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
https://www.melani.admin.ch/

INFORMATION ASSURANCE

SITUATION IN SWITZERLAND AND INTERNATIONALLY

Semi-annual report 2018/I (January – June)

8 NOVEMBER 2018

REPORTING AND ANALYSIS CENTRE FOR INFORMATION ASSURANCE MELANI
https://www.melani.admin.ch/

1 Overview / Content

2 Editorial

Dr. Bruce Nikkel
Head of Cybercrime Intelligence & Forensic Investigation, UBS
Chairman of the European FI-ISAC
Professor of Digital Forensics, Berner Fachhochschule

Dear reader,

Historically, Switzerland was born out of trusted relationships between leaders of early Cantons who collaborated to defend against threats they had in common. This original example of trust among communities resulted in the successful long-term development of a safe and secure society. Today trust continues to play a central role in the safety and security of our digital society. The concept of "trust groups" of like-minded people has become important in every industry sector. These are groups of people working together to defend and fight against cyber threats and cybercriminal activity common to the group.

Trust groups can be ad-hoc communities of like-minded individuals who meet to discuss technical threats and possible technical solutions at an informal level. More formally, Government agencies and industry bodies organize structured trust communities like ISACs (Information Sharing and Analysis Centers) or CERTs (Computer Emergency Response Teams). MELANI has established the coordination of trust communities across multiple sectors like Energy, Telecommunications, Finance, and other industries with infrastructure critical to society. These trust groups bring together people from competing organizations to collaborate in a non-competitive way for the overall greater good of their industry, and ultimately, for the safety and security of society.

Cyber threats transcend national borders, so collaboration must extend to people and communities outside Switzerland. Many international trust groups exist to analyze threats to society at a global level. MELANI participates in these global trusted communities together with many other Swiss organizations. Typically these trusted communities consist of people from industry, Governmental CERTs (like MELANI), Law Enforcement agencies, and other security specialists.

The safety and security of our digital society depends on this national and international collaboration, both formal and informal. We need to continue fostering the growth of these security communities. Cyber threats and cybercrime cannot be stopped by any single organization - they require collaboration between competing organizations, and between public and private sectors. Trust between individuals is key, and this is only achieved by making an effort to develop relationships between people across organizations, locally and internationally. MELANI's contribution to develop and coordinate such trust groups is important and brings valuable security to our Cyber World.

Dr. Bruce Nikkel

3 Key topic: vulnerabilities in the hardware

3.1 Spectre and Meltdown

Handling security vulnerabilities is now part of everyday life in the ICT area. Security vulnerabilities become known on a weekly basis. However, not every vulnerability is equally critical, many have little or very specific impact. Headlines are mainly caused by those vulnerabilities that can be exploited from outside and thus by any person active on the internet ("Remote Code Execution"). Here the damage potential is also particularly high. This applied, for example, to the "Heartbleed" vulnerability or the "Wannacry" malware, which exploited a vulnerability in the SMB protocol. Fortunately, the corresponding software updates were usually available in a timely manner after the vulnerability is getting public, as the software companies have adapted to them and optimised their processes with regard to eliminating security vulnerabilities. But what happens if a vulnerability does not affect the software but the hardware? There have already hardware vulnerabilities such as the "Pentium-FDIV-Bug" in 1994[1] or "Rowhammer" in 2014[2] where it was possible to create an error in certain types memory chips if the same area was read over and over again. This led to interactions with adjacent memory areas. The hardware vulnerabilities "Spectre" and "Meltdown", which became known in the first week of January 2018, were much more serious.[3] An error in the design of processors allows an attacker to read data on the processor. Such errors cannot be eliminated with a simple software update.

3.2 Why this design error?

To make applications faster, processor manufacturers have come up with the following idea: Processors make assumptions about arithmetic operations that could be required next, execute them and store the results ("speculative execution" and "out of order execution"). If the assumption does not apply, the results are dropped, if the assumption applies, the result will be available much faster. Such frequently used operations and data are stored in the so-called cache. This memory is implemented directly on the processor to accelerate the access to this data. The required computing time, which is needed to access the data, allows the attacker to receive the corresponding memory address. Results that have already been calculated will be delivered faster.

To access protected information, an attacker exploits the fact that also results will be written in the memory for which a user has no rights. Only if the corresponding result is really needed the rights will be checked. If these are missing, the operation aborts with an error message.

---

1 https://en.wikipedia.org/wiki/Pentium_FDIV_bug (as at 31 July 2018).

2 https://en.wikipedia.org/wiki/Row_hammer (as at 31 July 2018).

3 https://meltdownattack.com (as at 31 July 2018).

Regardless of this, the information remains in the memory for a short time and can be read out if the corresponding memory area has not yet been overwritten.

The procedure has been used for 20 years. It leads to faster computer performance and thus to time savings. Twenty years ago, computers mostly were self-contained systems. In the age of cloud computing and virtual systems, the discovery of these vulnerabilities falls into a period where multiple users access a processor and is therefore particularly serious. This is why cloud providers were the main focus of interest when finding solutions. This is because it is here that several virtual systems typically share the same hardware.

But most computers, servers, smartphones and tablets are affected. Virtually all users of such devices are likely to be affected by this vulnerability in some way. Infected systems become available to attackers at the processor level and thus allow broader access to the information available in the system.

3.3 Possible solutions

If a device has safety-relevant defects, it is usually recalled by the manufacturer. In the car industry, vehicles are regularly recalled and defective parts replaced. In the computer world such an approach is a challenge because an exchange of the affected hardware component, in this case the processor, is barely practicable. Under the pressure of the users an exchange was forced after the Pentium-FDIV bug in 1994 became public, but nowadays the number of affected devices and the associated logistical effort would be much higher. There would also be the danger of faulty implementation, since the systems are not standardised as in the car industry, but configured very differently. The processor manufacturers have therefore decided to correct the error with a mix of software- and microcode-updates (Code for controlling operations in a processor). To fix a hardware error with a software update sounds paradoxical at first. However, the update reduces the accuracy of the time resolution for example or disables partly those areas where the processors perform the advance precalculations and the resulting acceleration. Remote troubleshooting is bought at a loss in processor performance and must in turn be compensated by more computing power. This approach will therefore not be suitable as a long-term solution. Therefore a different approach will have to be found.

The microprocessors will therefore have to be redesigned in the future and the processor architecture revised. But this will probably take years. In today's systems, the processor is the centre and the most optimised element. Memory and communication support the processor[4]. In a new architecture, storage and thus also security would have to be more and better

[4] https://www.netzwoche.ch/storys/2018-03-07/wie-meltdown-und-spectre-zukuenftige-computerarchitekturen-beeinflussen (as at 31 July 2018).

integrated into the system (security by design). Generally, the question arises which methods can increase the security during the development process of hardware elements.

3.4 Possible developments

"Spectre" and "Meltdown" have sparked a discussion about hardware vulnerabilities. Security researchers around the world are now increasingly working on this topic in order to find further vulnerabilities. For example, "Spectre-NG" (NG stands for "next generation") became public in May and contained a total of eight further weaknesses based on the "Spectre" and "Meltdown" methodologies.[5] Among them "Foreshadow" alias "L1 Terminal Fault", a weakness that makes it possible for an attacker to access from a virtual machine (VM) the supposedly protected memory of another VM running on the same computer. In July 2018, three more CPU vulnerabilities (ret2spec, SpectreRSB and NetSpectre) were announced.

It can be assumed that further hardware vulnerabilities will be discovered because most computer systems are still based on developments that are 20 years old and more. Due to reasons to do with compatibility, the opportunity was missed to renew systems and architectures from scratch. Instead, attempts were made to further develop that which already existed, although the system and architecture were in part not developed for these new functions. This is particularly remarkable in the dynamic ICT environment and will play a greater role in the future when vulnerabilities occur. In contrast to software, a worldwide replacement of hardware is unrealistic. What will be decisive is how the risk of such vulnerabilities can be minimised and to what extent the associated loss of performance can be tolerated.

Recommendations:

Recommendations regarding hardware vulnerabilities you will find on the MELANI website (German, French and Italian only)

https://www.melani.admin.ch/melani/de/home/themen/hardwareluecken.html

[5] https://www.heise.de/ct/artikel/Super-GAU-fuer-Intel-Weitere-Spectre-Luecken-im-Anflug-4039134.html (as at 31 July 2018).

4 Situation in Switzerland

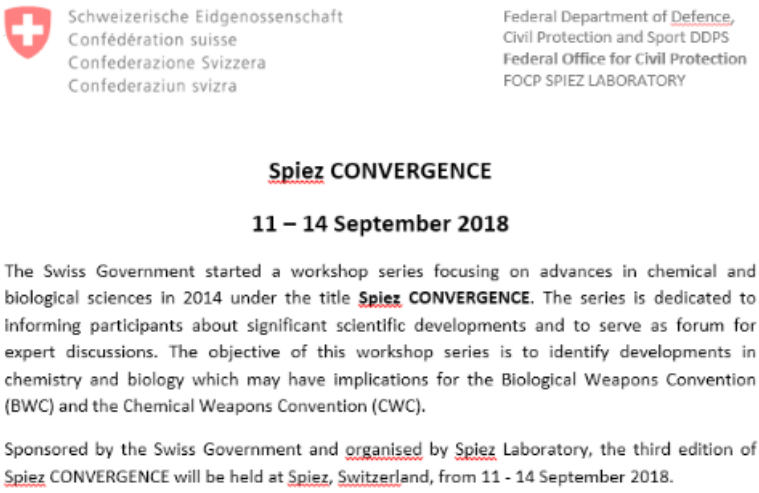
4.1 Espionage

4.1.1 Spiez Laboratory name misused as sender of "Olympic Destroyer"

On 19 June 2018, the software security group Kaspersky published a report on the use of the "Olympic Destroyer" malware. The malware first appeared at the 2018 Winter Olympics in Pyeongchang, South Korea. At that time the worm with sabotage functionalities had committed an attack on the infrastructure of the organiser during the opening ceremony. Various security experts assumed this was a so-called "false flag" operation and suspected the attacker of trying to direct the suspicion to a third party (in this case North Korea). So this at first sight obvious assignment of blame or finger-pointing turned out to be wrong afterwards and showed once more that assignment of blame in the cyber area is not easy. "Olympic Destroyer" is now associated with the "Sofacy" hacker group by the software security group "Kaspersky" (see chapter 5.1.1).

In May and June 2018, targeted phishing emails, so-called "spear phishing", were discovered. The documents attached to the emails were associated with parts of the above-mentioned "Olympic Destroyer" malware of February 2018. According to "Kaspersky", the targets of these attacks were financial organisations in Russia as well as biology and chemistry laboratories in the field of defence against threats. When a recipient opened the email, the malware attempted to infect the computer and integrated it into a botnet infrastructure. The infection was complex and based on various technologies such as VBA, Powershell and MS HTA with JavaScript. "Kaspersky" published technical details in a blog entry.[6] Sabotage actions were not observed during this attack. In order to carry out a targeted attack and tempt the recipients to click on the attachment, the attackers in one case took a publicly available invitation from the Spiez Laboratory for an international conference as a template for their email. The email was subsequently sent to various recipients with a bogus sender on behalf of the Federal Office for Civil Protection (FOCP) and the Spiez Laboratory. Servers of the Federal Administration were not involved at any time. Contrary to various reports in the media, the Spiez Laboratory was not attacked. The name of the laboratory was only misused for the attack in order to give it more integrity.

[6] https://securelist.com/olympic-destroyer-is-still-alive/86169/ (as at 31 July 2018).



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection
FOCP SPIEZ LABORATORY

Spiez CONVERGENCE

11 – 14 September 2018

The Swiss Government started a workshop series focusing on advances in chemical and biological sciences in 2014 under the title **Spiez CONVERGENCE**. The series is dedicated to informing participants about significant scientific developments and to serve as forum for expert discussions. The objective of this workshop series is to identify developments in chemistry and biology which may have implications for the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).

Sponsored by the Swiss Government and organised by Spiez Laboratory, the third edition of Spiez CONVERGENCE will be held at Spiez, Switzerland, from 11 - 14 September 2018.

Figure 1: *Email sent to recipients on behalf of the Federal Office for Civil Protection (FOCP) (source: Kaspersky)*

On 12 and 14 March 2018, spear phishing emails were sent to European governmental organisations in a similar manner with an alleged invitation to an international conference. The emails contained a Word document called "Defence & Security 2018 Conference Agenda.docx". Again, attackers copied the agenda directly from the website and sent it to potential conference participants. In this case, the document contained a Flash object with an action script that attempted to download the actual malware (called "payload"). What was special about this attack was that the malicious component was activated only after the victim scrolled to the third page of the document.[7] This method was probably chosen to make the detection of the attack more difficult. Security specialists of PaloAltoNetworks suspected that the "Sofacy" group was behind this attack.[8]

Assessment

Invitations to conferences are popular with attackers to carry out targeted attacks. On the one hand, such data is typically public and thus freely available to the attacker. This allows an attack to be very targeted, as only those people will be interested in the invitation who also work in the area. On the other hand, the attackers do not have to do much research. The story is authentic and usually contains no errors in content or language.

[7] https://www.zdnet.com/article/hackers-are-using-a-flash-flaw-in-fake-document-in-this-new-spying-campaign/ (as at 31 July 2018).

[8] https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/ (as at 31 July 2018).

4.2 Industrial control systems

4.2.1 Open systems on the net - threat or "daily business"?

The increasing networking and penetration of practically all areas of life by information technology opens up economic and social potential that a highly developed and industrialised country like Switzerland cannot do without. At the same time, however, new risks are emerging as a result of increasing digitalisation.

Industrial control systems previously operated in isolation are increasingly connected to the internet. This makes it possible to take advantage of the benefits that such networking brings. However, not all of these devices have been developed for networking and, to a large extent, still have older and no longer supported operating systems. Various safety measures must therefore be taken to ensure secure operation.

Some systems rely on central and important functions, but these have historical vulnerabilities or have not been designed to be used by critical systems. The detection and elimination of any vulnerabilities is therefore becoming increasingly important. Collaborative approaches help to detect malfunctions using heuristics. Such a solution was presented by the Federal Office for Defence Procurement (armasuisse) in February 2018: many services are now based on GPS signals. Drones, helicopters and even aircraft use GPS signals for guidance. Interference or deception signals can cause drones to deviate from their course. To prevent this, a new system called "Crowd-GPS-Sec"[9] continuously monitors the airspace using digital air traffic signals from aircraft and drones. With novel algorithms, researchers can detect false GPS signals within a few seconds. After a few minutes, the location of the attacker can be pinpointed to within a few metres.

Everyday objects are also increasingly connected to the internal network or the internet. For example, webcams, intelligent light switches, refrigerators and smart TVs are increasingly equipped with a network interface. This increases not only the number of communication participants in the internet, but also the number of vulnerable devices that can be misused by hackers. Particularly problematic are devices that are connected openly and without protection to the internet or whose security vulnerabilities can be exploited directly via the internet. The "Shodan" search engine records such systems and makes it possible to create exposure maps for individual countries. According to "Shodan", 478 industrial control systems in Switzerland are visible from the outside and the most common security vulnerability that can be exploited from the outside is still "Heartbleed".[10] It is also evident that 405 "Cisco Smart Install Clients" (tool for installing new switches under Cisco) should be publicly accessible (see also chapter 5.1.5).

---

9 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-69896.html (as at 31 July 2018).

10 Reference date was 31 August 2018

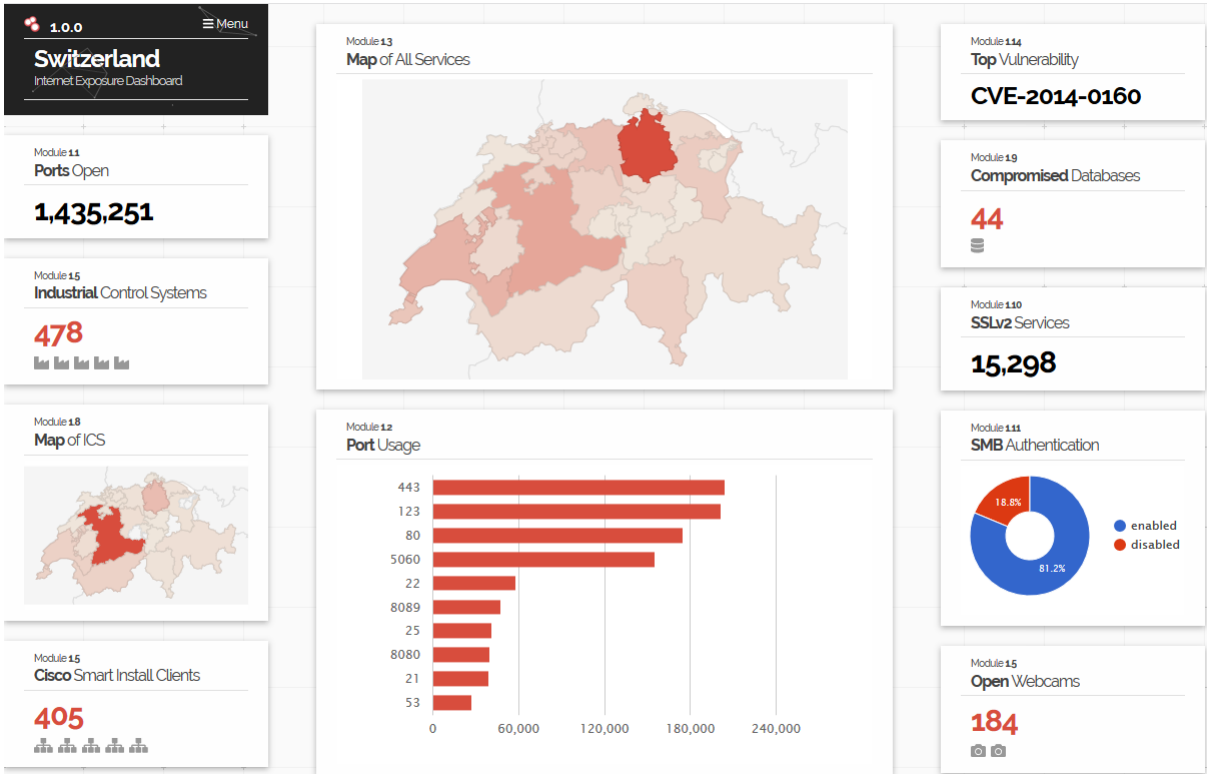


Figure 2: *Overview of vulnerable and internet-accessible systems in Switzerland (source: https://www.shodan.io/. Reference date was 31 August 2018)*

For attackers, better tools are becoming available to exploit such vulnerabilities without great expertise. A new tool called "Autosploit" hit the headlines at the beginning of the year. This tool connects the search engine "Shodan" with the "Metasploit" framework. The "Metasploit" framework is a tool for developing and executing exploits against a target computer. By combining these two services, security vulnerabilities can be exploited automatically and without specific knowledge. The program starts with a "Shodan" search for a specific service such as an "Apache" server or Microsoft's "Internet Information Service". Another command subsequently starts the attacks. The script should automatically find the right exploits from the "Metasploit" library.

Up to now, attackers had to have in addition to the criminal energy the appropriate knowledge. With such tools, the latter requirement has been eliminated and the circle of perpetrators has been considerably enlarged.

It is not always easy to assess how critically open systems should be classified and whether and how sensitive systems are affected[11]. Two years ago, hackers at the Chaos Communication Congress (CCC) published numerous screenshots of systems they had

11 https://www.suedostschweiz.ch/zeitung/wasserwerk-wurde-gehackt (as at 31 August 2018)

apparently penetrated. These included the water supply of a small Swiss commune. Further analysis and enquiries at the commune revealed, however, that this access had not been published but interested citizens were able to look at this data. It could be seen on the charts how much water flows into the reservoir from the individual sources. However, no critical data had been visible and it had also not been possible for any harmful action to be taken via remote access.

Assessment / recommendation:

Objects and devices networked with the internet can in principle be found by anyone (e.g. using a portscan or a search engine like "Shodan") and thus are an especially large target. Devices connected to the internet must be secured (customised passwords, restricted access) and updated regularly. Updates should be installed as soon as they are available. Unlike in the case of a desktop computer or smartphone, however, hardly anyone remembers that intelligent light switches and refrigerators might also be devices requiring software updates.

As part of the national strategy for the protection of Switzerland against cyber risks (NCS) adopted by the Federal Council in 2012, the Federal Office for National Economic Supply (FONES) carried out vulnerability analyses on cyber risks in various vital sectors. The study examined, for example, electricity supply, drinking water and food supply, as well as road and rail transport. On the basis of the results, FONES developed the minimum standard for strengthening ICT resilience. The standard is aimed in particular at operators of critical infrastructures in Switzerland. However, it is applicable to any undertaking.

The minimum standard for strengthening ICT resilience includes the functions identification, protection, detection, reaction and recovery and offers users 106 concrete instructions for improving their ICT resilience to cyber risks:

Minimum standard for strengthening ICT resilience

https://www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html

Recommendation:

If you discover openly accessible or poorly secured control systems on the internet, notify us of the details so that we can contact the operator:

MELANI reporting form

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

Checklist with 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 Attacks (DDoS, defacements, drive-bys)

Individuals, organisations and companies in Switzerland continue to be targeted by different kinds of attacks.

4.3.1 Apophis Squad activities in Switzerland

Apophis Squad is a group initially known for claiming false bomb threats against US and UK schools in March and April 2018.

In June 2018, the group made itself known through another type of activity. Through its Twitter account, the group claims to be responsible for numerous DDoS attacks. This activity was used to promote its booting (or stressing) service. While these attacks often remain relatively short in duration, the one that affected the Swiss based secure email service provider Protonmail has last several days and generate periods of inaccessibility. One hypothesis to explain this determination is to be found in the reaction of a company manager, who called the attackers "clowns" on his Twitter account and provoked probably the attackers with that message. These various activities did not remain without legal consequences and led to an arrest at the end of August 2018.

These various activities and their media coverage seem to have motivated opportunistic actors to use the name Apophis Squad with the DDoS attack. In August, many companies in the financial sector received an extortion e-mail on behalf of Apophis Squad. In the email, there was a clear reference to the group's past exploits. If the recipient did not pay the odd sum of 2.01 Bitcoin before the given deadline, a promise was given of a high-intensity DDoS attack. The first email was followed by various reminders. Several elements quickly guided MELANI's assessment towards the suspicion of an opportunist actor wishing to take advantage of Apophis Squad's reputation, without intending or even without the capability to carry out an attack. First of all, the actor frequently used the same Bitcoin addresses, making it impossible to identify the origin of a possible payment. Furthermore, the twitter account used by Apophis

Squad reported that "copycats" were currently at work, and that their mode of operation did not reflect that of the original actor. At the planned date of the attack, no activity was reported, thus confirming MELANI's assessment. However, for companies, a good level of preparation for DDoS attacks remains necessary, as many other groups can carry out this type of attack.

Recommandation

DOCU

On the website of MELANI a list of measures is published to deal with DDoS attacks.

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

4.4 Social engineering and phishing

The basis for a good attack is a credible story that causes the potential victim to do something. So-called "social engineering" attacks work best when the attacker can collate a lot of information on a potential victim. To do this, fraudsters use both freely available sources and information originating from data theft. Stolen data is secured, coupled with other stolen or public data, prepared and sold on to other criminals.

4.4.1 Phishing

Numerous phishing emails were again sent out in the first half of 2018. The content of the emails did not differ greatly: some requested credit card data for "verification" purposes, while others directed the victim to linked pages requesting usernames and passwords for online services. Frequently, phishing emails also contain the logos of well-known companies or of the service in question so that the emails can be made to look official.

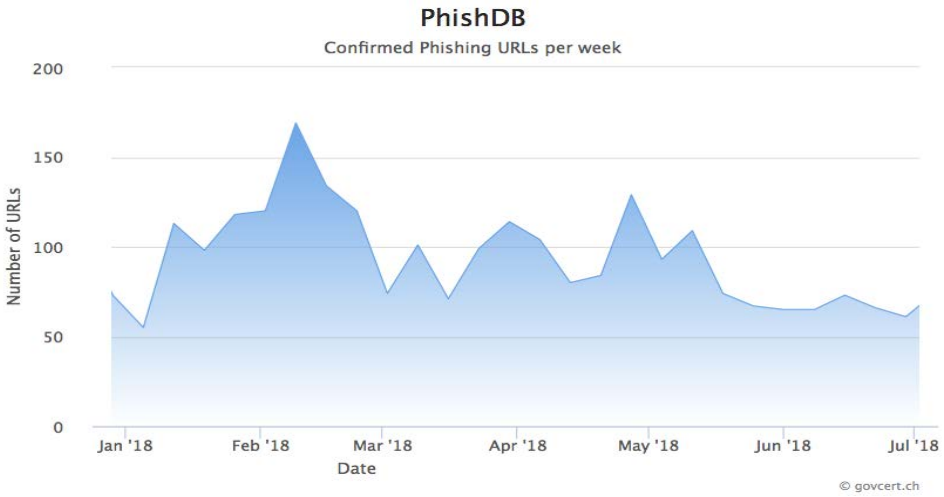


Figure 3: *Reported and confirmed phishing sites per week on antiphishing.ch in the first half of 2018*

Overall, 2,501 different definite phishing sites were reported in the first half of 2018 via the antiphishing.ch portal operated by MELANI. Figure 3 presents the number of reported phishing websites per week, with variations of the number over the course of the year. The reasons vary: firstly, some of the fluctuations are due to holidays, as fewer phishing sites are reported during holidays; secondly, attackers regularly shift their attacks from country to country.

4.4.2 Calls on behalf of banks

Again, fraudulent calls to companies where attackers pretended to be bank employees were increasingly detected. The callers ask for the execution of payments or pretend to have to carry out an e-banking update which then needs testing.

The attackers typically try to convince the company's employees to install remote access software (e.g. NTR cloud, Teamviewer), then connect to the victim's computer and pretend to perform an e-banking update. Subsequently, the perpetrators pretend that the update must be tested and try to convince the victim to enter his access data for the company's e-banking. The attackers pretend that they want to check the system is working properly by making a test payment. If the payment is protected by a collective signature, the fraudsters try to convince the victim to organise all authorised signatories to release the payment.

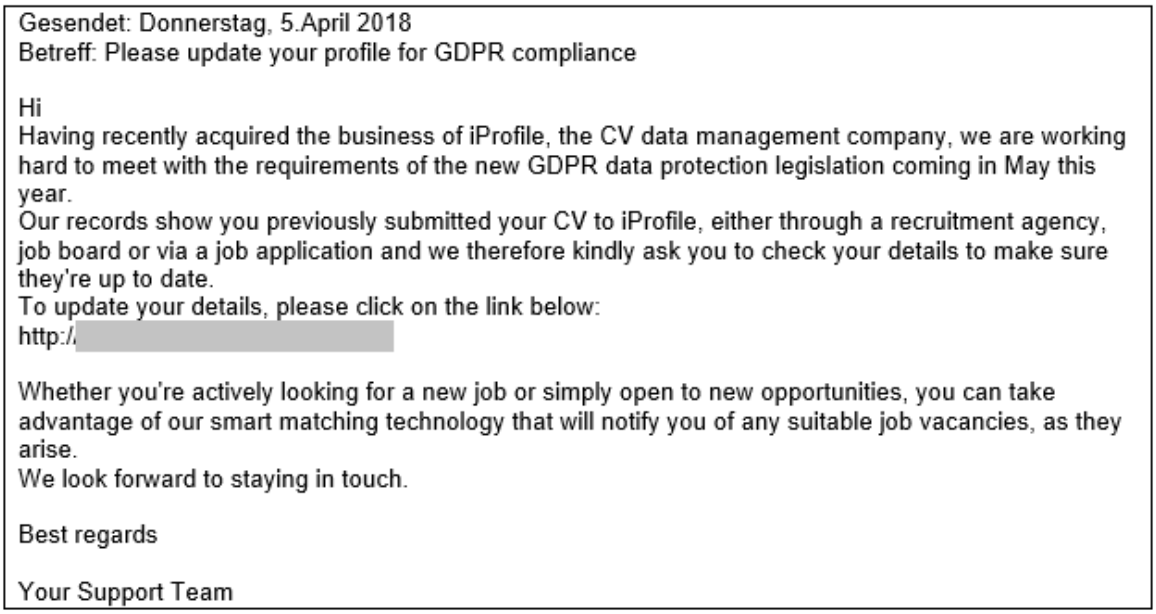
In another variant, victims are instructed to refrain from e-banking for a few days due to urgent e-banking updates. In the case of urgent transactions, the victim should contact a telephone number provided by the fraudsters. If the victim calls the alleged bank employee to carry out an e-banking transaction, both user name and password as well as the one-time password are requested. This gives the attacker access to the company's e-banking. This procedure can be repeated until the victim becomes suspicious.

Evaluation:

The examples show how up-to-date social engineering methods still are. Awareness within companies, adhering to ICT processes, and checking the information disclosed online about employees, management and board members is the key to effective protection from such fraud attempts.

4.4.3 GDPR phishing

On 25 May 2018, the two-year transitional period expired and the European Union's General Data Protection Regulation (EU GDPR) entered into force (see chapter 7.3).
As expected, the end of the transition period for the introduction of the GDPR was exploited for abusive phishing purposes. In the period before 25 May 2018, a lot of emails with information concerning the forthcoming measures in the context of the implementation of the GDPR were sent by companies to their customers. Such timeframes were taken advantage of by resourceful fraudsters and they speculated that the recipients would be informed about the introduction of the GDPR and would also feel obliged to prepare their profiles accordingly (see example figure 4).


Gesendet: Donnerstag, 5.April 2018
Betreff: Please update your profile for GDPR compliance

Hi
Having recently acquired the business of iProfile, the CV data management company, we are working hard to meet with the requirements of the new GDPR data protection legislation coming in May this year.
Our records show you previously submitted your CV to iProfile, either through a recruitment agency, job board or via a job application and we therefore kindly ask you to check your details to make sure they're up to date.
To update your details, please click on the link below:
http:/

Whether you're actively looking for a new job or simply open to new opportunities, you can take advantage of our smart matching technology that will notify you of any suitable job vacancies, as they arise.
We look forward to staying in touch.

Best regards

Your Support Team

Figure 4: *Example of a fraudulent email in which GDPR is taken as a pretext to gain access to the data of a victim.*

Compliance with the Ordinance and the imposition of high fines for data breaches will not only keep businesses busy, but will also inspire criminals to take new blackmail measures. Similar to social engineering, publicly known information is systematically used to create new opportunities.

4.4.4 Espionage attacks via the calendar

At the beginning of any fraudulent modus operandi, a hacker will seek to contact a potential victim using various reasons. While email is often the preferred method, criminals do not hesitate to diversify their methods of operation. Sending text messages, WhatsApp messages or using social networks is getting more and more popular. Another tactic, which has been observed during the reporting period, is to send invitations to the victim's calendar. Depending on the settings of the latter, the invitation will be displayed even though the event has not yet been accepted, and reminders will be sent automatically to the email account. This method was used during the period under review. In this case, the victim saw the invitation displayed in his Google calendar. This was an offer of a loan of money, for which the victim was asked to get in touch by email or WhatsApp message with the contact using the details provided in the message. The final purpose of the attack was not established, but it can be assumed that it was an attempt at phishing or fraud. In any case, this example shows that the prudent attitude of the user must be applied on all platforms. Even events in one's own calendar can have malicious content. It cannot be excluded that some internet users may be fooled, and that an entry or notification from their personal calendar may appear legitimate to them and encourage them to take careless action. It is recommended to set up the e-mail account so that only accepted events are displayed in the calendar.

4.4.5 Supposed prizes - chain letters in the name of IKEA, Milka and Co

A year's supply of chocolate, an IKEA gift voucher or a new iPhone. WhatsApp messages, text messages and emails promising such prizes are in circulation at regular intervals. In the end, however, there is no chocolate, just frustration. Behind such emails are data collectors. The questions in all these competitions are chosen in such a way that everyone can easily answer them. The authors want as many players as possible to "win" and thus get as much data as possible. In order to win a prize, you have to provide personal information such as your name, age, email address or mobile phone number and sometimes your home address on a bogus website. International domains are also used in this procedure (see chapter 4.4.7). For example, in a variant of a "Milka" competition, the "Milka" domain used an "i" without a dot, as found in Turkish. Users do not notice this at first glance and think that they are on the official "Milka" website.

Another trick in these competitions is the requirement that you only get the prize if the message is forwarded to 20 contacts. This form of chain letter means the initiator is not even required to arrange its dispatch. This is carried out by the victim. The fact that the message comes from a person the recipient knows is another advantage of this approach. This increases the chance that a victim will trust the competition and take part.

Recommendation:

Messages with tempting promises of winnings must therefore be critically questioned and certainly not forwarded. The best thing to do is to ignore them.

4.4.6 From the internet to the real world - when attackers make personal visits

Offences on the internet have the advantage that they can be carried out remotely. The perpetrators are mostly located abroad, far away from the local criminal prosecution authorities. Since the fraudsters can carry out the crimes from their familiar surroundings, their inhibition threshold is also lowered. For example, a bank robbery requires significantly more criminal energy than sending phishing emails. During the reporting period, however, there were some incidents that required being physically present. In June 2018 there were warnings about phone fraudsters, which pretended to be from "Google" [12]. Apparently, in some cases, an attempt was also made to establish an on-site contact. In one case, for example, the victims were told that "Google" was planning a personal appointment to verify data that was collected about the victim. Even if this procedure would make sense at first glance, a personal visit by "Google" employees seems a bit exaggerated. The actual intentions of the fraudsters could not be conclusively clarified.

[12] https://www.itmagazine.ch/Artikel/67409/Polizei_warnt_vor_Anrufen_von_falschen_Google-Mitarbeitern.html (as at 31 July 2018).

In another case, telephone calls were made on behalf of the Swiss Federal Office of Energy (SFOE). The callers claimed to want to conduct an on-site energy check. It is not known whether the callers wanted to spy on the victim, talk him into something or access the computer.

Recommendation:

In many companies with customer contact there are computers in the customer area. When employees have to leave the computer, they often do not lock it out of laziness. During this time, potential attackers have the opportunity to activate programs from USB sticks or access any malicious sites. The computer should always be locked, even if you are absent for the shortest period of time. In addition, the protection of the USB interfaces can also bring an improvement in security, especially if they are not used. Operating systems are meanwhile set up so that they no longer automatically execute files on a USB stick. The user must confirm that he wants to perform the action. Nevertheless, there are always security vulnerabilities that this security device can undermine.

4.4.7 "Look alike" domains

As early as 2005, MELANI warned against the following phishing trick: using so-called internationalised domain names (IDNs), fraudsters conned internet users with fake URLs that looked similar to the real ones. For example, the domain www.epic.com with Cyrillic characters is virtually indistinguishable from the website www.epic.com of the software manufacturer Epic. If the corresponding security certificate is issued in addition, it is also possible to establish a connection protected with "https://". Thus the website appears secure to visitors thanks to the padlock in the browser and therefore trustworthy. Very many international characters look practically identical to those in our alphabet, leading to abuses. This approach is called a homographic attack or homographic phishing. After this type of attack had attracted hardly any attention in recent years, cases were again observed in Switzerland in the current reporting period.

Because the Cyrillic letters a, c, e, o, p, x and y look virtually the same as the Latin letters a, c, e, o, p, x and y, Cyrillic characters are most commonly used for homographic attacks. հ, i, j and s can also be used. In the Greek alphabet, only the omicron "o" and the Nu "v" resemble a Latin lowercase letter. Armenian and Hebrew characters are rarely used.[13]

The remedy for individual browser manufacturers in 2005 was to display the special characters in the address bar as so-called "Punycode", so that the user could easily recognise such a domain. The domain name paypal.com with a Cyrillic a is then xn-pypal-4ve.com. "Firefox" also introduced a whitelist with verified domains for which "Punycode" was not displayed. This strategy was changed in 2012 because the maintenance and size of the whitelist became too

[13] https://en.wikipedia.org/wiki/IDN_homograph_attack (as at 31 July 2018).

large in the wake of the spread of IDN domains. IDNs are now displayed if all characters belong to the same character set or if the top-level domain (TLD) restricts the use of IDNs. It is also handled in a similar way in "Internet Explorer" and "Opera". "Safari" also displays problematic character sets in Punycode.

This mainly affects transnational TLDs such as .com, .net or .biz. The attackers make sure that all letters come from one character set and that the browser therefore does not display the Punycode. This may be restrictive. The above letters can be used to create one or another combination of homographic phishing domains.

In the case of country-specific TLDs, the character sets are usually restricted, as is the case with the .ch TLD.[14] Only 32 additional characters are allowed here. Nevertheless, attackers can also take letters that look similar here. An î with an accent is difficult to distinguish from a normal i. The browser does not display a Punycode if the character set is restricted.

Figure 5*: Illustration of the 32 additional characters allowed for domain names in Switzerland (source:nic.ch)*

Assessment / recommendation

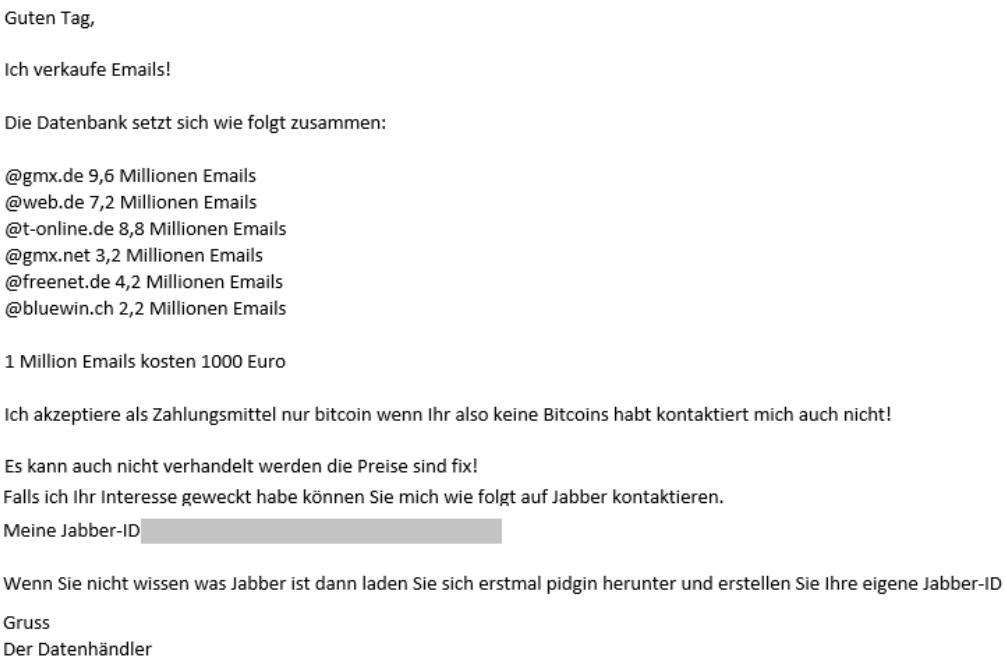
The measures taken by the browser manufacturers largely solve this problem. Experience has shown that the attackers do not put too much effort into generating phishing pages. Websites are usually hacked in order to place fraudulent pages on them. Hardly anyone is concerned about correct URLs. The situation is different for very targeted attacks. This method could well be a way to install a spy Trojan on the victim's device.

In Firefox you can deactivate IDN completely. Then all URLs are displayed in the address line in Punycode. For this you have to set the variable "network.IDN_show_punycode" from "false" to "true" on the configuration page (about:config).

4.4.8 Email addresses for sale

As early as December 2017, a large number of email addresses were offered for sale on the internet. In May 2018, another large number of email addresses was offered for sale to Swiss recipients. It is not possible to say whether the sender actually owned the specified number of email addresses.

[14] https://www.nic.ch/faqs/idn/ (as at 31 July 2018).



Guten Tag,

Ich verkaufe Emails!

Die Datenbank setzt sich wie folgt zusammen:

@gmx.de 9,6 Millionen Emails
@web.de 7,2 Millionen Emails
@t-online.de 8,8 Millionen Emails
@gmx.net 3,2 Millionen Emails
@freenet.de 4,2 Millionen Emails
@bluewin.ch 2,2 Millionen Emails

1 Million Emails kosten 1000 Euro

Ich akzeptiere als Zahlungsmittel nur bitcoin wenn Ihr also keine Bitcoins habt kontaktiert mich auch nicht!

Es kann auch nicht verhandelt werden die Preise sind fix!
Falls ich Ihr Interesse geweckt habe können Sie mich wie folgt auf Jabber kontaktieren.
Meine Jabber-ID

Wenn Sie nicht wissen was Jabber ist dann laden Sie sich erstmal pidgin herunter und erstellen Sie Ihre eigene Jabber-ID

Gruss
Der Datenhändler

Figure 6: *In May 2018, another large number of email addresses was offered for sale to Swiss recipients.*

Creating collections of email addresses and reselling them is a lucrative business model for internet criminals. The fraudsters use information from data thefts as well as freely available sources. Spammers have the internet automatically searched for valid email addresses published on websites (for example in forums or guest books, etc.). Compromised email accounts are also a good source for email addresses. Address books as well as emails are searched for addresses here. Another method is to try out common first and last names. If an email is sent to addresses obtained in this way, most email servers report that this address does not exist - for all others, the sender can assume that the address actually exists. These attempts are carried out fully automatically.

Collections with valid email addresses are circulating in great numbers in the underground market. As a rule, the sale of such data takes place within this market. It is very uncharacteristic that such sales offers are sent in large numbers to "normal" internet users. The attackers' motives in the case of such mass mailings is unclear. It is conceivable that this is an attempt to trick the recipients into paying money in advance without the perpetrators even being in possession of the email addresses. It may also be an attempt to check that an existing spam database is up-to-date and see which email addresses are rejected by the email servers.

Assessment / recommendation:

The email wave in May 2018 led to numerous reports to MELANI and also to some confusion, as in many cases it was suspected that the password associated with the email address would also be stolen and sold. This was fortunately not the case. Although the appearance of one's own address in such a database is unpleasant, it can hardly be prevented because the email address is the central hub of all internet services and is therefore used in many places. However, security is not compromised if you adhere to the usual guidelines for handling emails:

See rules of conduct for handling emails on the MELANI-Website

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

In such cases, MELANI recommends ignoring the email and never replying to it. A reply confirms to the spammers that the email address they have chosen is working and that the messages are being read. This can result in an increase in spam emails.

4.5 Data leaks

4.5.1 Swisscom sales partners lose customer data

In autumn 2017, cybercriminals stole the contact data of around 800,000 Swisscom clients. However, the Swisscom network was not directly compromised: the cybercriminals obtained the access data of a distribution partner who was responsible for processing this data. It is not known how the access data was stolen from the distribution partner. Swisscom discovered the incident during a routine inspection.[15]

The stolen data is information required to identify the customer, such as name, home address, telephone number and date of birth. Such information can also be found in telephone directories or on social media. According to Philippe Vuilleumier, Head of “Group Security” at Swisscom, no sensitive data as considered to be "particularly sensitive personal data" under the Data Protection Act.such as passwords, call or payment data were affected. Such sensitive data is secured with correspondingly more effective protection mechanisms.[16]

[15] https://www.srf.ch/news/wirtschaft/massnahmen-eingeleitet-datendiebstahl-bei-swisscom (as at 31 July 2018).

[16] https://www.swisscom.ch/en/about/medien/news/interview-philippe-vuillemier-head-group-security.html (as at 31 July 2018).

As an immediate measure, Swisscom blocked the affected access of the partner company and in a second phase tightened the security measures. In particular, more rigorous monitoring of access by partner companies, an alarm system for suspicious activities and two-factor authentication were introduced.[17]

The immediate measures also included transparent communication. The Federal Data Protection and Information Commissioner (FDPIC) was informed, fixed-network and corporate customers were informed in writing and a free information service was set up via text message. This enabled mobile phone customers to check whether they were affected by this data leak.

4.5.2 The use of stolen data

On 26 April 2018, the Swiss company "Epsitec", manufacturer of administrative software for small and medium-sized enterprises, reported on its website that it had been the victim of a data theft. The attack affected email addresses, telephone numbers and the postal addresses of some 35,000 customers. According to "Epsitec" no credit card numbers and passwords were stolen.[18] What was remarkable in this case was the intended use of the data by the criminals: With the stolen data they generated personalized e-mails to distribute the malware Retefe. Since users are increasingly suspicious of unexpected and impersonal emails, criminals must come up with some ideas. A personal salutation or a reference to an existing company contact can help to tempt the victim to open an attached file. In the current case, not only the first name and surname were used, but also the data from the "Epsitec" data theft in order to give the email more credibility. The email either announced an alleged DHL delivery or simulated a request from the Federal Tax Administration (FTA).Passwords for sextortion

During the reporting period, a further use of data from data leaks was observed. What is special about this is that although sensitive data such as passwords is involved, some of this data is several years old. At first glance, such outdated data is not very valuable. However, criminals have also come up with a use for data of this sort. In the summer of 2018, MELANI registered various waves of blackmailing emails. The recipients are threatened with the publication of compromising material that has been previously compiled on the victim's computer using malware.[19] The blackmailers claim to have control of the recipient's webcam as well. As alleged evidence, the criminals mention a password or a mobile phone number which is actually used by the victim or has been used before. The purpose of providing such personal data is to give the claim more credibility and to unsettle the recipient. It is precisely here that the data from the old data leaks come into play. In all the reported cases, the data came from older databases.

---

17 https://www.swisscom.ch/en/about/medien/press-releases/2018/02/20180207-mm-swisscom-verschaerft-sicherheitsmassnahmen-fuer-kundenangaben.html (as at 31 July 2018).

18 https://www.watson.ch/digital/schweiz/581594688-hacker-klauen-35-000-kundendaten-bei-schweizer-software-firma-epsitec (as at 31 July 2018).

19 https://www.skppsc.ch/de/themen/internet/sextortion-erpressung/ (as at 31 July 2018).

Assessment:

The blackmailers tried their luck and sent the emails in the hope that the recipients would include people who had recently looked at pornographic websites. The recipients can thus be intimidated by the email. No such case was reported to MELANI in which the perpetrators were actually in possession of compromising images or video material, let alone had sent or published such material.

4.5.3 Credential stuffing with old passwords

Many users change their passwords regularly. However, if a criminal can fall back on a large number of data records, there are always some valid passwords among them. Many users use the same password for different services over a longer period of time. This is a welcome simplification for criminals and allows them to systematically try out the collected login data from the diverse data leaks at various internet service providers. This is referred to as "credential stuffing". When users use a password more than once, they enable criminals to log in under their identity with a little luck or perseverance and abuse the service. In one case reported to MELANI in 2018, nearly a million such stolen login/password combinations were used to attempt to log into an online portal. In the case in question, the misused access data originated in some cases from very old leaks from other providers.

Assessment / recommendation:

Web shops and other internet services are regularly hacked and the corresponding customer data extracted. If passwords are not or insufficiently encrypted, criminals can come into possession of access data. With this data, the criminals try to log on to a host of other internet platforms. They hope that users will use the same login data for multiple services.

Services that detect such login attempts can report to MELANI. MELANI integrates this data into the check tool (www.checktool.ch). Internet users can then use the check tool to check whether their data is affected.

Passwords used online must be long enough so that they are not easy to guess. A separate password should be chosen for each shop/service. Where available, a second login factor should be enabled.

4.6 Crimeware

In the first half of 2018, there were also numerous infections with criminal software (crimeware). The statistics in figure 7 show the distribution of the most significant malware in Switzerland. There is also malware, which is also very significant but does not appear in the statistics, such as the "Retefe" e-banking malware. "Retefe" is not malware in the true sense of the word, but merely changes the browser settings.

As in previous years, the majority was due to the "Downadup" malware (also known as "Conficker"). This worm has been around for over ten years and is spread via a security

vulnerability in Windows operating systems that was discovered in 2008. The corresponding patch has also been available since 2008. Second place goes to "Gamut" - a spam malware which would appear to be responsible for 37% of the international spam volume in the last quarter of 2017. The "Gamut botnet" mainly sends job offer spams for the purpose of money mule recruitment.[20] In third place is "Gamarue"[21] - also known as "Andromeda". This is a downloader that can download additional malware. In fourth and fifth place follow the malware "Spambot" and "Stealrat". These two are also responsible for sending spam. "Stealrat" does this via infected domains or IP addresses on which "WordPress", "Joomla!" and "Drupal" run. Spam messages are thereby sent through legitimate email servers and are more difficult to filter. In sixth place follows the first cryptominer malware "Monerominer" and in ninth place the first e-banking Trojan "Gozi". The botnet "Mirai", known since the attack on the internet service provider "Dyn", has disappeared from the top eleven.

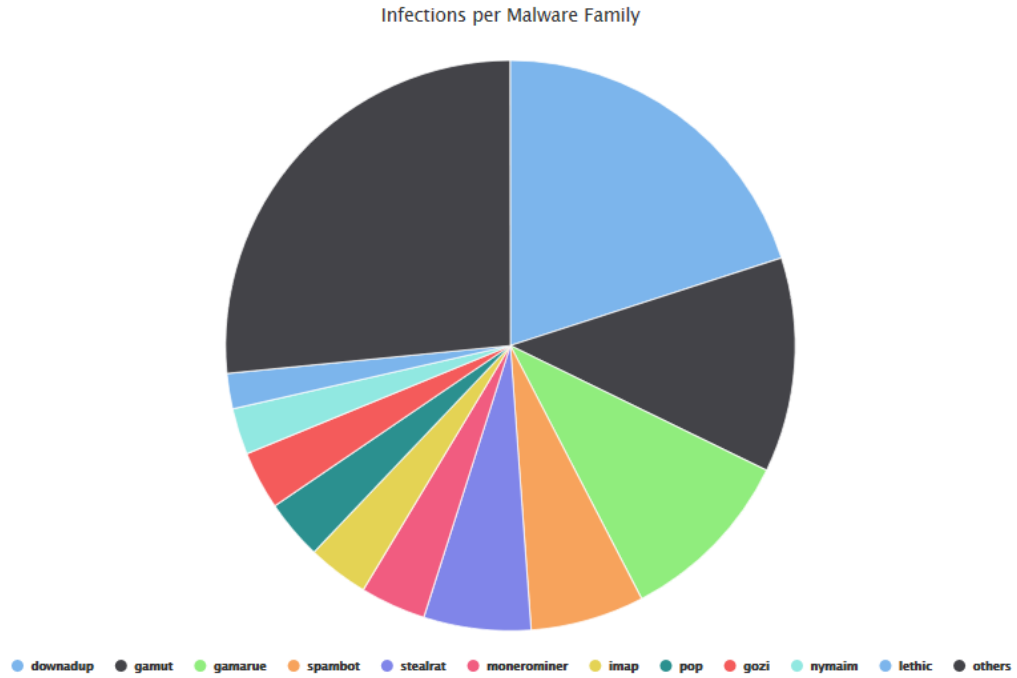


Figure 7: *Distribution of malicious software in Switzerland known to MELANI. The cut-off date is 30 June 2018. Current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/*

[20] https://sensorstechforum.com/necurs-gamut-botnets-spam/ (as at 31 July 2018).

[21] https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/Schadsoftware/Andromeda_Gamarue.html (as at 31 July 2018).

4.7 E-banking Trojans in Switzerland

Online payment systems are attractive targets for cyber criminals because you can make big profits with them with a small overall risk. Most cyber campaigns observed today combine social engineering methods and the use of malware. In addition, various tricks are used to circumvent the antivirus programs, to protect one's own infrastructure against take-down attempts and to make it more difficult for criminal prosecution authorities to take action. Various e-banking Trojans were again in circulation in the period under review.

4.7.1 "Retefe" und social engineering

"Retefe" is currently one of the most widespread Trojan in Switzerland. In the past, malware was mainly spread via counterfeit invoices from online shops such as Zalando or Ricardo but more recently "Retefe" has expanded its mailing list to include many well-known companies. In the first half of 2018, MELANI recorded several waves of spam on behalf of DHL, SBB, the police of various cantons, the Federal Tax Administration (FTA) and the airline Swiss. In addition, "Retefe" has shifted from nationwide spam mailings to targeted mailings with personalised content. For example, emails were provided with the correct name and telephone number of the recipients. Although personalisation requires greater preparation for the attack, the effort seems to be worthwhile, as the victims can be more effectively deceived and the chances of the infection being successful increase accordingly.

The malware aims to change the settings of the web browser (Internet Explorer, Firefox and Chrome) so that the victim is redirected to a copy managed by the cyber criminals when calling up an e-banking website. During the login process to the supposed e-banking portal, a QR code is first displayed, which, when opened with a smartphone, leads to a so-called text message stealing Trojan. After this Android app has been installed, all text messages from the bank for dual authentication are forwarded to the attackers. Fraudsters can then log into the victim's e-banking account and make payments. In another case, the cybercriminals tried to obtain activation data. These letters are normally sent to bank customers by post and contain a QR code that must be scanned using a corresponding app when logging into e-banking for the first time. This means that the smartphone is recognised by the bank as a means of communication for two-factor authentication. The fraudsters asked the victims via email to scan or photograph the letter.[22] Retefe is mostly directed at Windows systems but in 2017 various malware waves were also observed that were targeted at Swiss users of the MacOS operating system.[23]

The "EternalBlue" vulnerability has also been part of the repertoire since September 2017. If an employee in a company accidentally opens an infected attachment, the malware can use this vulnerability to jump to the computer from which the company makes its e-banking

[22] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html (as at 31 July 2018).

[23] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html (as at 31 July 2018).

payments. However, this only works if the vulnerability for which a security patch was released on 14 May 2017 has not yet been closed. The implementation of "EternalBlue" suggests that "Retefe" is mainly targeting SMEs.

4.7.2 "Dridex" and offline payment software

The e-banking Trojan "Dridex" is also widespread in our latitudes. It is a computer worm that first appeared in 2012 under the name "Cridex". However, the worm-like spread had disadvantages, since open security vulnerabilities are required and the distribution is also very noticeable. Earlier versions were thus distributed almost exclusively using comprehensive spam mailings. Infected Word documents are used which are disguised as an invoice, confirmation of an online order, payment request or similar methods. Apparently real companies are used as email senders, which often have their headquarters in the same country as the victims. The emails tailored to Switzerland are mainly written in German. In the first half of 2018, only one email wave was recorded in Switzerland for the distribution of "Dridex": emails sent on behalf of Swisscom contained an e-bill that was very similar to the bill of the telecommunications company. Behind one field with the note "View invoice" field a link to a harmful JavaScript was hidden, which then tried to install the "Dridex" bank Trojan.

Once installed, Dridex uses the man-in-the-middle (MITM) method. With this technology, the attacker switches unnoticed into a communication channel between two partners, in this case the bank and the e-banking customer, so that the exchange of data can be followed and manipulated. Dridex is decentralised and its network architecture is divided into several levels and subordinate networks which are maintained by different criminal groups. This makes countermeasures by the authorities more difficult. For this reason, "Dridex" remains a significant threat, although it is said that in October 2015 the US Department of Justice and the FBI was able to arrest the head of the network and since then other members of the network have been arrested.[24]

In July 2016, "Dridex" expanded the modus operandi to offline payment systems.[25] After infection, the Dridex malware searches for offline payment software on the infected computer. Such software is used by many companies to transmit large volumes of payments via the internet to one or more banks. If Dridex finds such payment software on the computer, further malware can be downloaded from the internet, which is then used to transmit fraudulent payments. In some cases, for example, the malware Cobalt Strike was used, in other cases "Carbanak". If no offline payment software was found on the infected computer, "Dridex" attacked the e-banking sessions according to its capabilities.

Since 2016, Dridex has also been targeting crypto currency exchanges. This year the number of targets in the configuration files has increased.

---

[24] https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/bugat-botnet-administrator-arrested-and-malware-disabled (as at 31 July 2018).

[25] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/offline-payment-software.html (as at 31 July 2018).

At present, only moderate activity is seen both nationally and internationally. But that does not mean that the danger is diminishing. The current period of calm can also serve as an update and preparation phase. In addition, other organisations such as the "Cobalt gang", which probably collaborate with "Dridex", continue to use the resources.

4.7.3 "Gozi ISFB" and drive-by dissemination

The e-banking malware "Gozi" was first observed in Switzerland in January 2009. It is assumed that "Gozi" was created by the Russian Nikita Kuzmin, who was arrested by the FBI in August 2011.[26] However, the spread of Gozi on the black markets led to the fact that it is currently still used by various cybercriminals. The new version, called "ISFB", targeted the customers of Swiss banks for the first time in May 2015. Gozi also uses the man-in-the-middle (MITM) method for e-banking fraud.

The new variant of Gozi is mainly spread via website infections. The online versions of daily newspapers, which are visited daily by numerous readers, are ideal targets for this type of malware. Their popularity allows them to reach a large number of victims. For example, in March 2017, the 20min.ch website was attacked in order to distribute the banking Trojan.[27] Email waves with infected .zip attachments are also being observed. For example, at the beginning of March 2018 as an alleged parcel notification from Fedex. In 2018, Gozi also used malvertising for the first time to spread the malware. This technique consists in using advertisements to mislead the user into downloading manipulated software. In search engines, the advertisements are often displayed above the actual search results. This leads to confusion among users. Specifically, the cyber criminals advertised Java and Firefox software on google.ch, which included malware in addition to the desired program.

Currently, Gozi seems to be targeting not only e-banking systems, but also offline payment software and crypto currency exchanges. Interest in these modern targets seems to be a major trend for the near future.

---

[26] https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-virus-sentenced-manhattan-federal-court (as at 31 July 2018).

[27] https://www.srf.ch/news/schweiz/nach-malware-attacke-auf-20-minuten-was-sie-jetzt-tun-koennen (as at 31 July 2018).

Assessment / recommendation:

The three campaigns highlight some trends in the field of attacks on payment systems. In addition to the classic attack vectors such as infected emails and websites, the misuse of advertising for criminal purposes is also proving to be a successful method of spreading e-banking malware. It is becoming increasingly difficult for users to detect such attacks. First and foremost, the operators of websites are therefore required to systematically check advertisements and other dynamic content, especially from external third parties. Users must continue to be particularly careful when receiving emails, even if they appear to be reputable and personalised. Therefore clicking less rather than more on a link or attachment It is therefore the better approach. A further trend is that SMEs are increasingly targeted in e-banking attacks because they tend to be less well protected than large companies, but still generate more banking transactions than private individuals. Swiss SMEs are therefore confronted with growing challenges in the field of IT security. With regard to the measures to be taken internally, MELANI recently published an update of the "Information security checklist for SMEs". It contains advice and tips on how companies can increase their resilience:

Information security checklist for SMEs:

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/merkblatt-it-sicherheit-fuer-kmus.html

5 Situation internationally

5.1 Espionage

5.1.1 "Sofacy" linked to various incidents

"Sofacy", also known as "APT28", "Fancy Bear" and "Tsar Team", remains one the world's best-known and most active espionage groups. "Sofacy" uses all manner of types of infection vectors: well-made and targeted "spear phishing" emails with infected attachments or links, as well as "water hole" attacks. This form of campaign uses a broad arsenal of command-and-control servers. The developers behind "Sofacy" do not only adapt the malware to individual victims. They also go to considerable lengths in order to carry out targeted "social engineering" attacks.[28] In addition to the highly targeted attacks previously seen, much more widespread attacks, which aim to reach a maximum number of potential victims, have now also been

[28] https://securelist.com/a-slice-of-2017-sofacy-activity/83930/ (as at 31 July 2018).

observed. In the "Zebrocy" malware attacks, a backdoor downloader, the targets (email addresses) were chosen at random rather than on a specific basis and could easily be found using search engines etc. Such a method is rather atypical for an APT campaign and is otherwise usually employed by cyber criminals. This type of strategy increases the chance of successful infection but it also increases the likelihood of being detected.[29] It is particularly notable that attacks have been extended to the Far East with strong interest in military, defence and diplomatic organisations.[30] The choice of different targets and tactics makes pinpointing attackers difficult. This could also be the motivation behind the current development of "Sofacy".

In 2018, the "Olympic Destroyer" malware made the headlines in connection with the Olympic Games in Pyeongchang (South Korea) when the ICT infrastructure of the winter games and certain partners was attacked by this worm. Although it is not possible to conclusively pinpoint the attackers, the software security group Kaspersky was able to establish certain similarities with "Sofacy" (see also chapter 4.1.1).

On 10 January 2018, the "Fancy Bears Hack Team" published data which was purported to have been stolen from the International Olympic Committee and the USA National Olympic Committee between the end of 2016 and beginning of 2017. Again connections with the "Sofacy" group are suspected.[31]

5.1.2 VPN filter - at least 500,000 devices affected

On 23 May 2018, Cisco's security firm "Talos" published data on a bot network called "VPN filter" which is said to comprise over half a million router and NAS devices.[32] When the attacker issues the relevant command, the malware overwrites the first 5,000 bytes of the first memory block, after which the device can no longer start. It is not difficult to imagine the impact of over half a million devices failing simultaneously. The devices are located in a total of 54 countries, with a particularly high number in Ukraine, evoking memories of the "NotPetya" malware. The centre of the attack then was also in Ukraine but the effects were felt around the world.

All infected devices were connected to the internet and had security vulnerabilities or were protected by standard passwords. "VPN filter" was discovered on various devices including those made by router manufacturers "MikroTik", "Linksys", "Netgear" and "TP-Link"; NAS

---

29 https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/ (as at 31 July 2018).

30 https://www.kaspersky.de/about/press-releases/2018_sofacy-erweitert-sein-operationsgebiet-in-richtung-fernost (as at 31 July 2018).

31 https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/ https://www.mid-day.com/articles/russia-apparently-hacking-winter-olympics-emails-report/18923160 https://www.eclecticiq.com/resources/russian-hacking-group-fancy-bear-prepares-to-attack-winter-olympics-u-s-senate (as at 31 July 2018).

32 https://blog.talosintelligence.com/2018/05/VPNFilter.html (as at 31 July 2018).

devices produced by the manufacturer "QNAP" were also affected. The malware is constructed in three stages. Only the first stage is permanently installed on the device and it then downloads the actual malware and its functions in two further stages.

At the beginning, the malware could only be eliminated by restoring the factory settings. The FBI was able to take over the server at almost the same time as the bot network was made public. When restarted, the server delivers information for the second stage about where and when the malware should be installed next. In specific terms, the malware reads the necessary information for the new installation from the meta data of an image stored on the "photobucket.com" photograph platform. Although a restart does not remove the malware from the device, it does mean it can no longer download the actual functions from stages 2 and 3. The FBI measures effectively neutralised the harmful malware and also allowed infected devices to be identified. During its analysis, "Cisco Talos" encountered a typical error in the implementation of the RC4 encryption used which was also noticed in the "BlackEnergy" malware.

5.1.3 Attack on the German Federal Government network

At the end of February 2018, it became known that the German Federal Foreign Office had become the victim of a hacker attack. The hacker attack is said to have taken place as early as at the turn of 2016/2017.[33] The attackers had access to the central data network of the federal government, known as the Berlin-Bonn information network (IVBB). The IVBB is a type of intranet for the Bundesrat, Federal Chancellery, Federal Ministries, Bundesrechnungshof (Germany's supreme audit institution) and various security authorities. This is the second large known attack on the German government's ICT infrastructure since the German Parliament hack in 2015.[34]

The attack is said to have occurred via a learning platform which is used at the Federal University of Applied Administrative Sciences for further training purposes.[35] More detailed information concerning security vulnerabilities which might have been used was not available.[36] Numerous media reports speculated that the attack could have been conducted by the "Sofacy" group. It was only later that suspicion turned to the "Snake/Turla" group which

33 https://www.zeit.de/politik/2018-04/hackerangriff-bundesregierung-russland-verfassungsschutz-hans-georg-maassen (as at 31 July 2018).

34 https://www.zeit.de/digital/datenschutz/2018-03/hackerangriff-bundesregierung-outlook-auswaertiges-amt (as at 31 July 2018).

35 http://m.faz.net/aktuell/politik/inland/hacker-angriff-war-gezielter-angriff-auf-das-auswaertige-amt-15476826.html (as at 31 July 2018).

36 https://www.tagesschau.de/inland/hackerangriff-bundesregierung-101.html (as at 31 July 2018).

is also held responsible for attacks in Switzerland. The defence company "Ruag" was also attacked with "Snake/Turla".

5.1.4 Attacks on energy providers

On 15 May 2018, the "Süddeutsche Zeitung" made an attack on the telecom company and "EnBW" subsidiary "Netcom BW" public. The attack had occurred back in summer 2017.[37] The newspaper reported that although it was possible to avert the attack at an early stage, spying on internet traffic remained possible for a short time. The attackers were able to access the router via an external service provider's employee account. Furthermore, it is said that weaknesses in "Cisco's" router software were exploited, although no details on the weaknesses were given. Once the attackers had taken over control, they were able to run programmes and siphon off data. There was no risk of sabotage as the supply network does not use the "Netcom" network. The attack was also discovered at an early stage. Those behind the attacks could not be conclusively identified. The "Sandworm" group, which is said to be responsible for the attacks on the Ukrainian electricity grid in winter 2015/2016, is one suspect. On the other hand, the "Dragonfly" group is another suspect. This group already attracted attention last year with attacks on Western energy suppliers.[38]

On 7 June 2018, the German Federal Office for the Protection of the Constitution addressed German energy companies in a publication. Information on the "Dragonfly" APT group's current attacks would be available. The energy supply, water disposal and supply, as well as information technology/telecommunications, were to be targeted. It has been seen that attacks in recent months have been particularly aimed at infrastructure components such as routers.[39] The attackers use attack tools which are readily available in the public domain and attempt to bring insufficiently protected systems under their control. In order to obtain access, the attacker's first step is usually to scan a potential victim's grid with a port scanner. For its part, the German Federal Office for Information Security (BSI) also warned of attacks on the energy sector on 13 June 2018, but also highlighted the risk of attacks on other sectors.[40]

---

37 https://www.sueddeutsche.de/digital/enbw-tochter-hacker-haben-deutschen-energieversorger-angegriffen-1.3980625 (as at 31 July 2018).

38 MELANI Semi-annual report 2017/II https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2-2017.html (as at 31 July 2018).

39 https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-spionage-und-proliferationsabwehr/broschuere-2018-06-bfv-cyber-brief-2018-01 (as at 31 July 2018).

40 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html (as at 31 July 2018).

In July 2018, the "Department of Homeland Security (DHS)" announced that hundreds of targets across the USA power grid had been attacked in recent years. It appears that the attackers managed to gain access as far as the control centres which meant they had penetrated deep enough into the systems that they would have been able to "flip switches" and damage or interrupt the power supply.[41] The attackers generally tried to make their way via third-party companies with less secure networks. For example, they sent out phishing emails in order to access suppliers' login details. Once they were in this network, the attackers concentrated on their actual target, the energy suppliers.[42]

5.1.5 Attackers focus on "Cisco's" "Smart Install"

There have been regular reports of attacks on "Cisco" switches using the "Smart Install (SMI)" remote maintenance function since as early as 2016. The problem lies with devices which are connected to the internet without protection as the tool does not require any authentication. Operators must additionally install such protection.[43] "Cisco" published information on this problem back in February 2017.[44] However, as the devices work exactly as they should, "Cisco" did not consider this a weakness and instead referred to users' responsibility who it said were responsible for protecting the devices. The problem is that users neither configure nor disable the protocol. The client is then constantly waiting in the background for configuration and installation commands. An attacker can therefore modify the server setting, determine and modify the configuration data, replace the operating system and create accounts and freely execute commands.

At one point over 200,000 vulnerable devices were accessible via the internet and could theoretically have been reconfigured or completely taken control of. In Switzerland around 1,500 IP addresses potentially exposed systems were known.[45] At the end of 2017, "Cisco" received indications that attackers were systematically searching through devices for this vulnerability. As a graph from Cisco shows, the traffic at corresponding port 4786 has significantly increased since this time.

---

41 https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110 (as at 31 July 2018).

42 https://www.nzz.ch/international/russische-hacker-sitzen-schon-an-den-hebeln-der-amerikanischen-stromversorgung-ld.1406263 (as at 31 July 2018).

43 https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k17-0274_update_1.html (as at 31 July 2018).

44 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi (as at 31 July 2018).

45 As at May 2018

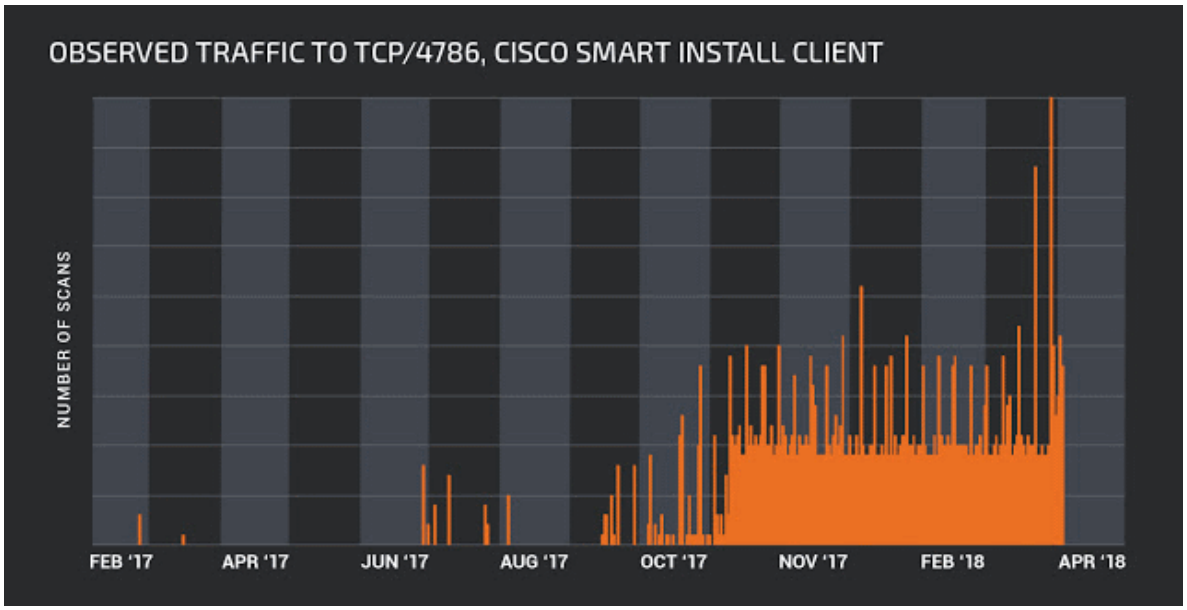


Figure 8: *Number of scans on Cisco Smart Install clients between February 2017 and April 2018 (source: Talos, https://www.talosintelligence.com/)*

At the beginning of 2018, "Cisco Talos" issued another publication in which it wrote that there were indications of increased attacks on critical infrastructure using the SMI protocol.[46] Specifically, a link to the "Dragonfly" espionage group was suspected. US-CERT had previously warned of "Russian actors" who have attacked and infiltrated the networks of companies in the energy sector as well as other critical sectors.[47]

Also in April, experts from the security firm "Kaspersky" uncovered a hacker campaign which primarily affected "Cisco" devices in Iran and Russia. A bot network was purported to be responsible for this series of attacks. It searched for open and unprotected ports 4786 in order to then take control of "Smart Install", overwrite the configuration and make the switch unusable. Finally, a message was left with a US flag and the words "Do not mess with our elections".[48]

The fact that two vulnerabilities were published which allowed an attacker to disable or take over "Cisco" devices made more headlines at the end of March. The coincidence in the timing of the attacks and both the vulnerabilities led to numerous speculations concerning a possible connection. This caused "Cisco" to clarify that no vulnerability had been exploited in previously

46 https://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html (as at 31 July 2018).

47 https://www.us-cert.gov/ncas/alerts/TA18-106A (as at 31 July 2018).

48 https://www.kaspersky.com/blog/cisco-apocalypse/21966/ (as at 31 July 2018).

observed attacks and that these had been caused solely by poorly configured or unconfigured devices.[49]

Assessment/recommendations

Attackers are increasingly targeting routers. This is for two main reasons. Firstly, they are generally the weakest link in the chain as updates are not always swiftly installed. Secondly, routers are important network devices through which a company's communication flows. In addition, routers are often connected directly to the internet and can therefore be directly attacked by attackers via the internet.

As the Cisco "Smart Install" protocol does not require authentication, an attacker can attack any device which can be accessed via the internet and which is not additionally protected. These devices must urgently be protected from unauthorised external attacks. Furthermore, updates should always be installed promptly.

5.2 Industrial control systems

5.2.1 VW and Audi infotainment systems hacked

In April 2018, Dutch security researchers published their research on exploiting a vulnerability in the infotainment system in certain VW and Audi models. The researchers used the vehicle's WiFi connection as their attack vector. Through this they accessed a port which allowed the vehicle's IVI system (in-vehicle infotainment) to be compromised. This fairly generic term covers different interactive audio and video services which allow people to listen to music, receive information and make telephone calls etc. in their vehicles. The researchers explained that the hack allowed them to listen to conversations made using the hands-free kit, access the address book or even follow the vehicle's movements. The researchers decided to stop their work before attempting to access the critical systems such as the brakes or the accelerator. [50]

It is not the first time that the security of connected cars has been the centre of concern. It has even been a recurring research topic since the famous hacking of a Jeep Cherokee in 2015[51]. The separation of infotainment systems, which are often the target of attacks, and a vehicle's critical systems is key. This research was not able to demonstrate a porosity between the two systems. In terms of response to the disclosure of a vulnerability, remotely updating the entire fleet, respectively its software would always be desirable but is not always possible. Often only

---

49 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180409-smi (as at 31 July 2018).

50 https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/ (as at 31 July 2018).

51 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (as at 31 July 2018).

the systems of newly produced cars are up to date, even though clients also have the possibility of having a patch applied at their car dealership.

5.2.2 Cryptominers at European wastewater facility

The success of cryptocurrencies offers extremely tempting prospects for cyber criminals. Besides the large-scale bitcoin thefts, criminals have also spread out elsewhere by abusing the mining typical of this type of currency. Mining is the process by which transactions in a cryptocurrency are verified and new cryptocurrency is generated. Complex calculations have to be solved for this purpose, requiring considerable IT resources. The provision of these resources is compensated with a certain amount of "mined" money, corresponding to the share in the calculation. Mining ultimately contributes to money creation.

Because mining can be used to earn money, certain actors have been looking for ways to abuse it for quite some time already (such cases were already mentioned in our semi-annual report 2013/2[52]). In the meantime, attacks that abuse computing power for mining have multiplied. An article by the security company Palo Alto Networks discovered more than 470,000 versions of malware which were intended to exploit the computing power of its victims.[53] Furthermore, it is not always the private computers, office automation networks or webservers which are affected. Indeed, according to an article on the Newsportal SecurityWeek, a critical infrastructure operator active in wastewater treatment in a European country observed a cryptominer in its production network ("Operational Technology network").[54] In this case, the malware caused the network to slow down by using its computing power and network bandwidth.[55] Although this infection did not adversely impact the running of the network, it did cost the company in terms of electricity consumption and internet bandwidth. Furthermore, the infection could have had a long term impact on the infrastructure's operations with consequences for its clients.

5.2.3 "Hide'n Seek" - IoT botnet with peer-to-peer function

Since the "Mirai" malware, bot networks which misuse devices in the internet of things have become well known. At the beginning of January 2018, security researchers discovered a new IoT botnet known as "Hide'n Seek" which uses a worm-like mechanism to spread. To do so, the malware creates a random list of IP address with potential victims which are then contacted. If certain ports on the devices are open, the malware attempts to log in using standard passwords or dictionary terms; various vulnerabilities are also tested. The bot

---

52 MELANI semi-annual report 2013/2 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2013-2.html (as at 31 July 2018).

53 https://researchcenter.paloaltonetworks.com/2018/06/unit42-rise-cryptocurrency-miners/ (as at 31 July 2018).

54 https://www.securityweek.com/cryptocurrency-mining-malware-hits-monitoring-systems-european-water-utility (as at 31 July 2018).

55 https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility/ (as at 31 July 2018).

network is based on the decentralised peer-to-peer structure which is atypical for the IoT. Individual devices mutually exchange information on successful login attempts and learn from each other. Unlike "Mirai", "Hide'n Seek" does not focus on the Distributed Denial of Service (DDoS) function, instead it concentrates more on espionage and subsequent attempts at extortion. Its functions include data exfiltration, code execution and device failure. As the malicious code has not yet been able to stay permanently on the device, infected devices can be cleaned by rebooting.

Conclusion / recommendation:

The increasing computerisation and networking of all sorts of objects of everyday use (internet of things) offers many new and useful functions and conveniences. This includes consumer electronics and internet access in means of transport such as cars and aeroplanes. However, the associated risks should not be ignored. New possibilities always entail dangers as well, which must be taken into account already during the development phase (security by design).

Checklist with 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

5.3 Attacks (DDoS, defacements, drive-bys)

5.3.1 "Memcached DDoS" attack

The attack on the web-based service provider "Github" on 28 February 2018 with a bandwidth of approximately 1.35 Tb/s was of the most powerful DDoS attacks ever recorded. However, the attack was swiftly averted with the help of the provider "Akamai".[56,57] This was a DDoS attack assisted by the "memcached" function which is used on servers. "Memcached" is open source software used for caching data. Because the data is stored in the working memory, it can be accessed quickly, which generally improves the performance of online applications, for example (see also chapter 3). By default, the server listens on TCP and/or UDP port 11211 and is therefore accessible to all internet users. "Memcached" uses the connectionless UDP protocol in addition to TCP. Therefore it is possible for attackers to use "Memcached" services which are not protected by appropriate measures such as a firewall for DDoS amplification

[56] https://githubengineering.com/ddos-incident-report/ (as at 31 July 2018).

[57] https://blog.apnic.net/2018/03/26/understanding-the-facts-of-memcached-amplification-attacks/ (as at 31 July 2018).

attacks on other internet users. It is particularly critical that attackers can achieve amplification of a factor of up to 51,000 and thus a DDoS volume of 1 Tb/s and more without any problems with a single UDP packet to a server of this type.

At the time of the attack there were around 95,000 vulnerable systems worldwide.[58] Following the attack, many operators of vulnerable systems were written to and asked to provide protection. This was clearly a success as the number has significantly dropped since then. In Switzerland, MELANI also informed various operators about vulnerable systems and it was possible to reduce the number here too.

Recommendation:

The "Memcached" UDP port (11211 UDP) is not required for usual operation. We therefore recommend deactivating UDP completely when using "Memcached". This simply requires adding the following line to the "Memcached" configuration file (/etc/memcached.conf):

-U 0

Limit access to the "Memcached" server by using a firewall. Only systems which need access to the "Memcached" server should have this.

In addition, we recommend the commonly known measures to protect online services, e.g.:

- Ensure that updates are installed promptly so that you are always using the most up-to-date version of "Memcached".
- Configure Memcached so that the Memcached service listens on a port other than TCP/UDP 11211. However, please note that this measure alone is not sufficient as it only hides the problem instead of solving it.
- Monitor the server to quickly detect any misuse.

For more information about securing Memcached, please see:

https://www.digitalocean.com/community/tutorials/how-to-secure-memcached-by-reducing-exposure

https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/CERT-Reports/HOWTOs/Open-Memcached-Server/open-Memcached-server_node.html;jsessionid=1C616824044F51668CFF17441B4C5119.1_cid369

[58] https://blog.apnic.net/2018/03/26/understanding-the-facts-of-memcached-amplification-attacks/ (as at 31 July 2018).

5.3.2 Banks' internal systems remain the target of cybercriminals

Banks' internal systems have again been the target of criminals during the period under review. In February 2018, the Central Bank of the Russian Federation announced that an attack had been made on a Russian institution which allowed RUB 339.5 million to be stolen last year (the equivalent of approximately USD 6 million at the time of the announcement). In order to achieve their aims, the criminals managed to take control of a machine through which money transfers via the SWIFT interbank system were made. Neither the precise identity of the victim nor the attackers' modus operandi were provided in detail.

An even more spectacular attack was made public in August 2018. It resulted in the theft of USD 13.5 million from the Indian bank Cosmos. According to the information available, this attack is said to have compromised both the bank's ATM and SWIFT infrastructure. The criminals were then able to withdraw cash at ATMs in 28 different countries for a total of USD 11.5 million and carry out transactions via the SWIFT system to the tune of USD 2 million. Following an initial compromise, these operations were made possible via lateral movements which allowed the criminals to reach the bank's critical systems. The sophistication of the methods used and the level of coordination required for an attack which takes place across different countries appear to be signs that an advanced player was behind the act. Securonix, the company which investigated the incident, attributes the attack to the Lazarus group which is known to have attacked various banks' systems in the past.[59]

5.4 Data leaks

5.4.1 DHS privacy leak

In January 2018, the "US Department of Homeland Security (DHS)" announced that it had been the victim of an internal data leak. Personal data of over 240,000 DHS employees was affected, notably in 2014. In addition, data of people who were involved in the investigations of the "Office of Inspector General", the DHS supervisory authority, between 2002 and 2014 was also affected. Witness and claimants were also concerned by the data leak. The theft included names, social insurance numbers, postal and email addresses, telephone numbers and dates of birth.

In this case, the data leak was not caused by an external cyber-attack; it was an internal incident. In May 2017 during ongoing criminal investigations, it was determined that an ex-DHS employee had created an unauthorised copy of the authority's incident management system.

---

[59] https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/ (as at 31 July 2018).

The DHS informed its employees by post and set up a telephone support hotline for affected persons. It also offered those affected an 18-month service which protected them from misuse of identity and credit. Furthermore, the DHS implemented security measures in order to limit access to systems with personal data.[60]

5.4.2 "Exactis" data leak

For a long time, it was possible to externally access the database of the US company "Exactis" which contains personal information on millions of people without protection. "Exactis" is a marketing company based in Florida which collects data on the behaviour and preferences of millions of people. The precise extent of the data leak is unclear. It is estimated that data of 200 million people and 110 million companies was affected. The data included commercial information, telephone numbers, postal and email addresses. Fortunately, no financial information, social security numbers or other sensitive data is said to have been stored on the database. Although it is not expected that those affected will suffer any direct damage, the data could still be used in order to carry out targeted and personalised attacks on them in the future (see chapter 6.1).

What is special about this case is that it did not actually involve hacking. The security researcher Vinny Troia searched the internet for "ElasticSearch" databases using the "Shodan" search tool.[61] The "Exactis" database appeared in the results and was not protected either by a firewall or by other security measures and was therefore universally accessible. It is not known whether Troia was the first to discover the database or if the data had already been discovered and copied by other players. "Exactis" secured the database once it was informed by Troia.

5.5 Preventive measures

5.5.1 Member behind the Carbanak/Cobalt attacks arrested

On 26 March 2018, the Spanish police arrested a member behind the "carbanak" or "cobalt" attacks in partnership with Europol and other national police forces.[62] This small group made itself known in 2013 by attacking banks by using their cash machines to withdraw money (MELANI semi-annual report 2016/I[63]).The victims received phishing-like emails with a

---

60 https://www.dhs.gov/news/2018/01/18/privacy-incident-involving-dhs-oig-case-management-system-update (as at 31 July 2018).

61 http://www.vinnytroia.com/ (as at 31 July 2018).

62 https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain (as at 31 July 2018).

63 MELANI semi-annual report 2016/I https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-1.html (as at 31 July 2018).

malicious file. Once the file had been downloaded and executed, it allowed members of the group to infect the rest of the banking network by means of lateral movement. The group is suspected of attacking over 100 financial institutions worldwide and creating accumulated losses of over EUR 1 billion.

5.5.2 Cyber Europe 2018 - preparing for the next cyber crisis

Imagine the following situation: it is a normal day at the airport. All of a sudden, the check-in machines display a system error. Smartphone travel apps have stopped working. Employees at the check-in desks cannot use their computers anymore. Travellers cannot check in their luggage or go through security. Long queues build everywhere. The departure screens show all flights as cancelled. For unknown reasons, baggage reclaim no longer works and more than half of the aeroplanes are grounded. According to reports, a group of radicals has taken over control of critical airport systems through digital and hybrid attacks. It has already acknowledged responsibility for the attack and is using its propaganda channels to spread a call for action and attract new supporters to its radical ideology.

This extreme situation was presented on 6 and 7 June to over 900 European network and information security experts from 30 countries at this year's "Cyber Europe 2018 (CE2018)" exercise; the EU/EFTA's most comprehensive exercise to date. "Cyber Europe 2018" was organised by the European Union Agency for Network and Information Security (ENISA) in cooperation with network and information security authorities and agencies from across Europe. Switzerland also participated in this exercise with various participants from the administration and the private sector. The main objective of the exercise was to support organisations in testing their internal emergency plans for keeping their businesses running and their corresponding crisis management plans. At the same time, the aim was also to promote cooperation between public and private institutions. "Cyber Europe" reinforces this cooperation and is the answer to cross-border threats. It exists in close collaboration between European countries and organisations.

Key figures from this year's "Cyber Europe 2018" exercise:

- Participating countries: 30
  (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom)
- Participating organisations: 300
- Number of participants: over 900 cyber security experts
- Number of attacks: 23,222

"Cyber Europe" was created eight years ago and has developed into an important network and information security exercise in which hundreds of cybersecurity experts work together. It allows for a flexible learning experience as the participants, either individual analysts or entire organisations, can adjust the exercise to individual requirements. International cooperation between all participating organisations is one of the primary objectives. Switzerland has been

involved since the very beginning and since 2010 it has been a proud participant of the "Cyber Europe" exercise which is held every two years.

5.5.3 Lazarus C&C server take over

On 25 April, ThaiCERT announced that it had seized a command and control server at a Thai university[64]. According to the institution, the server was used by the "Hidden Cobra" group, known also as the "Lazarus Group". This group is notably suspected of having instigated the attacks on Sony Pictures in 2014 and the central bank of Bangladesh in 2016[65] (MELANI semi-annual report 2016/I[66]). The latter allowed them to steal USD 81 million.

According to McAfee, the operation named "Operation GhostSecret" targeted critical infrastructure as well as financial, health and entertainment institutions in over 17 countries, including one body in Switzerland. According to McAfee, the server was part of a campaign which targeted financial institutions in Turkey in February 2018[67].

The attacker had different malware to achieve its aims. US-CERT has published different analyses on the malware and believes that these activities are down to North Korean attackers[68]. According to McAfee, at the time of seizure, the campaign was still at its reconnaissance stage and was attempting to obtain information for future attacks.

6 Trends and outlook

6.1 The use of data in attacks

As mentioned in the last MELANI Semi-annual report[69], unwanted data leaks are occurring more and more frequently. Switzerland is not immune to this either, as the incidents at Swisscom, the dvd-shop and Epsitec show.

---

64 https://www.thaicert.or.th/alerts/admin/2018/al2018ad001.html (as at 31 July 2018).

65 https://threatpost.com/thaicert-seizes-hidden-cobra-server-linked-to-ghostsecret-sony-attacks/131498/ (as at 31 July 2018).

66 MELANI semi-annual report 2016/I https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-1.html (as at 31 July 2018).

67 https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/ (as at 31 July 2018).

68 https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity (as at 31 July 2018).

69 MELANI Semi-annual report 2017/II https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2-2017.html (as at 31 July 2018).

Cyber criminals are very versatile and innovative in the use of such data. An immediate way to convert data leaks swiftly into money is to directly blackmail the company where the data leaks occur. It is not so important how valuable the data is. The mere fact that data has been lost at a company puts it even more under pressure in the age of the European Union General Data Protection Regulation (EU GDPR). The best known example of this approach in Switzerland is the hacker group "Rex Mundi". However, this variant is only one of many possibilities for criminals. In general, the trend can be observed that criminals are increasingly recognising the value of data and are still profiting from apparently worthless data records.[70]

The criminals are helped by the fact that the resources of stolen data records in the underground market are almost inexhaustible. The portal https://haveibeenpwned.com/ alone, where anyone can check whether their access data has been stolen, contains over five billion combinations of user names and passwords. In addition, there is a multitude of other data from data leaks, data from hacked email accounts and computers. Thus an entire business branch has been created in the underground, which sifts through data, extracts important data and merges it into new databases. These are then resold to other criminals. Chapter 4.5 gives various examples of how such data can be used. A trend towards personalisation in a wide variety of approaches can be observed.

Fake sextortion attacks are a striking example. The victim is made to believe that the perpetrators have pornographic images of the victim at their disposal. To make this bluff more persuasive, blackmailers use personal information about the victim that comes from a data leak (e.g. first and last name, IP address or provider used, passwords or mobile phone numbers).

The spread of malware is also becoming increasingly personalised. Sometimes it is also possible that a stolen dataset has a direct impact on the business of a malware group. It is for example probable that the "Epsitec" data leaks had the consequence that after focusing the "Retefe" e-banking malware on German-speaking Switzerland, victims in French-speaking Switzerland now also receive malicious emails. "Epsitec" is a company based in French-speaking Switzerland.

Another type of fraud in which the available data about the victim plays a central role is the so-called "CEO fraud" or "president scam". The majority of fraudsters are currently still looking specifically on the company website or in social media accounts for information to work out a suitable scenario. But even here it can be assumed that data leaks will become more and more significant. Information losses in particular like at "Exactis", where one third of the data originates from companies, could be used for such attacks in the future.

---

[70] MELANI Semi-annual report 2015/I https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2015.html (as at 31 July 2018).

In general, information from data leaks helps criminals to conduct more targeted attacks. Personalisation seems to significantly increase the success rate compared to mass spam. It is therefore to be expected that many more criminals will choose this approach in the future.

6.2 Networked medical devices, health data and patient dossiers

Digitisation does not stop at the healthcare sector either. The term "eHealth" covers all electronic health services: electronic means are used to improve processes in the healthcare sector and to network those involved. The central element here is the digital health record, the electronic patient database. All of a person's medical data is stored in this. In this way, the quality of medical treatment is to be strengthened, the treatment processes improved, patient safety increased and the efficiency of the health system increased, and the health literacy of patients promoted. The health data can be accessed at any time by you and your health professionals via a secure internet connection. You yourself decide who is allowed to view which documents and when. A record is made each time the electronic patient database is processed. The access log records by name who retrieved documents or stored new documents at what time. This comprehensive log forms a chain of trust that can reliably verify that the information has been transmitted correctly and unchanged over several work steps.

Confidentiality, integrity and availability of the data as well as the traceability of processing must be ensured in the electronic patient database. Health data is not only sensitive personal data because of its private nature, but also because it cannot be changed. Data on our body and its medical history are a given and cannot be changed.

If a health record falls into the wrong hands, the data (e.g. a particular disease, prescribed medication, etc.) are known and inherently valid. This can be used by different actors. In addition to the obvious use for immediate extortion of affected persons, patient data can also be procured in advance in order to use it later, if necessary, since it cannot change. A person could be a more lucrative target at a later stage - either because he or she then takes a leading position in politics or business, or because of other reasons he or she becomes more susceptible to blackmail (or for a larger sum). However, health data is not only of interest to criminals for direct use, but can also be sold to economic and state actors. For example, personalised advertising could be used for impotence treatments or corresponding information could be used for targeted public denunciation.

Since even the best-secured system is not infallible, care should be taken to ensure that health data cannot easily be attributed to a specific person. When pseudonyms are used, care must be taken to ensure that an appropriate balance is found between patient safety against incorrect assignment by authorised health professionals and correct assignment by unauthorised third parties.

The electronic patient database is implemented in Switzerland in a decentralised system. The decentralised approach has advantages for information security, because there is not a single place where all electronic patient database documents of the Swiss population are stored. This avoids a cluster risk. The planned launch date for the electronic patient database is spring 2020. Until then, many tests will be carried out to ensure the security and confidentiality of the system when it is implemented.

6.3 Speed before security? - even in the future, not everything can be entrusted to mobile communications.

6.3.1 The known problems with the SS7 protocol in the case of 2G and 3G

Most users are now aware of the risks associated with the use of public WiFi[71] networks. Mobile networks, on the other hand, enjoy greater confidence in security among most owners of mobile devices. As reported several times in the past[72,73], certain risks must also be taken into account with mobile networks. Especially if they are used as a trustworthy second channel, for example in the form of a text-message code for two-factor authentication. The technical entry point of the attackers against second and third generation mobile networks contains the SS7 protocol, which regulates coordination between mobile providers, for example for roaming. In the meantime, dubious providers[74] on the darknet offer the exploitation of these vulnerabilities as a service for other criminals. Legitimate companies[75] also offer services to security agencies based on these services[76]. By using appropriate firewall technology on the part of the mobile phone providers, such misuse can be prevented in their own networks. As soon as one roams on a foreign network, however, one is exposed to such attacks again, without protection, if the foreign provider has not implemented the protective measures.

Hopes are pinned above all on the modern fourth and in particular fifth generation networks to increase security for mobile phone customers. No devices with 5G technology are available yet, but the discussions about the auctioning of the required frequencies and the results of initial bandwidth tests continue to fuel the discussion about the advantages of the latest mobile phone generation. The 5G standard is expected to become the pioneer of the internet of things

---

71 https://www.melani.admin.ch/melani/en/home/schuetzen/sekundaere-grundschutz.html (as at 31 July 2018).

72 MELANI Semi-annual report 2017/I, section 5.4.5. https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2017-1.html (as at 31 July 2018).

73 MELANI Semi-annual report 2/2016, chapter 6.2 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-201216.html (as at 31 July 2018).

74 https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime (as at 31 July 2018).

75 https://www.forbes.com/sites/thomasbrewster/2017/09/27/ability-inc-ss7-hackers-fail-to-sell-surveillance/#13d65f0d734c (as at 31 July 2018).

76 https://www.techrepublic.com/article/ss7-flaws-used-by-surveillance-firms-highlight-need-for-better-vendor-due-diligence/#ftag=RSS56d97e7 (as at 31 July 2018).

and Industry 4.0 through its high bandwidths and fast response times. The first pilot trials[77] have already demonstrated the successful use of next-generation technology.

6.3.2 LTE makes things better, but is still far from perfect

Currently, Long-Term Evolution (LTE), the fourth generation mobile communications standard, provides devices with the fastest and most frequently used connection option. Instead of SS7, LTE uses the diameter protocol. However, many of the known attacks can still be carried out with a little more effort due to insufficiently secure configuration and backward compatibility with the old standards. Dr. Silke Holtmanns of "Nokia Bell Labs" presented her findings[78] at the "34th Chaos Computer Congress". As in the case of attacks against older standards, there are certainly possible measures[79] to close the vulnerabilities on the part of mobile operators, but not all of them are implementing them with the same consistency.

In the last six months additional attack variants[80] against LTE have become known. Authentication relay attacks allowed security researchers at "Purdue University" and the University of Iowa to intercept text messages or retrieve location data from users at all major US network operators. With the help of equipment that costs less than USD 4,000 to purchase, bogus catastrophe warnings could even be sent to all network participants in a region.

With a little more effort, a research team from the Ruhr University, Bochum and the New York University Abu Dhabi was able to identify three new attack scenarios[81] on LTE networks. The two passive variants make it possible to identify users in the network and to trace which websites they have visited. The active variant uses a weakness of the encryption method used to redirect network participants to bogus websites through manipulated DNS responses. In this case, too, suppliers of network equipment reacted and showed[82] how such attacks can be averted.

6.3.3 Will 5G finally close the vulnerabilities?

In addition to the much-praised advances in data transmission, the fifth generation of the mobile communications standard also promises increased security for network operators and

---

77 https://www.inside-it.ch/articles/50396 (as at 31 July 2018).

78 https://www.heise.de/newsticker/meldung/34C3-Auch-4G-Mobilfunk-ist-einfach-abzuhoeren-und-zu-ueberwachen-3928496.html (as at 31 July 2018).

79 https://researchcenter.paloaltonetworks.com/2018/02/sp-prevent-bad-signals-harming-network-availability/ (as at 31 July 2018).

80 https://www.zdnet.com/article/new-lte-attacks-eavesdrop-on-messages-track-locations-spoof-alerts/ (as at 31 July 2018).

81 https://alter-attack.net/media/breaking_lte_on_layer_two.pdf (as at 31 July 2018).

82 https://blogs.cisco.com/security/protecting-against-the-latest-lte-network-attacks (as at 31 July 2018).

subscribers. Although improvements are planned, unfortunately some shortcomings from the predecessor standards have also been retained. Thus the Evolved Packet Core (EPC) architecture is also included in the new standard. EPC combines voice and data streams in a network. The absence of built-in encryption mechanisms in the included GTPv2 protocol allows mobile data streams to be monitored and enables DoS attacks on network components[83].

Telecommunication satellites are also used as the fallback level in the case of 5G. That which is to be welcomed with regard to the resilience of the network in the event of failures on the ground opens up new attack vectors[84] on mobile communications. If satellites are part of the setup, the associated risks should be taken into account in the security considerations.

Even the latest standard will not be able to eliminate all the security risks of telecommunications. A great deal of responsibility remains with the mobile operators, who have to decide what priority they give to security in the implementation of the standard. Tools such as modelling the threat[85] of one's own network as well as experience from classic ICT network security are available, but their use entails an effort that operators must be willing to make.

6.3.4 Network security alone does not protect

Even with the latest generation of mobile phones, users cannot assume that the standard or the operator will eliminate the risks of information security. In the case of mobile communications, it is also important to implement risk-adequate protective measures in one's own infrastructure and applications.

The past has shown that attackers do not just make their way via the network, they also try their luck via the business processes and the employees involved. Often, multi-factor authentication or password reset processes are linked to the account holder's mobile number. For example, attackers have already successfully transferred the number to their own device or had replacement SIM cards sent to them several times by calling the mobile operator's customer service department[86].

A rather unexpected challenge to network availability for the European mobile operators was the change of the EU rules on roaming tariffs in the member states. The adjustment also

---

83 https://www.darkreading.com/perimeter/new-4g-5g-network-flaw-worrisome-/d/d-id/1330062 (as at 31 July 2018).

84 https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/ (as at 31 July 2018).

85 https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/tackling-5g-security-with-threat-modelling/ (as at 31 July 2018).

86 https://krebsonsecurity.com/2018/02/how-to-fight-mobile-number-port-out-scams/ (as at: 31 July 2018).

enabled users in other European countries to benefit from the same conditions as with the home network. This prompted travellers to stop searching for WiFi and use the mobile network for data transmission while on the move, increasing roaming traffic by six to eight times[87]. This sudden increase pushed some of the providers in holiday destinations to their capacity limits.

7 Politics, research, policy

7.1 Switzerland: parliamentary procedural requests

Item	Number	Title	Submitted by	Date	Council	Office	Deliberation status & link
Po	18.3003	A clear overall cyber strategy for the Confederation	Security Policy Committee	22.01.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201830003
Mo	18.3249	Central body for combatting cyberstalking	Marchand-Balet Géraldine	15.03.2018	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201832449
Ip	18.3335	How does international law regulate cyberspace?	Dobler Marcel	16.03.2018	NC	FDFA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201833335
Ip	18.3511	Utilising Switzerland's strategic advantages in the development of a secure digital hardware market	Vonlanthen Beat	13.06.2018	CS	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201835511
PI	18,434	Finally make cybergrooming of minors a punishable offence	Amherd Viola	14.06.2018	NC	Parliament	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201804034
Ip	18.3556	Minimise cyber risks though awareness-raising among the population and businesses	Glanzmann-Hunkeler Ida	14.06.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201835556
Ip	18.3562	Cyber crime. MELANI reporting duty	CVP Group	14.06.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201835562
Po	18.3565	Damage cover. Cyber attack event limits.	CVP Group	14.06.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201835565
Mo	18.3006	Prevent the collapse of mobile telephone networks and ensure alignment with digitisation	Committee for Transportation and Telecommunications	29.01.2018	CS	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201830006

[87] https://www.lightreading.com/regulation/roam-like-at-home-the-impact-after-one-year/a/d-id/744836 (as at 31 July 2018).

Ip	18.3013	Amazon and other online traders. Does Swiss Post respect the principles of equal treatment?	Feller Olivier	26.02.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183013
Fr	18.5111	WiFi in federal asylum centres?	Keller Peter	28.02.2018	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185111
PI	18,407	Enshrine net neutrality in the constitution	Reynard Mathias	01.03.2018	NC	Parliament	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180407
Ip	18.3057	Destruction of direct democracy by e-voting	Zanetti Claudio	01.03.2018	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183057
Mo	18.3062	Strengthen democratic rights. Online collection of signatures for initiatives and referendums	Grüter Franz	05.03.2018	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183062
Ip	18.3197	Legal representation of service providers in Switzerland	Marchand-Balet Géraldine	14.03.2018	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183197
Ip	18.3222	Market distortion to Switzerland's detriment	Amherd Viola	15.03.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183222
Mo	18.3306	Strengthen law enforcement on the internet with a mandatory address for service for large commercial internet platforms	Glättli Balthasar	15.03.2018	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183306
Mo	18.3349	Ensuring net neutrality	Flach Beat	16.01.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183349
Ip	18.3367	Sciences. One of Switzerland's greatest advantages in international relations	Béglé Claude	16.03.2018	NC	FDFA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183367
Mo	18.3379	Prosecution authorities' access to data abroad	Legal Affairs Committee	23.03.2018	CS	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183379
Fr	18.5258	When will the minimum internet speed be increased to 10 megabits per second?	Candinas Martin	30.05.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185258
GBr	18.049	Federal act on electronic identification services	Federal Council dispatch	01.06.2018		FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180049
Ip	18.3443	Offer courses on using new technologies to older people	Marchand-Balet Géraldine	04.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183443
Ip	18.3448	Fake news and Swiss democracy	Marchand-Balet Géraldine	04.06.2018	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183448
Fr	18.5321	SBB. Free internet access	Derder Fathi	04.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185321

Mo	18.3507	Implementation of the SPTA in accordance with the will of the legislator	Molina Fabian	13.06.2018	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183507
Po	18.3590	Web 3.0 - What role should Switzerland play in a decentralised web?	Béglé Claude	14.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183590
Ip	18.3591	ch.ch website - how is it used and what is its future?	Wehrli Laurent	14.06.2018	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183591
Mo	18.3617	Create a digital identity 3.0. For a leading role for Switzerland in the blockchain area and maximum security for personal data.	Béglé Claude	14.06.2018	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183617
Ip	18.3670	WiFi connections in SBB trains	Ammann Thomas	15.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183670
Mo	18.3701	Voluntary digital motorway tax sticker	Candinas Martin	15.06.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183701
Mo	18.3702	Smart data. Switzerland should play a leading role in sustainable digitisation with high added value.	Béglé Claude	15.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183702
Fr	18.1044	Drones	Leutenegger Oberholzer Susanne	15.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20181044
Po	18.3601	Legislation concerning drones must be adapted	Marchand-Balet Géraldine	14.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183601
Po	18.3478	Federal Council report on measures to be taken in the area of drones	Brélaz Daniel	11.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183478
Ip	18.3397	Regulation for the private use of drones	Jositsch Daniel	28.05.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183397
Fr	18.5399	Drones in Switzerland	Leutenegger Oberholzer Susanne	06.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185399
Mo	18.3371	Safety and order when operating drones	Candinas Martin	16.03.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183371
Po	18.3245	Identifying drones and similar flying objects	Guhl Bernhard	15.03.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183245
Ip	18.3463	From smart cities to smart villages	Egger Thomas	07.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183463
Ip	18.3445	Automated vehicles and liability. When will the legislation in Switzerland be adjusted?	Marchand-Balet Géraldine	04.06.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183445

Fr	18.5220	Is the internet giant Amazon treated in the same way as other Swiss Post clients in terms of parcel delivery prices?	Feller Olivier	28.05.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185220
Fr	18.1021	As the owner of Swisscom, why does the Confederation not attach greater weight to a comprehensive and customer-oriented data protection policy?	Glättli Balthasar	16.03.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20181021
Fr	18.5209	5G network in Switzerland. The Federal Council can make its expansion possible by issuing an ordinance	Derder Fathi	07.03.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185209
Fr	18.5167	5G network without increasing the maximum limits for mobile telephones	Leutenegger Oberholzer Susanne	07.03.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185167
Ip	18.3044	Partnership between Swiss Post and Amazon	Reynard Mathias	28.02.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183044
Ip	18.3575	Child labour free IT devices in the Federal Administration	Masshardt Nadine	14.06.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183575
Ip	18.3374	New FOITT solution for cancer registration software. Is money being wasted because of questionable awarding?	Weibel Thomas	16.03.2018	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183374
Mo	18.3219	Digitisation further education campaign for older employees	Kälin Irène	15.03.2018	NR	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183219
Mo	18.3008	Make digital signatures standard for all Federal Administration internal documents	Dobler Marcel	26.02.2018	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183008
Mo	18.3517	Digitisation impulse programme in schools	CVP Group	13.06.2018	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183517
Mo	18.3664	Digitisation also in healthcare. All bills should be sent electronically to health insurers	Grossen Jürg	15.06.2018	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183664
Mo	18.365o	Increase patient safety with electronic documentation and electronic exchange of medical data	Humbel Ruth	15.06.2018	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183650
Po	18.3502	e-signature for documents internal to the administration	Dobler Marcel	12.06.2018	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183502

7.2 Political cyberspace developments - current status

The Eder (SR FDP-17.3508)[88], Dittli (SR FDP-17.3507)[89] and Grüter (NR SVP-17.3199)[90] motions mean that three extensive items of business were proposed last year. Since then, the Eder motion has been accepted by a large majority by both chambers. Consequently, the Federal Council was instructed to create a cybersecurity competence centre and establish a cyber-force with 100 IT/cyber specialists in the Swiss army. While the first cyber basic military training centre started in August 2018, implementing the mandates in the civil sector requires more time.

With the renewed "National strategy for the protection of Switzerland against cyber risks" (NCS II) for 2018 to 2022[91], the Federal Council wishes to actively tackle cyber risks and take the necessary measures to maintain the country's security in the face of threats from cyberspace. The NCS II was therefore adopted by the Federal Council on 18 April 2018. The implementation and allocation of the NCS II measures is performed in partnership with the cantons, businesses and higher education institutions. The additional mandate to create a cybersecurity competence centre should also be planned and advanced within the scope of NCS implementation.

Before the summer break, the Federal Council made initial policy decisions concerning the creation of a cybersecurity competence centre in order to intensify its efforts to prevent and combat cyber risks. According to the initial policy decisions, the competence centre should be affiliated to the Federal Department of Finance (FDF). The centre should deal with the internal communication within the Confederation in the fight against cyber risks, promote prevention and serve as the central point of contact for concerns from businesses and cantons. At the same time, cooperation with the world of research and science should be promoted. The competence centre is to be run by a high-ranking "Mr/Mrs Cyber", but without the authority to issue instructions which the Eder motion demanded. However, the degree to which all cyber units will be centralised in one centre is not yet known at this point in time.

The decision to provide a high-ranking Mr/Mrs Cyber with a coordinating role but without the authority to issue instructions was largely criticised. In open letters, the business associations[92], and the Defence Committee of the National Council[93] asked the Federal Council to include the power to issue instructions in the role of Mr/Mrs Cyber. Finally, the Security Policy Committee of the National Council is asking for human and financial resources

---

88 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508 (as at 31 July 2018).

89 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507 (as at 31 July 2018).

90 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173199 (as at 31 July 2018).

91 https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie.html (as at 31 July 2018).

92 https://www.satw.ch/cybersecurity/detail/publication/zu-den-grundsatzentscheiden-des-bundesrates-zur-cybersecurity/ (as at 31 July 2018).

93 https://www.parlament.ch/press-releases/Pages/mm-sik-n-2018-08-21.aspx (as at 31 July 2018).

as an immediate measure for the transitional period. These are required to expand the Reporting and Analysis Centre for Information Assurance (MELANI) and improve the cyber resilience of critical infrastructure.

The Federal Council's final decisions on creating a competence centre are not expected before the end of 2018[94].

7.3 GDPR and Data Protection Act

On 25 May 2018, the new European Union General Data Protection Regulation (EU GDPR) entered into force. Since this date, the following main changes have been enforceable: the right to be forgotten; data processing is only permitted with the express content of the person concerned; the right to data portability to another service provider; the right to be informed if one's own data protection is breached, as well as the threat of monetary fines of up to 4% of annual worldwide turnover from the preceding business year in the case of infringement. However, as before, there is still uncertainty concerning the legally compliant implementation of the GDPR in individual cases. Although the expected wave of cease and desist letters was not observed in the EU area, many businesses found the concrete implementation of the regulation a challenge, not least because no common practice exists. This meant quite a number of European websites went offline when the GDPR came into effect and American newspapers were temporarily no longer accessible to European clients. Smaller businesses, associations and self-employed people felt particularly insecure, as did smaller businesses from the digital sector such as online shops and bloggers. Due to financial and organisational reasons, many were unable to meet the requirements of the GDPR. The threat of monetary fines meant they feared for their existence and therefore initially limited or blocked their web presence.

Recommendation:

In principle, the European GDPR does not apply in Switzerland. The situations in which Swiss companies are affected by the direct application of the GDPR can be reviewed here:

For more information about securing Memcached, please see:

https://www.edoeb.admin.ch/edoeb/de/home/aktuell/rgpd-last-minute.html

https://www.kmu.admin.ch/kmu/en/home/concrete-know-how/sme-management/e-commerce/data-protection.html

https://www.economiesuisse.ch/en/node/43727

As before, Switzerland is still governed by the existing Data Protection Act of 1993. Parliament has not yet taken charge of the total revision of the Data Protection Act. Urgent changes are

94 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-71458.html (as at 31 July 2018).

brought forward which are necessary within the framework of the Schengen Agreement. However, Parliament wishes to allow itself more time for the total revision. Inevitably, this leads to a transitional period which is not without problems for Swiss businesses and the Swiss online world. This period must adapt to the new law and requires the relevant legal certainty. However, until the second part with the total revision of the Data Protection Act is completed, the legal framework will be relatively complex.

8 Published MELANI products

8.1 GovCERT.ch Blog

In the first half of 2018, MELANI did not publish any new GovCERT.ch blogs.

8.2 MELANI newsletter

8.2.1 Data leaks, crimeware and attacks on industrial control systems – topics in the MELANI semi-annual report

26.04.18 - The 26th semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI), published on 26 April 2018, addresses the most important cyber incidents of the second half of 2017 both in Switzerland and abroad. Among other things, the focus is on the widespread use of crimeware and attacks on industrial control systems in the medical technology sector. The spate of data leaks and their repercussions are examined in the main topic.

https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/semi-annual-report-2-2017.html

8.2.2 Wieder vermehrt betrügerische Anrufe bei Firmen (not available in english)

05.07.2018 - In den letzten Tagen mehren sich wiederum Anrufe bei potenziellen Opferfirmen, in denen sich Angreifer als Bankmitarbeiter ausgeben. Die Anrufer bitten um die Ausführung von Zahlungen oder geben vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll.

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/truffe-via-e-mail-e-telefono-in-aumento.html

8.3 Checklists and instructions

In the second half of 2017, MELANI did not publish any new checklists or instructions.

9 Glossary

Term	Description
Advanced persistent threats (APTs)	This threat results in very significant damage impacting an individual organisation or a country. Attackers are willing to invest a great deal of time, money and knowledge in the attack and generally have considerable resources at their disposal.
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 program.
Bitcoin	Bitcoin is a decentralised payment system that can be used worldwide, as well as the name of a digital monetary unit.
Bot	Comes from the Slavic word “robota” meaning work. Refers to a program that automatically carries out certain actions upon receiving the command. Malicious bots can control compromised systems remotely and have them carry out arbitrary actions.
Brute force	Brute force is a method for solving problems in the fields of computer science, cryptology, and game theory based on trying out all possible cases.
CEO-Fraud	CEO fraud occurs when perpetrators instruct the accounting or finance department in the name of the CEO to make a payment to the (typically foreign) account of the scammers. Generally, the instruction is sent from a spoofed email address.
Command & control server	Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called a command & control server.
CPU / processor	The CPU (central processing unit) is another term for processor, the central unit in a computer, and contains the logical circuits to run a computer program.
Cryptomining	Mining creates new blocks and then adds them to the block chain. The process requires considerable processing power and is therefore remunerated.

DDoS	Distributed denial of service attack. A DoS, or denial of service, attack where the victim is simultaneously attacked by many different systems.
Defacement	Unauthorised alteration of websites.
Domain name system	With the help of DNS, the internet and its services can be utilised in a user-friendly way, because users can utilise names instead of IP addresses (e.g. www.melani.admin.ch).
Downloader	A downloader is a program that downloads and installs one or more instances of malware.
DriveBy-Infection	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.
E-currency services	A monetary value in the form of a receivable from the issuing authority. The value is saved on a data carrier, issued in return for a sum of money – the value of which is not less than the issued monetary value – and accepted by companies other than the issuing authority as a means of payment.
Elasticsearch	Elasticsearch is a search engine written in Java based on Apache Lucene.
Exploit-Kit	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
Financial agent	A financial agent works as a legal money broker and thus engages in financial transfers. Recently, this term has been used in connection with illegal financial transactions.
Global Positioning System (GPS)	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation satellite system for determining position and measuring time.
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.
JavaScript	Is an object-based scripting language for developing applications. JavaScripts are program 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 computer of the website visitor. Aside from useful features, unfortunately dangerous functions can also be programmed. In contrast to ActiveX, JavaScript is supported by all browsers.
LTE	Long-Term Evolution (abbreviation LTE, also 3.9G) is a term for the third-generation mobile communication standard. An extension is called LTE-Advanced or 4G and is downward compatible.
Malware	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Metadata	"Metadata" and "meta-information" refer to data containing information about other data.
MITM	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.
mobileTAN	mobileTAN is a way to incorporate text messages (SMSs) as a transmission channel. After online banking clients transmit their completed funds transfer requests on the internet, the bank sends them a text message on their mobile phone with a TAN that can be used only for that transaction.
MS HTA	HTML application (abbreviation HTA) is a Microsoft term for computer programs that use Internet Explorer to run.
NAS devices	Network-attached storage (NAS) refers to file servers that are easy to manage. In general, a NAS is used to

	provide independent storage capacity in a computer network without much cost.
P2P	Peer to Peer Network architecture in which those systems involved can carry out similar functions (in contrast to client-server architecture). P2P is often used for exchanging data.
Patch	Software that replaces the faulty part of a program with an error-free part, thereby eliminating a vulnerability, for example.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting internet users. For example, this can be account information from online auctioneers (e.g. eBay) or access data for online banking. The fraudsters take advantage of their victims' good faith and helpfulness by sending them emails with false sender addresses.
PKI	Public Key Infrastructure Infrastructure for the management and use of digital certificates.
Port	A port is part of an address that assigns data segments to a network protocol. This concept is included, for example, in TCP, UDP and SCTP to address protocols on the higher layers of the OSI model.
PowerShell script	PowerShell is a cross-platform framework by Microsoft for automating, configuring, and administering systems, consisting of a command line interpreter and a scripting language.
Proxy	A proxy is a communication interface in a network. It works as a mediator, receiving queries on the one side and making a connection on the other side via its own address.
RC4 encryption	RC4 (Ron's Code 4) was developed in 1987 by Ronald L. Rivest, is a trademark of RSA Security and is officially classified (Security by Obscurity).
Remote Administration Tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
Router	Computer network, telecommunication, or also internet devices used to link or separate several networks.

	Routers are used in home networks, for instance, establishing the connection between the internal network and the internet.
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a standard advanced mobile phone.
SMB protocol	Server message block (SMB) is a network protocol for file, printing and other server services in computer networks.
SMS	Short Message Service for sending text messages (160 characters maximum) to mobile phone users.
Social Engineering	Social engineering attacks take advantage of people's helpfulness, credulity or lack of self confidence in order to gain access to confidential data or to prompt them to perform certain actions, for example.
Spam	Spam refers to unsolicited and automatically sent mass advertis-ing, into which category spam e-mails also fall. The person re-sponsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
Spearphishing emails	Targeted phishing attack. For example, victims are tricked into believing that they are communicating with someone they know by email.
SS7	Signalling System No. 7 (SS7) is a collection of protocols and procedures for signalling in telecommunication networks. It is often used in the public telephone network, in connection with ISDN, landline and mobile communication networks, and since about 2000 also more frequently in VoIP networks.
SSH	Secure Shell A protocol for encrypted communication. It may be used to securely login to a computer system via a network (e.g. the Internet).
Supply chain attacks	Attack in which an attempt is made to infect the actual target via the infection of a company in the supply chain.

Take-down	Expression used when a provider takes down a site from the network due to its fraudulent content.
Top-Level-Domains	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.
Transmission Control Protocol / Internet Protocol (TCP/IP)	Transmission Control Protocol / Internet Protocol (TCP/IP) is a family of network protocols, also referred to as the Internet protocol family because of its great importance for the Internet.
Two-factor authentication	For this, at least two of the following three authentication factors are required: 1. Something you know (e.g. password, PIN, etc.) 2. Something you have (e.g. a certificate, token, list of codes, etc.) 3. Something you are (e.g. finger print, retina scan, voice recognition, etc.)
UDP	The User Datagram Protocol, short UDP, is a minimal, connectionless network protocol that belongs to the transport layer of the internet protocol family.
USB	Universal Serial Bus (with a corresponding interface) which enables peripheral devices such as a keyboard, mouse, external data carrier, printer, etc. to be connected. The computer does not have to be switched off when a USB device is unplugged or plugged in. For the most part, new devices are automatically identified and configured (depending on the operating system).
Vulnerability	A loophole or bug in hardware or software through which attackers can access a system.
Watering-hole attacks	Targeted infection by malware via websites that tend to be visited only by a specific user group.
WLAN	WLAN stands for Wireless Local Area Network.
Worm	Unlike viruses, worms do not require a host program in order to propagate. Instead, they use vulnerabilities or configuration errors in operating systems or

	applications to spread by themselves from one computer to another.
Zero-Day	An exploit which appears on the same day as the security holes are made public.
ZIP-File	zip is an algorithm and file format for data compression, in order to reduce the storage space needed for the archiving and transfer of files.