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 2017/II (July – December)

26 APRIL 2018

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

1 Overview / Content

2 Editorial

Werner Meier
Delegate for National Economic Supply

Dear reader,

Digitalisation offers immense opportunities for our country – but also presents it with great challenges. The control and optimisation of processes in the economy through information and communication technology (ICT) can succeed in the long term only if ICT is available at all times, reliable, and resistant to disruptions and attacks. In short: digitalisation without ICT security is unthinkable.

Digitalisation is an important concern for the Federal Council. This is apparent in the Federal Council's Digital Switzerland strategy, in which it also established security as one of four core objectives. The advisory council set up by the EAER and DETEC in summer 2017 to implement the strategy also put cybersecurity at the top of its agenda.

The legal mandate of Switzerland's National Economic Supply (NES) is to secure the country's supplies of vital goods and services in the event of a crisis. ICT is vital for NES not only per se, but also as a resource for the functioning of our country's supply of electric power and logistics services, for instance. In order to achieve its objectives, NES has a modern legal basis in the revised National Economic Supply Act and, with its management organisation drawn from the business sector, the necessary expertise.

Over the past few months, NES has developed a General Minimum ICT Standard, which helps to increase the resilience with regard to the National Cyber Strategy (NCS). Based on the NIST Framework Core, 106 measures are described how operators of critical supply infrastructures can protect their ICT resources. The General Minimum ICT Standard will soon be presented to the public and will be freely available. It already serves as a basis for the Association of Swiss Electricity Companies (VSE) to create an equivalent standard for the electricity industry. This industry standard, in which NES played a major role, will become a self-regulation framework for this economic sector. Minimum ICT standards for wastewater as well as water, gas, and mineral oil supplies are also under development.

In this way, NES not only contributes to the digitalisation of Switzerland, but also promotes the ICT resilience of critical supply infrastructures to ICT outages, disruptions, and attacks. This semi-annual report of the Reporting and Analysis Centre for Information Assurance MELANI impressively demonstrates how necessary this is. I hope you enjoy reading it.

Werner Meier
Delegate for National Economic Supply

3 Key topic: data leaks

In the digital world, millions of records of personal data are generated and stored every day – whether at the supermarket checkout when showing your points card, paying with a debit or credit card, shopping online, checking emails, or visiting the doctor. The list could be continued indefinitely. Even when browsing the internet, everyone leaves dozens of tracks every day.

If these data records fall into the wrong hands, this can lead to misuse. Unfortunately, unwanted data leaks are becoming increasingly frequent, also in the second half of last year: in October 2017, the internet company Yahoo! announced that the 2013 data leak, with over three billion data records, apparently affected all users and not just some of them as had been assumed.[1] To date, this is the biggest data leak in history. The "have I been pwned" portal also cites an impressive number.[2] On this site, anyone can check whether their email address has ever been affected by a data leak. The stolen passwords recorded on the site have meanwhile reached the almost unbelievable number of nearly five billion.

Data leaks have also been registered in Switzerland in recent months. Swisscom announced that an unauthorized third party had access to more than 800,000 customer data records in October 2017. Galaxus/Digitec suspected in November 2017 that scammers had obtained customer data, and the health insurer Groupe Mutuel also informed the public about a data leak in December 2017. Likewise in December, MELANI was alerted to 70,000 leaked access data records that could subsequently be attributed to DVD-Shop, a Swiss company.

Meanwhile, leaked datasets with passwords, credit card data, or other personal data regularly surface on the relevant portals. In many cases, however, it is difficult to verify the origin, age, and quality of the data. In the case of a large number of stolen datasets, it can be assumed that the leak was not even noticed.

3.1 Definition

Data leaks are security incidents in which unauthorised third parties gain access to personal data, company secrets or other data which is not intended for them. The definition of the term "data leak" is very broad and besides data theft and espionage also includes data breaches, in which data will be made available unintentionally. The spectrum of concerned data includes not only passwords and credit card data, but also data from the health and financial sectors for example.

3.2 Extortion, data collection, and political motives

A common way for criminals to make money with data leaks is certainly blackmailing the company where the data has been breached. One of the first such cases in Switzerland dates back to 2014. A group called Rex Mundi blackmailed a company in French-speaking Switzerland

[1] http://www.sueddeutsche.de/digital/yahoo-hackerangriff-bei-yahoo-traf-alle-drei-milliarden-konten-1.3693671 (as at 31 January 2018).

[2] https://haveibeenpwned.com/ (as at 31 January 2018).

with the publication of data. In addition to the company, however, the affected customers can also be the target of such extortion.

Another use of data from data leaks is for targeted attacks. On the underground market, actors have specialised in gathering as much information as possible about a victim. In addition to freely available sources, they also use information originating in data leaks. If the attackers succeed in obtaining a precise picture of the victim with the help of a wide range of data, very targeted attacks are also possible. In the period under review, for instance, the spread of emails with malware was observed in which not only the recipient's first and last name were used, but also the recipient's phone number and/or postal address.

Data leaks with a political motivation must be considered separately. The best known case is the publication of the Snowden Files. In addition to Snowden, many other actors have since tried to shake up or change society with the same method. Examples include publication of the Panama Papers and the Paradise-Papers. With these publications, the actors revealed the worldwide financial and business practices of various politicians and celebrities.

3.3 Impact

But what impact do data leaks have on those affected, and what damage do they cause? This question can be answered in different ways, because everyone defines the value of their data differently. Some individuals do not care whether and what data is collected and what is done with it, while others try to keep the amount of data about themselves as small as possible. Accordingly, the latter consider the personal damage to be much higher.

The type of data involved in the breach also plays a role and can be divided systematically into two groups: data that can be easily reset, and data that lasts a lifetime. Passwords and credit card information can be changed quickly and only cause short-term damage to the person concerned. Data on one's own health, personal preferences, or financial situation cannot simply be "reset" and thus causes long-term damage if breached. This means that attackers can still cause problems for victims many years after a data leak. A further complication is that in some cases, victims know nothing about these data leaks and therefore cannot protect themselves or defend against them.

For companies, unwanted data leaks lead to a loss of reputation in addition to the hassle and the costs. Communication with customers is of crucial importance. It is therefore extremely important for a company to prepare well for a possible data leak. This includes emergency planning, prepared communication, and clearly defined responsibilities. In the case of data leaks, MELANI in general recommends the highest possible level of transparency vis-à-vis the customers concerned. It is important to inform them as soon as possible in order to minimise consequential damage. The art lies in communicating soberly and without panic.

3.4 Notification of the persons concerned

If data has been stolen from a company, the question quickly arises of how to notify customers. The company concerned is in the best position to carry out this communication. Only the company has an overview of the affected customers as well as the type and amount of data stolen, and only the company can implement suitable measures such as resetting passwords. It must be ensured in such cases that unauthorised parties cannot obtain information about the affected persons. For example, in responding to requests about whether a person was affected by a data breach, the health insurer Groupe Mutuel asked for a copy of the person's identity card.

An even greater challenge is informing those affected by a data leak if the origin of the data is not known. On portals such as Pastebin, combinations of usernames and passwords frequently appear without any clear indication of the origin of the data. On several occasions in the past, MELANI has received such lists with leaked data records. In these cases, MELANI has made a checktool available so that internet users can find out for themselves whether they are affected or not. In many cases, the origin of the data can also be determined retrospectively on the basis of feedback from the public. In MELANI's opinion, it is the company's responsibility to inform customers and the public about the data leak once the origin has been determined.

3.5 Data protection

The protection of personal data is governed by the Federal Act on Data Protection (FADP). The aim of the act is to protect the privacy and the fundamental rights of natural and legal persons when their data is processed. A distinction is made between personal data and sensitive personal data. The latter category includes data on religious, ideological, political, or trade union-related views or activities; health, the intimate sphere, or the racial origin; social security measures; and administrative or criminal prosecutions and sanctions. When processing such data, the express consent of the person concerned must be given. The Data Protection Act also takes sufficient account of the security aspect and defines that personal data must be protected against unauthorised processing through adequate technical and organisational measures.

The total revision of the Swiss Data Protection Act is currently underway. It can be assumed that the revision will embrace various new elements of the EU General Data Protection Regulation, which must be applied by all EU member states effective 25 May 2018 after a two-year transition period. The EU General Data Protection Regulation also applies to all Swiss companies, with or without headquarters in the EU, which offer products and services to persons in the EU (which is most likely the case if their website or webshop does this), process personal data of EU citizens, or analyse the behaviour of persons in the EU. The main changes arising from the new rules can be summarised as: the right to be forgotten; data processing is only permitted with the express consent 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 and, finally, a tougher crackdown on regulation infringements. The latter means that for businesses, monetary fines can be imposed of up to 4% of their annual worldwide turnover from the preceding business year.

The latter requirement in particular will probably fundamentally change the handling of data breaches and increasingly shift the focus to the security aspect of databases and data processing. However, this requirement will probably motivate cybercriminals even more to profit from data leaks. An extortion amount that is less than the amount of the fine might tempt a company to take advantage of the cheaper offer.

3.6 Causes and protection

The causes of data leaks are manifold, ranging from data theft by employees to forgotten and poorly maintained servers as well as backups that are not properly protected.[3]

3.6.1 No orphaned data

Once data has been gathered, people tend to store it somewhere, even if it has long been of no use or is no longer valid. Every address book on a mobile phone, for example, may contain contacts that are no longer valid. Such "forgotten" data unnecessarily increases the size of a data leak. Especially when migrating a server, it should be ensured that the data is subsequently deleted from the old systems. A lifetime should also be assigned to each dataset so that it is periodically checked for validity. Also, only the data that is really necessary should be queried and stored. This is a requirement of the Data Protection Act (Art. 4 para. 2 FADP on proportionality), but it also greatly reduces the impact of a data leak if only a small amount of data has been stored.

3.6.2 Protect access / reduce traffic

External access should be kept to a minimum and must be specially protected and monitored. Every company must consider who needs access to which data and how this access is protected. For example unused ports should always be closed. The use of a second factor for authentication is strongly recommended for external access. One Time Password (OTP) methods, such as the widely used Google Authenticator, which is installed as an app on the smartphone, have proven their value for widespread use.

Outgoing traffic should be reduced to the necessary connections too. Many attacks rely on automatically downloading further code from the internet after the infection. The ban of outgoing traffic considerably increases the hurdles for an attacker.

Regardless of the criticality of user data entered in a contact form or business application, it should be passed on, as fast as possible, to a backend system which is not directly accessible from the internet.

All server software and applications must always be kept up to date. If there is no patch for a vulnerability or if it cannot be implemented, appropriate risk-reducing measures must be taken. The use of a web application firewall is recommended: Many commercial and open source products are available that can provide additional protection for a web application. Many of these products offer rules to protect against the most common vulnerabilities (OWASP Top 10)

3.6.3 Poorly protected backups

Backups are part of every company's life insurance, but they must meet the same security requirements as productive data. Archived data on external hard drives should therefore be encrypted too.

[3] The most common issues are documented in a top 10 list of the OWASP project (Open Web Application Security Project). The list is updated regularly. https://www.owasp.org/

3.6.4 Unprotected passwords

If passwords are included in the leaked data, they should not be easy to decrypt. This necessitates the use of a hash function[4] and a "salt". With salting, the password is supplemented with another value known only to the system and only then is it passed to the hash function. Salts that are as long as possible should be used, and they should be generated anew every time a password is created. It is also important to use a slow hash function. The calculation of the password hash should be as complicated and slow as possible. Normal users are unlikely to mind if the login procedure takes a few milliseconds longer. But for the hacker who has to perform the calculation millions of times, the computing time is drastically extended.

3.6.5 Insider theft

Data is sometimes also stolen by active or former employees who want to harm the company out of discontent or to have a personal advantage. This can be counteracted by creating a good and open working atmosphere and by talking openly about problems. But it is also important to ensure that employees have access only to the data they need to carry out their work. Former employees must have all access withdrawn immediately, which requires a clean access policy.

4 Situation in Switzerland

4.1 Espionage

4.1.1 Another attack on internal federal systems

In July 2017, the Turla spyware was discovered on several servers of the Federal Department of Defence, Civil Protection and Sport (DDPS). This malware is not unknown to the Federal Administration. It was also the Turla spyware that in December 2015 attacked the technology group RUAG, which is an enterprise associated with the federal government whose responsibilities include securing the equipment of the army. At that time, the attackers managed to steal more than 20 gigabytes of data. In the current case, the malware was detected already at an early stage before it could steal important data or infect other connected systems in the network. This is despite the fact that the attackers have expanded their infrastructure and tools, and have increased the complexity of the attack. The responsible federal agencies were able to carry out the necessary checks in time and take appropriate measures. The cooperation of the individual federal agencies was very good and made it possible to gather information on the attack methods and technical indicators. The exchange of such indicators, both nationally and internationally, is a crucial element for detecting current or future attacks. The Federal Council, the members of the Security Committee of the Federal Council, and the chairs of the responsible committees were informed promptly, as is customary for such incidents. The DDPS also filed criminal charges with the Office of the Attorney General of Switzerland against persons unknown for cyber-attacks on its servers.[5]

[4] A hash function efficiently maps a string of any length (here, a password) to a string of a fixed length (hash value).

[5] https://www.vbs.admin.ch/de/aktuell/medienmitteilungen.detail.nsb.html/68135.html (as at 31 January 2018).

4.2 Industrial control systems

The media regularly report on endangered industrial control systems (ICS) accessible from the internet, such as factory controls, pumps for hydroelectric power plants[6] or medical equipment[7]. These systems are at risk because, for example, a vulnerability has appeared in one of the components used or because the components have not been configured securely enough.

Once such cases have become known, it is often criticised that the operators of the affected infrastructures do not install updates in a timely manner. However, there are certainly reasons that delay or make it impossible to install security patches. For example, updating a component may endanger the certification of the entire system. It would therefore be much more important that the system landscape and the network in which these devices are located are built and operated sufficiently robustly so that vulnerabilities can occur without endangering the core functions.[8] It is also evident in the MELANI checklist on "Measures for the protection of industrial control systems (ICS)" that patch management is only one of eleven measures. The checklist includes ten other risk-reducing measures: for example, a robust network architecture guarantees that the network zone in which the vulnerable device is integrated should in the best case include only those systems that need to communicate with the vulnerable device. Zone transitions should be reduced to what is absolutely necessary and well monitored. Employees should at any time only have the rights that are absolutely necessary to perform the envisaged tasks. The central log evaluation also makes it possible to inspect whether all systems are running as specified. If an attack is registered despite all the precautions, the security incident management process is helpful. Once the response to a security incident has been defined and rehearsed by everyone involved, the potential damage can be kept to a minimum.

In the technical literature, the compensation of an unavoidable risk by one or more additional defensive strategies is described as "defence-in-depth".[9] A basic example of an ICS network architecture can be found in Figure 1.

[6] http://www.spiegel.de/netzwelt/web/so-bedrohen-hacker-wasserversorgung-stromnetz-und-kliniken-a-1181325.html (as at 31 January 2018).

[7] https://nakedsecurity.sophos.com/2018/02/01/hospital-mri-and-ct-scanners-at-risk-of-cyberattack/ (as at 31 January 2018).

[8] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (as at 31 January 2018).

[9] https://ics-cert.us-cert.gov/Abstract-Defense-Depth-RP (as at 31 January 2018).

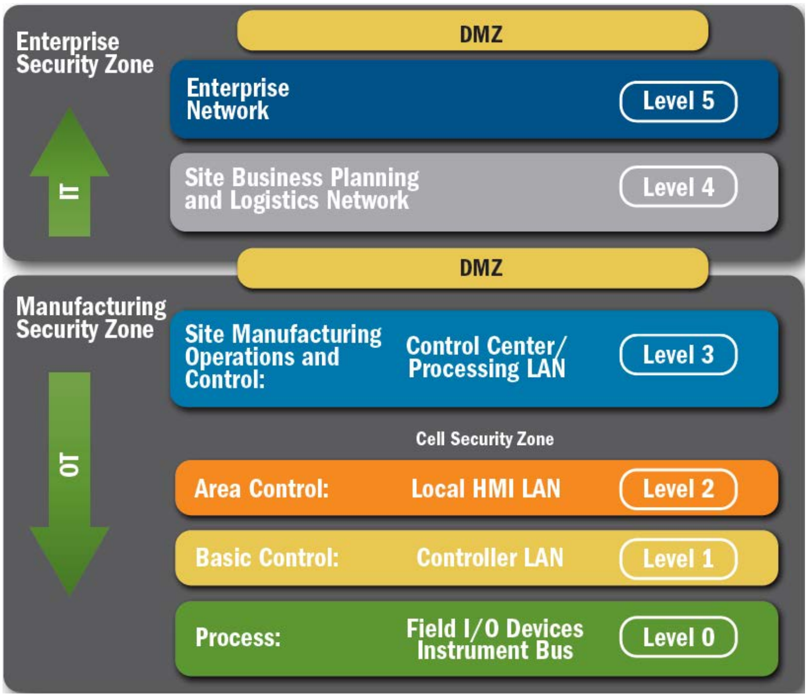

Enterprise Security Zone
DMZ
Enterprise Network
Level 5
IT
Site Business Planning and Logistics Network
Level 4
DMZ
Manufacturing Security Zone
Site Manufacturing Operations and Control:
Control Center/ Processing LAN
Level 3
OT
Cell Security Zone
Area Control:
Local HMI LAN
Level 2
Basic Control:
Controller LAN
Level 1
Process:
Field I/O Devices Instrument Bus
Level 0

Figure 1: ICS network zone architecture of the ICS-CERT[9]

Although these recommendations are all self-evident and appear easy to implement when looked at in isolation, the required resources for their implementation in complex system landscapes are considerable and often not available. In many cases, the timely completion of a project or the operational simplicity of the processes is also given priority over security. In order to deploy the scarce resources where they have the greatest impact, an overarching risk management system is indispensable in which residual risks are identified and addressed by management.

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.

REPORT

MELANI reporting form

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

DOCU

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

4.2.1 Hackers who set the pace

A pacemaker is a battery-powered microcomputer with the necessary sensors, evaluation electronics, and actuator elements in the form of a pulse generator. This allows the pacemaker to monitor heartbeats and stimulate them electrically if necessary. Many of these small lifesavers also have a wireless interface so that no further surgical procedures are required to analyse heart values and adjust the configuration.

On 29 August 2017, ICS-CERT at the US Department of Homeland Security (DHS), which focuses on control systems, published information on vulnerabilities in several pacemaker models manufactured by Abbott Laboratories.[10] The vulnerabilities discovered by MedSec Holdings Ltd allow the manipulation of data exchanged with the implant via the wireless interface. The attacker's transmitter would probably have to be placed directly on the body, as during a routine check at the doctor's, but could then carry out all reading or writing processes. The reason for this is that the authentication of the programming device deviates from the established standard. According to a publication[11] by the US Food and Drug Administration (FDA), which also regulates medical devices, such an attack exploiting vulnerabilities has not yet taken place.

The manufacturer has meanwhile released updates[12] for the affected devices. These updates can be downloaded during a visit to the attending physician. In Switzerland, approximately 5,000 patients[13] had to undergo the procedure, amounting to almost one seventh of the cardiac pacemakers used in Switzerland.

4.3 Attacks (DDoS, defacements, drive-bys)

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

4.3.1 DDoS extortion with a famous name

Extortion is currently a popular scam of cybercriminals who are looking for a quick financial gain. In addition to ransomware and the threat to publish previously stolen data, the threat to launch a DDoS attack is also part of the attackers' repertoire – even though many attackers do not actually have the capacity to launch a DDoS attack. They use this only as a threatening gesture to frighten victims.

Attackers also often take names of groups that are already known from previous attacks. They simply send an extortion email without bothering to actually launch an attack. They hope that the victim enters the name of the group in a search engine and then, scared by the purported group's actions in the past, pays the ransom.

[10] https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01 (as at 31 January 2018).

[11] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (as at 31 January 2018).

[12] https://www.sjm.com/~/media/galaxy/patients/heart-vascular/arrhythmias/resources-support/cybersecurity/pacemaker-firmware-update-patient-guide-aug2017-us.pdf (as at 31 January 2018).

[13] https://www.blick.ch/news/wirtschaft/sicherheitluecke-bei-herzschrittmachern-5000-schweizer-in-gefahr-id7255939.html (as at 31 January 2018).

The DDoS blackmail group "Fancy Bear", which surfaced in the summer of 2017 and was also active in Switzerland in November, also used this method. Surprisingly, this name is not used by a group involved in DDoS, but rather belongs to probably the most famous espionage group worldwide. "Fancy Bear" or the better known alias "Sofacy" is suspected of being a state actor which also includes zero-day exploits in its repertoire. Since Sofacy has not yet appeared in connection with DDoS extortion, it seems likely that this is a group that used the name "Fancy Bear" in order to benefit from the notoriety of the other group, and thereby expected a higher return.

4.4 Social engineering and phishing

The basis for a good attack is a credible story that causes the potential victim to do something. Social engineering attacks work best when the attacker is able to compile a lot of information about a potential victim. To do this, scammers use both freely available sources and information originating from data theft. Stolen data is analysed, coupled with other stolen or public data, prepared and sold on to other criminals.

4.4.1 Phishing

Numerous phishing emails were also sent in the second half of 2017. The content of the emails does not change significantly: some request credit card data for "verification" purposes, while others direct 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 in order to make the emails look official.

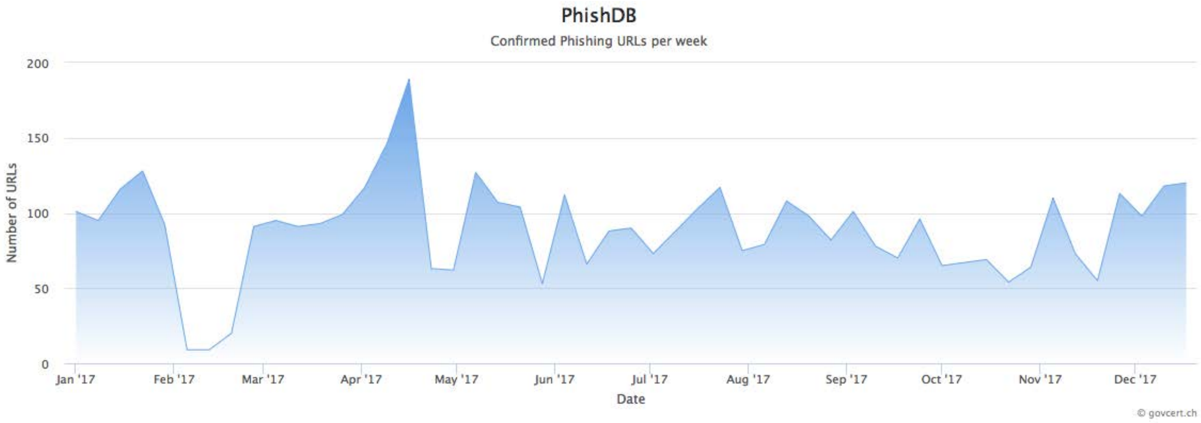


Figure 2: Reported and confirmed phishing sites per week on antiphishing.ch in 2017

Overall, 4,587 different definite phishing sites were reported in 2017 using the antiphishing.ch portal operated by MELANI. Figure 2 presents the number of reported phishing websites per week. The number fluctuates over 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 Bill swap fraud – Exchange of electronic invoices in email accounts

In addition to attacks on credit card data, criminals are mainly targeting access data for email accounts. Since every online service offers a password reset feature, one's email address has meanwhile become the focal point for virtually all internet services. However, an email account offers much more for criminals. Nowadays, criminals take the time to sift painstakingly through the emails of a compromised account looking for usable material. One method that was reported to MELANI several times in the second half of 2017, is to search the email account for electronic invoices. If the scammer finds such a current invoice, it is copied from the email inbox and then deleted. The attacker now has enough time to manipulate the PDF invoice attached to the email. For this purpose, the biller's bank account data is changed and the scammer's IBAN number is used. The modified document is then sent back to the email account. The scammer only has to forge the sender address and again use the email address of the invoicing company. The manipulation is then hardly detectable.

Recommendation:

Information about the recipient account is displayed for each transfer. In the best case, the name or at least the bank of the recipient appears. This information should always be checked for plausibility. Fortunately, criminals do not have so many financial agents at their disposal that they can always display a suitable account. Sometimes it may happen that the money should to be transferred abroad, even though the invoice was issued by a Swiss company. At the latest at this point, victims should become suspicious.

4.4.3 Office 365 phishing – the key to the office

Since June 2017, Office 365 phishing emails have been making the rounds. With over 100 million monthly users, it is not surprising that Office 365 accounts have become a popular target for attackers.[14] The attack starts with an ordinary phishing email claiming, for instance, that the memory limit has been exceeded and the user has to log in to Office 365 in order to remedy the problem. It goes without saying that the link provided leads to a fraudulent website. Once attackers are in possession of the Office 365 access data, they can cause various kinds of harm. The most common scenario is defining a forwarding rule in the affected email account. All incoming internal and external email traffic is then forwarded to an email account defined by the scammers and can be read by the them. Valuable targets of this approach are company email accounts. Information gained in this way can in turn be used to attack other employees. Since the attacker also has access to the user's address book, the attacker can write to individual employees within the company in a very targeted manner. Attackers send previously intercepted emails and manipulate them in such a way that, for example, employees are asked to download a document. To start the download, the Office 365 password (on a manipulated website) must be re-entered. Fraudsters work their way through the attacked company step by step to reach the people of interest to them.

Arriving at the desired target person, a very targeted CEO fraud is then carried out with the previously stolen data. It is also conceivable that the company will be blackmailed with the

[14] https://betanews.com/2017/08/30/office-365-phishing/ (as at 31 January 2018).

stolen email communication or that the stolen data will be resold to other fraudsters. The method could also be used for economic espionage.

Recommendation:

If the company operates in the Office 365 cloud, attackers also have access to all the company's documents using the stolen access data. Securing such data only with a username and password is extremely negligent nowadays. Instead, activate two-factor authentication wherever possible.

Employees should be made aware that defined company processes and preventive measures must be followed by everyone at all times. For money transfers, for example, the dual control principle with joint signature is recommended.

4.5 Vulnerabilities

4.5.1 Check customer orders also at the electronic payment counter

The payment management system Smartvista of the Swiss BPC Group had a vulnerability in 2017 that could be exploited for an SQL injection.[15] With specially formulated and precisely timed SQL queries on the transaction interface of the Smart Vista Front End (SVFE), an attacker would be able to access a list of all users and their passwords from the underlying database. According to a BPC announcement, the company was made aware of the vulnerability in May 2017 by researcher Aaron Herndon of the Rapid7 security company. On 19 July of the same year, the company delivered a patch to fix the problem.

4.6 Data leak

As explained in the key topic, numerous data leaks continued to occur in Switzerland in the second half of 2017. In this section we will summarise known Swiss incidents.

4.6.1 70,000 leaked records of access data for DVD-Shop

At the beginning of December 2017, MELANI was made aware of a list of access data consisting of usernames and passwords. Pursuant to a review, it was determined that there were 70,000 data records related to Switzerland. At the time, however, it was not yet clear exactly where the data had been breached. MELANI decided to integrate the data into the MELANI checktool[16] so that any person could check whether their username was affected. Based on feedback from the public, MELANI was then able to identify the webshop concerned: dvd-shop.ch, which was immediately informed by MELANI. The operator of the shop then reset all passwords and deactivated the webshop. According to the website operator, it was older data that had been stolen. Affected customers were informed directly by the website operator.

[15] https://blog.rapid7.com/2017/10/11/r7-2017-08-bpc-smartvista-sql-injection-vulnerability/ (as at 31 January 2018).

[16] https://www.checktool.ch To perform the check, you only need to enter your email address or username. This information is transmitted to MELANI not in plain text and is not stored (as at 31 January 2018).

Recommendation:

MELANI reminds that passwords must be long enough to make them difficult to guess. A separate password should be chosen for each shop/service. Where offered, a second factor should be activated for the login.

4.6.2 Data leak at Swiss health insurer

The health insurance company Groupe Mutuel announced in a press release that hackers had broken into the external IT platform ePremium Health launched in 2012 to steal data under a false identity on 19 December 2017. This platform is intended for the sales network of Groupe Mutuel in order to prepare offers and insurance applications. According to the health insurer, no insurance policies, medical reports, premium invoices, cost sharing invoices, or the like were stolen. Group Mutuel stated that its internal IT system, on which the data of around 1.4 million customers is stored, was at no time in danger. After the hacker attack, Groupe Mutuel filed charges against persons unknown. The Valais cantonal police then quickly succeeded in identifying the alleged perpetrators. The first offender was arrested already on 28 December 2017. One day later, the Thurgau cantonal police caught a second suspect. The perpetrators are a 29-year-old Swiss and a 30-year-old Macedonian. Both were taken into pre-trial detention. According to the police, the investigation is pending.[17]

In February 2018, Groupe Mutuel published a form for potential victims to find out whether they were affected by the data leak. Particularly at risk are persons/companies that requested an offer from an intermediary or broker for a Groupe Mutuel insurance policy in the period from 2012 to today.[18]

4.6.3 Medical data at debt collection agency – data leak at EOS

At the end of December 2017, the "Süddeutsche Zeitung"[19] reported on a data leak at the Swiss branch of the debt collection company EOS. The EOS Group operates in a total of 26 countries and comprises 55 individual companies. The incident that has now been disclosed probably resulted in the loss of around three gigabytes of data. In addition to information such as names, addresses, and amounts owed, this also includes other sensitive data such as medical records with information on pre-existing conditions and details of treatment. Identity cards and extensive credit card statements are also part of the data leak. The data records go back to 2002.

Apparently doctors uploaded or were able to upload entire medical records on an EOS portal. For what purpose and under what conditions this was done is not known. Sensitive data such as medical data is certainly not necessary for a debt collection agency to perform its functions.

[17] https://www.polizeiwallis.ch/medienmitteilungen/martinach-hackerangriff-auf-eine-versicherungsgesellschaft/ (as at 31 January 2018).

[18] https://www.groupemutuel.ch/en/clients-prives/page/cyberattaque.html (as at 31 January 2018).

[19] http://www.sueddeutsche.de/digital/it-sicherheit-schwerwiegendes-datenleck-legt-zehntausende-schuldnerdaten-offen-1.3805589 (as at 31 January 2018).

The data leak is said to have been triggered in April 2017 by a targeted attack exploiting the Apache Struts vulnerability. According to EOS, signs of an attack were discovered at the time, but it could never be verified. Nevertheless, the affected server had been completely reconfigured at that time. Whether the data is actually related to this incident or whether there was another vulnerability is not known.

4.6.4 Data leak at Digitec too

On 6 November 2017, Digitec announced on its website that data from an old database might have been lost. According to the current state of knowledge, customer data could be affected from 2001 until no later than mid-2014. The presumed vulnerability has been closed in the meantime and the new Digitec shop has not been affected[20]. When exactly the leak took place is not known.

4.7 Crimeware

Crimeware is a form of malware which, in criminological terms, ranks as computer crime and legally comes under causing damage to data and fraudulent misuse of a data processing system. Numerous crimeware infections were again recorded in the second half of 2017. The statistic in figure 3 presents data of single servers to which infected computers connect. There is also malware of high importance which doesn't appear in this statistic (for example the e-banking Trojan Retefe). 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 which was both discovered and eliminated in 2008. "gamarue",[21] also known as "andromeda", is now in second place, a downloader that can download more malware. In third and fourth place are the malware "spambot" and "cutwail", which specialise in sending spam and malware. The *bot* network "Mirai", which became known after the attack on the internet service provider "Dyn" and infects devices in the internet of things, fell from fourth to seventh place. The first e-banking Trojan "Gozi" follows in ninth place.

[20] https://www.digitec.ch/de/page/statement-zum-digitec-leck-6265 (as at 31 January 2018).

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

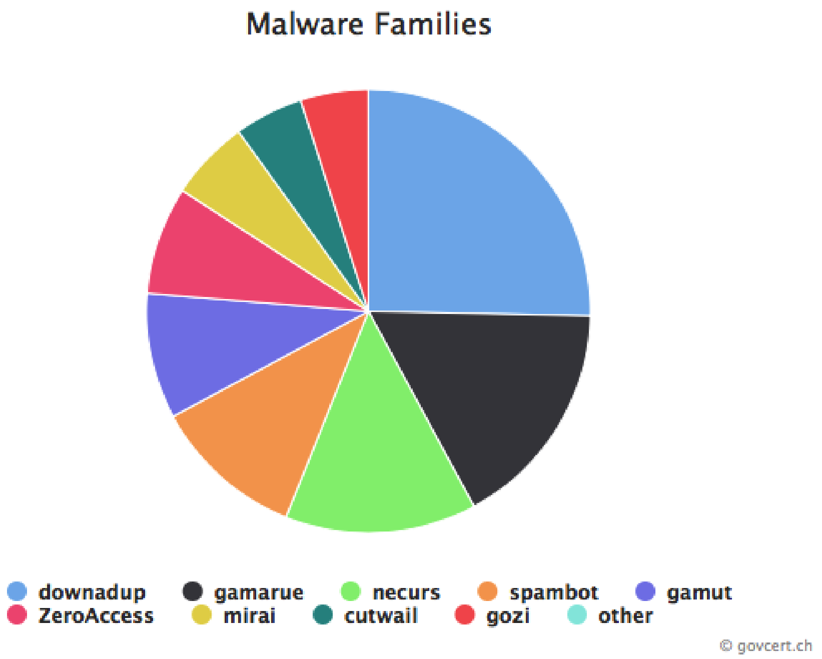


Figure 3: Breakdown of malware in Switzerland known to MELANI. The reference date is 31 December 2017; current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/

4.7.1 Ransomware

During the period under review, MELANI was again informed of numerous cases of encryption Trojans. A functioning backup on an external medium that cannot be affected by the encryption malware is essential. But it is even better not to let things get this far and to take appropriate precautions. Encryption and thus the temporary loss of data is only part of the problem. It should also be taken into account that during restoration of the backup, a substantial part of operations comes to a standstill. Since most companies today depend on functioning ICT, a standstill can result in a considerable financial loss. In addition, especially with critical infrastructures, a standstill of operations can have much more serious effects.

Recommendation:

INFO

MELANI information page on encryption Trojans

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

4.7.2 E-banking Trojans – Retefe still widespread

Various e-banking Trojans are still active in Switzerland to various degrees. These include, for instance, the Dridex malware, which has the ability to extend its functions in order to target and attack business customers. For this purpose, Dridex searches an infected system for offline banking software.[22] The Gozi ISFB Trojan spreads via website infections as well as manipulated email attachments. Trickbot is globally active and expanded its target list to Swiss banking institutions in 2017. Trickbot has a modular structure and is constantly being expanded with new functions. Emotet was originally an e-banking trojan. Criminals now also use it for the distribution of other malware like for example ransomware. The spreading mechanism of choice for Emotet nowadays is forged invoices.

However, Retefe is still one of the most aggressive malware in Switzerland. In the past, it only attacked Austria, Sweden, Japan, the United Kingdom, and Switzerland. MELANI already addressed Retefe in its semi-annual report three years ago. In contrast to other malware, which also spreads via website infections, Retefe only uses email for distribution. This happened in the past mainly through forged invoices from online shops such as Zalando or Ricardo. The most recent versions mainly imitate federal agencies or businesses associated with the federal government such as the Federal Tax Administration or Swiss Post.

After successful infection, Retefe changes the browser settings so that certain websites (in particular the e-banking portals of some Swiss financial institutions) are redirected via a proxy server. Retefe also installs a certificate on the computer for the purpose of issuing certificates for financial institutions and purporting to be such a financial institution. In this way, the malware avoids the certificate error message that would occur otherwise and make victims suspicious. When a victim logs in to the purported e-banking portal via a computer infected with Retefe, a QR code is displayed. This QR code leads to a website where the victim is asked to download and install an app "to increase security" – but which is in reality an Android malware, namely an SMS Trojan. If the victim installs the Android app, all SMSs sent by the bank for two-factor authentication are forwarded to a webserver abroad and thus to the hackers. They are now able to log into the victim's e-banking system and make payments.

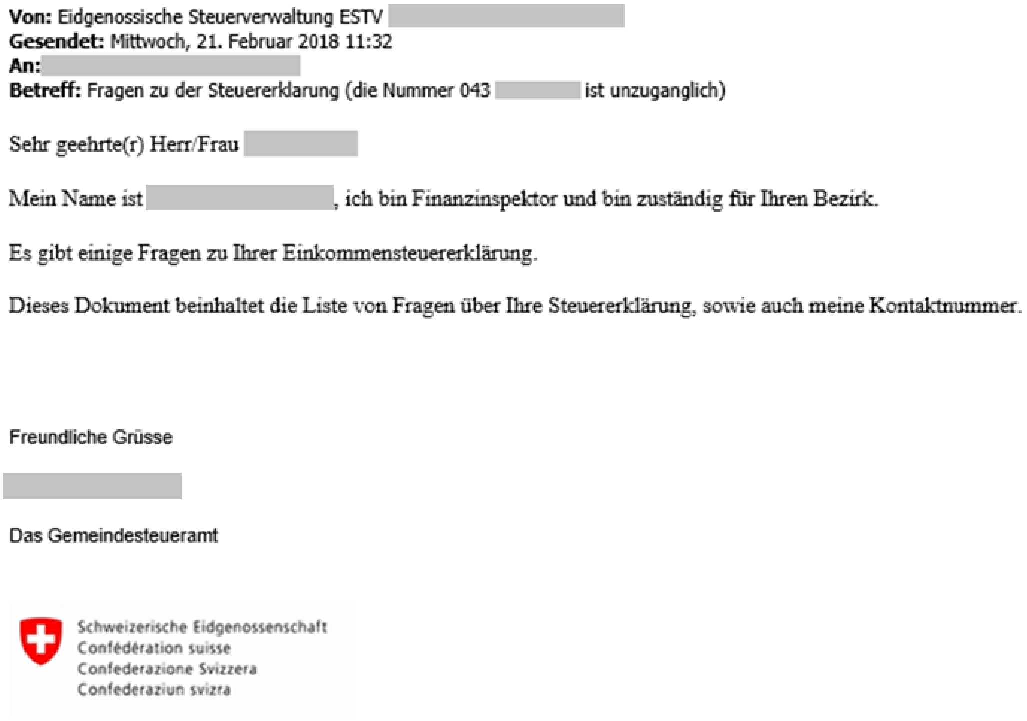
Over the past half year, this approach was expanded when perpetrators tried to obtain letters with activation data. These letters are usually sent by the bank by post to customers and contain a mosaic image which must be scanned in with an app the first time a device logs into e-banking. The bank then approves the device for the mobile authentication method. The attackers used social engineering to try to get the activation data and asked the victim to scan or photograph the activation letter and send it to the scammers.

In September, the malware was also expanded with EternalBlue exploit. This is the vulnerability that was exploited during the WannaCry encryption wave in May and caused damage worldwide. With the implementation of EternalBlue, Retefe probably aimed to spread in company networks. If an employee accidentally opens an infected attachment, the malware can move to the computer where the company makes its e-banking payments. Of course, this only works if the vulnerability has not yet been eliminated.

During the reporting period, MELANI repeatedly received reports of emails with Retefe which contained both a correct salutation and a correct phone number of the recipient in the subject line. Most of these emails were alleged contacts of the Federal Tax Administration (FTA) , in

[22] Semi-annual report 2016/2, section 4.6.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2016-2.html (as at 31 January 2018).

which it is pretended that there are still questions regarding the tax return. There were enough signs that should have made a recipient suspicious. However, it is likely that some recipients opened the attachment as a result of seeing their own telephone number.



Von: Eidgenossische Steuerverwaltung ESTV [redacted]
Gesendet: Mittwoch, 21. Februar 2018 11:32
An: [redacted]
Betreff: Fragen zu der Steuererklarung (die Nummer 043 [redacted] ist unzuganglich)

Sehr geehrte(r) Herr/Frau [redacted]

Mein Name ist [redacted], ich bin Finanzinspektor und bin zuständig für Ihren Bezirk.

Es gibt einige Fragen zu Ihrer Einkommensteuererklärung.

Dieses Dokument beinhaltet die Liste von Fragen über Ihre Steuererklärung, sowie auch meine Kontaktnummer.

Freundliche Grüsse

[redacted]

Das Gemeindesteueramt

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Figure 4: Example of a fraudulent email with the Retefe malware and the telephone number in the subject line

It is unclear how the attackers were able to connect the data of the email address, the first and last names and above all the telephone number. There are indications that the data could originate, among other things, from a data leak.

5 Situation internationally

5.1 Espionage

5.1.1 Targeting the Middle East

Cyber espionage campaigns can be roughly divided into two categories: namely economically motivated campaigns, or those aiming at strategic, military, and/or political information. In the following chapters some campaigns are described. The Middle East is an illustrative example as political tensions are high and their importance in oil and gas production make the countries in this region attractive targets for cyber espionage.

5.1.2 Example APT33

"Not only political or economic opponents have interesting data – information from partners can also be valuable." This could be the slogan of the cyber espionage campaign APT33[23], which the US security company FireEye attributes to an Iranian agency. APT33 has been active since at least 2013, with a particular focus on Saudi, US, and South Korean targets in the military, civil aviation, and energy sectors. From mid-2016 to early 2017, APT33 is claimed to have compromised an American aerospace company and targeted a Saudi organisation likewise involved in aviation. APT33 spreads its malware via emails disguised as job offers. Sender email addresses were registered that are similar to the domain names of Saudi and Western aviation companies cooperating with Saudi Arabia in both the civil and military sectors. The security company FireEye assumes that the attacks were aimed at obtaining military information about the Royal Saudi Air Force in order to increase the knowledge of the Iranian Air Force and to incorporate findings into Tehran's military and strategic decision-making.

During the same period, an espionage campaign was also active at a South Korean refinery. In May 2017, employees of a Saudi company and another South Korean company, both operating in the oil business, also received such emails. The emails disguised as job offers contained an espionage maalware and were purportedly sent by a Saudi oil company.

FireEye claims to have identified a person connected with these incidents, probably a former member of the Iranian government. Some of the malware programs used also contained words in Farsi, Iran's official language. The times and dates on which the attacks were committed as well as the use of specific malware found on Iranian hacker websites also seem to confirm the suspicion that Iranian perpetrators were involved.

The alleged Iranian cyber espionage campaign Shamoon, which targeted organisations in the Persian Gulf starting in 2012, also concentrated on the petrochemical sector.

5.1.3 CopyKittens – technical and strategic development[24]

On 29 March 2017, the German Federal Office for Information Security (BSI) declared that the website of the Jerusalem Post daily newspaper had been manipulated and misused for the distribution of malware. According to the BSI, the website infection was probably connected with several technical anomalies, which were not described in further detail, involving the network traffic of the German federal parliament since January 2017.[25] In the same month, the Israeli cyber-intelligence firm ClearSky confirmed the infection of the Jerusalem Post and also disclosed infections on other Israeli websites and those of the Palestinian Ministry of Health. It attributed responsibility for the attack to the CopyKittens espionage group.[26] From October 2016 to the end of January 2017, the compromised websites contained a JavaScript which downloaded a specific tool for web browser penetration tests from a domain registered by the hackers for that purpose. The JavaScript was not delivered for every website visitor, but rather only for certain selected victims.

[23] https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html (as at 31 January 2018).

[24] http://www.clearskysec.com/tulip/ (as at 31 January 2018).

[25] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Cyber-Angriff_auf_den_Bundestag_Stellungnahme_29032017.html (as at 31 January 2018).

[26] http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf (as at 31 January 2018).

CopyKittens is a cyber espionage group that has been active since at least 2013. Its name derives from the practice of copying code fragments from online forums and using them for their cyber attacks. The group mainly targets Israel, Saudi Arabia, Turkey, the United States, Jordan, and Germany, but also UN officials. The group's targets include governmental and scientific institutions, companies in the defence industry, suppliers to defence ministries, and large IT companies.

The campaign spreads not only through the watering-hole attacks described above, but also through targeted emails with malware attachments or links. An example of the latter is an email to employees of numerous government organisations. The email was sent at the end of April 2017 from a compromised email account. The title of the attached infected document referred to international relations between Iran, North Korea, and Russia. In two other cases, the group broke into the email accounts of people associated with the actual target. Existing conversations of the legitimate owner were misused to send an email with a link to a malicious website registered for that purpose.

The group has been creating and managing fake Facebook profiles since 2013. In this way, it builds up trust with potential victims and collects information about them for further attacks. These false profiles were also used to send links to infected websites. To appear more credible, the profiles also published harmless material and have an unsuspicious number of friends.

Conclusion:

In 2015, CopyKittens was still considered an attacker with only average potential for harm. But the latest publically known attacks show that the group apparently has developed in technical and strategic terms and uses tools developed itself alongside malware procured online.

5.1.4 The OilRig group develops new attack systems[27]

In the past, the OilRig group's espionage campaigns targeted public and private companies in North America and Europe, with particular interest in oil and gas production and trade in the Middle East. OilRig added new Trojans to its arsenal during the period under review and continues to attack the Middle East. Between July and August 2017, two new instruments were used in several attacks: the ISMAgent backdoor and an injector for its installation. The injector has a complex structure and contains techniques that make detection on the targeted computers even more difficult.

On 23 August 2017, OilRig attacked an internal government agency of the United Arab Emirates via a targeted phishing email with two ZIP attachments and an image in the email text. Because the image was downloaded from an external server, it was probably used to verify whether the recipient opened the email. The attack also used some other interesting technical tricks. The sender address was not forged, even though the sender was an internal address of the company. OilRig had probably phished the authentication data of a legitimate email account in the same domain, which it then used to send the email described above. Both ZIP files contained a Word document. The first contained a harmful macro, via which the injector

[27] https://researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/ (as at 31 January 2018).

installed the mentioned backdoor. The attackers used social engineering techniques to induce the recipients to permit execution of the macro. The second document attempted to exploit a vulnerability in Microsoft Word[28] for which the update had only recently been released. The group tries to combine the exploitation of technical and human weaknesses.

Once the hackers have entered the system, they use programs available on the black market such as Mimikatz to obtain the necessary authentication data within the company and to move from computer to computer in the company network. According to the security service provider Palo Alto, the group also carries out supply chain attacks:[29] this method consists of not directly attacking the actual target, but rather taking the detour via a service provider of the company. Since the service provider has access to the target's network or provides software and hardware, the target can be attacked indirectly. Because a company usually has several service providers, the attacker has a greater "selection" of possibilities (and vulnerabilities) to carry out the attack with this method. This method is being used with increasing frequency, as described in the international attacks section of semi-annual report 2017/1.[30] According to Kaspersky's annual predictions for advanced threats in 2018, this threat is expected to intensify in the current year.[31]

Conclusion:

In principle, Switzerland is not a target of the OilRig group. However, since there are numerous suppliers of specific products and services in the petrochemical field in Switzerland, attacks are also conceivable in Switzerland.

5.1.5 Advertising space on Facebook allegedly bought by Russian company for propaganda purposes[32]

The last semi-annual report discussed the interference of third countries in the US presidential elections with the aid of targeted cyber attacks. The targets were not only the systems for counting the ballots (where there are no indications of successful manipulations) and the correspondence of the Democratic Party: the US intelligence services stated that disinformation campaigns had also been spread in parallel, particularly via the social networks. Recently, an allegedly Russian company was also linked to a propaganda campaign on Facebook carried out during the US presidential elections. The Internet Research Agency is claimed to have bought advertising space on Facebook to spread political positions of the Russian leadership.

[28] CVE-2017-0199 Microsoft Word Office/WordPad Remote Code Execution Vulnerability

[29] https://researchcenter.paloaltonetworks.com/2017/12/unit42-introducing-the-adversary-playbook-first-up-oilrig/ (as at 31 January 2018).

[30] https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2017-1.html (as at 31 January 2018).

[31] https://www.kaspersky.com/about/press-releases/2017_kaspersky-labs-threat-predictions-for-2018 (as at 31 January 2018).

[32] https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html?utm_term=.936611ed98fb (as at 31 January 2018).

More than 3,300 advertisements can be traced back to the Russian campaign.[33] They were spread and advertised by over 470 false profiles. Although the names of the two US presidential candidates were mentioned sporadically in some posts, the emphasis was on sociopolitical content concerning sensitive issues such as same-sex partnership, immigration, and the right to bear arms. Some of the posts were not intended to convey any ideological controversy, but rather to spread panic on the internet and create chaos. The Washington Post newspaper, for example, cites a false report in connection with a chemical leak in the state of Louisiana. The propaganda was spread in a targeted manner, i.e. so that the content was visible only to people in certain regions.

Already in January 2017, the US intelligence services accused Russia of interfering in the presidential elections.[34] Russia is also said to have paid trolls to spread false news on social networks and influence public opinion. After these accusations, Facebook CEO Mark Zuckerberg promised to fight against false information on his platform.

5.2 Data leaks

The reporting period was once again marked by several cases of massive data theft that made headlines in the media.

5.2.1 Equifax

One of the most spectacular cases was undoubtedly the attack on Equifax, one of the largest credit rating agencies in the United States. On 7 September 2017, the company announced that it had discovered unauthorised access to its networks already in July. The entry point was apparently the Apache Struts vulnerability, for which Equifax had not installed a patch. This vulnerability may have compromised the personal data of 143 million customers in the United States. What makes this case particularly sensitive – apart from the large number of people affected – is the amount of personal and financial data that the company has access to and that it uses to calculate credit risks. This includes Social Security numbers (SSNs)[35]. The attack on Equifax underlined the security risks associated with this unique identification number, which was originally intended to identify individuals in the Social Security system but has evolved over time into a unique personal identifier in various areas such as healthcare, taxation, and lending. The theft of this number opens up far-reaching possibilities for fraud and identity theft, all the more so if other personal data of its owner is stolen at the same time.

[33] http://www.wired.co.uk/article/facebook-twitter-russia-congress-fake-ads-2016-election-trump (as at 31 January 2018).

[34] http://www.zeit.de/politik/ausland/2017-01/hacker-angriff-us-wahl-russland-barack-obama-geheimdienste (as at 31 January 2018).

[35] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/statistik--register-und-forschung/ahv-nummer.html (as at 31 January 2018).

5.2.2 Audit- and Consulting company

The media hype had hardly subsided when The Guardian announced another incident on 25 September 2017, again affecting a large US company[36]. According to the English newspaper, the email service of Deloitte, one of the four largest accounting firms in the world ("Big Four"), had been the target of cyber attacks since October or November 2016. An insufficiently secured administrator account had made it possible to access the email traffic between Deloitte and its major customers stored in the Microsoft Azure cloud. The company's security standard was the focus of particular criticism, especially after it became known that potentially critical elements of its network infrastructure had been visible on the internet (namely open RDP, VPN login data)[37]. Deloitte's activities also include advice on cyber security for companies operating in many sensitive sectors. In June 2017, Gartner named Deloitte the world's best security consulting firm for the fifth year in a row.

5.2.3 Extortion with data about driving habits

Data theft likewise did not spare Silicon Valley. In November, Uber confirmed that personal data of 57 million customers and drivers had been stolen from the company. The company had been aware of the details of this incident already at the end of 2016. According to a Bloomberg[38] report, the origin of the theft could be traced back to a private GitHub site used by Uber engineers. There, the perpetrators were able to steal login data giving them access to sensitive information hosted by Uber in Amazon's cloud service. They were then successful in blackmailing the company, which apparently paid USD 100,000 in exchange for the stolen data and for maintaining silence about the theft. The story was far from over with the payment of this ransom and the promised destruction of the data, however: The case eventually became public. By deciding not to inform the authorities or the victims upon learning of the data theft, the company failed to comply with its legal obligations. Various legal proceedings are currently in progress. It is not known, if the attackers have continued blackmailing the company after the ransom was paid.

5.2.4 Lost USB stick

A case from the United Kingdom shows that data leaks are not always caused by vulnerabilities or poorly configured systems. In October 2017, a passer-by on London's streets found a USB stick with unencrypted data in the order of 2.5 gigabytes. The USB stick included sensitive information about Heathrow Airport, such as information about the location of surveillance cameras, escape routes, and times of police patrols. The finder gave the USB stick to a newspaper, which then made the incident public. How the USB stick ended up on the street was unclear.

[36] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails (as at 31 January 2018).

[37] https://www.theregister.co.uk/2017/09/26/deloitte_leak_github_and_google/ (as at 31 January 2018).

[38] https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data (as at 31 January 2018).

Conclusion:

Minimising cyber risks is a holistic process and must also include physical security precautions. It must be clearly set out which data may be stored on external media at all and which security measures are to be applied (e.g. which encryption strength).

Further Information you will find in the key topic in chapter 3.

5.3 Industrial control systems

5.3.1 Dragonfly is spying on utilities infrastructure

In July, the New York Times reported that a nuclear power plant in Kansas had been targeted by hackers since May 2017.[39] Since then, several cyber attacks on the energy sector have become known in the US and Europe.[40,41] Even if the media reports give the impression that attacks on the energy sector are increasing and that a new group called Palmetto Fusion is causing a stir, all these operations may be traced back to a single player called Dragonfly, which has been active since 2011.[42] Since 2013, Dragonfly, alias Havex, Energetic Bear, Crouching Yeti, etc., has been attacking the energy sector in the US and Europe. Starting in 2017, these attacks – now subsumed under the name Dragonfly 2.0 – intensified noticeably and also improving in technical terms.

Dragonfly 2.0 uses spearphishing emails[43] for the attacks with infected attachments or links, as well as specially manipulated websites from the victims' environment, referred to as "watering holes".[44] The compromised websites used for the attacks point to Dragonfly's target audience: Companies operating in the energy sector, traders and lawyers specialising in the energy sector, and producers of IT solutions for European and US industry. In this way, the attackers try to obtain access data for critical networks. In its report on Dragonfly 2.0, the US software company Symantec refers not only to victims in the US and Turkey but also to an attacked company in Switzerland. MELANI was not able to verify this statement. No Swiss victims were identified up to now[45].

[39] https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html (as at 31 January 2018).

[40] https://www.wired.com/story/russian-hacking-teams-infrastructure/ (as at 31 January 2018).

[41] https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html (as at 31 January 2018).

[42] https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear (as at 31 January 2018).

[43] http://blog.talosintelligence.com/2017/07/template-injection.html (as at 31 January 2018).

[44] https://www.riskiq.com/blog/labs/energetic-bear/ (as at 31 January 2018).

[45] https://www.watson.ch/Digital/Schweiz/472496967-Droht-ein-Blackout--Hacker-attackieren-Schweizer-Energiesektor (as at 31 January 2018).

Conclusion:

Espionage targeting IT networks in the energy sector can serve several purposes. On the one hand, the attacker can gain access to the networks and steal information in order to gain a strategic and economic advantage. On the other hand, controlling computers in critical networks makes it possible to manipulate or interfere with processes.

There is currently no known case of sabotage committed by Dragonfly – in whatever version. But it cannot be ruled out that Dragonfly also intends to carry out such attacks in the future, especially if the political situation changes. The current espionage attempts might also serve to gain an overview of possibilities in order to prepare for any political eventualities in the future. Attacks by the Sandworm group – another actor with similar characteristics that sabotaged the Ukrainian power grid in 2015/2016 – have shown that it takes months of preparation to understand how the attacked control systems are configured and which command combinations are required for the targeted sabotage action. It is problematic that even espionage attempts, if their execution is faulty, can lead to unintentional collateral damage. The observed attempted attacks show the importance of applying a wide range of measures as described in section 4.2.

5.3.2 Attack against security control systems

In December 2017, several security companies published reports of a malware called Triton/Trisis, which targets process safety solutions for industrial control systems. The malware, which was discovered in mid-November 2017 and has been active since at least August 2017, very specifically attacks individual configurations of the Triconex system produced by the French company Schneider Electric. At least one target in the Middle East has been mentioned.

Previously, attacks had focused directly on the controls of the main process. A process safety solution, in contrast, monitors and controls the operation of a plant. If, for example, the pressure or temperature of the process to be monitored exceeds a critical value at which the system may be damaged, countermeasures (such as shutting down or preventing an operation) are automatically initiated. If such a safety system can be manipulated so that automatic shutdown is prevented when a malfunction occurs, a system can be damaged or destroyed, or people may even be harmed or killed. In some places, an operator intervenes manually in a system to trigger these measures.

Targeted attacks on industrial control systems are still rare. Triton/Trisis is only the fifth known malware specifically targeting industrial controllers. The best-known malware in this context is Stuxnet, a malware discovered in 2010 to disrupt or destroy centrifuges in Iranian uranium enrichment plants. More recent examples are the attacks in December 2015[46] and 2016[47] on

[46] MELANI semi-annual report 2015/2, section 5.3.1, https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html (as at 31 January 2018).

[47] MELANI semi-annual report 2016/2, section 5.3.1, https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2016-2.html (as at 31 January 2018).

the power supply in the Ukraine, including the malware Blackenergy and Industroyer/Crashoverride.

Conclusion:

Such attacks have been very restrained so far. This is probably due to the fact that such an attack always carries the risk of uncontrollable collateral damage, which could also have unpredictable consequences for the attacker. In the present case, this in fact happened to the perpetrators. Their manipulation attempts with the malware caused an automatic emergency shutdown of the attacked system. The investigation of this shutdown led to the discovery of the malware. For these reasons, such attacks are usually directed very precisely against a specific system configuration and are correspondingly complex. The effort is hardly worth it for attackers primarily with a pecuniary motive, and it is typically only carried out by states. Although the Triconex system is widely used in industry, each implementation is unique and the attack vector cannot be transferred to other systems without significantly greater effort. But the focus on process safety solutions demonstrates the intention of the attackers to cause as much physical damage as possible to the system itself or to the controlled analogue process.

5.3.3 Experimental hacker attack on an aircraft by DHS

The "CyberSat – Security in Aerospace" conference in the US focuses on cyber attacks in the satellite and aviation sectors. A representative of the US Department of Homeland Security (DHS) announced at CyberSat in November 2017 that DHS security experts had succeeded in penetrating the computer system of a Boeing 757 at Atlantic City International Airport during an experiment in September 2016.[48] The aircraft had previously been purchased by DHS to investigate possible vulnerabilities relating to cyber attacks. The Boeing 757 is a type of aircraft flown by many airlines, including in the US. The attack was performed remotely and without the help of insiders. The airplane's radio links were used for the hacker attack. The vulnerability exploited for the cyber attack was discovered by DHS within two days. The reason for this experiment was probably an incident in April 2015.[49] At that time, IT security expert Chris Robert claimed via Twitter that he had discovered and exploited vulnerabilities in the in-flight entertainment systems (IFEs) of the Boeing 757-200, Boeing 737-800, Boeing 737-900, and Airbus A-320 aircraft models that allowed access to critical on-board electronics systems. The experiment demonstrates the importance of a clean physical separation of avionics (aviation and electronics) from externally accessible information and communication systems, so that no connection between the new networks is possible or can be exploited even in the case of faulty configurations.

[48] https://www.bleepingcomputer.com/news/security/dhs-team-hacks-a-boeing-757/ (as at 31 January 2018).

[49] MELANI semi-annual report 2015/1, section 5.3.3, https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-1.html (as at 31 January 2018).

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 the Inflight Entertainment System and the Internet access in a plane. 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).

DOCU

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

5.4 Attacks (DDoS, defacements, drive-bys)

5.4.1 DDoS

DDoS attacks were again a widely used instrument for attackers with a wide range of motivations during this reporting period. The damage caused by such an attack depends to a large extent on the need to keep an online service up and running at all costs. The attackers are fully aware of this fact, which is why they focus more and more systematically on very specific industries – especially those for which an online presence is absolutely necessary from an economic point of view. In the second half of 2017, for example, the gaming industry was the target of several attacks. One of these attacks, which attracted particular attention, was directed against the UK National Lottery. On 30 September, it was not possible for 90 minutes to submit bets online or via the mobile app. The timing of the attack was cleverly chosen because the disruption occurred on a Saturday evening before the lottery numbers were drawn: i.e., at a time when the lottery is usually especially busy. The reason for the attack is unknown, and no blackmail demand has been made public.

With the hype surrounding cryptocurrencies, the various platforms used to buy or exchange such currencies have also become a popular target for DDoS attacks. An example of this trend is the attack against the cryptocurrency Electroneum, which was specially developed for smartphones. The incident forced the company to postpone the launch of its mobile app.

While DDoS attackers are always on the lookout for new victims, they are also adding new weapons to their arsenal. Poorly secured networked devices are increasingly being exploited.[50] In 2017, the "pulse wave" tactic described by the security solutions provider Imperva Incapsula was widely discussed.[51] In contrast to traditional attacks, the intensity of which increases continuously before they reach their peak, a pulse wave attack encompasses several attack waves, each immediately reaching its maximum strength of up to 350 Gbit/s. These waves are

[50] cf. semi-annual report 2016/2 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2016-2.html (as at 31 January 2018).

[51] https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html (as at 31 January 2018).

sometimes repeated over the course of several days. The success of such attacks is partly due to the peculiarities of the hybrid DDoS-defence, which means that a cloud-based solution is used only once the attack reaches a certain level and can no longer be managed at the application level. Pulse wave attacks cause particularly serious damage because the overload limit is reached immediately. Imperva Incapsula assumes that this attack tactic will be used regularly in future.

5.4.2 Ransomware: Bad Rabbit

At the end of October, the fears triggered by WannaCry and NotPetya were once again fuelled by new ransomware. This encryption software called "Bad Rabbit" spread via bogus updates of Adobe Flash. Apparently, the Eternal Romance exploit was also used to penetrate the system of victim companies, as was Mimikatz to steal login data. According to the security service provider Group IB, the malware is a modified version of NotPetya[52] with a different encryption algorithm. Most of the victims of Bad Rabbit are in Russia, but some cases have also been reported in other countries such as Ukraine, Germany, and Turkey.

5.4.3 Cryptocurrencies

Last year, cryptocurrencies were the focus of interest not only of the public and the media, but also of criminals looking for ways to benefit from the rapid rise in prices. In some attacks, the platforms themselves were targeted. With the help of often highly sophisticated methods, criminals target platforms to steal enormous sums of money in one fell swoop. In December 2017, for example, more than USD 70 million were stolen from the NiceHash mining marketplace, and over half a billion US dollars in crypto assets were stolen from the Coincheck exchange in January 2018. Although these incidents have not yet been solved in detail, they illustrate the risks associated with the centralisation of a large number of currencies on a single platform. The platforms were not the only targets, however, and tailored attacks were also directed against individual owners of virtual currencies. The New York Times reported on a particularly insidious approach that targeted numerous crypto investors in the United States.[53] In these cases, the attackers were able to obtain the phone numbers of individuals who were targeted because they were thought to have large amounts of virtual currencies. The attackers called the mobile network operators of their victims and persuaded them, using considerable social engineering, to reassign the mobile phone numbers of the victims to a device under their control. This made it easy for the perpetrators to reset passwords using the mobile phone number, allowing them to access the accounts associated with the number. Another method is to hijack the computing power of internet users to mine crypto assets. In 2017, special scripts built into websites surfaced several times, allowing cryptocurrencies to be mined directly via the browser. This trend is discussed in section 6.2 of this report.

5.5 Vulnerabilities

Numerous serious vulnerabilities made headlines in the period under review. The pinnacle was the publication of the vulnerability Spectre/Meltdown in the processors of various manufacturers. This type of vulnerability, which cannot be patched with a simple update, forces security

[52] https://www.group-ib.com/blog/badrabbit (as at 31 January 2018).

[53] https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html (as at 31 January 2018).

officers to define new strategies to minimise the impact. The Spectre/Meltdown vulnerability will be discussed in detail in the next semi-annual report.

5.5.1 Vulnerability in the WPA2 encryption standard, previously considered secure

In October 2017, two researchers from the University of Leuven published a vulnerability in the WPA2 encryption standard. With the vulnerability – called "KRACK", short for "Key Reinstallation AttaCK" – it is possible to read encrypted data and also account for connections between two devices – such as a browser and a web server. This sounds very critical at first. But special conditions must be met for the vulnerability to be exploited. In particular, an attacker must be in the immediate vicinity of the WLAN device and be able to receive the wireless signals. This means the vulnerability cannot be widely exploited from the internet. It is also not possible to access the WLAN password or the router, for example in order to access the device directly at a later time. Only individual existing connections can be accessed.

The vulnerability is not based on a programming error, but rather on a design flaw in the WPA2 standard.

Conclusion

Security-relevant internet services such as online banking are already encrypted in the browser, indicated in the address bar with https://. The encryption of these https connections is not endangered by this vulnerability. The higher-level encryption of the wireless connection is affected.

Nevertheless, it is recommended to install the updates provided by the companies for this vulnerability as soon as possible.

5.5.2 ROBOT - The return of a vulnerability

The "Bleichenbacher attack" made the headlines again – and the word "again" is astonishing, since the attack was already discovered 20 years ago. A systematic review revealed that 27 of the 100 most popular domains are still vulnerable to this type of attack. These include Facebook and PayPal, for example. The vulnerability has accordingly been referred to as the "Return of Bleichenbacher's Oracle Threat" – or ROBOT for short.

The Swiss cryptographer Daniel Bleichenbacher recognised in 1998 that the error messages of an SSL server reveal information about the data to be decrypted. Through cleverly selected and repeated requests, a message can gradually be deciphered. The current TLS 1.2 standard continues to use the faulty version PKCS #1 v1.5 RSA. In order to prevent attacks from being successful, a server should report random data instead of decrypted data and thus continue the handshake, even if a data block is not correctly formatted. To prevent possible timing attacks, the returned random data must be generated already before decryption. The entire process is extremely complex. It is therefore not surprising that some servers do not have a correct implementation.[54]

Aside from the mentioned error messages, the current ROBOT-attacks also identifies vulnerable servers by other means like TCP connection failures, Timeouts or protocol errors.

Overall, products from different manufacturers are affected. Particularly problematic are devices whose end-of-life cycle has already been reached and for which updates are therefore no longer provided.

5.5.3 Vulnerability in security chip manufactured by Infineon

In October 2017, researchers discovered a vulnerability in the generation of the RSA key in Infineon's security chips. This makes it possible to calculate the private key using the public key. The vulnerability for the attack, called ROCA, is located in a software library on the chip. This library is used to generate the prime numbers for RSA. These prime numbers are now apparently too weak. A public RSA key consists of two numerical values. One of them is the product of two large, randomly generated prime numbers. Anyone who now knows the two prime numbers can calculate the private key. However, the effort for such a calculation is considerable, which puts the magnitude of the vulnerability into perspective. With a key length of 2,048 bits, 141 CPU years would be required. Nevertheless, it is possible to exploit the vulnerability with sufficient computing power. The affected Infineon chips are installed in various products, for example in smart cards, mobile devices, and notebooks. Estonia, as a pioneer in everyday digitalisation, or more precisely the Estonian eID, was also affected. This has led the government to permanently withdraw and block all of the affected 760,000 certificates in its systems.

5.5.4 Vulnerability even before the operating system is released

Like any operating system, macOS is also regularly affected by vulnerabilities. The time when third parties make the vulnerabilities public is always unfavourable for the company affected. In this case, however, the timing probably could not have been worse: shortly before the macOS 10.13 High Sierra operating system was released in late September 2017, security researcher and former NSA employee Patrick Wardle published a zero-day vulnerability in this system. Older versions of the system are also affected. With this vulnerability it is possible to access all passwords stored on the computer, via the password manager. The password manager may include all kinds of sensitive data such as credit card numbers as well as passwords for email accounts or webshops. The discovered vulnerability can be exploited and the sensitive data can be accessed using malware that infects the computer via an email attachment or is even packaged in a legitimate app. The bug was reported to Apple already in early September 2017. But Apple was unable to provide an update in time, and High Sierra was shipped with the vulnerability.[55]

[54] https://www.golem.de/news/robot-angriff-19-jahre-alter-angriff-auf-tls-funktioniert-immer-noch-1712-131607-2.html (as at 31 January 2018).

[55] http://www.zdnet.de/88313439/macos-high-sierra-sicherheitsforscher-macht-zero-day-luecke-oeffentlich/?inf_by=5a91d408671db898358b4e40 (as at 31 January 2018).

At the beginning of September 2017, Wardle already published details about a method that make it possible to circumvent a security function of High Sierra without major effort. The affected Secure Kernel Extension Loading function is intended to prevent third-party kernel extensions from being loaded without the user's consent.

5.6 Preventive measures

5.6.1 Training malware is a concern for antivirus manufacturers

For three years, the security researchers of the Japanese software and service provider Trendmicro[56] had repeatedly noticed the same malware directed against people in influential positions in the South Korean energy and transport sector. The attacks were summarised under the pseudonym "OnionDog". Other companies also encountered the malware, analysed it, and published reports.[57] On closer inspection, however, it turned out that OnionDog was part of a large-scale training exercise.

While the infected devices communicated with a command and control system, they never received commands from it. The system merely registered the infection. The underlying addresses were attributable to the South Korean National Cyber Security Center (NCSC). It turned out that the malware was part of the Ulchi Freedom Guard exercise organised by South Korea and the United States.

[56] https://blog.trendmicro.com/trendlabs-security-intelligence/oniondog-not-targeted-attack-cyber-drill/ (as at 31 January 2018).

[57] http://zhuiri.360.cn/upload/APT-C-03-en.pdf (as at 31 January 2018).

Recommendation:

While realistic exercises are welcome, the malware should not break out of the exercise scenario. This allows actors with malicious intent to gain new insights and use them for future attacks. In the worst case, such an attack is given less priority because the malware is known and classified as safe in light of the past exercise. Another aspect is coming to premature conclusions regarding attribution. The more than 200 publicly identified malware instances in this case caused rampant speculation about the origin and intent of the attacker. However, assignment of blame can quickly lead to unwanted escalation. If malware is used in an exercise, it must be ensured that it does not leave the training exercise or at least does not function outside of it. Solid, ongoing sensitisation of employees is one of the main pillars when it comes to security on the internet. Exercises are one way to achieve such sensitisation. In order to ensure a smooth performance of the exercise, at least all the actors involved in the infrastructure should be informed before the test is carried out: these actors include in particular the top-level domain name registry (for .ch domains, SWITCH), the registrar and hosting provider, as well as the (external) email provider, if applicable. Finally, it makes sense to notify MELANI so that any reports can be responded to as desired by the organisers of the awareness campaign and so that no measures are initiated by MELANI against the website.

REPORT

MELANI reporting form

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

5.6.2 Re-registration of APT-Domains

The group Fancy Bear (also known as APT28, Sofacy, or Strontium) uses domain names similar to the names of known companies or products to make links or senders appear trustworthy. Due to their widespread use, names with a clear allusion to Microsoft products such as livemicrosoft[.]net and rsshotmail[.]com were very popular.

While Microsoft was unable to hold the people behind the campaign accountable, the software giant's lawyers did succeed in convincing the judge that the domains should be reassigned to Microsoft with regard to trademark rights.[58] This meant that from the time of re-registration, victims no longer connected to servers under the control of the attackers, but rather to servers under the authority of Microsoft. This made it possible to identify and inform victims so that they could clean their devices.

[58] http://www.zdnet.com/article/us-election-hack-microsoft-wins-latest-round-in-court-against-fancy-bear-phishers/ (as at 31 January 2018).

5.6.3 Rescam bot – artificial Intelligence against advance fee fraudsters

In advance fee fraud, potential victims have for years been told hair-raising stories with the aim of persuading them to make an upfront payment.[59] The best known of these scams are probably the Nigerian princes who claim they will be able to inherit the monarch's estate if only they can obtain an advance fee.

New Zealand's non-profit organisation Netsafe[60] estimates the damage caused by this type of fraud at USD 12 billion a year. Because Netsafe was aware that sending out such fraud attempts could hardly be prevented, the organisation chose a different approach. Using a chatbot equipped with artificial intelligence, Netsafe tried to keep the scammers busy for as long as possible.[61] Fraudulent emails can be forwarded to the bot via an email address. The chatbot analyses the content of the email, generates meaningful answers, and involves the attackers in long discussions. By keeping attackers busy for as long as possible, the chatbot tries to keep them away from other real attacks. Sample conversations can be followed on rescam's Twitter account.[62] The communication generated in this way can also be humorous and demonstrates the awkwardness of the scammers when they fall for their own tricks.

6 Trends and outlook

6.1 Net neutrality

Net neutrality refers to the principle according to which all data is treated equally when transported through the internet – regardless of sender, recipient, service, application, device, or content. The goal of net neutrality is to protect against discriminatory interference with data traffic. Concerns raised in the discussions of net neutrality include the blocking, prioritisation, and slowdown of services as well as product differentiation in internet access. Net neutrality is intended, for example, to ensure that mobile service providers do not block VoIP services; connection providers do not prioritise their bundled IP-TV products over streaming services; peer-to-peer protocols and video transmissions are not throttled; and messenger and streaming services are treated equally with regard to billing for the volume of data used.

In the United States, the Federal Communications Commission (FCC) issued a regulation[63] on 14 December 2017 that reversed provisions on net neutrality previously issued by the FCC in 2015.[64] Specifically, internet providers have been legally reclassified: they are no longer

[59] https://www.skppsc.ch/de/faq/was-versteht-man-unter-vorschussbetrug/#was-versteht-man-unter-vorschussbetrug (as at 31 January 2018).

[60] https://www.netsafe.org.nz/ (as at 31 January 2018).

[61] https://www.rescam.org/ (as at 31 January 2018).

[62] https://twitter.com/rescambot/ (as at 31 January 2018).

[63] Restoring Internet Freedom Order: https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf (as at 31 January 2018).

[64] Open Internet Order: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf (as at 31 January 2018).

deemed telecommunications services and common carriers, but rather merely information services, so that they are no longer subject to regulation and supervision by the FCC, which previously ensured compliance with net neutrality.

Attempts are being made by several US-states and also by Congress to take action against the FCC's decision. In the EU, net neutrality was laid down in a regulation in 2015 as "rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services".[65] However, various exceptions have been defined. "Specialised services" such as telemedicine, for example, for which a specific quality level is objectively necessary, may be given preferential treatment – but only if the specialised service cannot be used for general internet access. Moreover, traffic management measures are permitted which differentiate between objectively different traffic categories. However, any such differentiation should only be permissible on the basis of objectively different requirements for the technical quality of services (for example in terms of latency, jitter, packet loss, and bandwidth), but not on the basis of commercial considerations. Furthermore, it is permitted to exclude data volumes used for selected services from the calculation of limited monthly transfer volumes or to charge them differently ("zero rating"). Member States have the right to adopt stricter rules on net neutrality.

In Switzerland, there are no legal provisions governing net neutrality. As part of the current partial revision of the Telecommunications Act (TCA),[66] the Federal Office of Communications (OFCOM) commissioned a report on net neutrality in 2014 to analyse the need for regulation.[67] However, the draft law is limited to comprehensive obligations to disclose restrictions. In the foreseeable future, Switzerland will probably not prescribe net neutrality. However, various stakeholders have already announced that they will address the topic of net neutrality during the debate on the TCA revision in Parliament.

It remains to be seen whether the transparency rules and the associated risk of public criticism will discourage internet providers from violating net neutrality. It is also conceivable that the topic will not have the same impact in Switzerland as in other countries due to the high standard of the network infrastructure and the structure of providers' product offerings.

In the US as well as in the EU, there is a basic obligation of transparent disclosure of restrictive measures. It is therefore the task of civil society to monitor developments in the field of net neutrality and to intervene if necessary.

6.2 Cyber parasites: when malware hijacks your CPU

The success of cryptocurrencies offers extremely tempting prospects for cyber criminals. Section 5.4.3 of this report, for example, discusses large-scale bitcoin theft. But criminals have also spread out elsewhere by abusing the mining typical of this type of currency. Mining is the

[65] Regulation (EU) 2015/2120, http://eur-lex.europa.eu/eli/reg/2015/2120/oj (as at 31 January 2018).

[66] Overview on the website of the Federal Office of Communications: https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesgesetze/fmg-revision-2017.html; dispatch on revision of the Telecommunications Act: https://www.admin.ch/opc/de/federal-gazette/2017/6559.pdf; draft law: https://www.admin.ch/opc/de/federal-gazette/2017/6705.pdf (as at 31 January 2018, available only in German, French, and Italian).

[67] https://www.bakom.admin.ch/bakom/en/homepage/digital-switzerland-and-internet/internet/net-neutrality.html (as at 31 January 2018).

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[68]). In the meantime, attacks that abuse computing power for mining have multiplied. 2017 was particularly eventful in this respect – so much so that some experts are wondering whether this may be one of the most lucrative business models for cybercriminals. Additionally, certain types of malware were used for mining, although other criminal options would also have been possible. One example of this is WannaMine: a sophisticated malware that spreads particularly via the EternalBlue exploit, already used by the ransomware WannaCry and NotPetya. Unlike the latter, however, the WannaMine criminals used this to create virtual currency once it is installed, instead of encrypting user data.

Installing malware is not the only way a computer can be used to mine cryptocurrency without the user's knowledge. Certain websites also contain scripts that are used to mine cryptocurrency via the visitor's browser. Some website operators request the consent of visitors, who then consciously make their computers available in order to participate in the financing of a website. Others do not bother to do so. In many cases, websites are manipulated to place such scripts without the operator's knowledge.

While using a computer's resources may seem less harmful than other forms of attack such as data encryption, the damage potential of such attacks should still not be underestimated. First of all, the price of secret mining is the power consumed by the computing resources used. In addition, stability problems or crashes can result if the malware makes use of computing power that otherwise would be allocated to other processes. This is all the more worrying when sensitive systems are affected. There is also a risk of interruption when such software is removed.

The development of this type of attack indicates that the cost-benefit ratio is currently very attractive. For criminals, these methods must be implemented on a large scale in order to be profitable; the computing power of a few machines does not suffice. In return, however, this type of attack offers the advantage of regular income. An infected machine simply starts making money automatically. Ultimately, this is the most direct link between infecting a computer and generating income. Moreover, this type of manipulation has the advantage that it is often difficult to detect. The goal is therefore to have a large number of computers at the attackers' disposal, each of which generates a small amount of money discreetly, regularly, and with as few interruptions as possible. The most worrying question is what will happen to these infected machines if the process becomes less financially attractive someday. Then there is a danger

[68] 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 January 2018).

that the malware will be converted for other uses that may be more destructive. It would therefore be naive to regard secret mining simply as harmless parasitism.

6.3 Outsourcing? Then safely!

In today's globalised and specialised world, virtually no company can afford to run all business processes in-house. To be competitive, processes must be designed as efficiently as possible and costs must be kept low. Outsourcing certain services can contribute to optimisation. However, safety must be a crucial factor when choosing an external partner. The cheapest provider is not necessarily the safest. While services can be outsourced, responsibility and risk never should. When outsourcing, each company must always consider what data it wants to hand over to someone else and what the impact on the company would be if this data were compromised. Data whose loss would lead to an existential threat to the company does not belong in the hands of third parties.

Swedish Prime Minister Stefan Löfven had to experience this for himself. In July 2017, he had to admit to the media that data belonging to the Swedish military, the driving licence authority, and even the witness protection programme was in danger of being accessed without authorisation. The authority had previously outsourced its IT administration to the IBM computer company. IBM in turn commissioned subcontractors in the Czech Republic and Romania. While all the files concerned were stored in Sweden, technicians from both subcontractors had access to them without a security check. The authority did stress that there was no evidence of data misuse.

Recommendation:

In order to prevent such unpleasant surprises, precise requirements must be defined in advance of such projects, and an IT security concept must be developed for the outsourced areas. The risks involved in outsourcing data and the measures to be taken to minimise these risks must be precisely defined. It is important to engage in honest risk management, not to downplay risks, and not to be blinded by cost savings. Measures to be taken include, for instance, a clear definition of access rights, the involvement exclusively of authorised persons in both the installation and maintenance processes, and the encryption of data during transport and storage. In addition to regular data backups, the requirements also include secure physical access controls. Companies should not simply trust in the promises of service providers, but rather must demand and check their assurances regularly (for example in the form of security certificates). In advance measures must also be defined in the event of an incident despite all precautions.

Conclusion:

The complexity of risk management, especially for outsourced services, will continue to grow in the coming years. This was exemplified by the hardware vulnerabilities Spectre and Meltdown that became known at the turn of the year. Hardware can also contain vulnerabilities, and no element in an IT system can be considered absolutely secure. Accordingly, a security policy must consist of a wide range of (organisational and technical) measures in order to keep the risk of a vulnerability in a component as low as possible. Virtualised environments and outsourced services were particularly affected by these vulnerabilities. Companies processing data in third-party data centres must therefore be assured that the data centre operators have taken all necessary precautions to minimise the risks of a vulnerability. In such cases, guarantees regarding measures taken may be demanded contractually.

7 Politics, research, policy

7.1 Switzerland: parliamentary procedural requests

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Ip	17.4285	Clearly defining the role of actors in the field of cyber defence and cyber security in Switzerland	Fathi Derder	15.12.2017	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174285
Ip	17.4100	Digitalisation of foreign and security policy. Risks and opportunities for Switzerland?	Damian Müller	13.12.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174100
Ip	17.4004	Need for an overview – and also for coordination?	Sylvia Flückiger-Bäni	30.11.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174004
Ip	17.3905	Cyber Risk Act	Sibel Arslan	29.09.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173905
Po	17.3875	Armed Forces. Strengthening scientific research, deepening cooperation with research institutions	Fathi Derder	29.09.2017	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173875
Mo	17.3849	Swiss Armed Forces. How can our sovereignty and independence be safeguarded when digitalisation increases interdependencies?	Claude Béglé	28.09.2017	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173849
Ip	17.3731	Comprehensive cyber security for everyone instead of cyberwar only for the DDPS	Edith Graf-Litscher	27.09.2017	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173731
Ip	17.4296	Fair taxation of internet giants. For an equalisation tax on sales generated online	Balthasar Glättli	15.12.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174296
Ip	17.4090	Measures against discriminatory tendencies	Nadine Masshardt	13.12.2017	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174090

Ip	17.3864	Illegal offers on the internet. Reducing losses and risks	Raphaël Comte	28.09.2017	CS	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173864
Ip	17.4314	What was the role of Swiss Post in Amazon's market entry in Switzerland?	Regula Rytz	15.12.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174314
Po	17.4249	Expanding the mountain region into a data and digitalisation hub	Martin Candinas	15.12.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174249
Po	17.4041	Fewer traffic accidents thanks to driving assistants? More data on driving assistance systems and their impact on safety	Jürg Grossen / Green Liberal Group	07.12.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174041
Qu	17.5619	Should social media be subject to the Radio and Television Act?	Edith Graf-Litscher	06.12.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175619
Qu	17.5614	Is the legal basis sufficient against the distribution of fake news via social media?	Edith Graf-Litscher	06.12.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175614
Qu	17.5592	Cyber defence. Capacities for strategic communication and management of information operations	Priska Seiler Graf	05.12.2017	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175592
Ip	17.3896	How can a digital platform be created across all public transport modes?	Claude Béglé	29.09.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173896
Ip	17.3870	Expansion of the mobile network	Susanne Leutenegger Oberholzer	29.09.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173870
Mo	17.3847	Internet of things. Designing the framework for a national and international ecosystem	Claude Béglé	28.09.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173847
Ip	17.3733	Civilian drones. Can the dangers be ignored?	Manuel Tornare	27.09.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173733
Ip	17.3734	Hate speech on social networks. Just let it be?	Manuel Tornare	27.09.2017	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173734
Ip	17.3723	Swisscom's mobile network. How should the mobile phone coverage figures and the network coverage map be interpreted?	Jacques Nicolet	25.09.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173723
Qu	17.5397	Securing Switzerland's locational advantage with an efficient 5G mobile network	Karl Vogler	13.09.2017	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175397
Po	17.4017	Seizing the opportunities offered by "Civic Tech"	Damian Müller	04.12.2017	CS	FC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174017
Po	17.4295	Reviewing security standards for internet of things (IoT) devices because they are one of the biggest threats to cyber security	Balthasar Glättli	15.12.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174295

Po	17.4273	Regtech solutions: encouraging their dissemination among economic operators and public authorities	Claude Béglé	15.12.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174273
Ip	17.4062	Optimising the validator.ch validation service	Marcel Dobler	12.12.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174062
Ip	17.3854	A second chance for a digital tax	Géraldine Savary	28.09.2017	CS	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173854
Ip	17.3717	Consequences and challenges of digital transformation for the Federal Office of Culture	Kathy Riklin	25.09.2017	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173717
Qu	17.5415	Cryptocurrencies. Production, use, governmental control, damage potential	Maximilian Reimann	18.09.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175415

7.2 The Global Commission on the Stability of Cyberspace and the Call to Protect the Public Core of the Internet

The Global Commission on the Stability of Cyberspace (GCSC) was launched at the Munich Security Conference in February 2017 and comprises prominent Commissioners representing a wide range of geographic regions as well as government, industry, technical and civil society stakeholders. Its mission is to enhance international peace, security, and stability by proposing norms and initiatives to guide responsible state and non-state behaviour in cyberspace.

In November 2017, GCSC Commissioners issued a “Call to Protect the Public Core of the Internet“, in which all stakeholders are urged to adhere to the following norm that sustains the general availability and integrity of the Internet:

Non-Interference with the public core

Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

According to the Commission, elements of the public core include, inter alia, Internet routing, the domain name system, certificates and trust, and communications cables.

Conclusion:

Modern society relies more and more on connected information technology and becomes increasingly dependent on the stable and predictable function of it. With view to the interconnected global cyberspace, consequences of actions affecting the public core of the internet may have global effects and unintended consequences as well as collateral damage becomes very difficult to predict. It is therefore in the interest of all actors that have the good of humanity in mind to refrain from activities that put the general functionality of cyberspace in danger as well as help prevent and mitigate such activities.

8 Published MELANI products

8.1 GovCERT.ch blog

8.1.1 The Retefe saga

03.08.2017 - Surprisingly, there is a lot of media attention going on at the moment regarding a macOS malware called OSX/Dok. In recent weeks, various antivirus vendors and security researchers published blog posts on this threat, presenting their analysis and findings. While some findings where very interesting, others were misleading or simply wrong.

➔ https://www.govcert.admin.ch/blog/33/the-retefe-saga

8.1.2 Leaked accounts

29.08.2017 - MELANI/GovCERT has been informed about potentially leaked accounts that are in danger of being abused. MELANI/GovCERT provides a tool for checking whether your account might be affected: https://checktool.ch

➔ https://www.govcert.admin.ch/blog/34/leaked-accounts

8.2 MELANI newsletter

8.2.1 E-banking: Attackers targeting activation letters

17.08.2017 - At the end of 2016, MELANI pointed out in a newsletter that criminals are increasingly targeting mobile authentication methods in e-banking. Now attackers are going one step further and are trying to get victims to send a copy to the fraudsters of the letter received from the bank containing activation data for the two-factor authentication (2FA) necessary for e-banking.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html

8.2.2 21,000 access data records for internet services stolen

29.08.2017 - The Reporting and Analysis Centre for Information Assurance (MELANI) received about 21,000 access data records consisting of usernames and passwords that were evidently stolen and are now being misused for illegal purposes.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-21000-e-mail-konten-im-umlauf.html

8.2.3 Encryption Trojans and malicious emails in name of authorities on the rise

02.11.2017 - The 25th semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI), published on 2 November 2017, addresses the most important cyber incidents of the first half of 2017 both in Switzerland and abroad. The encryption Trojans Wanna Cry and NotPetya, which made the headlines worldwide in spring 2017, are the focal point of the report..

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/semi-annual-report-1-2017.html

8.2.4 70,000 access data records for internet services stolen

05.12.2017 - The Reporting and Analysis Centre for Information Assurance (MELANI) again received a list of access data consisting of usernames and passwords. This time there were 70,000 data records.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-70000-e-mail-konten-im-umlauf.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.
App	"App" (an abbreviation of "application") generally refers to any type of application program. In common parlance, the term now commonly refers to applications for modern smartphones and tablet computers.
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.
Backup	"Backup" means the copying of data with the intent of copying it back in the event of data loss.
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.
Browser	Computer programs that are mainly used to display diverse content in Web pages. The most well-known browsers are Internet Explorer, Opera, Firefox and Safari.
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.
Certificate	A digital certificate is the cyberspace equivalent of a personal identity card and is used to assign a specific public key to a person or organisation. This assignment is certified by the certification body by providing it with its own digital signature.

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.
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).
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.
Encryption Trojans/ Ransomware	A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts or deletes data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.
Ethernet	Ethernet is a technology for wired data networks.
Exploit-Kit	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
Hash function	A hash function maps a large input quantity (the keys) to a smaller target quantity (the hash values).
Industrial control systems (ICSs)	Control systems consist of one or more devices that control, regulate, and/or monitor the behaviour of other devices or systems. In industrial production, the term "industrial control system" (ICS) is often used.

IP-Address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
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.
Malware	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Managed service providers (MSP)	A managed services provider (MSP) is an information technology service provider which assumes the responsibility for the provision of a defined series of services for its client and manages these services.
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.
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.
Plug-in	A plug-in is an optional software module that extends or changes existing software.
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.
RAM	Random-access memory (RAM) is a data storage system which is used particularly in computers for data storage that is usually in the form of memory modules.
Remote Administration Tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
RootKit	A collection of programs and technologies which allow unnoticed access to and control of a computer to occur.
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.
RSA encryption	Abbreviation for Rivest-Shamir-Adleman encryption. Encryption method with public keys, introduced in 1978. RSA is an asymmetric method.
Salts	In cryptography, salt refers to a randomly selected character string that is appended to a given plain text before being used as an input to a hash function in order to increase the entropy of the input.
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.
Spearphishing emails	Targeted phishing attack. For example, victims are tricked into believing that they are communicating with someone they know by email.
SQL injection	SQL injection refers to the exploitation of a vulnerability in connection with SQL databases, resulting from insufficient verification of the variables to be transmitted. The attacker attempts to inject his own database commands in order to change the data as desired or to gain control over the server.
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.
Troll	In net jargon, a troll is a person who limits communication on the internet to contributions that aim at emotional provocation of other participants in a conversation.
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.)
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.
Web browser	Computer programs that are mainly used to display diverse content in Web pages. The most well-known browsers are Internet Explorer, Firefox and Safari.
WLAN	WLAN stands for Wireless Local Area Network.
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.