smartphone operating systems. The surveillance software produced by Hacking Team provides access to smartphones and computers and allows the intruder to read *SMS*s and listen into phone and Skype calls.

In the surveillance business, confidentiality is of utmost importance. As a result, not only did the attack cause immense reputational damage to the company hacked, it also had consequences for the company's customers. The published data contained for example emails, customer lists and other confidential documents. Not only was this data very probably trawled through by countless journalists and security providers but also by groups wanting to take advantage of the leaked security vulnerabilities and backdoors. The programmes used and paid for by the customers at best quickly became ineffective or, in the worst-case scenario, could be used by unauthorised third parties. As a result, the company issued a warning about misuse of the software by criminals and terrorists.[24] For this reason, a number of software providers had started to eliminate the vulnerabilities exploited. The Zurich cantonal police, which had purchased the Galileo software from Hacking Team for almost half a million Swiss francs, also stated that it would stop using this surveillance software. This incident clearly shows how difficult and dangerous dealing with vulnerabilities and backdoors is (see chapter 3 and section 5.1.2 (Juniper) for more on this topic).

The list of countries where the customers are located is long[25] and includes, in addition to countries such as Switzerland, the United States and Germany, countries such as Sudan, where a UN arms embargo is in force. This should in turn fuel the discussion as to what extent a computer program can be categorised under the term arms export.

The publication of Hacking Team's internal data caused considerable upheaval at the political level too: the head of the Cyprus Intelligence Service, Andreas Pentaras, resigned after it was revealed that he had purchased software from Hacking Team. Communications surveillance is prohibited in Cyprus. The Cypriot Parliament had revised the constitution five

[23] http://www.heise.de/newsticker/meldung/Hacking-Team-Kantonspolizei-kaufte-Ueberwachungssoftware-trotz-Bedenken-des-Bundesgerichts-2911887.html (as at 29 February 2016, not available in English)

[24] http://www.heise.de/newsticker/meldung/Hacking-Team-Terroristen-koennten-geleakte-Schnueffeltechnik-nutzen-2746071.html (as at 29 February 2016, not available in English)

[25] http://www.watson.ch/Digital/Best%20of%20watson/477908232-Die-uns%C3%A4glich-peinliche-Geschichte-der-gehackten-Hacker-(und-Kapo-ZH-Lieferanten)-in-25-Tweets-erz%C3%A4hlt (as at 29 February 2016, not available in English)

years ago and permitted surveillance under certain conditions. However, the legal foundations have not yet been implemented.[26] Pentaras claimed that all requirements had been complied with but nonetheless resigned to avert potential damage to the Cyprus Intelligence Service.

In Switzerland, Mario Fehr, head of the Zurich cantonal police, came under fire. Fehr had approved the ordering of software from Hacking Team. The software was procured as is customary via a Security Directorate decision and was intended for criminal prosecution measures only.[27] The use of technical surveillance measures must be ordered by the compulsory measures court responsible for authorising surveillance. The Young Socialists in the canton of Zurich lodged a criminal complaint against Fehr, claiming that the purchase violated the constitution in terms of personal freedom and privacy. However, Zurich's public prosecutor did not instigate criminal proceedings.

5.1.2 Espionage with Juniper, Synful Knock and an exportable certificate

The network equipment supplier Juniper found unauthorised lines of program code in its operating system ScreenOS when conducting an internal software examination. US-based Juniper is the second largest worldwide supplier of network equipment after Cisco and produces high-end routers which are used in internet *backbones*. Just before Christmas 2015, two vulnerabilities were published together with the corresponding update at the same time. The versions affected are not so widespread but are used for secure corporate communication.

One of the vulnerabilities concerned the implementation of a master password in the program code and had apparently been in the operating system since 2013. Whereas before the update, only a few (attackers) were likely to have been in possession of this master key, not much effort was required after publication to find the place where the password was to be found. It was only a few hours until the password was also published on the internet. The corresponding attacks were not long then in coming.

The second vulnerability is more complex. Specifically, this was a backdoor in the encryption which allowed attackers to snoop on VPN connections. It was thereby also possible for stored network data to be decrypted subsequently. The vulnerability is based on the random number generator EC_DRBG which has been in the headlines since the Snowden affair. The random number generator does not supply numbers quite as randomly as it should. Instead of replacing this random number generator in its entirety, Juniper only reset the controversial locks. One attacker suddenly changed these locks once again for its benefit.

[26] https://intelnews.org/tag/cyprus-intelligence-service/ (Stand: 29. Februar 2016).

[27] http://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2015_07/1507071c.html (not available in English)

Conclusions:

A government body is assumed to be the perpetrator in particular in the case of the second vulnerability mentioned. These vulnerabilities once again show the enormous interest attackers have in central ICT components. Another aspect which this example illustrates is the risk linked to consciously installing backdoors and vulnerabilities. Third parties can always find these backdoors and exploit them for their own purposes.

Even Cisco, the world's biggest supplier of network equipment, was subject to an attack on its network hardware according to FireEye.[28] In the incident which became known as SYNful Knock, at least 14 routers in the Ukraine, the Philippines, Mexico and India were compromised and backdoors were installed. The number of infected devices may be considerable higher.[29] In contrast to the Juniper incident, a security vulnerability was not exploited here to gain access to the systems: access was gained quite normally via an admin password. Afterwards parts of the *firmware* were overwritten with malware. The attackers obtained the passwords via various channels. In various cases, the attackers used standard passwords, which once again shows that often basic security considerations are lacking.

On 23 November 2015, it emerged that Dell had added its own *root CA certificate* to the Windows certificate store as a trusted root certification authority. This certificate makes it possible for anyone to generate valid certificates for Dell devices. The problem is that the certificate is marked as non-exportable, but can be exported with little or no effort anyway. In this way, encrypted connections from programs which use Dell's *Crypto API* can easily be snooped on using a *man in the middle* attack. This is the case for almost all Windows programs. However, malware can also be easily installed on a Dell computer by this means. An invalid signature normally prevents untrusted software from being installed or at least asks the user whether or not the software should be installed. This security mechanism is eliminated if the attacker has a root CA certificate and can thereby sign for any (malicious) software with a valid signature. Dell took action in response to this development and made an update available which removes the certificate.

[28] https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html (as at 29 February 2016)

[29] http://www.theregister.co.uk/2015/09/22/synful_knock_spreads_embaddened_boxen_in_31_countries/ (as at 29 February 2016)

Conclusions:

The above mentioned examples bring up two fundamental points. First of all, states will continue attempting to intercept communications for intelligence purposes. Secondly there are two major approaches. Either monitoring can be established when states have access to the main knots and lines of the worldwide communication, or they collect information by targeted operations against specific endpoints (for example the computer of a suspect). Besides the basic legal problems of the first method (see semi-annual report 1/2013 and 2/2013) the usefulness of such data is decreasing as the encryption of communication increases. The only way to save the first approach would be to forbid or weaken encryption. The second approach focuses on the point before or after the encryption process and is self-regulating and self-restricting, due to the needed resources, its complexity and the risks of each targeted operation.

There is already an international discussion about the pros and cons of weakening encryption and it will probably intensify. In this context countries based on human rights and the rule of law, that cannot relinquish on the need of communication interception because of internal and exterior security, will sooner or later need to make a commitment to the one or other approach.

5.2 Data leaks

5.2.1 Talk Talk

Talk Talk is a company that provides telephone, internet access and pay television services in the UK. On 21 October 2015, this company fell victim to an attack resulting in the theft of the personal data of nearly 157,000 customers, amongst which more than 15,000 also had their bank details stolen. But this was not the first time: in December 2014, and again in February 2015, the theft of information had allowed criminals to target Talk Talk customers in the context of attempted fraud using social engineering.

The company came under fire both for the way it managed the current incident and its internal procedures, and also because it did not learn any lessons from what had happened in the past. The failure to use encryption in the storage of personal data was an aspect that was particularly singled out for criticism.

According to a number of experts, the attack started with an *SQL injection*. An interesting aspect is that Talk Talk was also targeted by a *DDoS attack*. It would be fair to assume that the DDoS attack was launched as a smoke screen to allow the attackers to compromise the systems while Talk Talk was busy ensuring the availability of its services.[30] Subsequently, the data captured suffered a familiar fate in this type of case, as it was sold on underground markets and finally used to design tailor-made scams targeting Talk Talk customers.

[30] Although this was not confirmed, mention was also made of a demand for a ransom.

Conclusions:

This incident shows how important it is for every company that holds personal information to carry out an analysis of risks affecting them. Questions concerning the methods an attacker could use to get at this personal information and the risk that such an occurrence could pose for the customers concerned should be examined. After that reflection, protective measures must be put in place, including encryption. Moreover, a detailed response procedure to an event of this kind, which in particular includes the method of communication with the victims, i.e. the customers, and also the competent authorities, must be established.

5.2.2 Other data leaks

For two whole weeks, attackers had apparently succeeded in stealing customer data from the UK telecommunications company Carphone Warehouse. The incident was discovered on 5 August 2015. Almost 2.4 million data sets in all were illegally copied from the Carphone Warehouse portals like OneStopPhoneShop.com, e2save.com and mobiles.co.uk. These also included nearly 90,000 sets of credit card data. Affected customers were informed. A hotline was set up for concerned customers.

In an attack on the Irish Experian information services group, which examines the creditworthiness of T-Mobile customers, 15 million data sets in all were reported to have been stolen between 1 September 2013 and 16 September 2015. What was stolen was information such as social security numbers and driving licence numbers. These had been stored encrypted but were assumed to be decrypted thoroughly. Data concerning bank accounts and credit cards were apparently not affected.

The crowdfunding platform Patreon was also the victim of an unauthorised data leak on 28 September 2015. Encrypted passwords, tax data and social security numbers were copied in this case. By contrast, email addresses were in plain text. In addition, messages from the internal messaging system were among the stolen information. In spite of assurances from the operator that passwords had only been saved encrypted, it still recommended that users change their passwords. The trigger for the successful attack was that a database *backup* for the production systems had been stored on a test server. Apparently this server was accessible from the internet via a web application, which the attackers exploited. The 2.3 million stolen email addresses were published on the internet. Particularly noteworthy was an extortion letter discovered in connection with this case. The perpetrators threatened the email addresses with publishing other sensitive data if 1 *bitcoin* was not paid within 48 hours. It is not known if the attackers really did possess this data or simply wrote to the publicly available email addresses on the off-chance.

5.3 Industrial control systems

The dangers posed by insufficiently protected industrial control systems (*ICS*, also known as *SCADA*) has long been pointed out. *Programmable logic controllers* (*PLC*s), which are often freely accessible from the internet and may be part of a networked SCADA system, offer various options to attackers who want to smuggle malware into industrial systems, for example, for espionage purposes. The software needed for this is readily available for downloading. Time and time again, warnings of this nature are dismissed as dangers which are valid only in a laboratory environment. The technical inspection organisation TÜV-Süd illustrated, by using a fictitious waterworks exposed on the internet as a *honeynet*, that all types of attacks take place even on seemingly insignificant systems.[31] The results were published at the end of July 2015.

The first attempt to gain access to the fictitious waterworks took place almost at the same time as the launch of the honeypot system. During the eight months the experiment was in operation, the TÜV-Süd experts recorded over 60,000 incidents of access being gained from over 150 countries. The *IP addresses* of the majority of the attempts were from China, the USA and South Korea, although IP addresses do not allow conclusions to be drawn about the actual location of the attacker. Experience shows that access is gained in cases of this nature as a rule using covert or masked IP addresses.

Attempts to gain access to standard protocols have become widespread. However, in the test set-up described above, inquiries via industrial protocols such as Modbus/TCP or S7Comm were also observed. This type of experiment shows operators of such facilities that vulnerabilities in the configuration are being sought, found and even exploited.

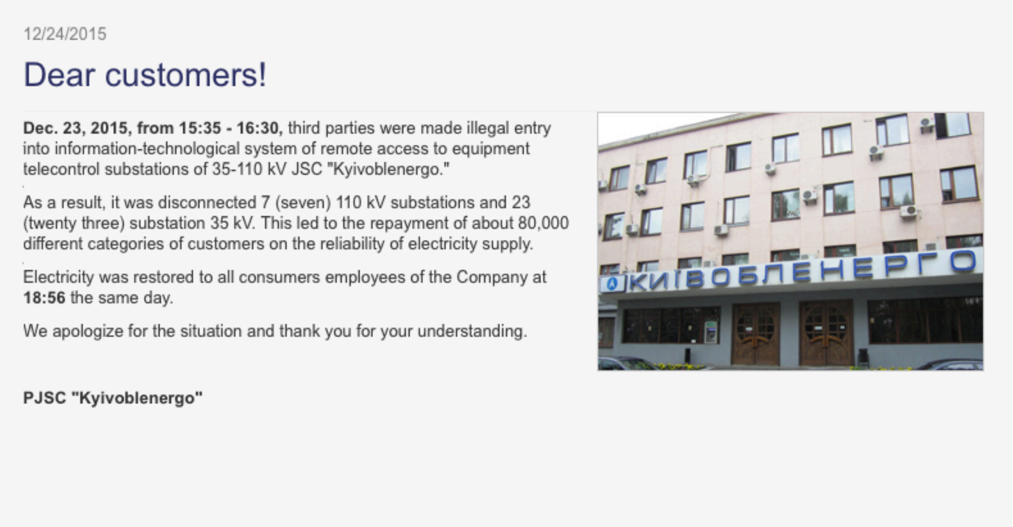
The following example in section 5.3.1 shows that interest is not limited to fictitious systems. It describes the first large-scale power cut caused primarily by a cyberattack. But other areas such as medical devices (section 5.3.3) or cars (section 5.3.4) should not be forgotten and in the future will come under increased scrutiny from attackers.

5.3.1 Power cut in the Ukraine – malware had been used

Shortly before Christmas on 23 December 2015, 80,000 people in the Ukrainian region of Ivano-Frankivsk Oblast were without electricity. Several regional electricity suppliers reported that their systems had been the victims of a cyberattack. This resulted in seven 110 kilovolt and twenty-three 35 kilovolt substations being disconnected from the grid.[32]

[31] http://www.tuev-sued.de/tuev-sued-konzern/presse/pressearchiv/potenzielle-angreifer-sind-ueberall (as at 29 February 2016, not available in English)

[32] http://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid (as at 29 February 2016)



12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

Figure 9: Customer information from a local Ukrainian electricity supplier

The attack on the electricity supplier occurred at several levels. With international support, the Ukrainian CERT (CERT-UA) was able to identify the BlackEnergy (BE) malware in several guises (BE2 and BE3) on the computers of the energy companies concerned. However, up to now the malware itself could not be determined as the primary cause of the power cut.[33]

According to current knowledge, the following sequence of events is the most likely: computers in the network of the energy companies concerned were infected by means of *spear phishing* and prepared Office attachments. With the help of the BlackEnergy malware, the attackers scouted out the network and in this way gained access to other devices, including those of operators on which they found SCADA consoles to control the substations. The power cut itself was probably caused by circuit breakers being triggered in the consoles, just like a legitimate operator would do on site for maintenance purposes. To impede recovery of the power supply, the attackers also used the *KillDisk* malware, which rendered the hard drives of the computers concerned unusable and erased traces. At the same time, they overloaded the company's website and call centre with *DDoS attacks* to make reporting the power cuts and communication with the customers more difficult.[34]

Shortly after the incidents occurred, Ukrainian government representatives accused Russia of being responsible for them. The same accusation was made in January 2016 when BlackEnergy was discovered in the network of the Boryspil International Airport in Kiev but did not cause any damage. However, there was no evidence for the accusations. The security firm iSight Partners suspects that the Sandworm team was responsible for the attack, as it had acted in conspicuously similar ways in earlier attacks carried out in the interests of the Russian government. However, BlackEnergy is widely used and is in some measure available on the black market, which further complicates identifying the perpetrators.

[33] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B (as at 29 February 2016)

[34] http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (as at 29 February 2016)

Conclusions/ Recommendations:

The incident described above is the first large-scale power cut which was largely due to a cyberattack. Operators of infrastructure of this kind can use the findings from this example to better arm their own networks and installations against similar attack patterns.

MELANI provides a checklist of measures for the protection of industrial control systems. The enumerated measures should be embedded in an overarching security process, ensuring that the measures are applied, regularly verified, and continuously improved. Moreover, it is important for operators of installations to know their current threat situation, to monitor that situation regularly, and to incorporate the findings into the implementation and improvement of the security measures. For this purpose, close cooperation between risk management, engineering, and operations is of the utmost importance.

DOCU

Measures for the protection of industrial control systems

https://www.melani.admin.ch/melani/en/home/dkumentation/checklists-and-instructions/measures-for-the-protection-of-industrial-control-systems--icss-.html

5.3.2 Manipulations through data-based automation in oil and gas supplies

Even before Stuxnet, attacks on the control systems of critical processes were feared. As already mentioned in the last chapter about suspicions relating to BlackEnergy, the control system does not necessarily have to be disrupted, as the processes can also be influenced by data manipulation in neighbouring systems. In November 2015, Alexander Polyakov and Mathieu Geli from the security experts ERPScan showed at the Black Hat Europe conference how the valves of pipelines in the oil and gas industry can be affected by manipulation of *ERP systems*.[35] The complex and in many areas automated system landscape (see figure 11) can be attacked in three ways according to the ERP experts:

In one of these types of attack, measurements such as temperature and pressure are falsified in a resources management application. This triggers the costly dispatch of service teams, in the worst case to an oil rig in the middle of the ocean. If in addition the fill levels and cubic capacity of oil tanks are deliberately altered, this can lead to an explosion in the worst case. To improve efficiency, certain commands from third-party systems to the command level are partially permitted. This means that vulnerabilities do not even have to be present in the control system itself for sabotage to occur.

[35] https://www.blackhat.com/docs/eu-15/materials/eu-15-Polyakov-Cybersecurity-For-Oil-And-Gas-Industries-How-Hackers-Can-Manipulate-Oil-Stocks-wp.pdf (as at 29 February 2016)

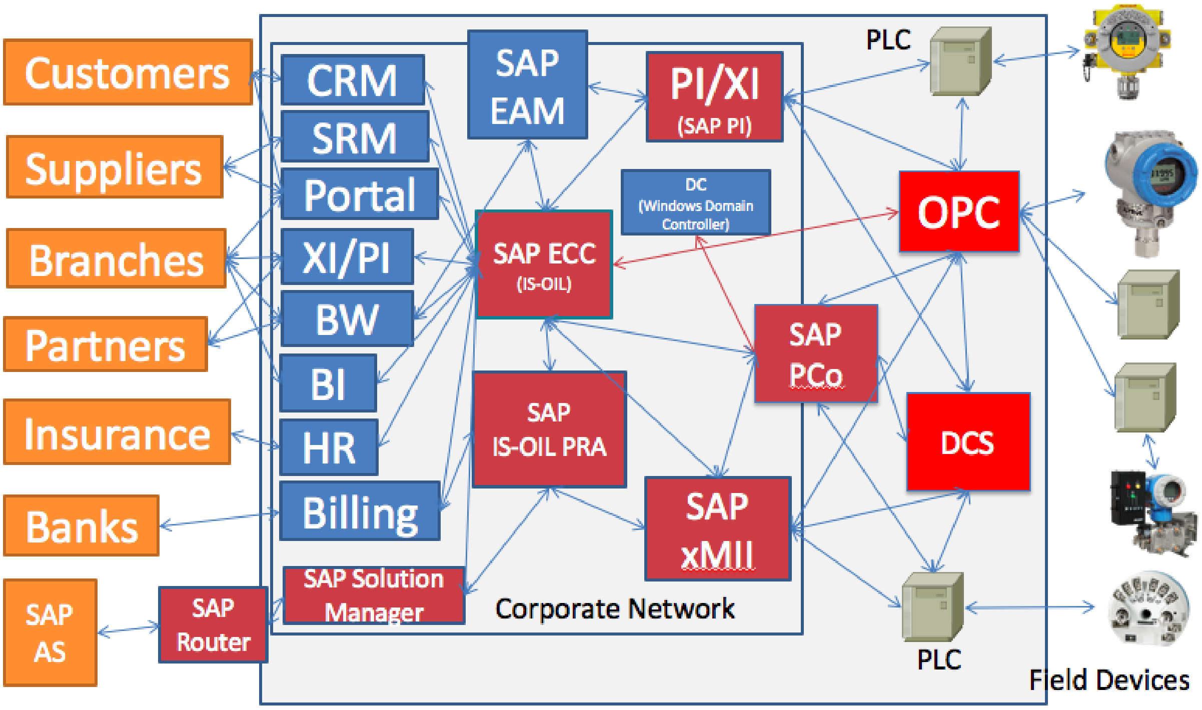


Figure 10: Example of a system landscape in the oil and gas industry. Source Alexander Polyakov und Mathieu Geli

Conclusions:

The example highlights the problem that is introduced into processes via data-based automation. The increasingly widespread use of intelligent smart meters not only provides more efficient business processes, but also more efficient vectors of attack in the event of abuse.

5.3.3 Thousands of medical devices open to online attack

Rapid action is often required in hospitals. Lives depend on decisions that are based on laboratory and diagnostic data. This data must be available immediately for the staff carrying out the treatment. It would seem that more importance is attached to user-friendliness and speed than to security factors even in the configuration of medical devices and its interfaces to the patient data management.

At the Derbycon 2015 security conference,[36] researchers Scott Erven and Mark Collao presented the results of a study which showed that in just one medical company, over 68,000 medical devices were apparently accessible and open to direct online attack. They supported the claim that attacks of this nature happen at all with the results from ten *honeypot* systems which simulated a defibrillator or an MRI system. The decoy devices were attacked 299 times with malware and 24 of these attacks were successful.

[36] http://www.irongeek.com/i.php?page=videos%2Fderbycon5%2Fbreak-me14-medical-devices-pwnage-and-honeypots-scott-erven-mark-collao (as at 29 February 2016)

However, the risks in healthcare are not restricted to unauthorised access to medical technology devices. Access to particularly sensitive health data has also repeatedly been in the headlines recently.[37] In addition, individual patients are exposing their data themselves by using insecure apps. 23 of the 79 apps tested by the Imperial College[38] did not have basic encryption mechanisms, even though they were endorsed by the NHS, the UK healthcare authority.[39] In the case of four apps, medical information was even transmitted unencrypted.

5.3.4 The intelligent car – the responsibility of the car industry

The scene could come from a horror film: during a car journey in the summer, all of a sudden the heating comes on full blast, the radio arbitrarily switches to the dreaded special interest station, the wipers take on a life of their own, and a strange face appears on the satnav display and announces that it has taken control of the vehicle. Any attempts to accelerate or, even worse, brake after this are futile.

Even if attacks of this nature are not yet possible in reality, they are not pure fiction: a vulnerability in the Uconnect infotainment system enabled the security researchers Miller and Valasek to remotely take over the system.[40] It was sufficient for them to know the system's *IP address*. Once it had been taken over, this allowed their own code to be planted in the Uconnect *firmware*, which gave them access to the adjacent processors of the control electronics. They were able to send commands to the engine and brakes via the internal communication network, known as a CAN *bus*, and thus remotely deprive the driver of control of the vehicle.

The researchers presented their findings at the 2015 Black Hat conference, including the *patch*[41] which they had developed together with the Fiat-Chrysler company and Sprint, the telecommunications provider involved. This vivid scenario drew considerable attention from the car industry and from the public. However, this subsided again quickly because consumers continue to appreciate the ease of use of certain vehicle functions from the associated smartphone app.

Let us hope that security considerations are given top priority in the separation of entertainment and control electronics given that new vectors of attack are constantly being discovered. The immobilisers of keyless entry devices have already been overridden[42] and commands were planted in entertainment systems[43] by manipulating radio signals.

[37] http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (as at 29 February 2016). http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html (as at 29 February 2016)

[38] https://www.imperial.ac.uk (as at 29 February 2016)

[39] http://www.theguardian.com/society/2015/sep/25/nhs-accredited-health-apps-putting-users-privacy-at-risk-study-finds (as at 29 February 2016)

[40] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (as at 29 February 2016)

[41] https://ics-cert.us-cert.gov/advisories/ICSA-15-260-01 (as at 29 February 2016)

[42] http://www.heise.de/make/meldung/Wegfahrsperre-VW-Hack-ist-offen-2778194.html (as at 29 February 2016, not available in English)

[43] http://www.bbc.com/news/technology-33622298 (as at 29 February 2016)

Conclusions:

If we keep delegating more responsibilities to the intelligent car, inevitably new problems will emerge. In view of autonomous vehicles and intelligent, self-regulating Car2X systems, the boundaries between physical security and information security are increasingly being blurred, which at best will lead to the same level of testing intensity for ICT systems as for crash tests.

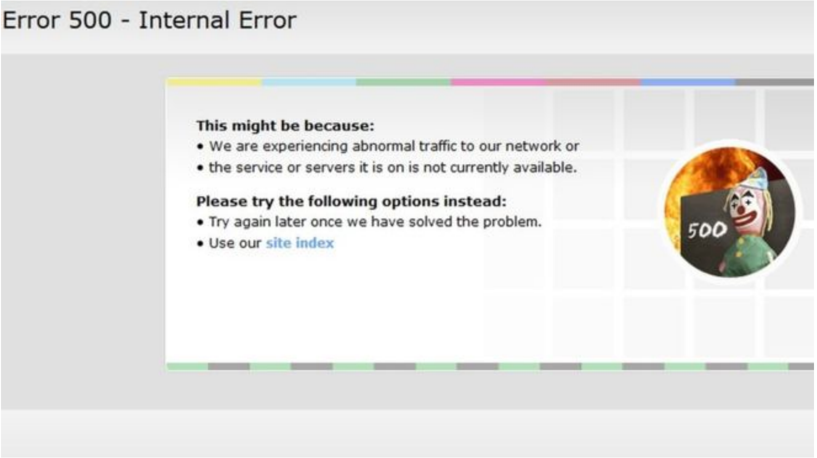
5.3.5 Dam hacked probably as retaliation

It was probably Iranian hackers who in 2013 managed to infiltrate the control systems of a dam close to New York. This was reported by the Wallstreet Journal[44] in December 2015 referring to two people who were entrusted with resolving the matter. The rather small dam should have been attacked as part of alleged retaliatory measures following the discovery of the Stuxnet sabotage incident. It is important to learn from the analysis of this type of "close shave" and to further improve the security precautions for critical infrastructures.

5.4 Website attacks: DDoS, defacement

5.4.1 New World Hacking overshoots the mark in a test run against the BBC

On New Year's Eve, many British viewers who wanted to watch their favourite BBC programme on catch up before the festivities or listen to BBC radio online as they got on with the preparations were disappointed. All that was to be seen on the BBC websites was an error message (see figure 12).



Error 500 - Internal Error

This might be because:

- We are experiencing abnormal traffic to our network or
- the service or servers it is on is not currently available.

Please try the following options instead:

- Try again later once we have solved the problem.
- Use our site index

Figure 11: Error message on the BBC website on New Year's Eve 2015[45]

[44] http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559 (as at 29 February 2016)

[45] http://www.bbc.com/news/technology-35213415 (as at 29 February 2016)

According to the New World Hacking group, it was not a technical fault which caused the break in transmission lasting several hours, but a test which the group carried out to test its own capabilities. One of the attackers, nicknamed Ownz, speaking to the BBC technology correspondent Rory Cellan-Jones, claimed responsibility for the DDoS attack. The group targets online activity linked to the Islamic State (IS). However, to test its newly applied tool Bangstresser, it selected the BBC as a demonstration target. According to statements from the attackers, they had not intended to cause such a lengthy break in transmission. They themselves were surprised at the server power of their own attack infrastructure.

5.4.2 Anonymous versus ISIS – online propaganda war

Around the time of the attacks on the satirical magazine *Charlie Hebdo* in January 2015, the Anonymous hacker group had already launched its campaign #OpISIS which mainly attempts to sabotage the communication channels of the suspected terrorists and to impede the recruitment of new members. Just one day after the new attacks in Paris, the loose grouping published a video[46] declaring war on the Islamic State.

Because Anonymous does not have a clear structure, the measures following the attacks were not very coordinated. For example, there was intense discussion on whether or not a separate #OpParis operation might be needed alongside the existing #OpISIS operation. Further disagreement on the sense of a declaration of war and a diverse range of statements from subgroups prompted the hacker group to publish a press release[47] on 18 November 2015. The aims of the group for the ongoing activities and recommendations on the preferred communication channels were outlined in the press release. The Ghost Security (GhostSec) subgroup's aim is to identify and block social media accounts linked to terror organisations. Not all members are in favour of GhostSec's limited cooperation with state authorities.

In addition to the call[48] for Trolling Day on 11 December 2015, to poke fun at IS terrorists, it was the *doxing* activities of GhostSec that made the press. "Doxing" refers to publicly revealing the true identities and whereabouts of the people responsible for social media accounts and websites. Apart from issuing instructions[49] on how to better protect oneself online, IS seems scarcely to have reacted. Along with many other applications in the instructions, IS recommends the apps Swisscom IO and Threema from Swiss providers and the communications solutions of the Silent Circle company based in Geneva. This publicity could lead to these companies and their clients also being targeted by the hacktivists.

5.4.3 Manipulated QR codes

Barcodes and, in recent years, increasingly the two-dimensional *QR codes* are used in the most diverse application scenarios. Familiar to us all, the barcode on packaging does not only contain information about the price but also other diverse information. The QR code has

[46] https://www.youtube.com/watch?v=RwGGcZoRs-k (as at 29 February 2016)

[47] https://www.docdroid.net/hUQ7Ez2/anonymous-operations-isis-11-2015.pdf.html (as at 29 February 2016)

[48] https://ghostbin.com/paste/ucsf3 (as at 29 February 2016)

[49] http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/ (as at 29 February 2016)

caught on particularly in air transportation for providing the airline with proof of identity before boarding.

The danger associated with these barcodes up to now was above all misuse of the information contained in it. However, the cyber security researcher Yang Yu showed that the printed codes can also be used as vectors for attacking the scanning computer systems.[50] He published several videos and presented his findings under the title "BadBarcode" at the PacSec conference in Tokyo in 2015. Yu exploited a series of vulnerabilities in the programs which are responsible for scanning the codes. By printing barcodes which he himself had manipulated, he was able to induce the scan systems not only to read information but also to carry out commands.

To date, no malicious applications of these capabilities are known, but according to Yu, these vulnerabilities absolutely harbour potential dangers.

5.5 Crimeware

5.5.1 New TLDs and malware

A number of *top-level domains* (TLDs) have varying security levels. It is thus not surprising that several TLDs are considerably more popular than others with criminals. The introduction of generic TLDs has given criminals new opportunities to get their hands on convenient and rarely controlled domains. They then operate their *command and control infrastructure* on these. However, the most well-known domains (e.g. .com and .biz) are also very often misused by criminals.

According to ntldstats.com, the following generic TLDs have high levels of malware:

* .science
* .click
* .link
* .party
* .xyz

However, there are also country code TLDs which are popular with criminal groups. There are various reasons for this: for example, the registrar freenom.com provided the opportunity of registering various TLDs of African countries free of charge, which led to a sharp increase in domain registrations for criminal purposes in these countries.

Country code TLDs with a high proportion of malware are for example:

.gq (Equatorial Guinea)
.tk (Tokelau)
.ga (Gabon)

[50] http://motherboard.vice.com/read/badbarcode-project-shows-customized-boarding-passes-can-hack-computers (as at 29 February 2016)

.cf (Central African Republic)
.ml (Mali)

Registries and registrars must have clear rules on *abuse*, which set out what is to be done if a domain is used for criminal purposes. Of course they must also enforce these rules. In addition, established processes and abuse teams are required to deal with these incidents and resolve them swiftly. In section 6.2, you will find more detailed information on combating the abuse of Swiss domain names.

5.6 Other topics

5.6.1 Stage fright in the case of Google's Android

On 27 July 2015, a vulnerability discovered by the Zimperium security company was published, which allowed hackers to access the data of Android smartphones via MMS without interacting with the users. It is estimated that up to 95% of all Android smartphones were apparently affected. In order to exploit the vulnerability, the attacker only had to send a prepared MMS message to the victim which the victim did not even need to open. The smartphone was already compromised as soon as the message was processed by the system. Until the corresponding updates were published and installed, the only solution was to switch off the MMS reception function. In the meantime, Deutsche Telekom even suspended delivery of MMS messages to protect their customers from potential attacks.

6 Trends and outlook

6.1 Mobile payment

Sweden is about to become the first country to do away with cash. One could hardly have imagined ten years ago that credit and debit cards would completely replace cash. Nowadays, however, the accepted means of payment in Scandinavia is almost exclusively digital, even at the Christmas market. According to current forecasts, smartphones are taking the place of the card payment method, and mobile payment will become the payment method of the future. In the USA, four out of ten shoppers said they had paid at least once with their mobile, and according to the website “the Statistics Portal”, this trend will increase continuously by 20% each year. Although cashless payment methods have been established in Switzerland for years now, it is still struggling to introduce *mobile payment* devices. Mobile payment was first introduced in Switzerland in 2011 with Mobino.

Mobile payment was the subject of debate just a few months ago when the large players found their way onto the market. The green Twint hexagon has been visible at over 3,000 Coop check-outs since the end of 2015. This service provided by PostFinance makes it possible to pay using your mobile phone at specific sales outlets with the corresponding *Bluetooth* terminal. Paymit, a rival product provided by UBS, SIX and Zürcher Kantonalbank, was chosen as the best Swiss app of 2015 and, with over 170,000 downloads, it is the most widely used app for cashless payment using a smartphone. More and more new products are being launched by other service providers too: customers of Migros, Manor and Starbucks can now use their mobile phones to pay for their purchases. A more recent product is Swiss One Wallet, a digital platform belonging to the companies Aduno, Swisscard and Netcetera for mobile payment and paying in online shops. Then there are the products of companies like Apple, Facebook and Google. For the time being, however, these services appear to be having difficulty taking off in Switzerland, despite the wide range of offerings. Apart from the fact that it takes time for people to change their habits, other possible reasons for the slow development are the number and complexity of service providers, customers' concerns regarding data protection, and the fact that some service providers have chosen technologies that are not as widely used or that have only limited support from mobile providers. A likely reason for the failure, for instance, of the Swisscom payment app Tapit is the fact that the *NFC (nearfield communication)* communication method used then was for a long time only available for Android users. Apple did not introduce this method until the iPhone 6.

These apps differ from each other in terms of their technologies, target groups and the service they provide. The following analyses therefore concentrate only on the services Paymit and Twint, which are likely to soon dominate the Swiss market.

Paymit was first introduced in shops in February 2016 and can be used for online shopping too as of April 2016. The Paymit app also facilitates mobile payments between private individuals. It is not essential to be a UBS customer to register with Paymit, but you do need a telephone number and bank account in Switzerland as well as a credit or pre-paid card. The transactions are paid directly to the bank account and are checked by the bank, just as they are with standard payments. Should the mobile phone be stolen, the application is protected with a security code, but no additional authorisation is required to perform payment transactions. To limit the risks further, there is a daily withdrawal limit of CHF 500, which can also be increased.

Twint can be used not just to pay in shops via Bluetooth but also for payments between private individuals and in certain online shops via a peer-to-peer system. Again, it is not essential to be a PostFinance customer to use Twint. However, the direct bank account connection only works with six partner banks. Unlike Paymit, Twint works without a credit card as the sums of money to be transacted are loaded directly to the app's digital wallet with the PostFinance card, direct debit, a payment slip or a Twint credit code. As a safety precaution, a maximum sum of CHF 3,000 can be loaded to the wallet, and the minimum user age has been set at twelve.

Bluetooth is actually safe technology because it uses both a password and encryptions for authentication. Nevertheless, it still involves risks: Cabir, the first smartphone virus, was spread via Bluetooth and the espionage program Flame that the ICT security service provider Kaspersky discovered in May 2012 was able to access the address book using Bluetooth among other things.

All in all, mobile payment is a simple and practical service. The risk of the digital wallet ending up in the wrong hands is no higher than for a conventional wallet, and unlike the latter, it has additional protection in the form of a PIN code. However, the drawback is that we can expect other, more malicious attacks. Cybercriminals prowl the network constantly in search of new methods to gain access to devices that are connected to the internet and serve their moneymaking purposes. While withdrawal limits may deter attackers for now, as soon as the prospect of larger sums of money is raised, attacks using techniques such as *man in the middle* or via social engineering, where the sums end up in an account controlled by the attackers, should not be ruled out.

Recommendations:

- Switch off bluetooth if it is not used
- Define low withdrawal limits
- Activate security settings of the mobile phone (for example PIN-code)

INFO

How to protect myself? Software and Parameters:

https://www.melani.admin.ch/melani/en/home/schuetzen/grundschutz.html

6.2 Combating abuse of Swiss telephone numbers and domain names

The rise of the internet generated new addressing resources in telecommunications: domain names and IP addresses. Although IP addresses are not managed by state authorities, every country was allocated a top-level domain based on its two-letter ISO abbreviation under which it can assign domain names. So, Switzerland was allocated the country domain .ch, which is managed by – and on behalf of – the Federal Office of Communications (OFCOM). Switzerland has opted for a very liberal system for assigning domain names. Essentially, anyone anywhere in the world is free to register and use a domain name under .ch. However, accompanying measures have been taken in order to efficiently and effectively combat abuse: for instance, a Swiss authority acting within the scope of its remit can ask a foreign registrant to set up an address for correspondence in Switzerland[51] to facilitate the delivery of letters from the authorities. It does so in order to avoid mostly long-drawn-out mutual administrative or legal assistance proceedings as well as disputes over jurisdiction and the applicable legislation. Swiss law applies to Swiss domains. This can be implemented via the mechanism described above. However, it is a process that requires time (a deadline has to be set for the registrants to comply with the request). For this reason, powers have been established for the immediate blocking of domain names for cases where Swiss domain names are used to pose urgent threats to internet users, such as *phishing* or *malware*.[52] The consistent enforcement of these powers – particularly at the level of register operator – has clearly resulted in the increasingly good reputation of the Swiss domain and its security.[53]

Even traditional addressing resources are experiencing fresh impetus: *internet telephony* did not remain exclusive to the internet for very long. Nowadays, calls on almost all conventional telephone lines run on *IP networks* as soon as the networks have covered the "last mile" to

[51] Art. 23 para. 3 of the OID: https://www.admin.ch/opc/en/classified-compilation/20141744/index.html#a23 (as at 29 February 2016)

[52] Art. 15 of the OID: https://www.admin.ch/opc/en/classified-compilation/20141744/index.html#a15 (as at 29 February 2016)

[53] https://www.switch.ch/news/cybercrime/ (as at 29 February 2016)

the customer on the service provider's network. Accordingly, there are many ways to use the interfaces between the internet and telephone networks: for instance, calls can be made on telephone lines in distant countries using internet telephony for the cost of a local call there because the service provider maintains a line in that country, or an international service provider can offer a customer hotline at the local rate because it has purchased a number in every country.

However, you no longer need your own telephone number from a technical perspective to be able to make outgoing calls. This means that the number displayed when a call is made can be assigned freely and facilitates caller ID *spoofing*. In recent years, the State Secretariat for Economic Affairs (SECO) has recorded a considerable increase in the number of complaints as a result of unsolicited marketing calls.[54] However, nothing can be done in terms of official measures at the phone number level to combat these calls. To take action against the callers, an often lengthy international procedure must be undertaken – usually against the provider of the products or services marketed via the telephone. The fight against and prosecution of scam callers, such as those masquerading as Microsoft Support[55], is more or less unfeasible given the huge obstacle posed by the process of requesting international mutual legal assistance.

Something that also often occurs is the phone only rings once. This prompts the call recipient to call the number back. The callers need a valid telephone number for this. If this is a Swiss number, the chances of the recipient returning the call are much higher than they are for a foreign number. Scammers often provide working Swiss telephone numbers on the websites they use for carrying out their scams in order to gain the trust of their potential victims.

SECO combats fraudulent marketing calls by way of criminal proceedings (often against persons unknown) and civil actions in connection with preselection providers.[56] Moreover, by threatening legal measures, it has succeeded in several cases in getting misused phone numbers withdrawn from telecommunications service providers.

Telephone numbers are managed at the highest level of OFCOM, which assigns the numbers in blocks of 10,000 to telecommunications service providers (including foreign providers that merely require an address for correspondence in Switzerland), which in turn distribute the numbers further in smaller blocks or one by one to their end-users (customers) in Switzerland and abroad. Given the higher number of reports concerning abuse of Swiss

[54] http://www.seco.admin.ch/themen/00645/00653/05456/index.html?lang=de; see also the brochure "Staying calm when faced with marketing calls" (not available in English): https://www.seco.admin.ch/seco/it/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Werbe_und_Geschaeftsmethoden/Unlauterer_Wettweberb/ruhe-vor-unerbetenen-werbeanrufen_seco.html (as at 29 February 2016)

[55] See MELANI newsletter https://www.melani.admin.ch/melani/en/home/themen/fake_support.html (as at 29 February 2016)

[56] http://www.seco.admin.ch (as at 29 February 2016)

phone numbers, OFCOM's possibilities for cancelling phone number assignment were increased last year.[57]

In addition, the Federal Council initiated the consultation on the amendment of the Telecommunications Act and the Unfair Competition Act (UCA) on 11 December 2015. The focus of the amendment includes enhancing the range of technical and legal resources for combating marketing calls. Like in the fight against spam, telecommunications service providers should be forced to filter marketing calls.

Conclusions:

The more liberal the allocation of addressing resources, the more straightforward the powers and measures for cancelling them in the case of abuse must be so that trust can be maintained in the addressing resources of the allocating offices. Providers of new domain name spaces (New gTLDs) have also acknowledged this principle: registries proceed rather aggressively at times when cancelling domain names that are cheap and easy to buy and hence also attract criminals. If they did not act in this way, the reputation of their TLDs would suffer. In principle, internet users could steer clear of addresses with the ending in question or even filter them at the technical level. The consequence of this could also be that reputable players refrain from registering addresses like these.

This problem does not apply to phone numbers to the same extent, although it should be remembered that Swiss phone numbers (at least within Switzerland) have always enjoyed a high level of trust. In order to maintain this trust, abuse must be prevented insofar as possible and effectively countered when it does occur.

6.3 When hackers play with children's toys

There has always been a wide range of toys for children to imitate the world of grown-ups: baby dolls to feed and rock to sleep, battery-operated toy cars to whizz around in, miniature houses to furnish and arrange, and their own kitchens to bake plastic treats in. Nowadays, the effect of digitisation can also be seen in children's preferences: if parents spend a lot of time on the computer or smartphone, children soon start to copy this too, and the toy industry adapts by bringing tablets and high-tech dolls to the market for our little ones. The internet of things, with all its advantages and risks, has arrived in the toy room too.

VTech Holdings Ltd., which is headquartered in Hong Kong and manufactures technological applications for children and digital games, was the victim of one of the largest hacker attacks ever in November 2015. The database of the Learning Lodge app store for downloading apps, games, videos and e-books was affected by the attack, as were the databases of the Kid Connect social network, where parents and children can communicate on tablets and smartphones, and the PlanetVTeach database.

[57] See Article 11 of the Ordinance on Addressing Resources in the Telecommunications Sector (TSRO): https://www.admin.ch/opc/de/classified-compilation/19970410/index.html#a11 (as at 29 February 2016, not available in English)

After a hacker used an *SQL injection* to obtain the root access rights and thus access to the accounts of 5 million adults and 6.3 million minors, he contacted the online media website Motherboard to inform it of his actions and stated that his intention with the attack had been to highlight the lack of security precautions taken by the company. VTech conceded that it had not ensured optimum protection for its network and confirmed that the stolen data included the names, addresses, email addresses, IP addresses, passwords and confidential answers to security questions of parents as well as the names, genders and dates of birth of children. Social security, driving licence and credit card numbers had not been stolen however. The company did not comment on the accusations that photos and videochats of children had fallen into the wrong hands.

The Japanese company Sanrio, which owns the well-known Hello Kitty brand, also fell victim to a security incident. The personal data of 3.3 million users was stolen from its database at the end of November. This case was also clearly caused by a lack of security precautions.

VTech and Kittyleaks are not isolated cases. Mattel and the start-up company Toy Talk also eliminated security vulnerabilities which, according to ICT security experts, would have made it possible to use the interactive doll "Hello Barbie" as a spying device. The doll, which is connected to the internet via WLAN, can hold interactive conversations. It has a microphone for this purpose and compares the data with the server of a partner company via WLAN. By exploiting this security vulnerability, it would have been possible, for example, to gain control of the microphone.

These examples show that awareness in today's society of what data is particularly worth protecting has not yet developed to the same extent everywhere. The data of children is especially sensitive and therefore must be especially well protected. Toys connected directly to the internet are a relatively new phenomenon and will develop rapidly in the coming years. We can only hope that companies will not just invest in new features, but in toy security too.

Recommendations:

- Change passwords frequently.
- Bear in mind that every device connected to the internet can pose a risk.
- Explain the issue of security to children.
- Do not use children's details when ordering and paying for products for them.

INFO

Rules of Conduct:

https://www.melani.admin.ch/melani/en/home/schuetzen/verhaltensregeln.html

7 Politics, research, policy

7.1 Parliamentary procedural requests

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Ip	15.4073	Are the Armed Forces really able to protect Swiss cyberspace?	Derder Fathi	25.09.2015	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154073
Po	15.5064	Public service debate. Responding to the challenges of an information society without discriminating against innovative media channels	Balthasar Glättli	25.09.2015	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154064
Po	15.3980	Industry 4.0. Assessment of opportunities and risks	Green Group	24.09.2015	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153980
Mo	15.3979	Industry 4.0. Assessment of opportunities and risks	Adèle Thorens Goumaz	24.09.2015	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153979
Po	15.3957	Measures for combating illegal online trade in endangered species	Guillaume Barrazone	24.09.2015	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153957
Ip	15.3917	Crowdfunding. The trade-off between economic innovation and investor protection	Konrad Graber	23.09.2015	CS	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153917
Mo	15.3903	No more delays for online casinos	Peter Schilliger	23.09.2015	NC		https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153903
PI	15,482	Equal treatment of private broadcasters and private online broadcasters	Thomas Matter	22.09.2015	NC	TTC-N	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20150482
Ip	15.3959	Temporary continuation of email services after contract termination	Anita Fetz	24.09.2015	CS	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153959
Ip	15.3882	Health risks of the use of ICT in the information society	Thomas Böhni	22.09.2015	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153882
Qu	15.5466	Involvement of Swiss Post in the development of an e-voting platform	Cédric Wermuth	15.09.2015	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20155466
UQ	15.1059	Urgent financial assistance from the Confederation following the cyberattack on TV5 Monde	Didier Berberat	10.09.2015	CS	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20151059
Ip	15.3822	Teething problems with the new public transport card "Swiss Pass" need to be swiftly resolved	Jean Christophe Schwaab	09.09.2015	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153822

Mo	15.3799	Decision on the motorway network and the motorway tax e-sticker	Transportation and Telecommunications Committee NC	18.08.2015	CS	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153799
Ip	15.4062	Swift implementation of bureaucracy-reducing projects	Hans Grunder, BD Group	25.09.2015	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154062
Ip	15.3994	Measures to ensure the success of the Federal Administration's ICT projects. Excessive staff numbers	Thomas Maier, Martin Bäumle	24.09.2015	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153994
Po	15.4045	Right to use personal data. Right to obtain a copy	Derder Fathi	25.09.2015	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154045

7.2 German IT Security Act

On 25 July 2015, the widely discussed "Act for increased security of information technology systems (IT Security Act)" came into force in Germany. The act aims to raise the level of ICT security considerably and thereby contribute to the security of businesses and private users.[58] It primarily targets the operators of critical infrastructure and those of websites that are not purely private. The act introduces duties for critical infrastructure operators to protect their ICT based on the state of the art and to report major security incidents. The oversight body for this has been created with the "Central Office for the Information Security of Critical Infrastructure" at the German Federal Office for Information Security (BSI). Violations of the newly enshrined duties (e.g. failure to report or to do so correctly, fully and on time) will in future incur a fine of up to EUR 100,000.

Although the overall purpose of the IT Security Act is described as the greatly enhanced security of IT systems in Germany and the protection of critical infrastructure, the specific objectives of this piece of legislation strongly characterised as secondary criminal law are not immediately apparent. It is still not clear if enforcement will centre on the inspection of those subject to the act for their observance of the provisions on the protection of different categories of sensitive (personal) data or on compliance with the duty to report ICT incidents, or both. The bodies in charge will first have to develop implementing practices and the corresponding assessment criteria particularly for proportionality and the vague legal term "state of the art".

The IT Security Act does not affect Switzerland directly as it is German law. Nevertheless, similar efforts (e.g. introduction of a duty to report) have got under way in the EU with the drafting of a directive on network and information security (NIS directive), which ultimately could result in such proposals being adopted here too as part of Switzerland's voluntary implementation of EU law. Swiss companies with subsidiaries in Germany that are now subject to the IT Security Act, however, will have to deal with the issue earlier. The possibility

[58] http://dipbt.bundestag.de/extrakt/ba/WP18/643/64396.html (as at 29 February 2016, not available in English)

of investigations into subsidiaries for possible violations of the act having repercussions on the parent company in Switzerland cannot be ruled out.

7.3 NCS conference

The second conference on the national strategy for the protection of Switzerland against cyber risks (national cyber strategy, NCS) was held in the "Stade de Suisse" in Bern on 2 November 2015. Over 250 participants from the private sector, politics, administration and the general public received information on NCS status and were given an impression of the measures taken by Switzerland to protect against cyber risks. National and international speakers discussed the different aspects of cyber risks, which included a presentation by GovCERT.ch on the specific steps involved in an incident analysis. MELANI presented the prototypes of the situational picture being developed as part of the NCS. The conference also focused on combating cybercrime. The Cybercrime Coordination Unit Switzerland (CYCO) presented the status of work on the development of a national overview of cases, and the Public Prosecutor of Zurich provided examples from the everyday work of criminal prosecution authorities. The live hacker demonstration that showed how to systematically identify control units in industrial systems and their vulnerabilities generated huge interest.

The conference made it clear that protecting Switzerland against cyber risks remains a major challenge. It also showed, however, that progress has been made in recent years. The key to success lies in good coordination between all those involved. Strengthening this collaboration will be the NCS's main concern next year too.

8 Published MELANI products

In addition to the semi-annual reports for the general public, MELANI also offers a number of diverse products. The following sections provide an overview of the blogs, newsletters, checklists, instructions and fact sheets published during the reporting period.

8.1 GovCERT.ch Blog

8.1.1 TorrentLocker Ransomware targeting Swiss Internet Users

21.01.2016 - On Wednesday, Jan 20 2016, we have noticed a major spam campaign hitting the Swiss cyberspace, distributing a ransomware called TorrentLocker. We have already warned about similar TorrentLocker attacks against Swiss internet users last year via Twitter. TorrentLocker is one of many ransomware families that encrypts any local file on a victim’s computer and demands that the victim pays a ransom to have his files decrypted again. Since some ransomware families do not only encrypt files stored locally on the infected machine but also on any mapped network share, ransomware also represent a serious threat to corporate networks. To make sure that the malicious email goes through spam filters and gets opened by the recipient swiftly, the TorrentLocker gang is using a handful of tricks.

➔ http://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users

8.1.2 Ads on popular Search Engine are leading to Phishing Sites

23.11.2015 - GovCERT.ch and Reporting and Analysis Centre for Information Assurance (MELANI) are aware of an ongoing phishing campaign that is targeting a large credit card issuer in Switzerland. What makes this phishing campaign somehow unique is the way how the phishers are advertising their phishing sites: while traditionally phishing sites are being promoted through phishing emails that are usually being sent to a large audience, the phishers are using advertisements (Ads) on a popular search engine to promote their phishing sites.

➔ http://www.govcert.admin.ch/blog/16/ads-on-popular-search-engine-are-leading-to-phishing-sites

8.1.3 Update on Armada Collective extort Swiss Hosting Providers

08.11.2015 - During the recent days and weeks, various Hosting Providers in Switzerland have been blackmailed by a hacking group that calls themselves Armada Collective. As the Distributed Denial of Service (DDoS) attacks carried out by the Armada Collective have grown in terms of intensity and frequency, we have decided to publish an update to our previous blog post about Armada Collective, providing a short overview on the current situation in Switzerland and some additional information.

➔ http://www.govcert.admin.ch/blog/15/update-on-armada-collective-extort-swiss-hosting-providers

8.1.4 Armada Collective blackmails Swiss Hosting Providers

22.09.2015 - Earlier this year, we warned about DD4BC, a hacker group that tried to extort money from high value targets in Switzerland and abroad. While DD4BC is still around, MELANI / GovCERT.ch as well as the Cybercrime Coordination Unit Switzerland (CYCO) did receive several independent reports from hosting Providers in Switzerland recently that they are being blackmailed by a hacker group that calls themselves Armada Collective.

➔ http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers

8.1.5 Swiss Advertising network compromised and distributing a Trojan

22.09.2015 - On September 11, 2015, MELANI / GovCERT.ch got informed by security researcher Kafeine about a popular advertising network in Switzerland that obviously got compromised by cybercriminals, leading to an exploit kit called Niteris.

➔ http://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan

8.1.6 Analysing a new eBanking Trojan called Fobber

11.09.2015 - Some weeks ago we read an interesting blog by Malwarebytes about Fobber, a new e-banking focussed malware in the arena that seems to be a Tinba spinoff. We decided to have a closer look at it to find out whether Swiss critical infrastructures are targeted by it. We'd like to share our findings with you, because it contains some interesting advanced techniques that at the same time are implemented in a comparably simple way; we think this makes Fobber an ideal case study.

➔ http://www.govcert.admin.ch/blog/12/analysing-a-new-ebanking-trojan-called-fobber

8.2 MELANI Newsletter

8.2.1 Ransom payments finance and strengthen DDoS attack infrastructure

19.11.2015 - Extortion is currently a popular method used by cybercriminals seeking rapid financial gain. Different types of attack are used as leverage to extract money from a victim, including DDoS attacks, which disrupt the availability of websites and online services. MELANI has reported several times this year on such attacks and the associated extortion by the Armada Collective and DD4BC groups, which attracted media attention in Switzerland. MELANI strongly advises against agreeing to the blackmailers' demands.

➔
https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/ddos_extortion.html

8.2.2 21st MELANI semi-annual report covers key topic of website security

29.10.2015 - The 21st MELANI semi-annual report is dedicated to incidents such as espionage attacks, including those which affected Switzerland, the ever-present phishing attacks and the key topic of website security. The key topic is one of several innovations which the semi-annual report underwent.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/MELANI-21-semi-annual-report.html

8.3 Checklists and instructions

In the second half of 2015 MELANI didn’t publish any checklists and instructions.

9 Glossary

Term	Definition
Abuse unit	A unit where complaints (e.g. website abuse) can be sent.
Application programming interface (API)	An application programming interface (API) is a program component that a software system makes available to other programs to connect to the system.
Autonomous system	An autonomous system is a collection of IP networks that are administered as a unit and connected via a common internal routing protocol.
Backbone	A telecommunications network with a very high transmission speed. The internet backbone is the core of the internet.
Backdoor	"Backdoor" refers to a software feature that allows users to circumvent the usual access control of a computer or of a protected function of a computer programme.
Backup	"Backup" means the copying of data with the intent of copying them back in the event of data loss.
Bitcoin	Bitcoin is a globally available, decentralised payment system and is the name of a digital monetary unit.
Bluetooth	A technology for wireless communication between two terminals and which is mainly used in mobile phones, laptops, PDAs and input devices (e.g. computer mouse).
Booter or stresser service	A service that enables even users with a lack of technical experience to carry out DDoS attacks.
Border Gateway Protocol (BGP)	Border Gateway Protocol is the routing protocol used on the internet. It connects up autonomous systems.
Bot / Malicious Bot	Comes from the Slavic word “robota” meaning work. Refers to a program that automatically carries out certain actions upon receiving the command. So-called malicious bots can control compromised systems remotely and have them carry out arbitrary actions.

Bug bounty	A bug bounty programme is an initiative run optionally by companies, interest groups, private individuals or government offices for the identification, elimination and disclosure of bugs in software. A reward in the form of cash or a gift is offered in return for uncovering the bug.
Bus	A bus is a system for transferring data between several participants over a shared transmission route, whereby the data is transferred by a standardised communication layer that is independent of the sender and recipient.
Captcha	CAPTCHA is an acronym for Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs are used to distinguish whether the counterpart is a human or a machine.
CERT	A computer emergency response team (CERT) is a group of security experts that offer solutions for the resolution of specific IT security incidents.
Certificate	A digital certificate is the cyberspace equivalent of a personal identification card and serves to assign a specific public key to a person or organisation. This assignment is certified by the certificate authority with its own digital signature.
Cloud computing	Cloud computing (synonym: cloud IT) is a term used in information technology (IT). The IT landscape is no longer operated/provided by the provider himself, but rather obtained via one or more providers. The applications and data are no longer located on a local computer or corporate computing centres, but rather in a cloud. These remote systems are accessed via a network.
Command & control server	Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called command & control server.
Contentmanagementsystems	A content management system (CMS) is a system that makes possible and organizes the joint preparation and processing of content, consisting of text and multimedia documents, generally for the World Wide Web. An author may operate such a system even without programming or HTML knowledge. The information to be displayed is referred to as "content".

Crimeware kit	A module that enables even inexperienced users to easily configure malware.
Cryptosystem	A cryptosystem is a system used for encryption. Cryptography originally referred to the science of encrypting information.
DDoS-Attack	Distributed-Denial-of-Service Attacke Eine DoS Attacke, bei der das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird.
Defacement	Unauthorized alteration of websites.
Doxing	Doxing is the internet-based practice of compiling and subsequently publishing personally identifiable information, usually with malicious intent towards the person concerned.
Drive-By-Infektionen	Infection of a computer with malware simply by visiting a website. Often the websites concerned contain reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
End-to-end encryption	A method in which encryption/decryption is performed only at the end points.
ERP system	Enterprise resource planning (ERP) describes the business task of planning and managing resources such as capital, personnel, operating equipment, information and communication technology, ICT systems based on needs and time in line with the company's mission.
Exploit-Kit	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
Firmware	Instructions stored in a chip to control a device (e.g. a scanner, graphics card, etc.). Firmware, as a rule, may be modified by upgrades.
Flash	Adobe Flash (or simply "Flash", formerly "Macromedia Flash") is a proprietary, integrated development environment for creating multimedia content. Flash is now used on many websites, whether as web banners, as part of a website (e.g. as a control menu) or in the form of entire Flash pages.
Honeypot	In the field of computer security, a honeypot is a

	computer programme or server that simulates the network services of a computer, an entire computer network, or the behaviour of a user. Honeypots are employed to obtain information on attack patterns and attacker behaviour.
Industrial control systems (ICSs)	Control systems consist of one or more devices that control, regulate, and/or monitor the behaviour of other devices or systems. In industrial production, the term "industrial control system" (ICS) is often used.
IP-Adresse	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
Jailbreak	Jailbreaking is used to overcome the network restrictions on Apple products by using suitable software.
JavaScript	An object-based scripting language for developing applications. JavaScripts are programme components integrated in HTML code enabling specific functions in internet browsers. For example, while checking user input on an internet form, a JavaScript can verify that all the characters entered of a telephone number are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the client's computer. Unfortunately dangerous functions can also be programmed with Javascripts. In contrast to ActiveX, JavaScript is supported by all browsers.
KillDisk	Low-level formatting for secure and unrecoverable deletion of data on a hard disk.
Libraries	In programming, a program library is a collection of subprograms or subroutines that provide solutions for topically related problems.
Macros	In software development, a macro is an abbreviated sequence of instructions or statements for performing these instructions by calling them up just once.
Malware	Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses.
Man-in-the Middle	Man-in-the-middle attacks (MITM) Attacks in which the attacker infiltrates unnoticed the communication channel between two partners and is thereby able to spy on or even modify their data exchanges.
Mobile payment	Mobile payment is a payment procedure where at least the payer uses mobile electronic techniques to

	initiate, authorise or perform payment transactions.
NFC (Near Field Communication)	Near field communication is an international communication standard for the contactless exchange of data across short distances.
Patch	Software which replaces the faulty part of a programme with a fault-free version. Patches are used to eliminate security holes.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting Internet users. This may, for example, be account information from online auctioneers (e.g. eBay) or access data for Internet banking. The fraudsters take advantage of their victim's good faith and helpfulness by sending them e-mails with false sender addresses.
Programmable Logic Controller (PLC)	A programmable logic controller (PLC) is a digitallyprogrammed device used to control or regulate a machine or facility. For some years, it has replaced hardwired control
QR-Codes	A QR code is a method of writing information so that it can be very quickly found and read by a machine.
Ransomware	A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.
Remote Administration Tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
Routers	Computer network, telecommunication, or also Internet devices used to link or separate several networks. Routers are used, for instance, in home networks, establishing the connection between the internal network and the Internet.
SCADA	Supervisory Control And Data Acquisition Systems. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).
SmartMeter	A smart meter is an energy meter that displays the actual energy use and actual usage period to an energy consumer; the information can also be transmitted to the energy supplier.
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a

	standard advanced mobile phone.
SMS	Short Message Service Service to send text messages (160 characters maximum) to mobile phone users.
Spam	Spam refers to unsolicited and automatically sent mass advertising, into which category spam e-mails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
Spearphishing	Targeted phishing attacks. The victim is made to believe that he/she is communicating via e-mail with a person they are acquainted with.
Spoofing	In information technology, "spoofing" refers to various deception attempts in computer networks to conceal one's own identity.
SQL-Injection	SQL injection refers to the exploitation of a vulnerability in connection with SQL databases, resulting from insufficient verification of the variables to be transmitted. The attacker attempts to inject his own database commands, in order to change the data as desired or to gain control over the server.
Streaming	Streaming media refers to the simultaneous transmission and reproduction of video and audio data via a network.
Switch	A distributor that connects up network segments.
Top Level Domain	Every name of a domain on the Internet consists of a sequence of character strings separated by periods. The term "top level domain" refers to the last name in this sequence, constituting the highest level of the name resolution. If the full domain name of a computer or website is de.example.com, for instance, the right-most member of the sequence (com) is the top level domain of this name.
Tor	Tor is a network for enabling anonymous communication.
Trojan horses	Trojan horses (often referred to as Trojans) are programs that covertly perform harmful actions while disguised as a useful application or file.
USB Memory Stick	Small high capacity data storage devices, connected to a computer via the USB interface.

VoIP	Voice over IP. Telephony via internet protocol (IP). Frequently used protocols: H.323 and SIP.
VPN	Virtual Private Network Provides safe communication between computers in a public network (e.g. the internet) by encrypting the data flow.
Watering Hole Attack	Targeted infection with malware using websites preferentially used only by a specific user group.
Zero-Day (Vulnerabiliy)	A vulnerability which is not publicly known