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

INFORMATION ASSURANCE

SITUATION IN SWITZERLAND AND INTERNATIONALLY

Semi-annual report 2018/II (July – December)

30 APRIL 2019

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

1 Overview / Content

2 Editorial

The current and future role of the state in the cyber area

Dr Myriam Dunn Cavelty is Deputy Director at the Center for Security Studies at ETH Zurich where she researches and teaches cybersecurity policy.

Only ten years ago, cybersecurity was a niche issue that was primarily discussed in technical expert circles. In the meantime, due to a worsening threat situation, it has become a permanent security policy issue that is dealt with in the highest government circles.

Here the role of the state and its bureaucracy is subject to a political negotiation process that has not yet been completed in many countries of the world. Cybersecurity is an overarching issue that overlaps with many other policy areas. One of the main challenges in times of scarce resources is to find the right mix between new structures and efficient use of existing skills and to integrate relevant actors from business and society in a meaningful way. In comparison, the (vertical) integration of national cybersecurity strategies into the framework of national security and into a comprehensive overall strategy across all policy areas as well as the (horizontal) coordination and control of the various units in the cybersecurity environment prove to be particularly difficult.

There is a consensus that a satisfactory level of cybersecurity can only be achieved if government, business and society work in unison. However, the different sectors often pursue different objectives and interests. This gives rise to at least three areas of tension in which every cybersecurity policy must be positioned.

In the first area of tension between the state and business, a policy must be formulated to secure critical infrastructures, which absorbs the negative consequences of liberalisation, privatisation and globalisation from the point of view of security policy without hindering the positive effects. In the second area of tension between state and citizen, it is necessary to find the politically desired balance between more security and safeguarding civil rights in digital space. In the third area of tension between citizens and business, it is necessary to set the framework conditions for the development of a successful security ecosystem, in which an optimal balance between security and functionality is created and incentives for more security obligations for service providers are created.

What is self-evident for business and civil society actors also applies to the state: it plays a variety of roles at the same time. The recognition of the diversity of state action is a good starting point for dealing with role conflicts at the political level and systematically addressing them, thus shaping a proactive policy for the future.

Myriam Dunn Cavelty

3 Key topic: dealing with manufacturers of critical hardware and software solutions

Not only since the Snowden documents have manufacturers of hardware and software of certain states been in the spotlight. Shortly after the Chinese manufacturer Huawei entered the global market, doubts about the integrity of its products and independence from the authorities were raised. The Snowden leaks in 2013 confirmed at least part of the suspicion that US manufacturers such as Cisco, Microsoft, Google and others were also granting the authorities access to their products for the purpose of monitoring users. On the basis of accusations of Russian espionage in the USA, in 2017 the US authorities imposed a ban on the use of Kaspersky products within US federal authorities. In Switzerland, this topic is also being discussed in business and at the administrative level.

On the one hand, with regard to precautionary safety measures, there are good reasons to take a closer look at the use of products from certain manufacturers. On the other hand, however, a not insignificant part of this discussion is also due to purely economic policy interests. A differentiated, manufacturer-independent discussion is therefore required.

3.1.1 Hardware and software as a means to an end for state interests

With the increasing digitalisation of business processes, the hardware and software solutions required for this form a central and critical component. At first glance, the supplier market appears to be extremely diverse and broadly based with a view to a wide variety of solutions. If one looks at the countries of origin of the providers, however, this apparent diversity is not what it seems. The market is clearly dominated by US companies, closely followed by China and isolated global players such as Korea (Samsung), Russia (Kaspersky) and Germany (SAP).

An analysis of the legal bases applicable in the countries of origin with regard to the local information and communication technology (ICT) industry shows that it is not just a welcome economic engine. Their central status in the processing, delivery and storage of information is well recognised and the corresponding aspirations of state authorities are legally anchored.

The fact of the matter is that without hardware and software solutions from US, Chinese and other companies, the dense digitalisation of processes as we know them today will not take place. And this digitalisation is accompanied by the theoretical simplification of access to the ICT systems of domestic manufacturers and thus to the stored, processed or delivered information.

3.1.2 Manufacturer exclusion, cyber sovereignty and international standards

The potential access to ICT manufacturers by the respective countries in which they are registered and the associated possibility of gaining global control over hardware and software lead to discussions about how to deal with these risks properly.

In principle, some of the approaches practised are aimed at manufacturers and providers of hardware and software solutions in the broadest sense.

Manufacturers can generally be excluded from the procurement process if they are suspected of being a means to an end of a country. This happened, for example, in the US administration, which in December 2017 prohibited the use of products of the Kaspersky Group, which is domiciled in Russia. Also with regard to the procurement of Huawei products, demands have

emerged in various countries in recent weeks and months to exclude this manufacturer from the procurement process.

In the short to medium term, these approaches can offer apparent (security) solutions in order to avoid the possibility of foreign government control of digital processes. In several countries, including Switzerland, a general discussion is taking place on how to extricate oneself from dependence on the two de facto technology giants USA and China.

At the level of international security policy, too, the issue of government access to and intrusions into manufacturers of ICT solutions has been an issue for some time. For example, the 2015 report of the UN Group of Governmental Experts set the first standards to curb such action. However, the 2017 follow-up report, which should have specified these standards, failed to reach the necessary consensus in a much rougher intergovernmental climate.

3.1.3 Hardware and software manufacturers are and will remain at the mercy of state interests

In Orwell's Nineteen Eighty-Four, a pessimistic allegory set on the nature of absolute power, the credo that whoever controls the past controls the future, and whoever controls the present controls the past is repeated several times. At the centre of this statement is the idea of absolute, unhindered access to information and data. None of the countries of origin of the leading ICT manufacturers is said to have the same global-totalitarian intention. The fact, however, that within the framework of the existing legal bases, information and data can be accessed selectively via the domestic hardware and software manufacturers represents a striking comparative advantage that none of these states will voluntarily and autonomously give away.

It is against this background that the public statements of the USA must be seen, which do not want China to replace the USA in terms of technology leadership. Accordingly, sanctions and manufacturer bans are to be understood as purely economic and security policy decisions, which are only conditionally based on differentiated security concerns in the sense of self-protection. A decline in the number of ICT components sold by US manufacturers is accompanied by a loss of selectively targeted control over these hardware and software solutions in the end customer's operations.

Manufacturers of ICT solutions will be at the mercy of the interests of their countries of origin and will continue to be obliged, in accordance with the applicable legal bases, to cooperate with the relevant government units. It cannot be assumed that, even in extreme cases, any private company will violate the law in its home country. And it is still foreseeable that China and the USA will continue to fight for dominance in the battle for global shares of ICT products.

3.1.4 Lack of alternatives

It is more than questionable whether Switzerland, as an industrial location, could in the foreseeable future develop any alternatives at all to the predominant hardware and software solutions of foreign suppliers. Even a coordinated industrial policy in this area, which is unusual for Switzerland, would only have a long term effect, if at all. However, the digitalisation of business processes, "eHealth", the development of 5G and the like is already taking place today and the ICT components and solutions required for this are practically not produced at all, or only in small amounts, at great expense in Switzerland.

As a small, open economy, Switzerland is on the one hand dependent on foreign ICT manufacturers. At the same time, it can also benefit from being able to balance the different interests

of different countries with corresponding leading ICT industries. The Swiss economy will continue to depend in part on foreign ICT manufacturers for digitalisation. Thus, consistent risk management should be established with a view to possible government intervention and enforcement, which addresses handling manufacturers, suppliers and providers of hardware and software solutions throughout.

Assessment:

The above findings lead to the following fundamental assessments of the threat situation in the area of ICT manufacturers with foreign parent companies:

- The legal instruments of those countries in which the most important global players in the field of hardware and software solutions are located legitimise practically all information gathering about foreign objectives, provided this is in the interest of the respective states.
- A purely contractual obligation on the part of ICT companies to comply with Swiss law cannot be regarded as a sufficient guarantee. This would have to be subject to conditions and accompanied by periodic onsite audits. This also includes facilities abroad, insofar as these are suitable for exerting technical or organisational influence on the Swiss company affiliated in terms of organisation or ownership.
- Depending on the hardware and software as well as the selection of service providers, appropriate measures should be taken to prevent unauthorised access to systems and data as far as possible, but at least to detect and stop such access.
- Risk-adequate measures must be planned in every procurement project and included in the costs. For example, it may happen that the apparently most competitive offer from a provider leads to additional internal costs as a result of indicated accompanying measures or that an additional service would have to be purchased for control and protection.

4 Situation in Switzerland

4.1 Espionage

4.1.1 Cyber-attack on the Organisation for the Prohibition of Chemical Weapons (OPCW) – Spiez Laboratory also a target

In the last semi-annual report, MELANI reported here on the misuse of a publicly available invitation to an international conference of the Spiez Laboratory. In order to carry out a targeted attack and to induce the recipients to open an attachment, the attackers took this invitation as a template and subsequently sent it to various recipients with a bogus sender on behalf of the Federal Office for Civil Protection (FOCP) and the Spiez Laboratory.

The fact that the Spiez Laboratory is also directly targeted by attackers is shown by the news that became public knowledge in September 2018 of the arrest of four people, which took place

in the Netherlands[1] on 13 April 2018. The arrested persons were accused of attempted intrusion of the wireless network of the OPWC. The four alleged Russian employees of the military secret service GRU allegedly entered the Netherlands via Schiphol airport with diplomatic passports and then rented a car, which they parked in the parking lot of the Marriot Hotel in the Hague. This is located directly next to the offices of the OPCW. In the boot of the car, equipment was seized that could be used to gain access to radio networks and could be used for cyber-attacks. The antenna for the operational device was hidden under a coat on the rear shelf of the car. The four people arrested were deported from the Netherlands on the same day and had to leave their equipment behind.

As it turned out, this group was also interested in the Spiez laboratory. Among other things, a train ticket was found in the luggage of those arrested for the journey from Utrecht to Basel. On a notebook computer, investigators discovered search queries to the consular section of the Russian embassy in Bern and to the Spiez laboratory[2]. Both the OPCW and the Spiez laboratory were involved in the investigations into the poisoning of former Russian double agent Sergei Skripal and his daughter in March 2018 in Salisbury in the UK. As the Federal Intelligence Service (FIS) confirmed, it was actively involved in this operation together with its Dutch and UK partners, thus contributing to the prevention of illegal action against critical Swiss infrastructure.

The Spiez laboratory had already fulfilled the requirements for particularly endangered premises in advance. Nevertheless, protection was further increased and additional measures were taken to further improve safety standards.

4.1.2 Operation "Sharpshooter" targets critical infrastructures

In December 2018, security firm McAfee released a report on a newly discovered APT campaign against defence, energy, nuclear, and financial companies[3]. The campaign called "Sharpshooter" began on 25 October 2018 with the sending of weaponized documents to individuals from 87 organisations around the world, mainly in the USA. According to the report, Swiss companies in the financial sector were also hit by the campaign. The Federal Intelligence Service has so far found no traces of infection in potentially affected companies in Switzerland.

Social engineering was used to get the recipients to open the infected documents. The letter was disguised as a letter of application and contained a link to a document on Dropbox which allegedly contained the application dossier. This method is particularly insidious because HR departments often receive unsolicited applications and therefore usually open such documents. However, companies with correctly implemented security measures did not run a major risk of becoming victims of this attack. The infection occurred via a macro contained in the Word document. Such macros are now blocked in many companies, or are activated only after confirmation of a corresponding warning message. If the macro is executed despite all warnings, the malware will smuggle Sharpshooter into the working memory of Word. The malware then installs a modular backdoor called "Rising Sun". The functions of this component include

---

1 https://www.government.nl/government/members-of-cabinet/ank-bijleveld/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw (as at 31 January 2019)

2 https://www.justice.gov/opa/page/file/1098571/download (as at 31 January 2019)

3 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf (as at 31 January 2019)

collecting and sending information about documents, user names, network configuration, and system settings. The malware can also reload other functions. The malware also has the ability to cover its traces so as not to be detected. In this way it can empty the memory or delete its activities. The malware communicates via a command and control server controlled by the attackers.

In analysing the campaign, McAfee found evidence of connections to the "Lazarus" group: "Rising Sun" contains code and configuration data from the "Duuzer" family. Duuzer was also used in the hacker attack on Sony, which is associated with the Lazarus group. Several cyber security companies have linked these attacks to North Korea. However, a different decryption routine is used in the current case. This in turn suggests that Rising Sun could be a further development of Duuzer. Whether this campaign can really be assigned to the "Lazarus" group cannot therefore be conclusively clarified. Methods, traces and malware are now known worldwide, and would be also suitable for so-called false-flag operations. This involves an attempt to direct the suspicion to uninvolved third parties.

4.2 Industrial control systems

4.2.1 Industrial control systems and IoT

Fortunately, there were no spectacular sabotage attacks in the second half of 2018. No targeted attacks against industrial control systems have been publicised, but infections generated with traditional malware, such as ransomware in control system networks abroad, have generated some attention[4] (see also chapter 5.3.5). Modern networked systems are continuously put into operation and older, previously isolated systems are also connected to the internet in order to increase efficiency through integration into other business processes. With the networking and integration of various things into the internet (internet of things [IoT]), the risk of being affected by the complex dangers of the internet, which may be directed against accessible vulnerable systems, also increases.

4.2.2 No success for hackers in Ebikon - commune fends off alleged attacks on water supply

Switzerland is known for its high-quality drinking water. In order to ensure the supply, the communes go to great cost and renew their facilities at regular intervals. In the case of such renovations, the most modern control systems are also installed. Even delegations from other European countries want to be informed about the operational experience in Switzerland with the new systems[5].

Unfortunately, attackers from all over the world are also interested in such systems. Last autumn, for example, the commune of Ebikon registered several thousand attempts to access the autonomous operational control network of its water supply[6].

Attackers with various motivations are constantly on the lookout for externally accessible services. They test them for vulnerabilities and try to penetrate the systems found with known

---

4 https://dragos.com/year-in-review/ (as at 31 January 2019)

5 https://www.ebikon.ch/verwaltung/aktuelles/news/daenemark-auf-besuch-in-ebikon (as at 31 January 2019, only available in German)

6 https://www.inside-it.ch/articles/53204 (as at 31 January 2019, only available in German)

standard access data as well as with identities which have been stolen elsewhere. In the case of Ebikon, the attempts were fortunately unsuccessful and as a side effect, the discovered attack attempts served to readjust the security measures. However, even in the event of a successful attack and the failure of prevention and detection, the commune would have been able to shut down the automated systems and continue to operate the facilities manually.

The Ebikon case is an example of how measures in various phases of the Cyber Security Framework[7] can help fend off real attempts to attack a vital infrastructure and, if necessary, respond to them. It is worth investing not only in preventive protection, but also in precautions to be taken in the event of an incident. The ICT minimum standard of the Federal Office for National Economic Supply (FONES) offers an approach for implementation, which are based on the Cyber-Security Framework.

Recommendation:

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

The minimum standard to strengthen ICT resilience includes the following functions: identify, protect, detect, respond and restore. In addition, it offers users 106 specific instructions on how to improve their ICT resilience to cyber risks:

Minimum standard to strengthen ICT resilience

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

4.2.3 MadIoT – the potential danger of a botnet from household appliances

The power cut in Italy on 28 September 2003 is probably still remembered by many. A chain reaction overloaded the transmission networks and cut off the electricity throughout the country[8]. This power blackout was due to an electrical flashover to a tree in Switzerland, Several unfortunate circumstances led to this instability and congestion of the electricity grid. But what would happen if this instability was deliberately caused by manipulating the electricity consumption of a large number of household appliances?

Researchers at Princeton University made this kind of reflection as part of a study[9] that they presented at the USENIX Security Conference in August 2018. The study is based on the

7 https://www.nist.gov/cyberframework (as at 31 January 2019)

8 http://www.rae.gr/old/cases/C13/italy/UCTE_rept.pdf (as at 31 January 2019)

9 https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf (as at 31 January 2019)

assumption that a malicious actor succeeds in building a botnet of internet of things (IoT) devices with high power consumption such as air conditioners, heaters and washing machines. If their power consumption is geographically coordinated and influenced to a large extent unexpectedly, the scenarios of the researchers could lead to similar instabilities in the power grid as those that provoked the blackout in Italy mentioned previously[10].

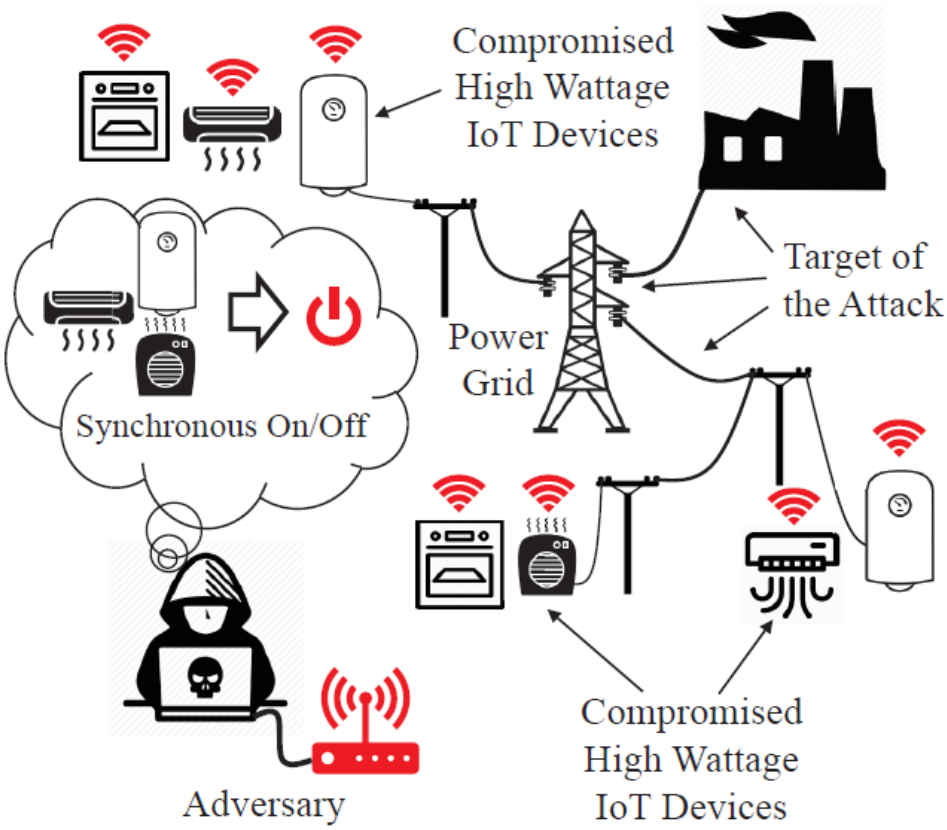

Figure 1: Schematic diagram "Manipulation of demand via IoT" (source: usenix.org, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf))

The novelty of the attack scenarios described is that the failures are not caused by impairment of energy production or transmission, but are targeted at the consumer side. In many cases, consumers' terminal equipment is only marginally protected, especially in comparison to power plants or transmission grids, where many resources have been invested in security for years.

The stability of the electricity grid is based on the reliability of consumption forecasts, which are mainly based on past experience. Coordinated manipulation of vulnerable devices with high consumption, contrary to consumption forecasts, allowed the usual tolerance reserves to be exceeded. As an example, in the height of summer all electric heaters could be switched synchronously to full blast by an attacker. This procedure is called manipulation of demand via IoT (MadIoT).

10 https://securityintelligence.com/how-an-iot-botnet-could-breach-the-power-grid-and-cause-widespread-blackouts/ (as at 31 January 2019)

The assumptions underlying the simulations may seem far-fetched. However, the impact of the Mirai botnet in 2016 impressively demonstrated the damage potential of an IoT botnet. As early as 2017, the British security software company Sophos showed in a trial that exposed IoT devices in smart homes could be attacked from many sides in a short period of time[11]. The security service provider also noted a high concentration of such exposed IoT devices in Switzerland.

Not only operators of energy infrastructures, but also manufacturers of IoT devices must make their contribution so that such attacks do not become reality. There are many efforts to define minimum best practices. However, these are still only mandatory in very few regions and areas. An interpretative document[12] of the UK Department for Digital, Culture, Media & Sport (DCMS) provides a good overview and compares existing standards and guidelines.

Recommendation:

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

MELANI reporting form

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

Checklist with measures for the protection of industrial control systems

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

4.3 Attacks (DDoS, defacements, drive-bys)

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

4.3.1 Quickline modems abused for SNMP amplification attacks

As reported by the internet provider Quickline in a press release on 11 October 2018, it had to struggle with irregular disruptions for two weeks. The disruption affected television, internet and telephony services, although the problem did not occur in the same way and to the same extent for all customers. A vulnerability in a modem type was identified as the cause. Analyses revealed that customers were not directly targeted by the attackers. They were merely a means to an end to carry out an attack on third parties. This was a so-called SNMP amplification attack. In the process, the Simple Network Management Protocol of the devices is used to amplify a request and ultimately direct it to the target in order to overload it. The modems are

11 https://www.computerworld.ch/security/hacking/smart-home-in-minuten-hacker-da-1435426.html (as at 31 January 2019, only available in German)

12 https://iotsecuritymapping.uk/ (as at 31 January 2019)

not infected for this purpose; instead, the attacker simply uses the fact that the SNMP system is openly available to the outside world. The customer disruptions occurred because the requests unintentionally overloaded the modems too and are likely to have caused instabilities. Since not all Quickline customers use the same modem types, only 5%, or around 9,000 customers, were affected. It is not known how long the modems were vulnerable to SNMP amplification attacks. Quickline took several measures to eliminate the vulnerability. These included mainly filters in the network and additional protection for the modems concerned. Quickline has taken legal action.

4.3.2 Tax data online – app with wrong setting

Filling out a tax return is not exactly a favourite pastime for many people and is often painstaking. That is why a Zurich company called Zurich Financial Solutions (www.zufiso.ch) developed the smartphone app Steuern59.ch, which is intended to make the whole process easier. Steuern59.ch can be purchased and downloaded from the Play Store or App Store. The app promises to take care of completing the tax return for only CHF 59.00. All you have to do is photograph the necessary documents with your smartphone and upload them to the app. However, it transpired that all of these sensitive documents were loaded onto an unsecured Amazon Web Services (AWS) cloud server, making them freely accessible to all AWS users. The data is private in the default settings and therefore not available to the public. A warning is displayed if you change these settings to public.[13] However, the programmers who were said to be from India hired to develop the app made a mistake: they put this setting to public and apparently forgot to set it back to private again. A security researcher discovered this misconfiguration and informed the operating company. He was not taken seriously by the company until he contacted the German magazine Heise.[14] This raises the question of how to deal with vulnerabilities discovered ("responsible disclosure"): How should security researchers report gaps detected and how should these reports then be dealt with by companies? The company that manages Steuern59.ch admitted to having outsourced the production of the app to India. They were apparently unaware of how carelessly the developers were working. 80 customers who used the app were affected. They were informed of the incident after the security vulnerability had been eliminated in collaboration with the security researcher. Furthermore, the data is now stored on a Swiss cloud called n'cloud.[15]

4.4 Social engineering and phishing

4.4.1 Repeated increase in fraudulent calls to companies again

At the beginning of July 2018, calls were again registered in which attackers posed as bank employees. Here the callers ask each time for the execution of payments or pretend to have to carry out an e-banking update which then needs testing.

The attackers typically try to convince the company's employees to install remote access software (e.g. NTR cloud, Teamviewer). They then connect to the victim's computer and pretend to perform an e-banking update. Subsequently, the perpetrators pretend that the update must

---

13 https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html (as at 31 January 2019)

14 https://www.inside-it.ch/articles/52273 (as at 31 January 2019)

15 https://www.heise.de/newsticker/meldung/Steuern59-ch-Geschaeftsfuehrung-entschuldigt-sich-fuer-Daten-leck-4169772.html (as at 31 January 2019)

be tested and try to convince the victim to enter his access data for the company's e-banking and to make a test payment in order to verify that the system is working. If the payment is protected by a collective signature, the fraudsters try to convince the victim to organise all authorised signatories to release the payment.

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

Recommendation:

The examples show how effective social engineering methods still are. Companies should check what information about the company is available online. Never disclose the email addresses of board members or employees on your company website, use impersonal email addresses (e.g. "bookkeeping@xyz.ch").

Be suspicious if someone with unusual concerns contacts you and be on the lookout when dealing with the caller. When confronted with unusual contacts and requests, it is recommended to telephone those concerned within the company to verify the accuracy of the request. Raise employees' awareness of these incidents, especially those in key positions.

Never pass on personal access data to third parties by telephone, email or on the internet. Financial institutions will never ask you to provide confidential personal information in a telephone call, email or text message.

Never install software or follow any links if you are requested to do so by telephone or in writing. Never allow unauthorised access to your computer. No bank will ask you to participate in tests of any security updates.

All processes which concern payment transactions should be clearly defined internally and complied with by employees consistently in all cases.

4.4.2 Extortion attempts – bluffing is a good way to make money

For some time now there has been a scam that is closely related to the use of social media. Usually contact is made by a very attractive person via social media. This person flirts with the potential victim and tempts him or her to expose themselves in front of the webcam. The victim does not know that they are being filmed. The victim is subsequently blackmailed with this video footage. This extortion method is called "sextortion". If no money is paid, the material is published. This scam involves considerable effort. Since there is direct contact between perpetrator and victim, the risk of being arrested is also increased.

Since March 2018 (in Switzerland since July 2018), criminals have been using a scam that involves significantly less effort and risk. They still claim in an email to have access to computers and webcams and threaten to publish pictures and videos with sexual content, In these cases, however, the attackers are bluffing and there are no pictures or video recordings because there was no personal contact. This scam is called fake sextortion. With the help of this fraud method, criminals collected quite a lot of money overall in the second half of 2018, despite the individual, small sums demanded. Based on the analysis of the bitcoin addresses in the emails reported to MELANI, and to which the ransom should have been paid, almost 100

bitcoins were paid in the second half of 2018. This is currently equivalent to approximately CHF 360,000. Because sending mass emails is practically free of charge, the corresponding profit is huge. Whether or not these bitcoin addresses are used solely for fake sextortion and by Swiss victims is unknown.

In the emails a password from a data leak is usually given as "proof" that the computer has been compromised. In most cases, however, this password is outdated. To convince the victim that the mobile phone has been compromised, mobile phone numbers are now also used. Such "non-sensitive" data from various data leaks has recently been increasingly published. In another variant, as proof that the e-mail account has been compromised, the message is sent with the user's own email address as sender. In fact, the sender is bogus, which can be done very easily and without much knowledge. The attacker does not need access to the email account for this purpose.

Blackmail emails are written in several languages, including German, French, Italian and English. The approach has not changed by and large. However, the criminals are constantly working on optimising the blackmail attempts to increase the pressure on the victims and persuade them to pay. The table below shows the main innovations used by criminals in 2018.

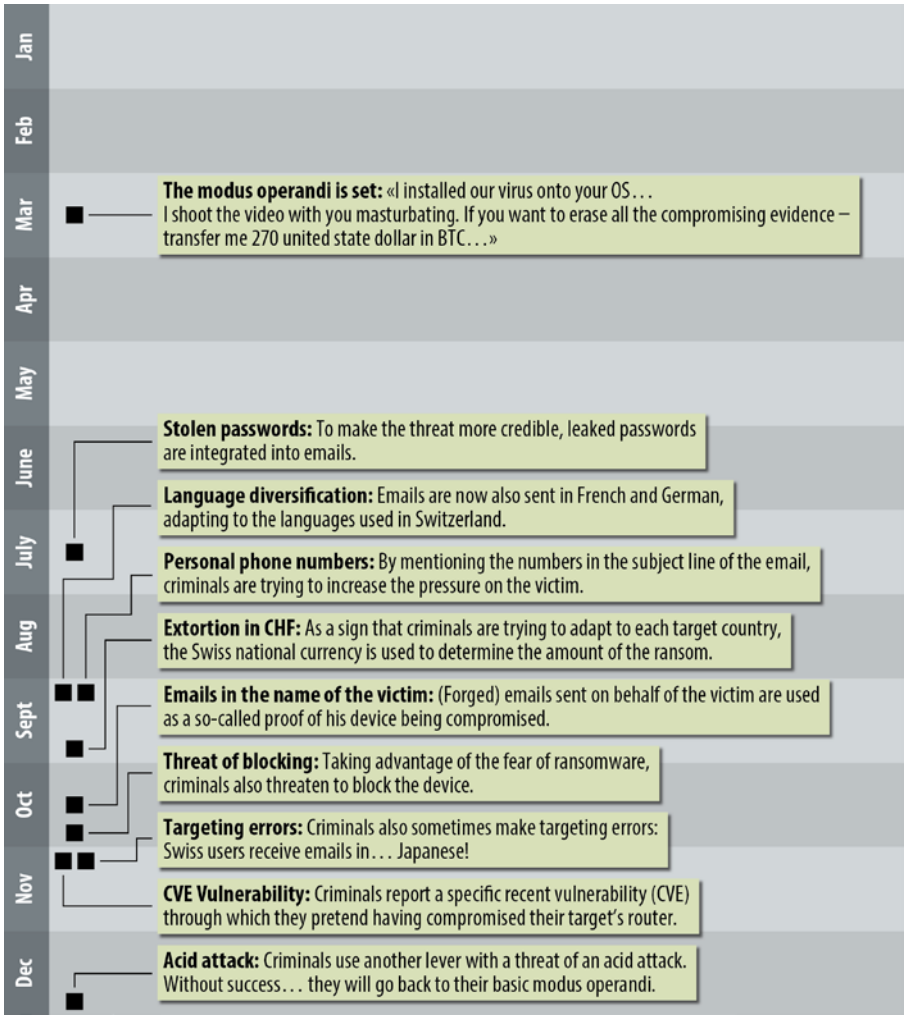

Figure 2: Development of fake sextortion variants in 2018

A subtype of this phenomenon is blackmail with threats of an acid attack or a bomb attack. With both types, a ransom is demanded in the form of bitcoins to halt the attack. However, it has been found that with the threat of physical consequences, the recipients are more likely to contact the authorities before they pay the ransom. This may be due to the greater potential for intimidation and the absence of apparently compromising material. In any event, no transactions could be detected on the Bitcoin addresses reported to MELANI in connection with this type of threat.

Recommendation:

However, so long as the recipients concerned do not stop paying the ransom demands, this scam will continue. It is to be expected that these waves will continue, that copycats will jump on the bandwagon and the number will increase even more. Under no circumstances should the ransom be paid. You can make a contribution to prevention by talking about these criminal tactics in your professional and personal circles. Raise the awareness of employees, acquaintances and relatives so that they will not fall for such machinations.

On the website https://www.stop-sextortion.ch , which was launched by the authorities, you can find information and report fake sextortion emails.

4.4.3 Office 365 access data used for transfer fraud

The fact that access data to Office365, the online version of Office products, is very popular with criminals has already been discussed in previous semi-annual reports[16]. With over 100 million monthly users, Office 365 accounts have become a popular target for attackers. The attack starts with an ordinary phishing email. This specifies, for example, that the storage space limit has been exceeded and that you should log in to resolve the problem. Of course, the indicated link leads to a fraudulent website.

During the reporting period, so-called wire fraud occurred with Office 365 access data obtained in this way. This is what happens when fraudsters search for existing electronic invoices in compromised accounts, then copy them, add a different IBAN and redeliver them. In particular, companies that issue large invoice amounts to foreign invoice recipients are targeted. On the one hand, the profit is particularly lucrative in these cases, on the other hand it is more difficult to detect an abusive recipient account, as these are foreign recipient accounts.

An example from the security service provider Proofpoint shows how sophisticated such attacks are. After gaining access to a company's CEO's Office 365 account, the attackers searched the emails and calendar for information to create an appropriate story. During a meeting between the CEO and a major supplier, which was recorded in the calendar, the attacker wrote to the CFO that he should transfer USD 1 million to close the deal. He further

[16] MELANI semi-annual report 2/2017 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2-2017.html (as at 31 January 2019)

wrote that he himself was stuck in a meeting and could not telephone. The CFO followed this request and paid.[17]

According to the US security authority, the FBI, this procedure, known as business email compromise (BEC), is now one of the most financially damaging. For example, the Internet Crime Complaint Center (IC3) in the USA has had BEC cases reported to it with total losses of USD 1.2 billion in 2018. Above all the real estate sector has been particularly affected by this type of attack. [18]

Recommendation:

If a company works in the Office 365 Cloud, attackers can use the stolen access data to access all the company's documents. Securing such data only with a user name and password is extremely negligent these days. Therefore, activate 2-factor authentication wherever possible. However, proper implementation is important. Even when using single sign-on or multi-factor authentication (MFA), compromise is possible if authentication is not implemented across systems. These vulnerabilities can then be exploited by attackers.

Employees should be sensitised to the fact that defined processes of the company and precautionary measures must be followed by everybody at all times. For transfers, for example, the dual control principle with collective signature is recommended.

4.4.4 Fake competitions

A year's supply of chocolate, an IKEA gift voucher or a new iPhone: purported competitions are very common on the internet. We already reported on this in our last semi-annual report[19]. The questions in all these competitions are chosen in such a way that everyone can easily answer them. The authors want as many players as possible to "win" and they thus get as many victims as possible. During the reporting period, a new variant emerged. Potential winners are lured via Facebook to a supposed Denner website because they have allegedly won CHF 750. After entering the telephone number and name, the participants are requested to call a 0901 number for which a charge is made. In order to get the supposed prize, as many questions as possible must be answered. In reality, the multitude of questions only serves to keep the victims on the chargeable line for as long as possible. It goes without saying that in actual fact there is no prize.

---

17 https://www.proofpoint.com/us/corporate-blog/post/microsoft-office-365-attacks-circumvent-multi-factor-authentication-lead-account (as at 31 January 2019)

18 https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf (as at 25 April 2019)
https://www.ic3.gov/media/2018/180712.aspx#fn2 (as at 31 January 2019)

19 MELANI Semi-annual report 1/2018
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2018-1.html6-2.html (as at 31 January 2019)

Recommendation:

Be critical about messages with enticing prize promises and do not forward them under any circumstances. The best thing to do is to ignore them.

INFO

Consumer protection has compiled various tips on this subject:

https://www.konsumentenschutz.ch/was-tun-bei-einer-abofalle/

4.4.5 Phishing

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

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

Overall, just 5756 different webpages which were indisputably phishing sites were reported in 2018 using the antiphishing.ch portal operated by MELANI. Figure 3 shows the number of reported phishing websites per week. The maximum in the last three months of 2018 is striking. The main reason was a large UBS credit card phishing scam during this period.

Figure 4: UBS credit card phishing scam in the last three months of 2018.

Several years ago, MELANI predicted that phishing sites would increasingly use encrypted websites with the URL "https://". However, this development was slower than expected. Since the third quarter of 2016, the security service provider PhishLab has recorded a continuous increase and, at the end of 2018, registered a 50% share of encrypted phishing sites for the first time.[20] However, this observation is probably to a great extent due to the fact that websites are increasingly being encrypted in general. Since a lot of phishing sites are hacked websites, the criminals "benefit" from this circumstance and use the encryption knowingly or partly also unknowingly at the same time.

4.4.6 Blocking applications in line with the Ordinance on Internet Domains (OID), Art. 15

To combat the misuse of Swiss Internet addresses and to defend against acute threats to internet users, the revision of the Ordinance on Addressing Resources in the Telecommunications Sector (TSRO, SR 784.104; in force as of 1 January 2010) includes a new provision according to which the ".ch" registry (SWITCH) must block domain names and cancel the respective assignment to a name server if there is justified suspicion that the domain name is being used either to obtain sensitive data by unlawful means (phishing) or to distribute malware via the domain and if an authority recognised by the Federal Office of Communications (OFCOM) for the purpose of combating cybercrime has applied for the block.

Since 15 June 2010, MELANI has been recognised by OFCOM as a corresponding body and can apply to SWITCH to block and revoke the relevant assignment to a ".ch" domain name server in the event of justified suspicion of phishing or the distribution of malware.

The majority of the blockings requested by MELANI are phishing sites. After more than 30 websites were blocked in 2016 and 2017, this number dropped to 16 in 2018. The low number is due to the fact that only sites used exclusively for phishing or malware distribution are blocked. Phishing sites are mostly located on compromised systems where other content is also stored. In these cases, the domain is not blocked, but the provider attempts to remove the fraudulent site from the network.

[20] https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https (as at 31 January 2019)

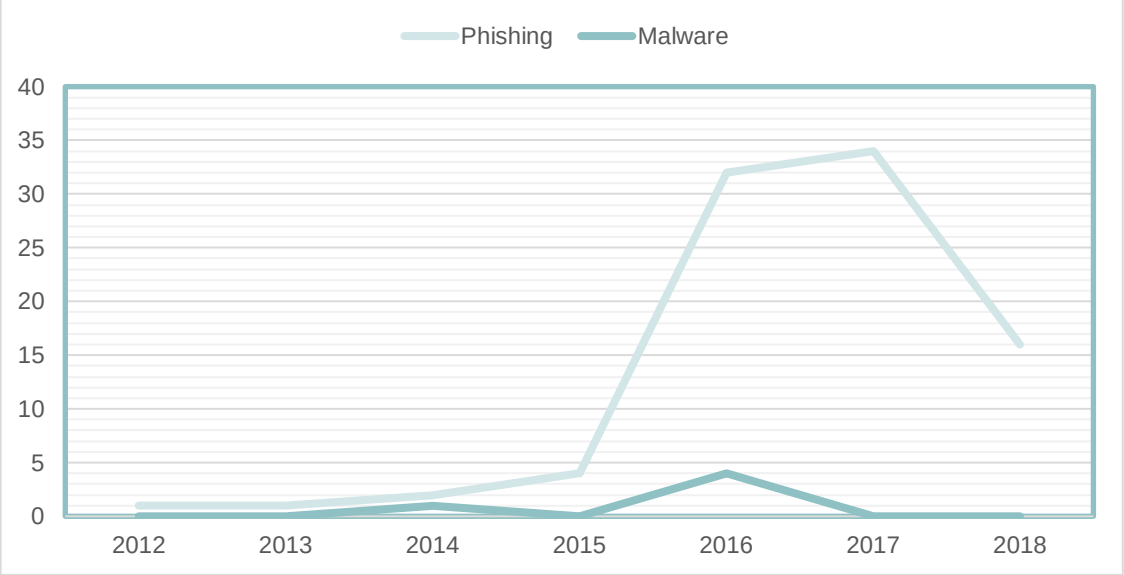

Figure 5: Blocking requests from MELANI according to OID, Art. 15. Blocking requests from phishing sites are shown in light blue, requests from sites with malware are shown in dark blue.

4.5 Crimeware

In the first half of 2018, there were also numerous infections with criminal software (crimeware). The statistics in figure 6 show the distribution of the most significant malware in Switzerland. There is also malware, which is also very significant but does not appear in the statistics, such as the "Retefe" e-banking malware.

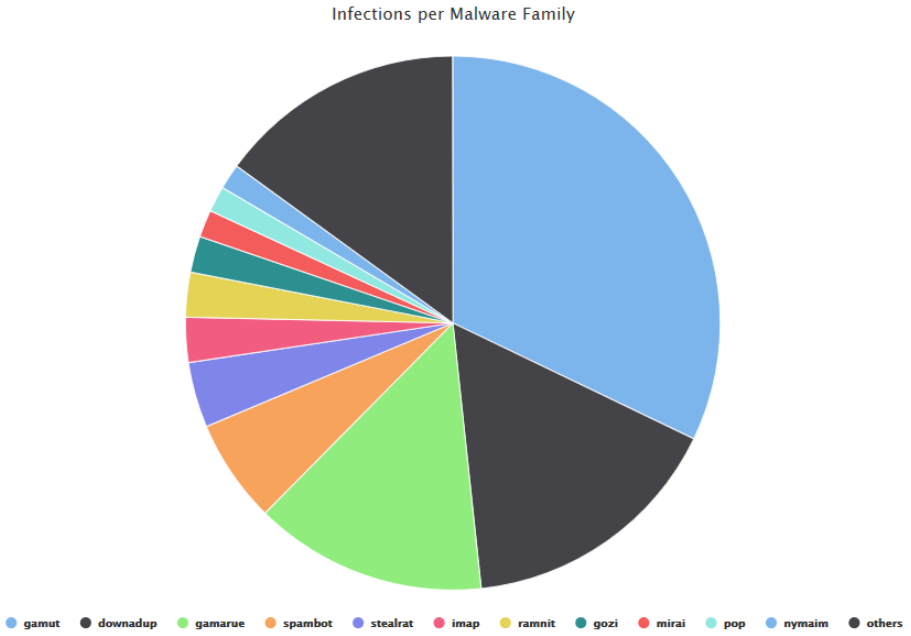

Figure 6: Breakdown of malware in Switzerland known to MELANI. The reference date is 31 December 2018. Current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/

For the first time since these statistics were created, the malware "Downadup" (also known as "Conficker") is no longer in first place. The new frontrunner in the second half of 2018 was the malware "Gamut", which is responsible for the majority of the worldwide spam volume. The "Gamut botnet" mainly sends spam on job offers for the purpose of money mule recruitment[21]. In third place is "Gamarue"[22], also known as "Andromeda", a downloader that can download additional malware. In fourth and fifth place follow the malware "Spambot" and "Stealrat". These two are also responsible for sending spam. "Stealrat" does this via infected domains, through which "WordPress", "Joomla!" and "Drupal" run. Spam messages are thereby sent through legitimate email servers and are more difficult to filter. The first e-banking Trojan Gozi follows in eighth place. The botnet "Mirai", known since the attack on the internet service provider "Dyn", has made it back into the top ten and has replaced the cryptominer malware "Monerominer", which is no longer on the list.

4.5.1 Retefe e-banking Trojan – most significant banking Trojan in Switzerland

Retefe continues to be one of the most significant banking Trojans in Switzerland. The malware is sent by email on behalf of well-known companies or institutions and targets both Windows and MacOS systems. The email attachments usually contain a malicious Word document, e.g. an purported invoice from an online shop, a delivery confirmation from a parcel supplier or information from the Federal Administration on contaminated drinking water. Figure 7 shows the number of spam waves over the last three years.

21 https://sensorstechforum.com/necurs-gamut-botnets-spam/ (as at 31 January 2018, only available in German)

22 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/Schadsoftware/Andromeda_Gamarue.html (as at 31 January 2018, only available in German)

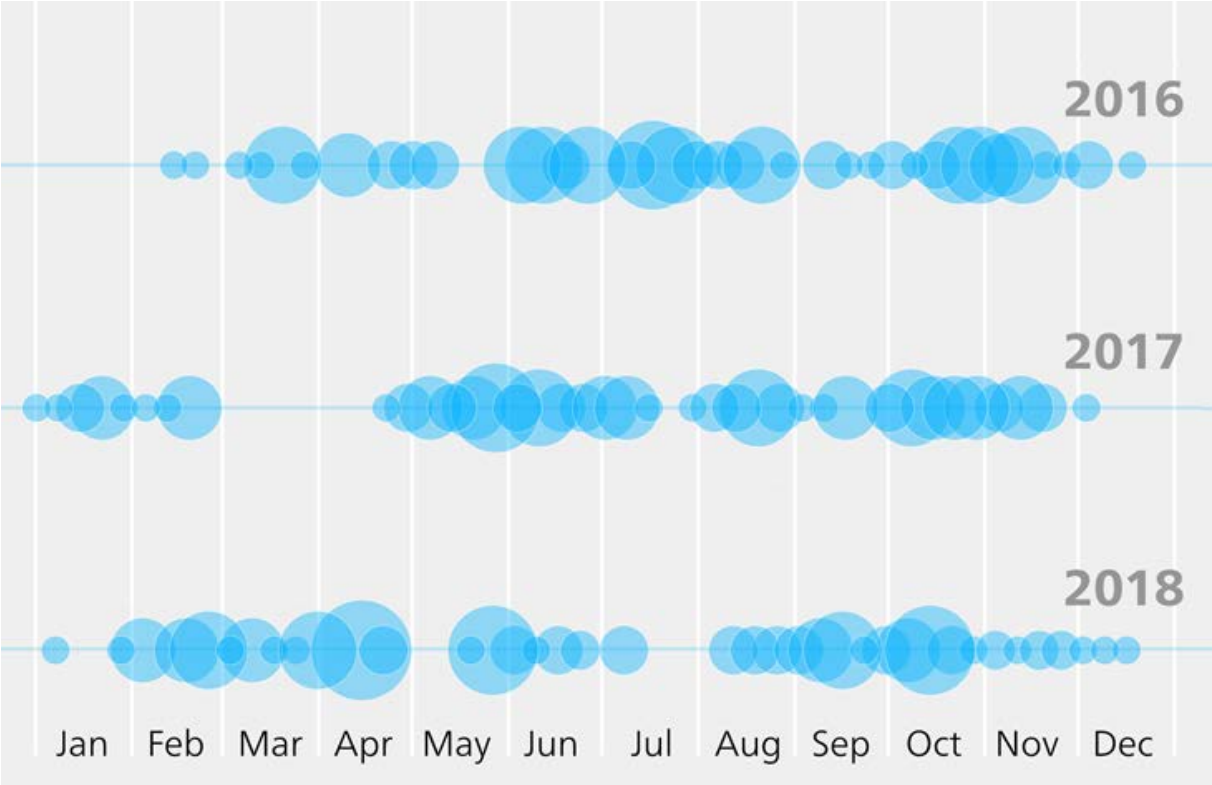

Figure 7: Retefe waves of the last three years. The blue circles represent the number and size of different spam waves.

In addition, Retefe tries to enhance the credibility of emails by providing personal information such as telephone numbers or the recipient's address. This information is obtained from data leaks. Retefe currently only targets private clients in Switzerland, Liechtenstein and Norway. Corporate customers are less affected by Retefe. On the one hand offline payment systems are not attacked directly, on the other hand Retefe has to change the proxy settings and install a root certificate and the software Tor. For company computers, these rights should be restricted so that such manipulation is not possible.

Recommendation:

Be particularly careful when opening Word documents, usually companies and organisations send business documents (e.g. invoices, quotes, etc.) as pdf files and not Word documents.

4.5.2 Gozi active again

After a quite long time with few Gozi attacks in Switzerland, an email wave with a fake Swisscom bill appeared on 28 November 2018. Here the attackers cleverly used social engineering methods.

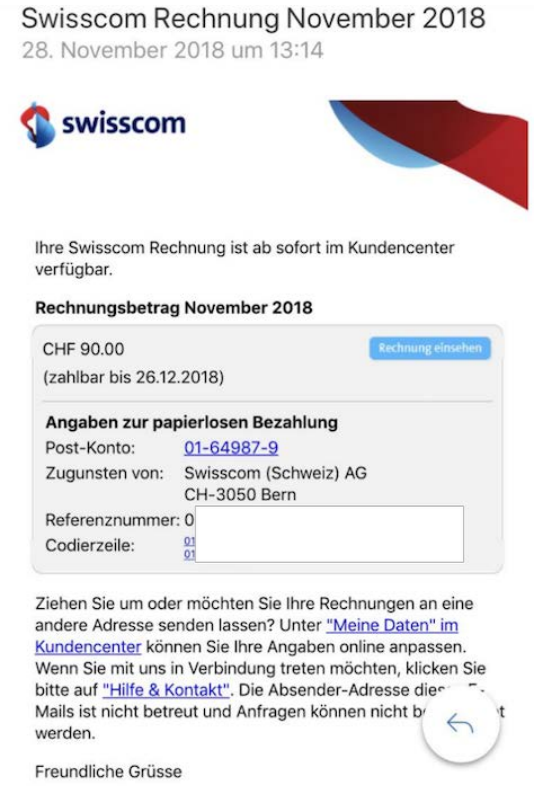

Figure 8: Fake Swisscom bill with a link to a malicious file

The email contains a link to a ZIP file containing an obfuscated Visual Basic Script that is started via Powershell "bitsadmin"[23]. The actual malware is downloaded, stored in the temporary profile of the respective user and then started.

In addition to the information on the fixed command and control servers, the configuration of Gozi contains information that is necessary for the use of a domain generation algorithm. These domain names are based on words in the US Constitution, which are randomly chosen and reassembled[24]. Dynamic contact points can be defined for control servers if the fixed contact points no longer work. In the current case, however, this function was not used.

In its configuration, Gozi contains both attacking banks and software products that are to be monitored. The malware also targets offline payment software and thus also directly targets companies.

[23] https://docs.microsoft.com/en-us/windows/desktop/bits/bitsadmin-tool (as at 31 January 2018)

[24] Gozi Blog: https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature (as at 31 January 2018)

Recommendation:

We particularly recommend SMEs to use their own dedicated devices with limited internet access for payments, not to surf or email on them, to keep the device and installed software up to date, and to store passwords in a password safe. When releasing payments, the principle of dual control is recommended and the release should be carried out on a second, equally secured device. Suspicious payments should always be reported to the bank as soon as possible.

4.5.3 Counterfeit banking apps

In the age of smartphones, apps play an important role. The disadvantage for criminals is that apps, unlike a standard browser, are mostly proprietary. If an app is misused, the provider and developer, in contrast to a standard browser, has the direct option of adapting the code and reacting to attacks with appropriate security mechanisms. So it is more difficult for a criminal to attack an app and manipulate it.

This is why criminals try above all to circulate counterfeit apps instead of manipulating legitimate apps. Especially in the financial sector, numerous such fake apps regularly find their way into official and unofficial stores. Such fake apps are relatively simply structured and display some form fields after starting where credit card data, login and passwords should be entered. Victims are lured to download such apps with the use of names and logos similar to those of banks. Other social engineering methods also belong to the repertoire of the attackers: for example, criminals claimed that the credit limit at the respective banks could be increased with a (counterfeit) app.

With "Google Play Protect", Google has developed a filter which last year for the first time resulted in a reduction in the spread of malware on "Android". Nevertheless, fake apps appear again and again.

At the end of September, Postfinance was also affected by such a fake app. No e-banking access data or other passwords were requested by the fake Postfinance app. The attackers were after credit card details. Once a victim had entered this data, a thank you page appeared and the app was closed again. By this stage at the latest, victims should become suspicious and contact the respective internet service provider or credit card company[25].

4.5.4 Ransomware

Extortion using encryption software, so-called ransomware, is certainly one of the types of attack with the greatest impact on SMEs at present, but also on critical information infrastructures, as the examples in chapter 5.3.5 show. The most common types at the moment are "Ryuk", "GandCrab", "Dharma" and "Locky". An overview of all ransomware types is listed on the website "botfrei.de"[26].

---

[25] https://www.blick.ch/news/wirtschaft/ueber-1000-opfer-falsche-postfinance-app-in-play-store-gebracht-id8881643.html (as at 31 January 2019)

[26] https://www.botfrei.de/de/ransomware/galerie.html (as at 31 January 2019, only available in German)

The "Ryuk" ransomware stands out above all for its way of collecting data in advance and then encrypting systems of lucrative victims. On 12 December 2018, MELANI published a corresponding warning against various malspam waves with infected Word documents attached[27]. Ryuk was spread via the Trojan "Emotet" which has been known for a long time. This tries to use social engineering to use fake emails on behalf of colleagues, business partners or acquaintances to trick the recipient into opening the attached Word document and executing the Office macros it contains. Originally known as an e-banking Trojan, Emotet is now mainly used to send spam and download other malware. In this case the "Trickbot" malware was reloaded, which tried to gain rights on the infected computers. Once installed, Trickbot performed a comprehensive network analysis to determine if the computer was part of a larger company or organisation and attempted to spread within that network using the known "SMB" vulnerability. The malware repeatedly communicated with the control server. Only if the target is considered large enough by the attackers, is the Ryuk ransomware finally loaded, which encrypts the data on the computers and servers in the company network. Through this very targeted deployment, the perpetrators are said to have collected bitcoins since August 2018 amounting to approximately USD 3.7 million[28]. How much of it could be converted into physical money is not known. It is also not yet known from where the perpetrators operate.

[27] https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html (as at 31 January 2019)

[28] https://derstandard.at/2000096143241/Ryuk-Neue-Ransomware-brachte-Cyberkriminellen-vier-Millionen-Dollar (as at 31 January 2019)

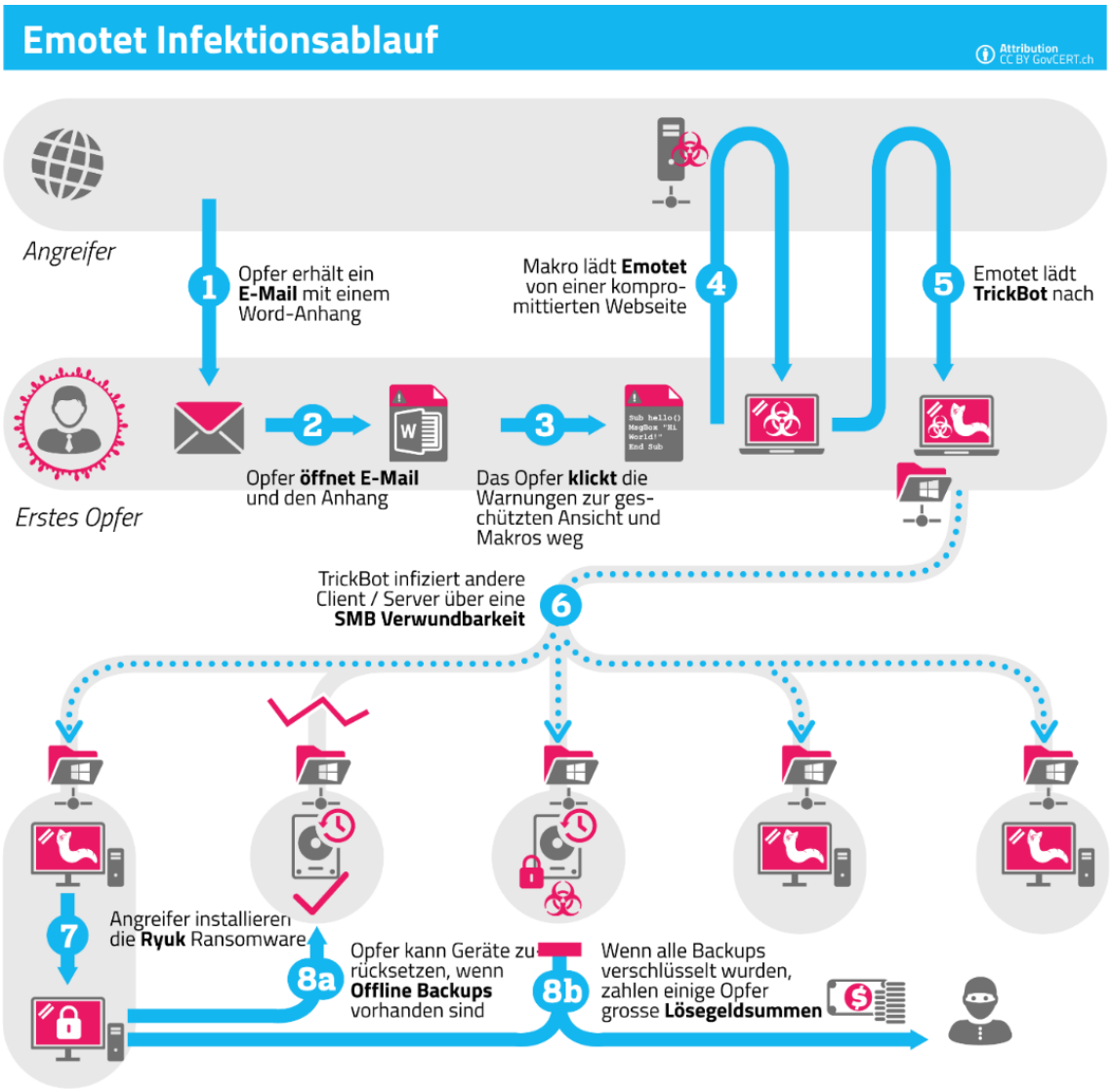

Figure 9: Schematic infection process of the Emotet malware

Cases involving the "GandCrab" ransomware were also reported several times to MELANI in the second half of 2018. The ransomware appeared for the first time in January 2018[29] and is characterised above all by a large number of infection vectors. Initially, GandCrab was distributed through spam emails. In the summer of 2018, the attackers changed the procedure with version 4 and used websites offering illegal cracked versions of paid software for distribution. These are often fake sites that were activated by the blackmailers themselves and can be found via Google search. Manipulated application documents are also part of the repertoire of

[29] https://blog.comodo.com/comodo-news/gandcrab-the-new-version-of-ransomware/ (as at 31 January 2019)

dissemination methods[30]. Furthermore, in August 2018 the security company "FireEye" reported that the ransomware Gandcrab uses an exploit kit on manipulated websites. This is embedded in infected websites and exploits two vulnerabilities in Windows[31].

The "Dharma" ransomware has been active since 2016. Nevertheless, it is still one of the most dangerous encryption Trojans. The perpetrators behind this malware continue to release new variants with new encryptions that cannot be cracked. In the second half of 2018, Dharma ransomware attracted particular attention due to two casualties that attracted considerable media attention: the Scottish brewery "Arran Brewery" and a large seaport were affected by Dharma (see also chapter 5.3.5).

However, there was also good news in the reporting period: on 26 November 2018, the FBI announced that it had identified two people behind the "SamSam" ransomware. They were two Iranian citizens aged 28 and 35. The US Department of Justice has published a corresponding indictment. The perpetrators are said to have received over USD 6 million in ransom payments from victims in various sectors, including critical infrastructure in the health, transport and administration sectors.

Recommendation:

Regularly make a backup of your data. The backup should be stored offline, i.e. on an external medium such as an external hard disk. After the backup operation, disconnect the external media on which you are backing up from the computer. Otherwise data on the back-up medium might be encrypted and rendered unusable in the event of a ransomware attack.

Segment your network. Disconnect particularly vulnerable locations, such as the human resources department or media office, which have to open attachments from unknown senders, from the rest of the network.

MELANI information page on encryption Trojans

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

30 https://www.heise.de/security/meldung/Erpressungstrojaner-Gandcrab-verbreitet-sich-ueber-gefaelschte-Bewerbungsmails-4154167.html (as at 31 January 2019, only available in German)

31 https://www.fireeye.com/blog/threat-research/2018/09/fallout-exploit-kit-used-in-malvertising-campaign-to-deliver-gandcrab-ransomware.html (as at 31 January 2019)

5 Situation internationally

5.1 Espionage

5.1.1 APT 10

On December 20, 2018, the US Department of Justice (DoJ) accused two Chinese citizens of infiltrating computers and committing money transfer fraud and identity theft. The two men are said to have been members of the cyber espionage campaign "APT10". This campaign is also known under the names "menuPass", "CVNX", "StonePanda" and "POTASSIUM", which is said to have attacked major managed IT service poviders (MSPs) worldwide since at least 2016 (see also MELANI Semi-annual report 1/2017, chapter 5.1.1[32]). In the DoJ's public document, targets are listed in 12 countries, including Switzerland.

Managed IT service providers (MSPs) are an attractive target because they support large companies in managing their ICT infrastructure and have direct access rights to their customers' systems and data. In this campaign, MSPs were not the actual target, but were used to gain access to networks in numerous large companies. However, the group did not choose this route until 2016. Before that, the targets were attacked directly. The group has been active since 2006 and has since gained unauthorised access to computer networks of more than 45 technology companies, the U.S. Department of Energy and NASA. In addition, the attackers are alleged to have stolen personal information from military personnel, including social security numbers, email addresses and salary data of 100,000 US Navy employees.

The US Department of Justice underlines the interdependence of the two defendants with the Chinese Ministry of State Security (MSS). At the same time, the remaining four members of the "Five Eyes" countries[33] supported the USA's statements regarding the Chinese government's involvement in the espionage campaign through public statements. They declared that they would make use of public attribution in the event of cyber incidents. This is particularly the case when global economic growth, national security and international stability are at risk. Furthermore, China and all other countries involved were called upon to respect the obligations of the various international conventions.

5.1.2 APT 28 Developments

Reports are regularly provided here on the APT28 spy group which is also known as "Sofacy" or "Fancy Bear". It is probably the most active and best-known campaign worldwide. In the second half of 2018, the Group's technical capabilities continued to develop and the range of functions expanded. The use of "LoJax" is particularly striking for a UEFI rootkit. As reported by the security service provider "ESET" at the end of September 2018, the rootkit was used for operations against organisations in the Balkans as well as in Central and Eastern Europe[34]. UEFI rootkits are sophisticated tools for preparing for cyber attacks. They are very difficult to

---

32 MELANI Semi-annual report 1/2017, chapter 5.1.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2017-1.html6-2.html (as at 31 January 2019)

33 USA, UK, Australia, New Zealand, Canada

34 https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/ (as at 31 January 2019)

track down and are able to withstand even radical security measures such as reinstalling an operating system or replacing a hard drive. It was the first time that a UEFI rootkit was discovered in real operation.

Sofacy is also said to be responsible for a function that can complicate the analysis of documents in an automated sandbox environment. The method is based on the so-called "autoclose" function, where a macro in the Word document is only executed and downloads malicious code when the document is closed by the user. With automatic analysis, the documents usually remain open for a certain period of time and are checked for their behaviour, but they are not closed. Since the malicious code only has to be downloaded from an external server at the time of closing and is not implemented in the Word document, a successful attack is only possible if this server is actually online at this time, otherwise no damage is caused. The campaign was targeted at several government offices around the world. In one case the crash of a Lion Air plane on 29 October 2018 was referred to and the file name "crash list (Lion Air Boeing 737).docx." was used.

We already reported on the use of the "Zebrocy" malware by Sofacy in our last semi-annual report. Zebrocy is a collection of downloaders, droppers and backdoors. Downloaders and droppers are used for reconnaissance, the backdoors ensure persistent access for espionage activities. New components were introduced during the reporting period and Zebrocy experienced an upswing. For example, the new components use protocols from the SMTP and POP3 mail services to transfer the stolen data from the victim's network. In December 2018, the security company PaloAlto[35] also reported that a new Zebrocy variant with virtually the same functionality had appeared, but was written in Sofacy's new programming language "Go". So far variants in "AutoIt", "Delphi", "VB.NET", "C#" and "Visual C++" have been seen. The background is not clear. It is assumed that the diversity of programming languages is intended to make detection more difficult.

5.1.3 Targeted attack on Italian naval and armaments industry?

Between 9 and 15 October 2018, emails with a manipulated Excel document were sent specifically to employees of the Italian naval and defence industry[36]. According to the Italian security company "Yoroi", the emails were about a request for spare parts for ship engines. In it, the attacker asked for an offer for the articles contained in the Excel file. So the recipient was forced to open the Excel file. The attackers seem to have researched the products well in advance to make the request look as real as possible. So the request went to the right place and also the language was clear and correct. After opening the file, the remote access tool "QuasarRAT" was downloaded to the victim's system. With this tool, the attackers had full access to the system and were able to steal data and manipulate the computer. The source code of QuasarRAT is public and available on the online service "GitHub". While Yoroi assumes that a state actor is behind the attacks, the software company "Kaspersky" tends more towards a criminal background in its analysis. According to Kaspersky, the campaign is on a larger scale and the documents have been sent under different names to companies in many different countries, including Germany, Spain, Bulgaria, India and Romania[37].

---

35 https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/ (as at 31 January 2019)

36 https://securityaffairs.co/wordpress/77195/malware/martymcfly-malware-cyber-espionage.html (as at 31 January 2019)

37 https://ics-cert.kaspersky.com/news/2018/10/22/yoroi/ (as at 31 January 2019)

5.2 Industrial control systems

Targeted attacks against process controls on a large scale were largely absent in the period under review. This does not mean, however, that the groups that have made their mark with such attacks in the past have given up their activities. Ukrainian security services accused the Russian military secret service "GRU" of having attacked a water treatment plant with the "VPNFilter" malware[38]. In addition, new groups appeared in the field of industrial control systems. The USA, Europe, the Middle East and East Asia observed various activities. Security service providers[39] refer to them as "RASPITE"[40] or "Leafminer"[41]. Three further examples of ongoing preliminary clarification attempts are discussed in more detail in the following subchapters.

5.2.1 GreyEnergy: further development of the tools of one of the most aggressive threats in the energy sector

The malware "BlackEnergy" made headlines after Christmas 2015. Attackers penetrated operating stations of control systems of several Ukrainian power providers and caused a power failure lasting several hours in the region with over 220,000 affected persons[42].

The Slovakian security service provider "ESET" has since observed another malware framework. Based on the incident mentioned above, ESET referred to it as "GreyEnergy"[43]. Over the past three years, the malware family has been deployed against several targets in Ukraine and Poland. In addition to noting that the disappearance of BlackEnergy malware is associated with the emergence of GreyEnergy, ESET sees the link primarily in the same modular architecture, the conduct of attacks, and the similar selection of targets. To date, no specific module for industrial control systems has been discovered in the GreyEnergy family. The attackers were observed, however, as they strategically targeted workstations with control systems operated on them.

In addition to the fundamentally more modern structure of GreyEnergy than its presumed predecessor, the use of certificates from the Taiwanese manufacturer of industrial and IoT hardware "Advantech" is remarkable. These most likely stolen certificates were used to trustworthily sign their own malware and thus increase the chances of success of an infection. An approach that was also applied to "Stuxnet", the first known malware against industrial processes[44].

---

38 https://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/ (as at 31 January 2019)

39 https://ics-cert.kaspersky.com/news/2018/08/06/raspite/ (as at 31 January 2019)

40 https://dragos.com/resource/raspite/ (as at 31 January 2019)

41 https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east (as at 31 January 2019)

42 MELANI semi-annual report 2/2015, section 5.3.1, 26.04.2016 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2-2015.html6-2.html (as at 31 January 2019)

43 https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/ (as at 31 January 2019)

44 https://www.welivesecurity.com/2010/07/19/win32stuxnet-signed-binaries/ 19.07.2010

GreyEnergy shows that attackers continue to carry out reconnaissance attempts against operators of critical infrastructures. As shown in 2015, they are also prepared to make the move from intelligence work to sabotage at a favourable moment for them.

5.2.2 Shamoon destroys data and configurations - infrastructure failure at Saipem

"300 to 400 servers and about 100 personal workstations were rendered unusable for some time by an attack", Mauro Piasere, head of "Digital and Innovation" at the Italian oil service provider "Saipem" told "Reuters"[45]. This was after the company reported a cyber attack on 10 December 2018 in a press release[46]. On 12 December, Saipem updated the message[47] and announced that servers in the Middle East, India, Scotland and to a limited extent Italy had fallen victim to "Shamoon" malware. The infected systems could be restored step by step through the use of backup infrastructure.

During this time, the security company "Chronicle" analysed a new variant[48] of the Shamoon malware, which had been uploaded from an Italian IP address to the public analysis platform "Virustotal". Shamoon became known in 2012 through an attack on "Saudi Aramco" in which data was destroyed on 35,000 systems. Four years later, a new wave of malware hit the same region. The updated malware version is characterised by the additional ability to overwrite files and the Master Boot Record (MBR), a part of the hard disk necessary to boot the system, with random data. Saudi Aramco is one of Saipem's largest customers, which confirms the suspicion that there is a connection to previous Shamoon incidents. Whether the malware variant analysed by Chronicle and Palo Alto Networks[49] was really used to attack Saipem is not known.

5.2.3 Drones at the airport

There are drones in many shapes and sizes with various different functions. These start with simple toys, include drones for delivery services up to drones in the military sector. It is clear that the number of drones and possibilities will rise in the coming years. The capabilities of drones were shown by the incident around Gatwick airport in the UK. Right at the beginning of the Christmas holidays, on 19 December 2018, unidentified persons with drones paralysed flight operations at the airport for 36 hours. A total of more than 200 drone sightings were reported. The police and also the army, which was called in, were not able to find the perpetrators during this time and to stop the drone flights. The perpetrators responsible for the Gatwick incidents have yet to be apprehended. Smaller drone incidents are now a regular occurrence worldwide. On 12 December 2018, a Boeing aeroplane belonging to the Mexican airline

---

45 https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA (as at 31 January 2019)

46 http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack.page (as at 31 January 2019)

47 http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack%20update.page (as at 31 January 2019)

48 https://www.bleepingcomputer.com/news/security/shamoon-disk-wiping-malware-re-emerges-with-a-third-variant/ (as at 31 January 2019)

49 https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/ (as at 31 January 2019)

"Aeromexico" landed with its nose ripped open after presumably colliding with a drone. Although there was no evidence of compromised systems in any of these cases, the threat of such incidents is on the increase.

Assessment:

The British government has drawn conclusions from the incidents and increased protection against drones. In Switzerland, a permit from the Federal Office of Civil Aviation (FOCA) is required for the operation of drones and model aircraft weighing more than 30 kg. The requirements for the operation of drones and model aircraft up to a weight of 30 kg are regulated in the DETEC Ordinance on Special Category Aircraft. For example, the operation of a drone within a radius of 5 km around airfields and heliports is not permitted without a permit. However, these rules do not protect against wilful actions or if a drone can be hacked and taken over by a third party.

5.3 Attacks (DDoS, defacements, drive-bys, etc.)

5.3.1 Digital skimming – prominent victims

In August 2018, hackers succeeded in stealing the data of more than 380,000 customers of the UK airline British Airways. This included not only names, postal and email addresses, but also credit card and account information. What looked like another attack on a database at first glance turned out to be a manipulation of the British Airways website and app. The attackers used so-called digital skimming to do so. In the case of classical skimming, criminals place a reader in an ATM in such a way that the magnetic strips of the cash card are read and stored. With digital skimming, an attempt is also made to intercept the credit card number and its security features, although not at an ATM, rather during the payment process at a webshop. At British Airways, for example, only customer data entered in the payment form when booking a ticket between 21 August and 5 September 2018 was stolen. The flight and destination information was not affected by the hack.

Another case was discovered on 23 June 2018: the UK ticket sales company Ticketmaster identified malware that had enabled an unknown third party to access customer names, email addresses, telephone numbers, payment details and login information since February 2018.

The payment page of the British online retailer Newegg was likewise affected by this. In this case, hackers introduced 15 lines of malicious code into the website on 14 August 2018. This malicious code remained undetected until 18 September 2018, more than a month later. The malicious code installed sent customer credit card data to a server that was controlled by the attackers.

E-commerce sites have been targeted by attackers since the early days of the internet. The reason is relatively simple: if an attacker wants to obtain valid credit card data, webshops are the perfect choice. As early as 2000, the discovery of a vulnerability in the then widely used webshop software Cart32 for Microsoft servers enabled attackers to gain administrator access to the application. They could use it to read credit card data and execute commands on the hosting server. In 2011, criminals were particularly interested in vulnerabilities in the software

OSCommerce. There were numerous cases of compromised websites also in Switzerland at that time, which prompted MELANI to issue a warning.[50]

Since March 2016, the security service provider RiskIQ has been monitoring the various campaigns with new attack infrastructures[51] and grouping them under the umbrella term Magecart. Lurking behind this term, there are at least seven groups that plant digital credit card skimmers on compromised e-commerce websites. Primarily vulnerabilities in the extensions of the Magento software are exploited. This online shop software was released in 2008 as an open source e-commerce platform. The Dutch security expert Willem de Groot identified zero-day vulnerabilities in at least two Magento extensions of third parties and asked for help to search the remaining 18 extensions for vulnerabilities as well. However, these attackers have also taken an interest in the webshop software Powerfront CMS and OpenCart.[52]

5.3.2 Risks related to VPNs: the example of Hola VPN

A virtual private network (VPN) is an encrypted communication channel that allows a connection to be established between two remote computers via the internet. For many users, using a VPN increases the level of privacy for their online activities. However, not all VPNs are the same and it is the user's responsibility to ensure that his or her VPN is trustworthy and meets certain security standards. A VPN provider is also not immune to an attack that compromises the security of its users. This is what appears to have happened last July, when MyEtherWallet (MEW), a very popular Ethereum portfolio management interface (which contained Ether cryptocurrency), informed its customers that they were at risk if they used the Chrome extension of the Hola VPN. According to MEW, Hola was compromised for a period of 5 hours on 9 July, during which time users who accessed MEW's services were at risk of having their virtual coins stolen. In a press release, Hola acknowledged the incident and stated that the company's Google Chrome Store account had been compromised in order to propose a modified version of the extension for Google Chrome, aimed at capturing information from users when they connected to their MEW account. Following this discovery, the company secured its Google Chrome Store account and removed the fraudulent extension.

Recommendation:

Recommendations from MELANI concerning the use of VPNs.:
https://www.melani.admin.ch/melani/en/home/themen/vpn.html

5.3.3 Banks attacked by physical network access

In December, security solution provider Kaspersky released the results of a series of cyber incidents that had affected various banks in Eastern Europe. The point of entry into the company's network is of particular interest because criminals connected their devices directly to

50 https://www.computerworld.ch/business/politik/melani-warnt-schweizer-webshop-betreiber-1321089.html (as at 31 January 2019)

51 https://www.riskiq.com/blog/external-threat-management/inside-magecart/ (as at 31 January 2019)

52 https://www.riskiq.com/blog/labs/magecart-keylogger-injection/ (as at 31 January 2019)

the network. Unlike for many remote attacks, such as malicious emails or hacking a vulnerable server, the criminals needed to have physical access to the company's premises. After entering the site, e.g. posing as job seekers or delivery workers, they connected their devices directly to the network. Depending on the case, they used either a small laptop, a Raspberry Pi nano-computer or Bash Bunny, a USB port penetration device. Once this initial access was established, the attackers then conducted a reconnaissance phase, aimed in particular at capturing identifiers and identifying stations from which payments were made. Subsequently, the attackers sought to ensure sustainable remote access to these stations.

This type of attack is a reminder of how crucial it is to envisage a comprehensive security strategy which is not limited to technical measures but also includes physical or organisational measures. Controlled access to the premises is therefore crucial. In these premises, network entry points (machines, Ethernet ports) should be documented and monitored, or even disabled if their use is not necessary.

5.3.4 Lazarus, still a highly enterprising player

The Lazarus group is known to have attacked the systems of various banks in the past, including those of the Bangladesh central bank in 2016. According to many experts, Lazarus is linked to the North Korean regime. This is the same player who was identified in a case that affected the Chilean Redbanc bank at the end of December 2018. The company Flashpoint claims that the malware used (PowerRatankba) is part of Lazarus' arsenal. The method used to install the malicious code on the company's networks is of particular interest. The attackers posed as a recruiter and contacted a bank employee through social networks in order to offer him a job interview on Skype. During this interview, the target was asked to download a supposed application necessary for the recruitment process. It was in fact a malicious executable. However, according to available information, the incident was detected in time and had no impact on the bank's infrastructure or activities.

As early as in October, US-CERT published information on the activities of Hidden Cobra, which since 2016 has targeted Asian and African banks as part of a "FastCash" campaign to simultaneously release large amounts of cash through ATMs. Accomplices then take care of recovering the money distributed by the machines. In one particular incident in 2017, withdrawals were reported to have been made simultaneously in more than 30 countries. According to some experts, including the security solutions company Symantec, which has also published its analysis of these cases, Hidden Cobra is none other than Lazarus. Symantec describes the attackers' modus operandi in more detail. After an initial compromise, the servers used to administer the ATMs are said to be infected by a specific Trojan horse (Trojan.Fastcash), which is then responsible for generating fraudulent transaction requests.

It is now also well known that Lazarus is closely interested in the cryptocurrency market and sees potential for diversifying its sources of income. According to an analysis by Kaspersky published in August, the group is responsible for an attack that targeted a cryptocurrency exchange platform based in Asia. In this case, a third-party trading application downloaded by a company employee was used as an entry point. The malicious code was then delivered in the form of an application update. It is particularly noteworthy in this case that versions adapted to the targeted operating system were used. While Lazarus has frequently targeted Windows systems in the past, this seems to be the first time the group has developed malicious code specifically for macOS.

5.3.5 Ransomware

When people talk about encryption malware, so-called ransomware, they first think of corrupted data and the backup that will hopefully work. However, one thing that should not be forgotten in preventive planning is the loss of production that such malware causes before the backup is restored and all systems are again working smoothly. This is of particular concern when entire production facilities are affected by such attacks. Numerous such cases made the headlines during the half-year under review.

In August 2018, the Taiwanese chip manufacturer "TSMC" (Taiwan Semiconductor Manufacturing Company) suffered an attack. In this case, too, the company had to cease production in several factories as a result of the encryption malware software used. TSMC is the world's largest manufacturer of semiconductors and processors and most notably a supplier of Apple's iPhone. A variant of the WannaCry-malware was identified as the cause. WannaCry hit the headlines in May 2017 and had a major effect worldwide. The Windows vulnerability in the SMB protocol that was responsible for spreading this malware was closed down back in March 2017. However, it is sometimes difficult to carry out prompt patch management, especially for control systems. The affected computers of the "material handling systems" therefore ran on unpatched Windows 7 systems. The malware was introduced via a newly installed software tool, for which a virus check had not been carried out.

Two seaports had to contend with cyber attacks in the second half of 2018: On 20 September 2018, the port of Barcelona denounced a ransom attack on the port's security infrastructure. The type of ransomware involved is not known. Ship operations could be maintained, as there is a contingency plan in place for such events. A week later, on 27 September 2018, the port of San Diego was disrupted due to ransomware. Here, too, the port and its services remained open and employees were able to continue working. However, certain functions and access to data were restricted.

On November 21, 2018, "KraussMaffei", the German engineering company, had to contend with the consequences of a ransomware attack on computers. KraussMaffei is one of the world's largest suppliers of machines for plastics and rubber production. Due to the attack, machines necessary for controlling individual production and assembly processes could not be started when the attack began. According to several reports, production subsequently had to be reduced. Although the backup has enabled KraussMaffei to get important computers up and running again, the company will still be struggling with the effects for a long time to come. In January 2019, a spokesperson confirmed that only three-quarters of the operationally relevant systems would operate normally again.[53] No information was disclosed on the nature of the ransomware, the amount of the ransom demand or whether ransom payments were made.

[53] https://www.zeit.de/2019/03/datenschutz-cyberangriffe-unternehmen-digitalisierung-risiken-datendiebstahl-hacker (as at 31 January 2019)

Assessment/recommendation

The human resources departments of companies are a particularly popular gateway for malware. As a rule, job applications contain all kinds of documents that have to be opened. In the second half of 2018, this type of attack increasingly occurred in ransomware. Company events or press releases are also opportunities to spread malware.

Cyber criminals have also discovered attacks on mobile devices to be a lucrative business. Accordingly, mobile Ransomware attacks continue to increase. The most common variant on Android and other mobile devices is the "Locker" ransomware. Instead of encrypting files, the malware locks the entire device. The increasing number of IoT devices is likely to open up another area of business for criminals.

An important measure to protect industrial companies from cyber attacks is to separate operational networks from IT networks. Even if the office IT is attacked, the machines continue to run smoothly. For the purpose of usability, however, the networks are often directly connected to each other, for example to simply send commands to machines.

5.4 Data leaks

5.4.1 The Ariane platform of the French Ministry of Foreign Affairs had been hacked

On 13 December, the French Ministry of Foreign Affairs announced that its "Ariane" platform had been hacked and that personal data had been seized. Since 2010, the Ariane service has enabled French citizens planning to spend time abroad to register online in order to receive security recommendations on the country they are visiting. If necessary, registered individuals will be contacted directly, as well as the contact persons provided. The data leak relates specifically to the latter category, since it is the surnames, first names, telephone numbers and email addresses of the people listed as contacts by Ariane account holders that are concerned. The French Ministry of Foreign Affairs points out that the stolen data is not considered sensitive, but it is conceivable that it could be used to send targeted emails or for fraud attempts, for example. The individuals affected, including Swiss citizens, were informed by email. Some recipients of the email, unaware that their data was in this database, suspected that it was a phishing email.

5.4.2 Fault in Facebook's "View As" function

On 28 September, Facebook revealed details of what could be the largest security incident in the application's history. The breach concerned the "View as" feature which allows users to see how their own profile is visible to other users. For security reasons, the 50 million affected users were logged out of their accounts and had to choose a new password. 40 million users who had used the vulnerable function also had to reconnect. The service was disabled. Exploiting this vulnerability would have allowed attackers to take possession of the token that allows users to stay connected to their account for several sessions. This gave them full access to their victim's account, but also to any other service for which Facebook is used for identification (single sign-on, single authentication). This now widespread practice consists in using identification to a service considered secure to connect to various other services, thus avoiding the need to connect individually each time. The incident demonstrates that the practice can also pose a safety risk.

5.4.3 Medical data leak in Singapore

In July, details of a massive attack on the health sector in Singapore were revealed. 1.5 million people who visited SingHealth's clinics, the largest group of health facilities in the country, between early May and early July 2018 had their personal data stolen. For 150,000 patients, information on their medical prescriptions has also been recorded. Among them is Prime Minister Lee Hsien Loong, who, according to the authorities, was specifically targeted.

5.4.4 Vulnerability in Movistar's online portal

The Spanish telecommunications company Telefonica was also affected by a serious vulnerability during the period under review. The incident was made public by the consumer organisation FACUA in July 2018. In this case, customers of the operator's Movistar brand were made available to unauthorised third parties. A vulnerability in the online portal's programming allowed anyone with a Movistar account to access the names, addresses and telephone numbers of all other customers. The company subsequently corrected the breach, with no knowledge of whether any malicious individuals had time to collect personal data.

5.4.5 Starwood hotel chain victim of a long-term leak

On 30 November 2018, Marriott announced that unauthorised access had allowed the data of 500 million customers of its Starwood hotel group to be accessed. This figure was revised downwards in January when the company announced that a maximum of 383 million one-off registrations were affected by the leak. In addition to personal data such as addresses and telephone numbers, in some cases more problematic data was also concerned: passport numbers and credit card data. The credit card data, and in some cases passport numbers were well encrypted, but Marriott cannot exclude that the attackers may also be in possession of the keys needed to read the data. The attackers reportedly had access to the data from 2014 and up until the incident was discovered in September 2018.

Starwood, the brand acquired by Marriott in 2016, includes more than 1200 hotels in nearly 100 countries. The leak reported in November is remarkable in terms of the number of people concerned, the duration of undue access, and also the nature of the data collected. While personal data, credit card data and passport numbers create vast opportunities for criminals to commit fraud or identity theft, it is also conceivable that those involved in espionage operations will be particularly interested to know in which hotels certain targets are staying. In the past, a number of sophisticated cyber-espionage campaigns have targeted hotels. As early as 2014, MELANI exemplified this type of possibility by referring to the Darkhotel campaign, in which wireless networks of major hotels were allegedly hacked to spy on business travellers.[54] However, before setting up an operation of this type, it is important to know which target will be in which hotel and at what time. The leak at Starwood potentially provided this type of information on a plate. Even if the perpetrator of the attack and its precise purpose are unknown, it cannot be excluded that this information could have been used to prepare an espionage attack, either by cyber or physical means. The information necessary for this preparation may also have been acquired by an actor other than the one who carried out the attack.

[54] MELANI Semi-annual report 2/2014
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2014-2.html (as at 31 January 2019)

5.5 Preventive measures

5.5.1 Combating computer support fraudsters

If the phone rings unexpectedly and a "Microsoft" employee responds at the other end of the line, it is likely to be a fraudster. There are also fraudsters behind messages that suddenly pop up while surfing the net which claim that the computer is endangered or even infected and that you should call a number. The perpetrators use this scam to gain remote access to computers and to obtain some money in addition to the data stored there, as they charge for their "support services" and sell invented licenses. People in Switzerland continue to be affected by this scam.[55] The perpetrators often falsify their number when calling and even use Swiss numbers to appear on the displays of the people called. The Swiss numbers displayed in pop-ups are usually assigned by foreign VoIP providers.[56]

Since the fraudsters mostly pretend to be "Microsoft" employees and Windows is still the most widespread operating system, Microsoft also has a strong interest in putting a stop to the perpetrators and actively cooperates with law enforcement agencies.[57] Persons affected by bogus support can file a criminal complaint with their local police and inform Microsoft directly.[58]

While the criminal clients and infrastructure operators are spread all over the world,[59] the calls are regularly traced back to call centres in India. Last autumn the Indian police searched 26 call centres in New Delhi and arrested over 60 people.[60] It remains to be seen to what extent these arrests will lead to the phenomenon being sustainably reduced. In any case, it is encouraging that international criminal prosecution is achieving increasing success and that globally active, organised criminals should not consider themselves safe from prosecution.

5.5.2 Fake call numbers to be limited

The British telecommunications regulator "OfCom" brought revised "General Conditions of Entitlement" for communication providers into force on 1 October 2018.[61] This obliges providers to make the calling line identification available free of charge and to ensure that the displayed

---

55 MELANI has been warning against this scam since 2011: https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/appels-d_escrocs-se-faisant-passer-pour-le-service-support-de-mi.htm; due to the continuing trend, it can still be found under "Current threats": https://www.melani.admin.ch/melani/en/home/themen/fake_support.htmlurrent threats (as at 31 January 2019)

56 As part of the current partial revision of the Telecommunications Act (TCA), the State Secretariat for Economic Affairs (SECO) is to be given powers to quickly block such numbers.

57 https://blogs.microsoft.com/on-the-issues/2018/11/29/new-breakthroughs-in-combatting-tech-support-scams/; https://www.zdnet.com/article/after-microsoft-complaints-indian-police-arrest-tech-support-scammers-at-26-call-centers/ (as at 31 January 2019)

58 The Microsoft report form can be found here: https://www.microsoft.com/en-gb/concern/scam

59 Among others in Germany and the United Kingdom: https://winfuture.de/news,96690.html; https://www.t-online.de/digital/sicherheit/id_81548210/trickbetrueger-mit-microsoft-masche-verhaftet.html (as at 31 January 2019)

60 https://www.nytimes.com/2018/11/28/technology/scams-india-call-center-raids.html (as at 31 January 2019)

61 https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/new-rules-protect-consumers

number actually belongs to the caller. Calls with fake numbers must be blocked. This measure is intended to protect consumers better against fraudulent and otherwise tiresome calls.

Whether such rules can be implemented in a meaningful way is contested. In Switzerland, the Telecommunications Act is currently being partially revised. The Federal Council's dispatch[62] highlights the problem of fake caller numbers and explains that, despite international efforts, the introduction of an effective procedure for the global verification of caller numbers is likely to take many years. Nevertheless, there are plans to extend the legal obligation of telecommunications service providers to fundamentally combat spam to include unsolicited advertising calls. In this respect, Switzerland would be prepared to prescribe and implement measures at ordinance level as soon as technology makes this possible.

5.5.3 Coordinated operation against those involved in voice phishing

An internationally active group is suspected of having obtained and illegally used e-banking data via spam emails and telephone calls (voice phishing). Customers of financial institutions in Switzerland are also affected.

Thanks to mutual assistance cooperation with the Netherlands, the suspects were identified and their operational base in the Rotterdam area was located. A coordinated operation took place in the Netherlands on 17 July 2018 with the support of the Dutch law enforcement authorities, the Federal Office of Police (fedpol) and thanks to coordination by the European Union's Judicial Cooperation Unit (Eurojust). As a result, two people were arrested and house searches carried out. Extradition was requested for the person suspected of being responsible for phishing calls to Switzerland. The other person will be prosecuted under Dutch criminal proceedings.[63]

Assessment:

As the successfully coordinated operation in the Netherlands shows, the prosecution of cybercrime must be tackled at international level.

5.5.4 Internet providers cut connections to BGP Hijack Factory

The Border Gateway Protocol (BGP) is the routing protocol used in the internet and connects individual networks, so-called autonomous systems (AS) with each other. IP addresses belong to each AS and the ASs as a whole make up the internet. "BGP Hijacking" refers to the unauthorised takeover of IP addresses by operators of an AS by manipulating internet routing tables.

A Portuguese company has attracted attention several times as a result of such takeovers. They then rented the hijacked IP addresses primarily out to spammers, as their addresses typically quickly feature on block lists and they always need new addresses to ensure that their emails are received. In recent years, a total of 130 fake routes are said to have been fed in, resulting in almost 225,000 IP addresses being used illegally. This situation was discussed on

62 https://www.admin.ch/opc/de/federal-gazette/2017/6559.pdf , pages 6581 and 6596 (as at 31 January 2019)

63 https://www.bundesanwaltschaft.ch/mpc/de/home/medien/archiv-medienmitteilungen/news-seite.msg-id-71647.html (as at 31 January 2019)

various mailing lists and eventually internet transit providers and internet exchange points mutually agreed to cut all connections to the company's AS.[64]

Assessment:

One can argue about whether such an approach should be regarded as self-regulation or vigilante justice. As a result, this first such ban can be seen as a warning to all network operators to abide by certain rules on the internet, even when these are not formal and enforceable laws. Manipulating the basic infrastructure, in particular, means facing a global community that does not appreciate such actions and can collectively adopt countermeasures.

6 Trends and outlook

6.1 Manipulation, a corollary of information flow

Since information has been circulating between individuals and allowing them to adapt their behaviour or opinions, there has been misinformation or manipulation of this information. As far back as the 4th century BC, Sun Tzu described these methods in the "Art of War". Today, our hyper-connected society offers extremely vast potential in terms of the transmission of information and its corollary, the manipulation of information. Against the backdrop of sustained societal, media and political attention, the debate sometimes loses clarity and it becomes difficult to distinguish between fake news, junk news, propaganda, influence methods etc. In this electoral year, there is no doubt that interest in these issues will not diminish. Examples from abroad have shown that the pre-electoral debate is indeed a period conducive to operations involving the manipulation of information, in this case the massive and organised dissemination of false, biased or not intended for public disclosure (personal or classified data in particular), when such dissemination takes place for hostile political purposes.

6.1.1 A favourable societal and technological context

While manipulation of information campaigns are based on characteristics specific to human nature, such as certain cognitive biases, they find fertile ground in some current trends that enable them to thrive.

In particular, they are giving way to online media and social networks, which are becoming the main source of information for many people[65]. Now anyone can become a news broadcaster, without having to worry about meeting any journalistic quality standards. These same social networks have opened up new perspectives for targeting the population. It is possible to send a specific message to a subgroup of the population that are known to be particularly responsive to a certain type of information. But social networks and the Internet do not only have an ad-

64 https://www.bleepingcomputer.com/news/security/internet-transit-providers-disconnect-infamous-bgp-hijack-factory/ (as at 31 January 2019)

65 According to the Reuters Digital News Report 2016, social networks are now a source of information for 62% of American adults and 48% of Europeans (as at 31 January 2019)

vantage when it comes to targeting users, they also make it possible to multiply the dissemination of information through the use of bots. Thus, even a small number of actors can achieve dominance in the social networks.

It has been shown that manipulated information circulates faster than true information[66]. Their flashy, simplistic and perhaps also distracting side increases their chances of being shared. Alongside average users, there are also actors who will act as conscious relays for manipulated information, sometimes even giving them a semblance of legitimacy by using it on blogs or even online newspapers.

6.1.2 Significant examples

The manipulation operations uncovered in recent years have been carried out in very specific contexts. In particular, pre-election or popular vote campaigns in highly fragmented contexts have been targeted. The most striking and telling example in this category is certainly the 2016 US presidential elections. In an already highly conflictual context, the contents of the email accounts of political personalities and organisations were made public. On 7 October 2016, the US authorities accused the Russian government of trying to disrupt the presidential elections. In February 2018, in an indictment document[67], Special Counsel R. Müller's team provided details on another aspect of the attempts to destabilise the 2016 elections: the manufacture and systematic dissemination of fake news, from the "Internet Research Agency", based in St Petersburg. The main aim of the operation was reportedly to erode confidence in democratic institutions, strengthen the fault lines of American society and radicalise voters. Completely fabricated content dealing with divisive issues (firearms, racism, etc.) was intended to give the illusion of being from the United States and was often relayed by local sympathisers or groups. Social networks, especially Facebook, played a major role in spreading this content. Europe has not been spared from this type of operation. The 2017 French electoral campaign was also marked by the spread of false information, including the alleged existence of an offshore account held by the former presidential candidate and current president Emmanuel Macron. Documents from the hacked accounts of Macron's close aides were also published shortly before the election. Although some experts have clearly accused Russia, the French authorities have not officially attributed the attack. But operations to manipulate information can also potentially target votes, for example in referendums. Suspicions of Russian interference, for example, clouded voting on the United Kingdom's exit from the European Union ("Brexit") and on Catalonia's independence.

6.1.3 Outlook in Switzerland

It is difficult to imagine a campaign such as the one that targeted the American or French elections taking place in Switzerland. First of all, Switzerland's strategic role is not comparable. Moreover, elections at the federal level are comparatively non-divisive, due to political culture and the use of proportional representation in particular. The most fierce political battles that lead to greater polarisation in society often take place during votes on referendums or popular initiatives on subjects such as immigration or, more generally, independence from the European Union. In this respect, the Swiss system of direct democracy could well lend itself to attempts at destabilisation. In addition, some one-off manipulations of information were carried

---

66 See in particular a study by the MIT: http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 (as at 31 January 2019)

67 https://www.justice.gov/file/1035477/download (as at 31 January 2019)

out following very specific events, which were difficult to predict in advance. For example, according to some experts, the destruction of Malaysia Airlines' MH17 flight resulted in extensive misinformation from Russia, a country that had been accused of destroying the aircraft. The same applies to the poisoning on British soil of the former Russian agent Skripal. In this sense, any country may be affected by such an operation when it is itself concerned by an event that is sometimes beyond its control but that is of interest to a third country. In view of the above, we cannot assume that our country is out of reach of this type of threat. And the disruptive potential of such a campaign should not be underestimated. Doubts about the legitimacy of the result of a critical vote could seriously affect the proper functioning of the Swiss political process and confidence in its institutions.

6.1.4 What is the answer?

Before implementing measures to counter possible manipulation of information, various tasks must first be undertaken. First of all, work is needed to clarify the debate and the concepts involved. The term "fake news" is for example too vague and encompasses many realities. It is therefore necessary to clearly define the problem, and based on this definition to decide what is acceptable in a democracy and what is not. Indeed, it is not possible to put in the same category erroneous information or the propagation of rumours that are more a matter of bad journalistic work than of a desire to harm, and a campaign of disinformation orchestrated from abroad in order to influence public opinion. Secondly, an entire capacity for detection must be developed. What are the indicators for detecting a campaign that is carried out with the intention of causing harm? At this level, intense collaboration with private stakeholders (content managers, Internet service providers) and international partners who are also working on these issues will be necessary. In such a system, key events (sensitive votes for example) will be examined particularly carefully. The measures envisaged will also require close collaboration with private stakeholders who have the opportunity to intervene, as well as to identify problematic content. The preliminary work of establishing a definition will take on its full meaning here, since an overly broad definition of the problem that we are trying to address may be interpreted as censorship. However, beyond the technical measures that can be taken, or even legal measures (criminal prosecution in particular), there is still a lot of awareness-raising work to be done. Awareness and political education at all levels are the basis for the protection of societies, groups and individuals from the manipulative effects of influence operations. Functioning institutions of the civil society are crucial. The success of a campaign of manipulating information depends on the way in which this information is ingested and then eventually retransmitted by users. An improvement in media and technological skills can thus help to limit the impact of a campaign. These skills will include, for example, the ability to verify the source of information or the legitimacy of a platform but more importantly the ability to develop a critical view of information in general.

6.2 Developing standards

Who governs the Internet? For a long time, many countries have ignored or sniggered at this new medium and its users. Civil society used the internet in every way that was on offer and possible. Companies did the same. The Internet players, in particular the telecommunications companies that provide lines and connections and also the domain name industry, largely regulated themselves. The focus was on expansion and growth. Controlling users and monitoring what they were doing was not a major issue. After all, the internet was the free space in which everyone was able to express their opinions without any restrictions. But the days when the

internet was only used to exchange information are long gone. Nowadays, connectivity permeates almost all areas of life and life without the internet is almost inconceivable. Many important economic and social processes require this medium. It should therefore function reliably and safely. Since security is traditionally a sovereign task, many authorities are now trying to assume this responsibility in relation to the internet and make up for missed regulations. However, the traditionally territorially limited approach of national legislation has limited effectiveness and countries must address the internet's global dimension. Regulation by countries hardly seems realistic. The UN has already convened several expert groups (United Nations Group of Governmental Experts, UN GGE) to discuss risks and measures for international security and peace in the context of the internet. However, the process is a long one and no consensual outcome was presented at the last UN GGE session in 2017. This not least reflects the rising geopolitical tensions which are being felt in all areas of international cooperation. A multilateral solution which is agreed to by every country in the world is therefore likely to be a long time coming.

But not everyone can or wants to wait. Digitalisation is progressing and the pressure from all sides on internet players, no longer just a few Internet infrastructure operators, but all providers and users, is noticeably increasing. Some countries are trying to regulate and control the internet, at least in their respective territories, for example by introducing rules on data protection and the deletion of certain content for foreign platform providers, by censoring information or by practising the isolation of their internet segment. On the other hand, there are globally active companies ("Google", "Facebook", "Microsoft", etc.) who want to maintain the worldwide network as such (as well as the global market) and do not want to be the pawn in geopolitical conflicts. In addition, there are representatives of civil society who oppose both excessive state power and entrepreneurial greed for profit.

Certain rules are therefore also needed on the internet, which is often referred to as a "legal vacuum". Since countries are not offering global legal security, more and more private stakeholders are jumping into the void and making proposals for norms of conduct or making statements about the principles they adhere to. Such initiatives often come from the ICT industry in the broadest sense or from multi-stakeholder bodies.

The following three examples illustrate efforts to make the internet and ICT use foreseeable, reliable and safer:

6.2.1 Global Commission on the Stability of Cyberspace (GCSC)[68]

The Global Commission on the Stability of Cyberspace (GCSC) brings together prominent individuals from governments, corporations, technical and civil society, each from a different geographical region. Its mission is to promote peace, security and stability in the international arena by proposing norms and initiatives for the responsible behaviour of state and non-state stakeholders in cyberspace.

[68] https://cyberstability.org/ (as at 31 January 2019)

6.2.2 Cyber Security Tech Accord[69]

The Cyber Security Tech Accord has so far been signed by around 80 IT companies.[70] They are committed to the following principles in order to improve the security, stability and resilience of cyberspace:

- Defence and protection: All users worldwide, regardless of their origin, must be protected from attacks.
- No attacks: Governments are not helped to launch attacks on innocent citizens or businesses. In addition, products or services should be prevented from being manipulated.
- Capacity building: Self-protection skills should be improved for developers and users.
- Collective action: Technical cooperation and coordinated disclosure of vulnerabilities should be further improved and the spread of malicious software combated.

6.2.3 Paris Call for Trust and Security in Cyberspace[71]

More than 400 organisations, companies and governments have signed the Paris Call for Trust and Security in Cyberspace, which aims to promote the development of a common basis for internet security. The supporters of the Paris Call commit themselves to working together towards the following objectives:

- improve prevention and resilience to malicious online activity;
- protect the accessibility and functionality of the internet;
- together prevent interference in elections;
- take joint action against disregard for intellectual property on the internet;
- prevent the spread of malicious software and internet technologies;
- improve the safety of digital products and services, as well as general "cyber hygiene";
- take measures against cyber mercenaries and offensive activities by non-state players;
- jointly improve relevant international standards.

69 https://cybertechaccord.org/ (as at 31 January 2019)

70 https://cybertechaccord.org/about/ (as at 31 January 2019)

71 https://www.diplomatie.gouv.fr/de/aussenpolitik-frankreichs/neuigkeiten/article/die-paris-digital-week-bietet-die-moglichkeit-zur-begrundung-einer-vielfaltigen (as at 31 January 2019)

7 Politics, research, policy

7.1 Switzerland: parliamentary procedural requests

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Mo	18.4387	2019 Federal Council and the Federal Department of Defence, Civil Protection and Sport (DDPS) give cyber security the highest priority	Guggger Niklaus-Samuel	14.12.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184387
Mo	18.4051	Cyber security, cyber defence. Where do we stand?	Golay Roger	28.09.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184051
Mo	18.4000	Switzerland joins Nato's Centre of Competence for Cyber Defence in Tallinn	Fridez Pierre-Alain	28.09.2018	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184000
Mo	18.4375	Evoting: a swift and determined commitment to an open source and public system	Sommaruga Carlo	14.12.2018	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184375
Po	18.4346	Comparison portals must become more honest: disclosure of all open and hidden commissions from comparison services	Reimann Lukas	14.12.2018	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184346
Ip	18.4230	Free WiFi on SBB trains: a minimum in the age of digital Switzerland	Tornare Manuel	13.12.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184230
Ip	18.4178	Implementable smart farming	Page Pierre-André	12.12.2018	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184178
Ip	18.4121	More and more children are being sexually harassed on the internet by strangers. What is the Federal Council doing?	Frei Yvonne	29.11.2018	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184121
Po	18.4004	Adapting the Package Travel Act to today's consumer reality	Birrer-Heimo Prisca	28.09.2018	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184004
Po	18.3858	Limit pornography consumption by children and adolescents on the internet	Nordmann Roger	26.09.2018	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183858
Mo	18.3856	More consideration for health in mobile communications (1)	Estermann Yvette	26.09.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183856
Mo	18.3855	More consideration for health in mobile communications (2)	Estermann Yvette	26.09.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183855
Ip	18.3800	What can be done about visual illiteracy?	Fehlmann Rielle Laurence	20.09.2018	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183800
Fr	18.5450	Does radio have a future?	Wasserfallen Flavia	12.09.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185450

Ip	18.4404	"Digital Switzerland" strategy: simplifying the procedure for consulting companies	Derder Fathi	14.12.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184404
Mo	18.4037	Competence Centre for Artificial Intelligence in the Federal Administration	Bendahan Samuel	28.09.2018	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184037
Mo	18.3788	Digital vehicle and driving licence	Grüter Franz	19.09.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183788
Fr	18.5478	Digital Switzerland strategy. Does political governance permit rapid implementation of the action plan?	Derder Fathi	12.09.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185478
Fr	18.5476	Digital Switzerland strategy. Include scientific and specialist digitalisation companies in the action plan	Derder Fathi	12.09.2018	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185476
Mo	18.3958	One-time collection of data by the government	Müller-Altermatt Stefan	27.09.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183958
Ip	18.3853	Questionable IT outsourcing affects older, long-standing federal employees	Gyse Barbara	26.09.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183853
Po	18.3783	Increased efficiency in the Confederation through intelligent process automation in the Administration	Radical Free Democratic Group FDP Dobler Marcel	19.09.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183783
Ip	18.4299	Potential of open source software in the Swiss education system	Quadranti Rosmarie	14.12.2018	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184299
Ip	18.4197	IT security of critical infrastructures - what measures is the Confederation taking?	Wasserfallen Christian	12.12.2018	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184197
Mo	18.4276	Easier exchange of information through the introduction of electronic interfaces in the Federal Administration	Vonlanthen Beat	13.12.2018	CS	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184276
Ip	18.4235	Switzerland is far behind in digital health: what measures does the Federal Council envisage?	Graf-Litscher Edith	13.12.2018	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184235

7.2 The development of the legal framework for blockchain technology

The blockchain issue is currently on everyone's lips, in particular one looks spellbound on the development of the cryptocurrencies and the cosmos of the Swiss Crypto Valley. How the Swiss legal system can grasp the underlying technology, however, and offer corresponding legal security for the economy, a prerequisite for development, has recently raised various questions.

In January 2018, the State Secretariat for International Finance (SIF) set up a working group on blockchain/initial coin offerings (ICOs) in order to find answers. Since block-chain technology not only affects financial market law, but also other areas of law such as civil law and the Swiss Code of Obligations, the Federal Office of Justice (FOJ), FINMA and representatives of the financial sector also sit on the working group. The aim of the work is to increase legal certainty, maintain the integrity of the financial centre and ensure technology-neutral regulation.

In August 2018, the working group consulted the financial and fintech industry and gave them the opportunity to comment on the work and recommendations made so far. The consultation raised general issues such as access to bank accounts for fintech companies, civil law, the fight against money laundering and terrorist financing and financial market law. Potential need for action was identified in particular in the area of civil law qualification and transfer of tokens, their treatment under insolvency law and the creation of new opportunities in the area of financial market infrastructures.

In mid-December 2018, the Federal Council adopted the report "Legal basis for distributed ledger technology and blockchain in Switzerland" of the blockchain/ ICO working group and decided to abandon the idea of a specific blockchain law. The report shows that Switzerland's legal framework is well suited to dealing with new technologies. Nevertheless, there is still a need for selective legal adjustments. The Federal Council has instructed the Federal Department of Finance (FDF) and the Federal Department of Justice and Police (FDJP) to draw up a consultation draft in 2019 which regulates the following aspects:

- in civil law, increase legal certainty for the transfer of rights by means of digital registers,
- in insolvency law, further clarify the segregation of cryptobased assets in the event of bankruptcy and examine the segregation of data with no asset value,
- in financial market law, devise a new and flexible authorisation category for blockchain-based financial market infrastructures,
- in banking law, reconcile the bank insolvency law provisions with the adjustments in general insolvency law, and
- in anti-money laundering law, more explicitly anchor the current practice of making decentralised trading platforms subject to the Anti-Money Laundering Act.

In summary, the Federal Council wants to create the best possible framework conditions for the promotion of Switzerland as a location for fintech and blockchain companies, as well as consistently combat abuses in order to guarantee the integrity and reputation of Switzerland as a financial centre and business location.

At the same time, the Federal Council published a report by the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF) on the money laundering and terrorist financing risks posed by cryptoassets and crowdfunding. The report states that crypto-based assets constitute a threat in the area of money laundering and terrorist financing. Due to the small number of cases, however, the real risk in Switzerland cannot be estimated conclusively. Improvements in this area should be sought above all by means of internationally coordinated measures. On the other hand, the FDF was charged with examining whether the money laundering law should be adapted with regard to certain forms of crowdfunding.

The future will show whether these measures will be sufficient to sustainably secure the attractiveness of the blockchain location and the anchoring of the Swiss Crypto Valley. The re-

cently founded "Swiss Blockchain Federation", under the leadership of Heinz Tännler, a member of the Zug Cantonal Council, aims to maintain and expand the appeal and competitiveness of Switzerland as a blockchain location, network relevant players and strengthen the blockchain ecosystem in Switzerland.

This task seems central, since Liechtenstein is proposing a blockchain law that is to come into force in the summer of 2019. These framework conditions also attract companies from the Swiss Crypto Valley.

The Principality of Liechtenstein notes that due to the high density of regulation in the financial market, innovative companies repeatedly come up against legal limits. From a state perspective, it is important to Liechtenstein's head of government, Adrian Hasler, that such companies have clarity about opportunities and limitations. Furthermore, it is clear that the potential of blockchain technology lies not only in the financial services sector, but that a much larger range of assets can be digitally represented and made available for every conceivable service. Liechtenstein has opted for a blockchain law because the fields of application of the token economy cover the entire economy and represent a further step in digitalisation. With the "token" as a new legal element, Liechtenstein is creating an instrument with which any law from the analogue world can be digitally represented. But also borders and activities worthy of protection are to be regulated in the new law in order to limit the risk of abuse.

This approach creates security and is an important basis for innovation and investment.

Information:

"Legal framework for distributed ledger technology and blockchain in Switzerland" report

https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf

Report of the interdepartmental coordinating group on combating money laundering and the financing of terrorism on "money laundering and terrorist financing risks posed by cryptoassets and crowdfunding"

https://www.newsd.admin.ch/newsd/message/attachments/55111.pdf

FINMA Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)

https://www.finma.ch/de/news/20v18/02/20180216-mm-ico-wegleitung/

Liechtenstein Government consultation report on the creation of a law on transaction systems based on trusted technologies (TT) (Blockchain Act; VT Act; VTG):

https://www.llv.li/files/srk/vnb-blockchain-gesetz.pdf

8 Published MELANI products

8.1 GovCERT.ch blog

8.1.1 Reversing Retefe

Approximately one year ago, we published our blog post The Retefe Saga. Not much has changed since last year except that we have seen a rise in malspam runs in the last couple of weeks and we want to use the opportunity to show how to reverse engineer the Retefe malware.

➔ https://www.govcert.ch/blog/35/reversing-retefe

8.2 MELANI newsletter

8.2.1 Increase in fraudulent calls to companies again

05.07.2018 - In recent days, calls to potential victim companies in which attackers pose as bank employees have increased again. The callers ask for the execution of payments or pretend to have to carry out an e-banking update which then needs testing.

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

8.2.2 Phishing attacks on online data exchange and collaboration platforms

02.10.2018 - Many companies allow their employees to share documents online and even access entire office systems online. Sometimes just a password is enough to access an email account, but also various other documents. It is therefore not surprising that this access data is of great interest for phishing attacks. Compromising a first account is therefore often used as a further attack vector against other employees.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/phishing_online_datenaustausch_kollaborationsplattformen.html

8.2.3 Whoever uses the same password more than once, helps attackers

08.11.2018 - The 27th Semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI), published on 8 November 2018, addresses the most important cyber incidents of the first half of 2018 both in Switzerland and abroad. The key topic is dedicated to the vulnerabilities in hardware. The focus is also on targeted malware attacks, for which the name of the Spiez laboratory was misused, as well as various data leaks and the problem of using a password multiple times.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/melani-halbjahresbericht-1-2018.html

8.2.4 Trojan Emotet attacks corporate networks

12.12.2018 - MELANI is currently witnessing various malspam waves with infected Word documents attached. This is a Trojan named "Emotet" (also known as Heodo) which has been known for some time. Originally known as an e-banking Trojan, Emotet is now mainly used to send spam and download other malware. Emotet tries to use social engineering to use fake e-mails on behalf of colleagues, business partners or acquaintances to trick the recipient into opening the Word document and executing the Office macros it contains.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html

8.3 Checklist and instructions

In the second half of 2018, MELANI did not publish any new checklists or instructions.

9 Glossary

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

Defacement	Unauthorised alteration of websites.
Domain name system	With the help of DNS, the internet and its services can be utilised in a user-friendly way, because users can utilise names instead of IP addresses (e.g. www.melani.admin.ch).
Downloader	A downloader is a program that downloads and installs one or more instances of malware.
DriveBy-Infection	Infection of a computer with malware simply by visiting a website. Often the websites concerned contain reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
E-currency services	A monetary value in the form of a receivable from the issuing authority. The value is saved on a data carrier, issued in return for a sum of money – the value of which is not less than the issued monetary value – and accepted by companies other than the issuing authority as a means of payment.
Exploit-Kit	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
Financial agent	A financial agent works as a legal money broker and thus engages in financial transfers. Recently, this term has been used in connection with illegal financial transactions.
Global Positioning System (GPS)	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation satellite system for determining position and measuring time.
Industrial control systems (ICSs)	Control systems consist of one or more devices that control, regulate, and/or monitor the behaviour of other devices or systems. In industrial production, the term "industrial control system" (ICS) is often used.
JavaScript	Is an object-based scripting language for developing applications. JavaScripts are program components integrated in HTML code enabling specific functions in internet browsers. For example, while checking user input on an internet form, a JavaScript can verify that all the characters entered of a telephone number are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the computer of the website vis-

	itor. 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.
Metadata	"Metadata" and "meta-information" refer to data containing information about other data.
MITM	Man-in-the-middle attacks (MITM) Attacks in which the attacker infiltrates unnoticed the communication channel between two partners and is thereby able to spy on or even modify their data exchanges.
mobileTAN	mobileTAN is a way to incorporate text messages (SMSs) as a transmission channel. After online banking clients transmit their completed funds transfer requests on the internet, the bank sends them a text message on their mobile phone with a TAN that can be used only for that transaction.
P2P	Peer to Peer Network architecture in which those systems involved can carry out similar functions (in contrast to client-server architecture). P2P is often used for exchanging data.
Patch	Software that replaces the faulty part of a program with an error-free part, thereby eliminating a vulnerability, for example.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting internet users. For example, this can be account information from online auctioneers (e.g. eBay) or access data for online banking. The fraudsters take advantage of their victims' good faith and helpfulness by sending them emails with false sender addresses.
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.

Remote Administration Tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
Router	Computer network, telecommunication, or also internet devices used to link or separate several networks. Routers are used in home networks, for instance, establishing the connection between the internal network and the internet.
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a standard advanced mobile phone.
SMB protocol	Server message block (SMB) is a network protocol for file, printing and other server services in computer networks.
SMS	Short Message Service for sending text messages (160 characters maximum) to mobile phone users.
Social Engineering	Social engineering attacks take advantage of people's helpfulness, credulity or lack of self confidence in order to gain access to confidential data or to prompt them to perform certain actions, for example.
Spam	Spam refers to unsolicited and automatically sent mass advertising, into which category spam e-mails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
Spearphishing emails	Targeted phishing attack. For example, victims are tricked into believing that they are communicating with someone they know by email.
Supply chain attacks	Attack in which an attempt is made to infect the actual target via the infection of a company in the supply chain.
Take-down	Expression used when a provider takes down a site from the network due to its fraudulent content.
Top-Level-Domains	Every name of a domain on the Internet consists of a sequence of character strings separated by periods. The term "top level domain" refers to the last name in this sequence, constituting the highest level of the name resolution. If the full domain name of a computer or website is de.example.com, for instance, the right-

	most member of the sequence (com) is the top level domain of this name.
Transmission Control Protocol / Internet Protocol (TCP/IP)	Transmission Control Protocol / Internet Protocol (TCP/IP) is a family of network protocols, also referred to as the Internet protocol family because of its great importance for the Internet.
Two-factor authentication	For this, at least two of the following three authentication factors are required: 1. Something you know (e.g. password, PIN, etc.) 2. Something you have (e.g. a certificate, token, list of codes, etc.) 3. Something you are (e.g. finger print, retina scan, voice recognition, etc.)
UDP	The User Datagram Protocol, short UDP, is a minimal, connectionless network protocol that belongs to the transport layer of the internet protocol family.
USB	Universal Serial Bus (with a corresponding interface) which enables peripheral devices such as a keyboard, mouse, external data carrier, printer, etc. to be connected. The computer does not have to be switched off when a USB device is unplugged or plugged in. For the most part, new devices are automatically identified and configured (depending on the operating system).
Vulnerability	A loophole or bug in hardware or software through which attackers can access a system.
Watering-hole attacks	Targeted infection by malware via websites that tend to be visited only by a specific user group.
WLAN	WLAN stands for Wireless Local Area Network.
Worm	Unlike viruses, worms do not require a host program in order to propagate. Instead, they use vulnerabilities or configuration errors in operating systems or applications to spread by themselves from one computer to another.
Zero-Day	An exploit which appears on the same day as the security holes are made public.
ZIP-File	zip is an algorithm and file format for data compression, in order to reduce the storage space needed for the archiving and transfer of files.