Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

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

INFORMATION ASSURANCE

SITUATION IN SWITZERLAND AND INTERNATIONALLY

Semi-annual report 2019/1 (January – June)

29 OCTOBER 2019

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

1 Overview / contents

2 Editorial

Ransomware – public administrations can also be hit

Martin Müller is ICT Security Officer for the city administration of Bern, member of various national working groups on ICT security and a Swiss Certified ICT Leader.

Ransomware, crypto-Trojan, encryption Trojan, blackmail Trojan ... whatever we call it, this kind of software, and the ransom demand that appears following successful infiltration by a Trojan, are well known since WannaCry and the accompanying media coverage. The ransoms demanded for unlocking the encrypted files range from a few hundred to several thousand US dollars, payable in bitcoins. However, there is no guarantee that the key for decrypting your files will ever be handed over.

The city administration of Bern was hit by such attacks in 2017 and 2019. The attackers did not target the administration specifically, but used a scatter-gun approach to garner as much money as possible. The aspect that keeps most security officers awake at night is the fact that such attacks can be carried out with the minimum of knowledge and resources nowadays. The so-called Ransomware-as-a-Service (RaaS) model can be bought cheaply from various suppliers on the darknet. As a result, this kind of attack is no longer available only to cybercrime professionals, but to everyone from attention-seeking script kiddies to politically motivated hacktivists.

In addition to all manner of technical security precautions, such as firewalls, intrusion detection and prevention systems, antivirus systems, email security solutions, and constant software and hardware updates, another important technical measure is regular backups. Storage for these backups should be physically or logically segregated from the rest of the company network. In this way, operations can be restarted and data losses kept to a minimum in the event of an incident. The city of Bern's backup management has so far proved its worth during the attacks on the administration.

Besides all the technical means that are available in the field of ICT today, it is still the people who are, and should be, the main focus. We therefore regard employee training and awareness as the most important measure and a core element of ICT security. With the digital transformation taking place in public administrations, we need to create the basis for employees to use the new technology safely, responsibly and with confidence. A healthy dose of scepticism and common sense also contribute to security. For this reason, in its digital strategy for 2021 and its 2019-2020 ICT security campaign, Bern's city administration has deliberately put people's empowerment and capacity building centre stage. We recommend that you do the same.

Martin Müller

3 Key topic: ransomware

Ransomware (*malware* using encryption or blackmail Trojans) is an established tool for attacks in the world of cybercrime. Encryption Trojans target the availability of data with the aim of extortion. However, albeit to a lesser extent, another goal can also be to harm a company. Encryption Trojans have evolved both technically and tactically over the years, making them one of the most dangerous threats for businesses. An increase in targeted attacks on organisations and a rise in ransom demands were observed worldwide in the first half of 2019.

3.1 Historical development

MELANI described the emergence of *malware* that blocks computers for blackmail purposes as early as eight years ago.[1] That was one of the first versions of ransomware, which blocked the screen and displayed a message purportedly from the Federal Department of Justice and Police (FDJP). The message claimed that a fine had to be paid because illegal material had allegedly been found on the computer. This type of *malware* was relatively harmless and could be removed in most cases by simply analysing the computer with an antivirus live CD.

Two years later, CryptoLocker was the first *malware* with an encryption function to hit the headlines.[2] CryptoLocker encrypted files on both the hard disk and all locally connected media. A specific key was generated for each victim on a *C2* server. This made data recovery more difficult than in the case of encryption Trojans that use a hard-coded and therefore extractable key. CryptoLocker spread through infected email attachments (*malspam*) and *drive-by infections* (manipulated websites), or was downloaded via a *dropper* already installed on the device (independently executable program file). Propagation via *droppers* is currently widespread.

In 2014, the SynoLocker ransomware was propagated by exploiting a security vulnerability in Synology *NAS* devices.[3] The vulnerability it exploited was known, and a security update had been released months earlier. This case demonstrated the need to update not only computer programs and operating systems, but also routers, *NAS* devices and similar components on a regular basis. Ransomware programmers began taking steps to make the detection and analysis of *C2* servers more difficult in 2014. For example, the encryption Trojan CTB-Locker, which was spread through hacked online media websites, communicated encrypted with its *C2* servers and used the Tor anonymisation service to cover its tracks and hamper detection and analysis by security players.

Criminals have always been on the lookout for new targets. For example, databases of poorly secured websites were also targeted and encrypted to demand a ransom from the website administrators.[4] TeslaCrypt and CryptoWall were the most active ransomware families in 2015.[5]

[1] MELANI semi-annual report 2011/2, section 3.5.

[2] MELANI semi-annual report 2013/2, section 3.1.

[3] MELANI semi-annual report 2014/2, section 3.6.

[4] MELANI semi-annual report 2014/2, section 5.3.

[5] MELANI semi-annual report 2015/1, section 4.6.1.5 and 2015/2, section 4.5.1.

The ransomware phenomenon was booming in 2016.[6] For the first time, it hit high-profile critical infrastructures, especially hospitals in Germany and the United States. The healthcare sector not only faces the challenge of installing security updates and keeping all ICT systems and certified medical technology up to date, but also has to react more quickly than other victims in the event of failures, as an inoperative ICT infrastructure can endanger human lives. As a result, there is quite a lot of pressure to pay ransoms in order to quickly become operational again. However, responding to extortionists' demands is not necessarily an effective approach, as evidenced by the example of Kansas Heart Hospital. The hospital received the key for only some data from the blackmailers and was then faced with a second ransom demand to decrypt the remaining data.[7]

Ransomware made further technical progress with Locky, which became active in Switzerland too from February 2016.[8] It encrypted files that were stored on connected network devices (cloud drives, network shares, etc.). The exponential increase in the phenomenon prompted security authorities to step up preventive measures. MELANI organised a ransomware awareness day in collaboration with various federal offices, Swiss associations and organisations, and software companies.[9] Germany's Federal Office for Information Security (BSI) published a report on the ransomware situation.[10]

In the first half of 2017, two international ransomware attacks clearly demonstrated the risk potential of such attacks. WannaCry attacked at least 200,000 computers in 150 countries, and its most prominent victims were the Spanish telecommunications company Telefonica, hospitals in the United Kingdom and Deutsche Bahn. Switzerland had several hundred victims, but no critical infrastructures were among them. Shortly afterwards, the *malware* NotPetya struck initially in Ukraine, where it successfully attacked Kiev airport, the Ukrainian central bank and the Chernobyl radioactivity monitoring station, for instance. The *malware* then spread globally via Ukrainian offshoots of multinational firms. Notable victims included Denmark's Maersk (the world's largest container shipping company) and the US pharmaceutical giant Merck. NotPetya also hit victims in Switzerland, such as the advertising firm Admeira.[11] The common feature of the WannaCry and NotPetya attacks is that the *malware* spread in networks like a worm, i.e. independently, by exploiting a vulnerability in the *SMB protocol*. While the spread of WannaCry seemed random, it is assumed that Ukrainian companies were generally targeted by NotPetya. Security experts raised questions about the existence of purely criminal motivation in both cases. Although there are no definitive answers regarding the attackers and their motivation, it is assumed that sabotage or the triggering of panic was the goal in both cases.

[6] MELANI semi-annual report 2016/1, section 5.4.3.

[7] https://www.csoonline.com/article/3073495/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html

[8] MELANI semi-annual report 2016/1, section 4.6.3.

[9] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/ransomwareday.html; https://www.switch.ch/news/ransomware-day/; https://www.ebas.ch/de/securitynews/509-nationaler-ransomware-awareness-tag

[10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Lagedossier_Ransomware.pdf

[11] MELANI semi-annual report 2017/1, chapter 3.

In the second half of 2017, the ransomware BadRabbit was at the origin of geolocated attacks, mainly in Russia, but also in Ukraine, Germany and Turkey. BadRabbit spread via fake Adobe Flash updates and used the EternalRomance exploit to, like Mimikatz, infiltrate the affected companies' systems and obtain access data for further propagation.[12]

In 2018, the Taiwanese microchip manufacturer TSMC (Taiwan Semiconductor Manufacturing Company) experienced the loss of productivity that can be caused by ransomware and persists until the systems affected by ransomware are restored. It had to stop production at several plants because of a WannaCry variant.[13]

Ransomware attacks were generally not targeted until 2018. Only the SamSam group was known for targeted attacks. It used encryption Trojans largely against US organisations. The emergence of Ryuk in 2018 marked the start of a form of ransomware apparently placed specifically within organisations from which high ransoms can be demanded. Ryuk was discussed in the last semi-annual report[14] and it has been very active also in 2019 (see section 3.4.1). Ransomware that is used in both a targeted and opportunistic manner likewise exists, e.g. GandCrab and Dharma.[15]

3.2 Latest incidents

The number of targeted ransomware attacks increased in the first half of 2019. The aforementioned Ryuk, GandCrab and Dharma were joined by LockerGoga, MegaCortex and RobbinHood. The last type of ransomware paralysed Baltimore city government computers at the end of May.[16] Ransomware attacks are one of the most dangerous cyberthreats for businesses, organisations and administrations. A successful attack not only requires time, manpower and money to clean up systems and recover lost data, but can also damage a company's reputation or result in a loss of productivity over a certain period.[17] For example, the aluminium producer Norsk Hydro was forced to switch from its basically automated production to partial manual mode due to a ransomware attack,[18] and police officers in Jackson County, Georgia, had to resort to writing their reports manually again after the government's systems were crippled by Ryuk.[19] In Switzerland, Ryuk's victim Offix Holding AG (see also section 3.4.1) avoided the worst of the impact by setting up emergency operations within a few hours, thereby making it possible to inform customers and continue the company's daily work while solving the computer problems. The company did not respond to the ransom demand of 45 bitcoins (approximately CHF 330,000).[20]

During the period under review, there have also been incidents involving the simultaneous use of two cyberthreats: ransomware and phishing. The encryption Trojan discovered not only

[12] MELANI semi-annual report 2017/2, section 5.4.2.

[13] MELANI semi-annual report 2018/2, section 5.3.5.

[14] MELANI semi-annual report 2018/2, section 4.5.4.

[15] https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

[16] https://www.tripwire.com/state-of-security/featured/ransomware-baltimore-network/

[17] https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

[18] https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/

[19] https://statescoop.com/georgia-county-paid-400k-to-ransomware-hackers/

[20] https://www.inside-it.ch/articles/54898

encrypts files, but also attempts to elicit sensitive data from the victims at the same time. Victims can choose to pay the ransom with bitcoins or PayPal. If they choose PayPal, they are directed to a phishing site, where they are asked to enter their credit card information, as well as their PayPal access data and other personal details.[21]

As attackers have realised that their plans can be thwarted by backups, they have changed their modus operandi. Now they first obtain the necessary access details and passwords so that they can also delete or encrypt the backups before they start encrypting the operational systems.

It is not surprising that companies that do not have a backup or whose backup has been rendered unusable decide to pay the ransom as they find themselves in a situation that threatens their very existence. As early as 2014, MELANI declared that ransomware would be successful as long as victims were willing to pay.[22] In the first half of 2019, the cases of two cities in Florida caused a sensation: Riviera City and Lake City. They said that they were willing to pay the exorbitant ransom demands of 65 bitcoins (around USD 600,000) and 42 bitcoins (around USD 500,000). In the case of Lake City, the ransom claim was negotiated directly with the city's insurance provider.[23] This trend could become established in Switzerland as well.[24] However, paying the ransom is not a "worthwhile investment" in the long term because the more companies are willing to pay a ransom, the more cybercriminals will be incited to switch to this business model.[25]

3.3 Ransomware-as-a-Service

With the increasing division of labour and specialisation in cybercrime circles, the underground market is likewise evolving. Preconfigured cyberattacks have been on offer in the Darknet for some time now.[26] These are known as Cybercrime-as-a-Service (*CaaS*) or, in the case of ransomware, as *RaaS*. As a result, even people without specialist computer skills can launch a cyberattack.[27] This type of service offers the components required for an attack at a certain price, i.e. instructions for creating the *malware*, the dashboard, which provides all the necessary information about successful infections, the decryption key and, if necessary, a tutorial on how to use the tools provided. "Customers" can take this basic package and then adapt their ransomware and attack to their needs.[28]

[21] https://www.bleepingcomputer.com/news/security/new-ransomware-bundles-paypal-phishing-into-its-ransom-note/

[22] MELANI semi-annual report 2014/2, section 5.3.

[23] https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/

[24] https://www.nzz.ch/wirtschaft/ransomware-warum-zahlreiche-firmen-loesegeld-zahlen-duerften-ld.1489507

[25] https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

[26] See MELANI semi-annual report 2009/2, section 4.7: "In the field of cybercrime, the commercial model of Crime-ware-as-a-Service (CaaS) was developed over the course of last year. Using this model, cybercriminals who are not very familiar with the technical aspects can "rent" the desired service."

[27] For more details, see MELANI semi-annual report 2016/2, section 6.1.

[28] https://securityaffairs.co/wordpress/84273/breaking-news/inpivx-ransomware-service.html

3.4 Particularly active ransomware at present

3.4.1 Ryuk

The Ryuk ransomware has been active since the second half of 2018 and was discussed already in the last semi-annual report.[29] Ryuk was used to attack Tribune Publishing in Los Angeles in December. The attackers encrypted the server, which supported the production platform for printing and distributing several US newspapers. The outage delayed or partly prevented the publication of the Saturday editions of the Los Angeles Times and the San Diego Union Tribune, as well as the West Coast publications of the Wall Street Journal and New York Times.[30]

Ryuk is used to launch targeted attacks on computers and corporate network servers. Data encryption is often the final stage of a three-stage attack that begins with an Emotet Trojan infection. Emotet is often distributed via email with an infected link or attachment (*malspam*). If someone in the company naively clicks on it, Emotet installs itself on their computers and then sends emails to their contacts in order to spread further. Emotet can act as a *dropper* for other *malware*. Trickbot is downloaded in some cases, for example (see section 4.6), and it analyses the attacked network to find out whether it belongs to an individual or a business. If it belongs to a business, Trickbot attempts to spread over the network by exploiting the *SMB* security vulnerability. In this way, further information is gathered about the potential victim. Ryuk is usually downloaded only if the victim is considered sufficiently attractive. [31]

Targeted attacks were carried out with Ryuk this year, and then exorbitant ransom amounts were demanded. The victims included the administrations of some US cities, which paid ransoms of between USD 130,000 and USD 600,000.[32]

In Switzerland, there were cases in construction, public transport and manufacturing. For example, Offix Holding AG, an office supplies and stationery company, was badly hit "by a targeted, planned, massive and orchestrated hacker attack"[33] in mid-May.[34] The conduit was a Word document sent by email that installed the Emotet *malware* via a macro. Trickbot and Ryuk were then downloaded. Two days later, a large proportion of the company's systems no longer worked: time recording, salary administration, image databases, telephone servers, Citrix servers, Exchange servers and others.[35] Only the web shops, running on Linux servers, and the merchandise management system were spared.

[29] MELANI semi-annual report 2018/2, section 4.5.4.

[30] https://www.heise.de/newsticker/meldung/Cyber-Attacke-verzoegert-Druck-grosser-Tageszeitungen-in-den-USA-4260103.html

[31] MELANI semi-annual report 2018/2, section 4.5.4.

[32] https://www.bleepingcomputer.com/news/security/la-porte-county-pays-130-000-ransom-to-ryuk-ransomware/

[33] Offix Holding AG client communication according to Inside-IT: https://www.inside-it.ch/articles/54898

[34] https://www.nzz.ch/wirtschaft/cyber-angriff-auf-schweizer-firma-offix-ein-kampf-ums-ueberleben-ld.1492862

[35] https://www.inside-it.ch/articles/54898

3.4.2 LockerGoga and MegaCortex

LockerGoga first appeared in January 2019, when France's multinational engineering and industrial consultancy Altran Technologies was attacked.[36] LockerGoga is typically only part of the second phase of an infection and is executed by a PsExec tool on a previously infected device. Attackers use hacking tools available online to gain access to the system and obtain administrator rights to deactivate security software and backups before installing the ransomware. This technique, together with the use of legitimate certificates, allows *malware* to escape detection by protective measures.[37] After installation, LockerGoga changes the system access data and attempts to terminate the session of connected users. LockerGoga thereby tries to encrypt as many devices as possible at the same time. However, the ransomware creates a separate process for each file to be encrypted, which is quite unusual, as it slows down the encryption considerably.[38]

In March, at least three prominent companies fell victim to LockerGoga: Hexion and Momentive, two US companies owned by the private equity firm Apollo Global Management that produce resins, silicones and other materials, and the Norwegian aluminium producer Norsk Hydro.[39] In the case of Norsk Hydro, it appears that a US subsidiary was first infected, and the *malware* then moved laterally through the network, infecting almost all workstations. It was necessary to switch to manual operation in some places, as the production system was no longer available. The criminals apparently changed Active Directory account passwords. The attackers possibly received the so-called Kerberos tickets with Mimikatz or a similar tool and were able to use them to fake their identity as users or prove their identity for the system.[40]

MegaCortex works in a similar way to LockerGoga. Attacks with this ransomware target companies and organisations. According to various sources, almost 50 companies in the United States, Europe and Canada were infected by MegaCortex in just 48 hours.[41] Sophos researchers say that there are no code similarities between MegaCortex and LockerGoga, but in both cases operators leverage a compromised *domain controller* to push *malware* out to machines on a target network. PowerShell commands are executed to contact the criminally controlled *C2* servers and initiate encryption. The researchers explained in a blog post that at least one of the *C2* servers that MegaCortex contacted had also been used by LockerGoga.[42] Like Ryuk, MegaCortex was often detected in companies with pre-existing Emotet and Qbot infections.[43] There have been reports of activity by these cryptotrojans also in Switzerland.

[36] https://ml.globenewswire.com/Resource/Download/0663f8d4-0acf-4463-b0fd-bb05042d1373, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

[37] https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

[38] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

[39] https://www.chemistryworld.com/news/hexion-momentive-and-norsk-hydro-all-hit-by-ransomware-cyber-attacks/3010328.article

[40] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

[41] https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696

[42] https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

[43] https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696

3.4.3 GandCrab

GandCrab accounted for 50% of the global ransomware market in the second half of 2018. This was possible because the *malware* developers worked according to a Ransomware-as-a-Service (*RaaS*) model and offered their *malware* on the darkweb. The price was 40% of the profits generated by attacks with this tool.[44] This also explains the large number of vectors used to spread the *malware*: several variants of mass emails (*malspam*), as well as supposed application letters and *drive-by infections* placed on hacked websites or on websites specifically set up by criminals for this purpose.[45]

Since it emerged in January 2018, there have been several versions and revisions of the GandCrab code, which have made attacks more effective and more difficult to combat. *Malware* authors also rely on redundancy: the use of a combination of GandCrab with BetaBot or AzorUlt was observed in some attacks this year. BetaBot has functions to avoid detection by deactivating antivirus programs and firewalls. It then analyses the victim's device and collects information such as access data and e-banking login details. Meanwhile, the second type of *malware* (e.g. GandCrab) ensures the redundancy of the affected system's infection even in the event of a system crash.[46]

The cloud service provider Meta10, based in Zug, was hit by the ransomware GandCrab v5.2 on 22 February 2019.[47] Some database and application servers were affected, as were backup servers. The system clean-up and document recovery led to noticeable performance losses for around 10% of the company's customers. Meta10 immediately opted for proactive communication and informed its customers about the incident. The "Service Status" page kept them constantly abreast of the incident. Bern's city administration likewise fell victim to a GandCrab attack in 2019, but it was able to recover quickly from the incident thanks to its exemplary backup management.[48]

At the end of May 2019, the operators of GandCrab announced that their ransomware had generated ransom payments of USD 2 billion and they intended to shut down their operations. They asked their partners to stop distributing GandCrab within 20 days and encouraged the victims to pay their ransom as quickly as possible to prevent their data from being lost forever.[49]

Since mid-June 2019, nomoreransom.org has provided a tool that can decrypt the versions (1, 4 and 5 to 5.2) of the GandCrab ransomware currently in circulation. The tool was developed in collaboration with law enforcement agencies from various countries with the support of Bitdefender and enables victims to recover their encrypted files.[50] A week before this tool was released, a Syrian father tweeted that he did not have enough money to pay the ransom and

[44] https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware

[45] MELANI semi-annual report 2018/2, section 4.5.4.

[46] https://www.scmagazineuk.com/gandcrab-returns-trojans-redundency/article/1523389

[47] https://www.computerworld.ch/security/hacking/cyberangriff-legt-zuger-cloud-provider-meta10-lahm-1684975.html

[48] See the editorial of the ICT Security Officer of Bern's city administration in chapter 2 above.

[49] https://securityaffairs.co/wordpress/86438/malware/gandcrab-shutdown-operations.html

[50] https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware

therefore could not retrieve the photographs of his dead son. The GandCrab administrators felt sorry for him and decided to provide a decryption key for the Syrian victims of their ransomware.[51]

It is conceivable that the "retirement" announcement was a step to divert attention and regroup. Some security experts believe that the GandCrab operators are already back in business and are behind a ransomware program known variously as REvil and Sodinokibi.[52] The Sodinokibi *malware* has already hit its first Swiss victims.

3.5 Outlook

There will continue to be technical and methodological developments in connection with ransomware in the years ahead. Attacks can be expected to be even more targeted and the attack vectors even more technically sophisticated. Eliminating vulnerabilities and keeping basic network protection high will be all the more important. Criminals are typically opportunistic: if too much effort is required and there is no success within a reasonable period of time, the goal is not worth striving for and they move on.

As has been apparent for some years now, the exponential growth of devices connected to the internet (Internet of Things, IoT) is providing criminals with an increasingly broad field of attack.[53] This development means that most of the electronic devices we use daily are connected to a home network or even directly to the internet and are thus potentially vulnerable. There are various scenarios in which criminals render a device temporarily unusable in order to blackmail its owner.

However, law enforcement agencies are also gearing up and working together with security authorities and private companies at various levels in order to put a stop to the perpetrators. They are coordinating matters both nationally and internationally, and initial successes have been achieved.[54]

3.6 Guest article: Joining forces to combat cybercriminals

by Daniel Nussbaumer, Head of Cybercrime, Zurich Cantonal Police, and Head of NEDIK

Criminals who are digitally agile require digitally agile law enforcement agencies. In the fight against cybercriminals, it is crucial for the Confederation and the cantons to maintain a constant exchange and be able to react quickly. The Swiss police corps has therefore joined forces in the police network known as NEDIK so as to work together and in close cooperation with MELANI to repress and prevent cybercriminals.

Targeted, professional cyberattacks on businesses can jeopardise their very existence. The businesses hit are regularly concerned about their survival. Accordingly, they have new or

[51] https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

[52] https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/ and https://www.tesorion.nl/aconnection-between-the-sodinokibi-and-gandcrab-ransomware-families/

[53] MELANI semi-annual report 2014/2, section 5.3.

[54] https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public; https://www.maketecheasier.com/man-arrested-for-spreading-shame-driven-ransomware/

changed needs vis-à-vis the authorities. If a company is attacked, it is important for it to know how the perpetrators entered a system, which systems are compromised, how it should deal with any ransom demands and whether it is the only company hit.

The Swiss police corps and MELANI can help in such situations. All police corps units in Switzerland have joined forces in NEDIK, the intercantonal Network for Investigative Support in the Fight against Cybercrime, in order to be able to respond quickly and jointly to cyberattacks. Thanks to a regular operational exchange in this network and the direct dissemination of current, new cases and case developments, we are now able to detect correlations very quickly and react appropriately and make corresponding recommendations – also due to the close exchange with MELANI in the event of an incident. Thanks to the participation of the Federal Office of Police (fedpol) in NEDIK and its cooperation with Europol, we can also act directly beyond national borders in the event of new incidents.

NEDIK offers added value, but not only in terms of incident management. Together with MELANI, we produce bulletins on the cyberspace situation within the framework of NEDIK and jointly develop prevention tips and strategies to avert and combat cybercrime. We provide these best practices to all police corps units in order to offer those affected in all cantons the best possible support to protect against cyber-risks, be it in the area of prevention or repression.

Recommendations:

MELANI recommends the following measures to protect against ransomware:

- **Make regular backups of your data, e.g. on an external hard drive, using the generation principle (daily, weekly, monthly / at least two generations). Make sure that the medium where the backup is saved is physically disconnected from the computer or network after the backup process. Otherwise, there is a danger that attackers could also gain access to the backup data and encrypt or delete it.**
- With cloud-based backup solutions, you should ensure that the provider has at least two generations, like with classical backups, and that these are not accessible to ransomware, e.g. they require *two-factor authentication* for critical operations.
- Operating systems and all applications installed on computers (e.g. Adobe Reader, Adobe Flash, Java, etc.) must be updated consistently and immediately. It is best to use the automatic update function if available.
- In addition, protect all resources accessible from the internet (especially terminal servers, RAS and VPN access) with a second factor. Place a terminal server behind a VPN portal.
- Block the receipt of dangerous email attachments on your email gateway, including Office documents with macros if possible.
- Monitor the log files of your antivirus software for irregularities.

4 Situation in Switzerland

4.1 Espionage

4.1.1 Lazarus attacks Swiss banks

In March 2019, security software company McAfee published a follow-up to its December 2018 report on the Sharpshooter campaign. Last year, the campaign targeted 87 companies from all over the world, but mainly in the US. The companies concerned were from the defence, energy, nuclear and financial sectors.[55] In this second report, McAfee confirmed their initial suspicion that the Lazarus group was behind the attacks. Lazarus is well known for having attacked systems at various banks[56] and is considered by many experts to be connected to the North Korean regime.

Already in its first report, McAfee described attempted attacks against Swiss financial institutions. MELANI is in contact with a number of banks, as mentioned in the previous semi-annual report.[57] However, then as now, no evidence of infection has been found at the potential target companies in Switzerland.

4.1.2 APT40

China's current strategy for fostering business relations between Asia and Europe is based on the development of logistical and transport infrastructures. The ICT security service provider FireEye has uncovered an espionage operation[58] which has been running since at least 2013 and is targeting countries that are of strategic importance for the new Silk Road (Belt and Road Initiative, or BRI), including Switzerland.[59] The APT40 group (also known as Leviathan or TEMP.Periscope), which is thought by FireEye to have links to the Chinese government, is behind this operation aimed at obtaining information in support of the modernisation of the maritime sector in general and shipbuilding capabilities in particular.

The group uses phishing emails with malware attachments and *drive-by infections* to attack the defence, transport and shipping technology sectors. Already in 2017, the identity of a manufacturer of autonomous submarines was usurped to infiltrate universities conducting research in the area of shipbuilding. This is a sector that, for both commercial and defence reasons, is of fundamental importance to the Chinese government.[60] This area of research has therefore become the focus of other espionage campaigns, to which Beijing is likewise thought to be connected (see also section 4.1.4).

[55] MELANI semi-annual report 2018/2, section 4.1.2.

[56] https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

[57] MELANI semi-annual report 2018/2, section 4.1.2; https://www.tagesanzeiger.ch/sonntagszeitung/nordkorea-greift-schweizer-banken-an/story/15090344

[58] https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

[59] Information about the Belt and Road Initiative at http://english.www.gov.cn/beltAndRoad/ and http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm

[60] Chinese strategy «Made in China 2025»: http://english.www.gov.cn/2016special/madeinchina2025/; http://en.people.cn/n/2015/0522/c98649-8895998.html

In addition to campaigns targeting research and manufacturing, APT40 also carries out espionage campaigns against organisations in South East Asia, or is involved in territorial disputes in the South China Sea. In 2018, a number of Cambodian authorities which had been involved in organising the country's elections were compromised.[61] Cambodia is among the strategically important countries for the new Silk Road.

To date, no evidence of infection has been detected at companies potentially affected in Switzerland.

4.1.3 VPNFilter

In May last year, Cisco's threat intelligence team Talos reported on the VPNFilter botnet. It is said to comprise at least half a million routers and *NAS* devices located in 54 countries, above all in Ukraine.[62]

The VPNFilter *malware* has a modular structure and various functionalities. For example, the *malware* can render an affected device completely unusable, but it is also able to spread through a network and infect other systems ("lateral movement"). It can steal information (especially access data) and divert internet traffic to another recipient. In addition, one module searches for and monitors any Modbus network traffic.[63] Modbus is a communication protocol that is often used by industrial control systems.

The VPNFilter botnet also had the potential for use in sabotage. But the FBI took control of part of the *command and control* infrastructure at virtually the same time as the existence of the botnet became known. As a result, not only were the infected devices identified, but the transmission of commands from the botnet operators was also prevented.

Although updates which allow security software to identify and stop the *malware* have been released, MELANI is aware of a few hundred active infections in Switzerland. In order to eliminate the *malware* and remove security vulnerabilities, devices will need to have the factory settings restored, and then be updated.

Recommendations:

The network infrastructure is increasingly the focus of attacks by cybercriminals. Routers and switches are rewarding targets, as they often have a direct connection to the internet but are not always adequately protected and can therefore offer an easy gateway into home or corporate networks.

Any device with a direct internet connection requires specific protection against unauthorised access. This includes not just the use of a strong password, but also the fastest possible importing of updates.

[61] https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

[62] MELANI semi-annual report 2018/1, section 5.1.2.

[63] https://blog.talosintelligence.com/2019/05/one-year-later-vpnfilter-catastrophe.html

4.1.4 APT10

In the first half of 2019, new victims of the APT10 cyberespionage campaign emerged. The group, which has been active since 2006, gained notoriety as a result of its Cloud Hopper operation, in which *managed service providers* (*MSPs*) were attacked starting in 2015.[64] The US Department of Justice (DoJ) and the other four members of the Five Eyes countries have issued official statements and criticised the involvement of the Chinese government in this espionage campaign.[65]

On 20 December 2018, the DoJ laid charges of fraud and identity theft against two Chinese nationals suspected of involvement in the Cloud Hopper operation. On that occasion, two large IT service providers were named as victims of the espionage campaign – Hewlett Packard Enterprise (HPE) and IBM. It was thought that, in IBM's case at least, the attacker had had access to its network for several years.

In June 2019, the Reuters news agency released the names of a further six victims of APT10:[66] Fujitsu, Tata Consultancy Services, Dimension Data, NTT, Computer Sciences Corporation and DXC Technology. This new revelation increased the number of potential victims hugely, since the MSPs themselves are not the intended target, but are simply used as gateways to the large companies whose ICT infrastructures they operate or support. For instance, the infection at HPE was discovered by the Ericsson ICT security team. The Swedish telecoms giant was looking for the attack vector for a number of *malware* infections that had occurred between 2014 and 2017. It is impossible to say how many companies have been infiltrated through this vector. Service providers are a very advantageous target, because they have direct access rights to their customers' systems and sometimes also process data for them.

The attacks are aimed at stealing intellectual property. The victims operate in areas such as military shipbuilding or nuclear submarine technology. For China, the modernisation of its marine and shipping technology is of critical importance.[67] Another reason for the attacks is to keep an eye on the competition: Ericsson, for example, is competing with Chinese mobile phone manufacturers. In addition, the theft of confidential turnover-related information allows companies to be assessed on their suitability as takeover candidates.

However, the espionage campaign could also have more than purely commercial motives. Among the confirmed victims, Sabre Corp stands out. It manages reservation systems for thousands of hotels worldwide, as well as plane tickets for hundreds of airlines. Although no

[64] MELANI semi-annual report 2018/2, section 5.1.1 and 2017/1, section 5.1.1.

[65] https://www.securityweek.com/five-eyes-nations-blame-china-apt10-attacks;
US: https://www.justice.gov/opa/press-release/file/1121706/download;
UK: https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign;
Canada: https://cse-cst.gc.ca/en/media/media-2018-12-20;
Australia: https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181221.aspx;
New Zealand: https://www.ncsc.govt.nz/newsroom/cyber-campaign-attributed-to-china/

[66] https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

[67] Chinese strategy «Made in China 2025»: http://english.www.gov.cn/2016special/madeinchina2025/;
http://en.people.cn/n/2015/0522/c98649-8895998.html

data leaks of travel information are thought to have taken place, the attackers might have been able to obtain the travel details of many people.

In the document issued by the DoJ, Switzerland was named as one of the countries in which organisations had come under attack. Despite there being no concrete evidence of infections at Swiss-based organisations, takeover candidates should always be viewed as potential targets for cyberespionage.

4.2 Industrial control systems

The conveniences of modern life are often only made possible by industrial control systems. The control systems at the local power distributor are partly responsible for ensuring a reliable supply of electricity from the dam's hydraulic turbines to our sockets at home. Section 4.2.1 describes how cybersecurity is handled at these small and medium-sized energy supply companies according to a study. When we travel, too, control systems everywhere make sure that we reach our destination quickly and comfortably. The challenges involved in, say, an instrument-assisted landing are explained in section 4.2.2.

4.2.1 Small and medium-sized energy suppliers need to do their homework

In the field of power generation, it is typically incidents involving power plants, dams or high-voltage power lines that hit the headlines. However, for end users the local distributor is usually more critical to the reliability of their power supply. The association Electrosuisse conducted a study[68] on cybersecurity at small and medium-sized energy suppliers.

The study showed that attention is paid to cybersecurity at all companies, but that there is potential for a greater degree of implementation and a more systematic approach to cybersecurity measures, particularly at smaller plants. Based on the NIST Cybersecurity Framework,[69] the study acknowledged the focus on preventive protection measures, but noted that other elements of the framework were being neglected.

In many cases, inventories were incomplete (asset management) and there was a lack of visibility in the network. This, combined with low readiness levels and the lack of emergency drills, poses considerable challenges with regard to incident detection and management. The study found that risks related to the prioritisation of measures and budgeting were not sufficiently factored into high-level organisational considerations. Yet, neglected supplier risk and the management of the risk factor posed by humans play a role. Often, these risk factors arise from a lack of skills and resources, especially at the small companies studied, which also results in cybersecurity not being actively pursued as a process.

One way in which small and medium-sized energy suppliers can remedy these shortcomings is to cooperate with each other in areas that are identical at all companies. In this regard, the cross-company initiative to cooperate on cybersecurity established by an alliance of public

[68] https://www.electrosuisse.ch/wp-content/uploads/2019/03/Electrosuisse_Cybersecurity-Erhebung-EVU_.pdf

[69] https://www.nist.gov/cyberframework

utilities is welcome.[70] This network will enable all the partners to benefit from each other's experience and work together to achieve an ongoing improvement in cybersecurity levels.

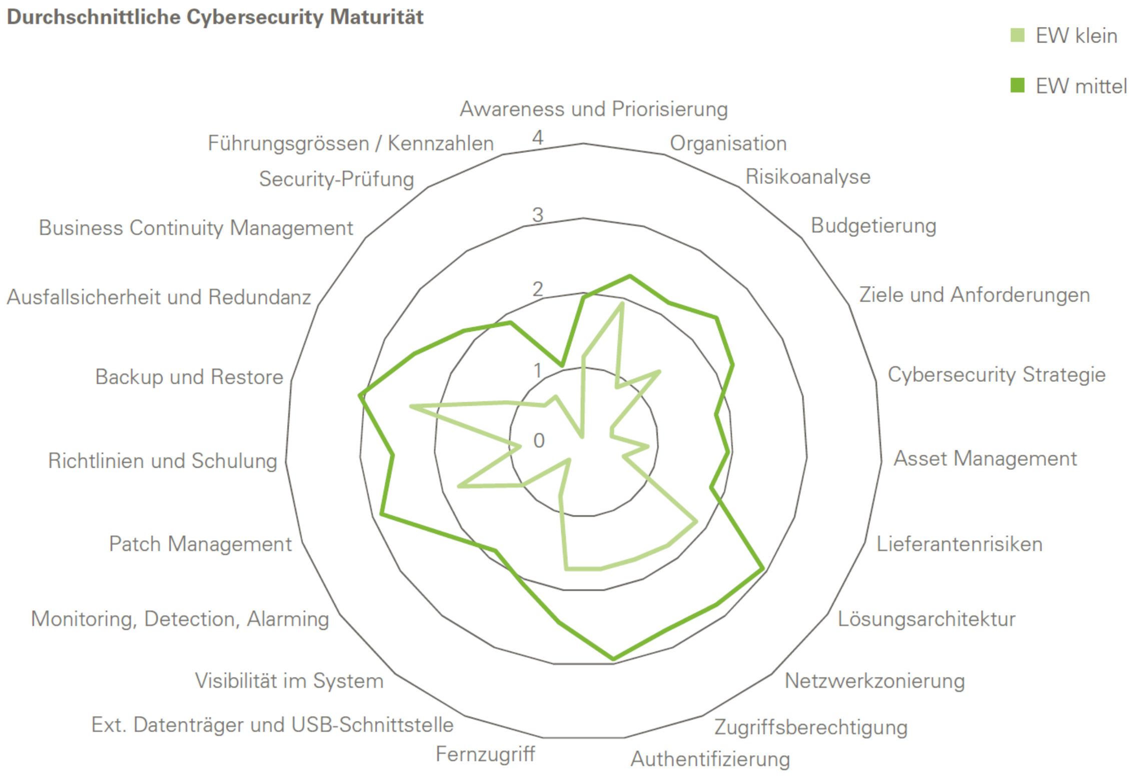


Figure 1: Overview of study results in the cybersecurity areas investigated.

4.2.2 Possible disruption of instrument landing systems

When landing at most civilian airports, pilots are supported by an instrument landing system (ILS). Such systems were developed at a time when the radio technology they use was only available, or affordable, for a small group of users. In that earlier, more exclusive environment, cryptographic security and authentication measures were not a priority. At the last Usenix[71] conference, researchers from Northeastern University of Boston demonstrated a cheap method to spoof radio signals from an ILS and provide an aircraft with an erroneous course reading.[72] The device described in the research paper[73] uses commercially available components to spoof ILS signals. For an attack to be successful, the device must be placed either inside the plane itself or within a three-mile radius of the runway to which the plane is heading. A prerequisite is that the spoofed signal must be stronger than the legitimate communication from the airport, in order for the aircraft to set its receiver to the malicious signal.

[70] https://swisspower.ch/medien/medienmitteilungen/swisspower-lanciert-kooperation-für-cybersecurity-in-stadt-werken

[71] https://www.usenix.org/

[72] https://arstechnica.com/information-technology/2019/05/the-radio-navigation-planes-use-to-land-safely-is-insecure-and-can-be-hacked/

[73] https://aanjhan.com/assets/ils_usenix2019.pdf

Similar problems have also been experienced with other radio-based navigation systems such as GPS (see also section 5.2.2). Since pilots are trained to deal with ILS malfunctions, they should be able to react appropriately to such an attack. However, if this approach continues to be refined and deployed, such attacks could cause disruption for flights and airports – similar consequences that have been witnessed during the incident in December 2018, when unauthorised drone activity brought London's Gatwick Airport to a standstill.[74]

Recommendation:

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

MELDEN

MELANI reporting form

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

DOKU

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 Distributed denial of service – DDoS

Once again, a number of *DDoS* attacks were reported to MELANI in the period under review, showing that various attackers are still using this method to render the target systems unavailable. These can be criminals simply trying to extort money, or activists aiming to damage a company or organisation. There are also cases in which the motivation remained unclear. It can be assumed that the attackers sometimes test their infrastructure on randomly selected victims.

Recommendation:

MELANI recommends a variety of preventive and reactive measures for dealing with *DDoS* attacks.

DOKU

Checklist with measures to counter DDoS attacks:

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

[74] MELANI semi-annual report 2018/2, section 5.2.3.

4.3.2 Website hacks

Legitimate websites also continue to be regularly compromised and used with criminal intent. Hackers usually gain access to the websites via an outdated version of a content management system (CMS) or stolen FTP access data, and then install *malware* or a phishing site. If MELANI detects such cases, it informs the website operator so that it can remedy the problem using our instructions.[75]

Recommendation:

Prevention is better than cure: If you are using a CMS such as Typo3, Wordpress or Joomla, MELANI recommends reading its checklist on measures to secure content management systems, so that you can protect your website.

DOKU

Checklist with measures to secure content management systems (CMS)

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-to-secure-content-management-systems--cms-.html

4.3.3 Domain grabbing – when the marksmen club suddenly starts selling shoes, or a political campaign advertises counterfeit accessories

This is not really an attack, but rather the exploitation of the system involving a takeover of domain names that have not been renewed. Domain grabbers keep track of which domain names have expired, and register them for themselves at the end of the grace period. Often, fraudulent web shops are set up on these domains,[76] although a number of other business models are used with newly "expired" domains. The domains benefit, at least for a short while, from the good reputation built up over the years by their former owners. As there usually still are links to the domain on third-party sites, the domains often continue to be ranked prominently on internet search engine results.

Recommendation:

Domain name registrations must be regularly renewed. If you have a website, you should keep track of relevant renewal deadlines, so that you do not unexpectedly lose your domain name. The intended closedown of a website also requires planning. It can be a good idea, and is not expensive, to carry out a controlled shutdown, i.e. to continue operating the domain for a while in order to inform all potential users that your web presence is being turned off. In addition, a *referrer's* evaluation can help to inform the operators of other websites linking to the domain. After all, it is important to protect the reputation, customers and supporters of the entity associated with the website, whether this be a company, an association, a private individual or any other kind of interest group.

[75] https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/instructions-for-cleaning-up-websites.html

[76] In Switzerland, an increase in this phenomenon has been observed since 2016, and SWITCH, the registry for .ch domain names, has been combatting it very effectively. Other country domains are lagging well behind: https://www.nzz.ch/digital/kampf-gegen-fake-shops-im-netz-ld.1484852

4.4 Social engineering and phishing

The key to a good attack is a credible story that prompts the potential victim to do something. So-called "*social engineering*" attacks work best if the attacker can collate a lot of information about the potential victim. To do this, fraudsters use both freely available sources and information originating from data theft. Stolen data is sifted, combined with other stolen or public data, processed and sold on to other criminals. This data can be used to tailor individual attacks or create automated personalised mass emails (*malspam*).

4.4.1 Phishing

The number of phishing attempts reported to MELANI increased in the first half of 2019. A total of 2,521 different URLs deemed to be phishing sites were reported and passed on to the various organisations combatting phishing (browser manufacturers, anti-phishing organisations, affected hosting providers). The aim of the attackers remains essentially the same: stealing credit card data and/or obtaining usernames and passwords for online services such as PayPal, Spotify or Apple. Phishing attempts are increasingly being aimed at email accounts, as these can then be used for further attacks. A relatively new method is so-called "real-time phishing" (see section 4.4.2).

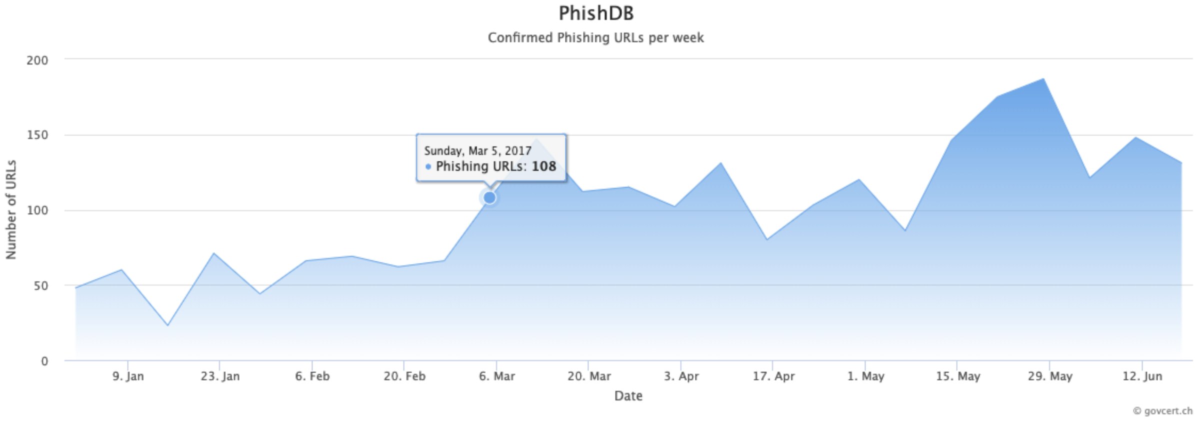


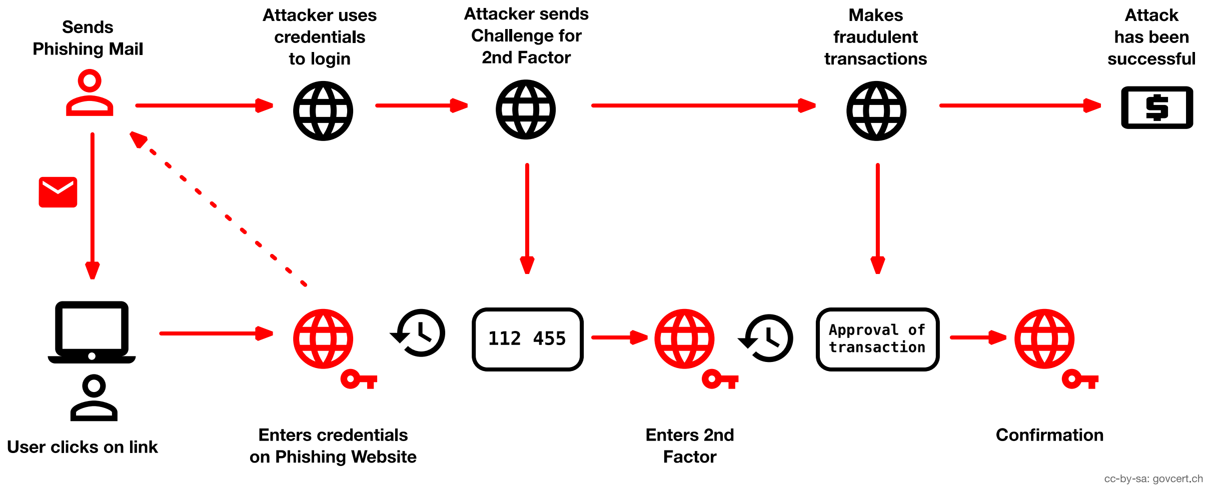
Figure 2: Reported and confirmed phishing sites per week on antiphishing.ch in the first half of 2019

Part of the increase can be attributed to major phishing waves aimed at stealing credit card information.

4.4.2 Real-time phishing aimed at PostFinance and UBS

In the most frequently used phishing method, attackers collect access data on a grand scale, and then wait a few hours or days before using it to log on to the victim's account. Often, the stolen access data is sold on. However, this method does not work if the user applies a second factor for authentication (e.g. a one-time password, or OTP). The attackers' response to the increased use of OTPs is real-time phishing. This requires the attacker to react as soon as the victim clicks on the phishing link in the email and is routed to the attacker's web server.

The attacker presents a perfectly replicated login page, on which the victim attempts to perform authentication. The attacker records this data and uses it to log themselves on to the real e-banking platform. The attacker is now challenged for a second factor, and displays this challenge to the victim on the fake web server. As soon as the victim has entered the second factor, the attacker gains access to the e-banking portal, while simultaneously fobbing off the victim with an error message.


Sends
Phishing Mail
Attacker uses credentials to login
Attacker sends Challenge for 2nd Factor
Makes fraudulent transactions
Attack has been successful
User clicks on link
Enters credentials on Phishing Website
112 455
Enters 2nd Factor
Approval of transaction
Confirmation

cc-by-sa: govcert.ch

Figure 3: Timeline of a real-time phishing attack

In the period under review, two such campaigns aimed at customers of Swiss financial institutions were observed.

4.4.3 Social media accounts are valuable

It is not just email accounts and credit card information that can be phished. Any online account is at risk. While a hacked Twitter account can be used to run a misinformation campaign discrediting the legitimate user, hacked Instagram profiles or YouTube accounts can also result in financial losses for the people affected.[77] The collected subscribers and followers are influencers' capital. If they lose control of their online presence, they have to start again and rebuild their community from scratch. Moreover, they are unable to upload any online content in the meantime, thereby losing a source of revenue. Loss of control over an online account does not have repercussions just for famous people. More and more people live their lives at least partly on social media platforms. If they lose access to their Facebook account for example, they can indeed have problems maintaining their contacts, at least temporarily.

Recommendation:

It is important to protect online accounts as much as possible, for example using two-factor authentication. Use complex and different passwords for every account.

Familiarise yourself beforehand with provider's security measures and any procedures for regaining control over a hacked account.

[77] See https://blog.trendmicro.com/trendlabs-security-intelligence/how-a-hacking-group-is-stealing-popular-instagram-profiles/

4.4.4 Small screens increase the risk of deception

Smartphones are small computers, and many people use them for the bulk of their communications. Appointments are often organised via the phone's calendar app. A major challenge for app programmers is to present as much relevant information as possible on the relatively small screen in an appealing way. This can often mean that background information, such as the full address of a link or the email address behind a display name (which, it should be noted, can be freely selected by the sender), is not easy to discern or is hard to access. For normal smartphone operating needs, this minimalism is logical and useful. Yet it also opens up many possibilities for criminals to trick the recipients of emails and other messages. Depending on the smartphone or app settings, not only can fraudulent emails, text messages and other short messages be sent, appointments can also be inserted automatically,[78] and notifications and other communications can be made to pop up on the screen.

Recommendation:

When using your smartphone, don't be fooled by unexpected messages, even if they come through regular channels and appear in a familiar format. Always stop to consider whether a message might not be from someone else who just wants you to click on it without thinking. Suspicious messages should be disregarded and deleted. Check your smartphone and app settings to ensure that only accepted appointments are inserted, for example, and that your privacy is adequately protected.

4.4.5 CEO fraud is proving persistent

MELANI first reported on *CEO fraud* in 2013.[79] Although not new, this scam is proving persistent. Various organisations continue to be the systematic target of such attacks. At the moment, in addition to private companies, the targets are increasingly sporting and other associations, and communes. Their websites often contain all the information the fraudsters need to launch an attack. Organisation charts contain the names and email addresses of people in various functions, including association or commune chairs, treasurers and financial officers. The classical approach to *CEO fraud* is to send an email purporting to come from the chairman requesting that the financial officer transfer funds for various reasons.

Using information which is freely available online, the fraudsters automated the emails, and apparently did not pay enough attention to quality control, with occasionally odd results. In small associations or communes, for example, the chair can also be responsible for finances. So both functions use the same email address. Thus, a case was reported to MELANI in which the treasurer of a commune who is also the commune chairwoman received an email – purporting to be from the chairwoman – sent from her own email address. This example shows that the fraudsters are using freely available sources (company websites, social networks) to gather the information they need for their attacks.

[78] MELANI semi-annual report 2018/1, section 4.4.4.

[79] MELANI semi-annual report 2013/1, section 3.4.

From: [fake address of association chairman]

Sent: Tuesday, 19 March 2019, 14:00

To: [Association treasurer]

Ref: REQUEST

Hallo Corinna,
I would like you to transfer some funds. Let me know if you can do it immediately, so that I can send you the account details.
Look forward to hearing from you

Regards
[Name of association chairman]

Sent from my iPhone

Email 1: The fraudster pretends to be the chairman and requests the treasurer to make an urgent transfer.

Hallo Corinna,

[Foreign bank account number]

Let me know when you've carried out the transfer.

Regards
[Name of chairman]

Sent from my iPhone

Email 2: Following the reply, the "chairman" sends the account number for the foreign funds transfer.

Recommendation:

MELANI recommends regularly checking what information relating to people, associations, companies, etc. is available online and whether it should actually be available. Other protective measures include raising employee awareness and introducing detailed procedures, particularly for payments.

INFO

Information and recommendations on CEO fraud:

https://www.melani.admin.ch/melani/en/home/themen/CEO-Fraud.html

4.4.6 Malspam: intimidating people and awakening their curiosity in order to spread malware

Internet criminals are constantly finding new ways to trick email recipients into clicking on a link or opening an attachment. There is no limit to their imagination. In the first half of 2019, users were approached with sometimes very far-fetched stories in a bid to fool them into downloading *malware*.

Paid subscription: A very concisely worded email thanked its recipients for having taken out a paid subscription to a certain newspaper or magazine. The payment details and terms and conditions were supposedly in the attached document. To fool the recipients, first and last names were inserted in the subject line of the email.

Legal action against former customers: After a small company's customer database was hacked, all the people in the address list received a personally addressed mail informing them that they had breached the terms of their contract and would be facing legal action. For further details, the recipients were referred to the attached document. The sender's address was not faked, but the display name used for the sender's address was the company's name, in order to fool careless recipients.

Legal action against restaurants: It was claimed in an email that a family member had gone down with food poisoning after visiting the restaurant, and that the restaurant was being sued. In these cases, the email was used to make the first contact. Anyone answering received another email with a link containing *malware*. With this method, rather than spreading their *malware* widely, the criminals target only those people who respond to the initial contact. This has two advantages. First, the *malware* is not widely distributed, so it takes longer for security providers such as antivirus software companies to become aware of it. Second, there is a higher probability that the recipients will click on the link, as they have already been in contact with the sender and are therefore expecting the email.[80]

Help for a girl being held captive: In an email, a girl who was supposedly being held chained up in a cellar by her abductor asked the recipient to inform her parents so that she could be rescued. All the details were to be found in the attached document.

Assisted suicide reserved and paid for: In this particularly shameless scam, recipients were informed that their assisted suicide had been reserved and paid for. In three days' time, they would be collected from their home by medical staff. An alleged accompanying documentation was attached to the email. Here too, recipients were addressed by name and the postal address mentioned was also correct.

Conclusion:

What all these methods have in common is the use of more or less credible stories to persuade the recipients to over-hastily click on a link or open a file in order to receive "more information". In almost all cases, the emails were personalised, i.e. the recipients were greeted by name and sometimes their home address or telephone number was mentioned. The corresponding data typically came from data leaks from web shops or from users' hacked address books.A personal greeting or the mention of someone's address or telephone number is not a reliable indication that a message is from a legitimate sender.

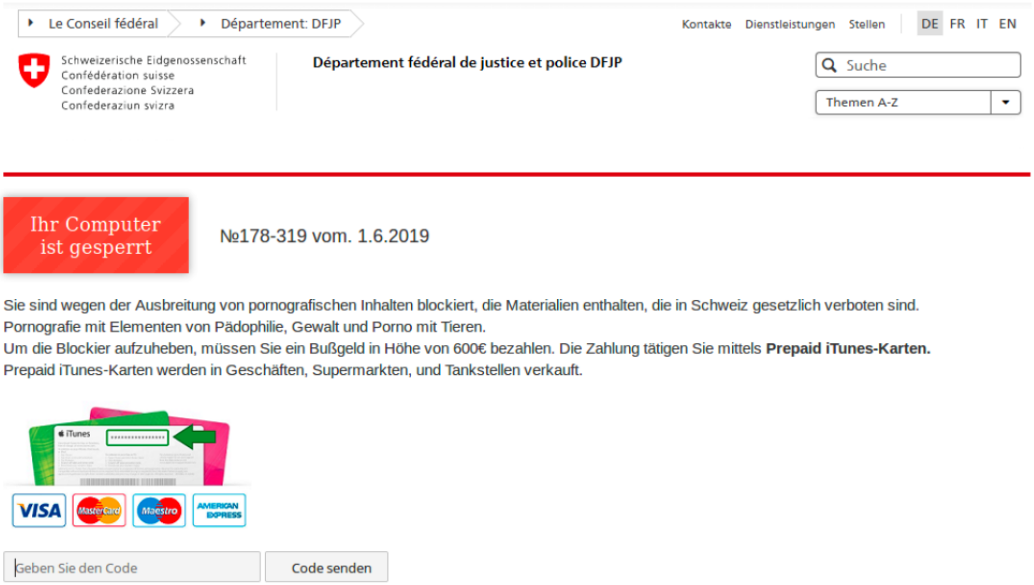
[80] The specialised press has warned restaurants about this scam: https://www.hotellerie-gastronomie.ch/de/artikel/achtung-ein-gastro-schreck-geistert-herum/ (dated 19.3.19); https://www.baizer.ch/aktuell?artID=6788&lvl=2 (dated 9.4.19); https://www.onlinewarnungen.de/warnungsticker/e-mail-lebensmittelvergiftung-trojaner-im-anhang-enthalten/ (dated 21.5.19)

Recommendation:

Be sceptical if you receive emails that require action on your part and that carry a threat of consequences (loss of money, criminal charges or criminal proceedings, blocking of account or card, missed opportunity, misfortune) if the action is not performed, especially if it is allegedly urgent. Do not open any attachments or click on any links in suspicious emails – not even out of curiosity. Otherwise, you run the risk of your device being infected with malware, or of ending up on dubious websites. In case of any doubt, contact the supposed sender using the information on their website, or other contact details already known to you, and enquire what the email is about exactly and whether or not it is actually from the sender.

4.4.7 Renewed extortion attempts using FDJP's name

In 2010 and 2011, online blackmailers first started operating on a grand scale. At that time, the usual practice was to block either the browser or the entire computer and claim, in the name of prosecution authorities or copyright collection companies, that the user had disseminated banned pornographic material or illegally shared music and film content.[81] This scam has largely been replaced by encryption Trojans,[82] but it has not disappeared completely, as demonstrated by the following example. Criminals have adapted the new layout of the Confederation website, but the language used is reminiscent of earlier phishing messages and fraud attempts, in which faulty grammar and the inconsistent use of languages give clear indications that the site displayed cannot be from the Swiss authorities. In this case, the computer was not infected with *malware*. The criminals simply tried to intimidate the victim into paying. However, the police would never block a computer as a means of exacting a fine or monetary penalty.



Département fédéral de justice et police DFJP

Ihr Computer ist gesperrt

№178-319 vom. 1.6.2019

Sie sind wegen der Ausbreitung von pornografischen Inhalten blockiert, die Materialien enthalten, die in Schweiz gesetzlich verboten sind. Pornografie mit Elementen von Pädophilie, Gewalt und Porno mit Tieren.

Um die Blockier aufzuheben, müssen Sie ein Bußgeld in Höhe von 600€ bezahlen. Die Zahlung tätigen Sie mittels **Prepaid iTunes-Karten.**

Prepaid iTunes-Karten werden in Geschäften, Supermarkten, und Tankstellen verkauft.

Figure 4: Blocking website with Confederation logo

[81] See semi-annual report 2011/2, section 3.5 and 2015/2, section 4.5.2.

[82] See also the section on ransomware in chapter 3 above.

4.4.8 Fake sextortion: Still many people falling into the trap

In the first half of 2019, there was once again a spate of fake sextortion emails, in which the sender claimed to have hacked the recipient's computer and filmed the recipient masturbating. MELANI published a newsletter on this topic in February 2019[83] and, together with the cantonal police and other partners, launched a website[84] to make the public aware of the problem. Unfortunately, many people are still paying the ransom without realising that the claims in the emails are baseless. The website stop-sextortion.ch also provides a short description of what to do if the blackmailers really do have compromising material (e.g. if a video chat has previously taken place or if the victim has sent nude photos to someone).

Various waves of fake sextortion emails have been observed in English, French, German, and even Italian. Most of them were more or less grammatically correct, although there continue to be some that have been poorly translated and contain very flimsy claims.

Overall, 4,565 different bitcoin addresses were reported to MELANI over a six-month period. The payment inflows observed were confined to only a few addresses; most of them saw no transactions. A total of 283 bitcoins were paid in (equivalent to around CHF 2.8 million at end-June 2019). Not all of these payments originated in Switzerland, as it is difficult to identify who made the payments, and from where. Nonetheless, these figures show that money is still being transferred, even though this phenomenon has been known for some time.

In an international context, the SANS Internet Storm Center has published an analysis of the bitcoin addresses reported to it and used for fake sextortion.[85] It analysed 434 bitcoin addresses. Only 56 of them ever received any payments. For a time, the money remained untouched. Before it is paid out, the attackers place the money in consolidation accounts. SANS identified two of these consolidation bitcoin addresses, one with 6,190 bitcoins (equivalent to around CHF 62 million at end-June 2019), and one with 5,312 bitcoins (equivalent to around CHF 53 million at end-June 2019). However, the author of the SANS article suspects that this is only the beginning of the cash-out, and that the actual figure is a multiple of those amounts. A successful cash-out requires the bitcoins to be broken down into smaller amounts so that the money can be more effectively mixed in a bitcoin tumbler, rendering it impossible to track.

Recommendation:

If you do not know the sender of the extortion email personally, and there has been no previous chat exchange between you, we recommend that you ignore the email and delete it. Do not pay the ransom under any circumstances.

If you received one of these emails, you can contribute to prevention by raising the subject with your friends and colleagues. In this way, you will increase the awareness of colleagues, acquaintances and relatives so that they are not taken in by the scammers.

[83] https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/fake-sextortion.html

[84] https://www.stop-sextortion.ch/en/index.html

[85] https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+Part+3+The+cashout+begins/24592/; https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+The+Final+Chapter/25204/

4.5 Data leaks

4.5.1 Swisscom traffic diverted via China Telecom

For more than two hours on 6 June 2019, a large proportion of European mobile phone traffic was diverted via China Telecom's infrastructure. The incident was caused by a *BGP* route leak[86] at the Swiss data centre Safe Host, which accidentally redirected over 70,000 routes from the routing table to the Chinese *internet service provider* (ISP).

Route leaks lead to the diversion of data traffic via an unintended path, which can cause an overload or a black hole.[87] As a result, data might not be transmitted and may be "dropped" (deleted) before it reaches its destination. Traffic analysis and eavesdropping are also possible. Route leaks mostly arise from accidental misconfigurations.

Instead of ignoring the BGP leak, China Telecom immediately took over the routes and redirected the traffic from a large number of European mobile phone networks to its own network. This went against filtering practices for the Border Gateway Protocol (BGP), which is used at ISP level to control the routing of data flows and prevent the spread of BGP leaks.

Among the European networks most affected were mobile phone operators in Switzerland (Swisscom), France (Bouygues Telecom, Numericable-SFR) and the Netherlands (KPN). The redirection lasted for over two hours – a relatively long time according to experts. Global communications were also severely impaired; this was reflected in slow connectivity for users of the affected mobile networks. Some servers were completely unavailable for users during this period. It is still unclear whether the redirection was deliberate, a technical fault or human error.

It is generally recommended that ISPs adhere to the BGP security standards in order to avoid such redirections of internet traffic happening in the first place.

4.5.2 ICT service provider Citycomp blackmailed after data theft

In April 2019, cybercriminals infiltrated the network of ICT infrastructure provider Citycomp.[88] They copied internal data and blackmailed the company, threatening to publish the misappropriated files. The company did not give in to the blackmail, so the attackers published the 516 GB of data they had collected, on websites specially created for the purpose. Affected customers included subsidiaries of big names such as Oracle, Volkswagen and Airbus. Some of the leaked data was also related to Swiss companies.

The cybercriminals blackmailed the service provider, not its customers, because they were not responsible for the company's "terrible security system". In a statement,[89] Citycomp emphasised that it had not given in to any of the blackmailers' demands and was cooperating with external specialists to deal with the incident. Both customers and relevant data protection authorities were informed in a transparent way, and an investigation by the Baden-Württemberg State Criminal Police Office is ongoing.

[86] https://www.thousandeyes.com/learning/glossary/bgp-route-leak

[87] https://en.wikipedia.org/wiki/Black_hole_(networking)

[88] https://www.vice.com/en_us/article/d3np4y/hackers-steal-ransom-citycomp-airbus-volkswagen-oracle-valuable-companies

[89] https://www.citycomp.de/English/enterprise/stellungnahme.html

Recommendation:

It is not just on a company's own systems that data can be lost. Suppliers, service providers and customers sometimes also store your sensitive data. It is worth drawing up contracts to ensure that your partners also have security measures and incident management procedures in place that are equivalent to those in your own organisation. This may entail an additional monitoring effort, but it will help to avoid surprises.

4.6 Crimeware

Crimeware (from "crime" and "software") describes a group of *malware* used for criminal purposes. The following charts, while not providing a complete overview of *malware* in Switzerland, show the trend in crimeware involving, on the one hand, waves of *malspam*, which MELANI monitors together with the security teams of critical infrastructures, and, on the other hand, *DNS* sinkhole[90] data.

A particular cause for concern in the first half of 2019 was the considerable damage caused by targeted ransomware attacks (see the key topic in chapter 3). Companies' access data, which had been stolen using Emotet, was sold on and used by the attackers to gain initial access to the company network and then move laterally.

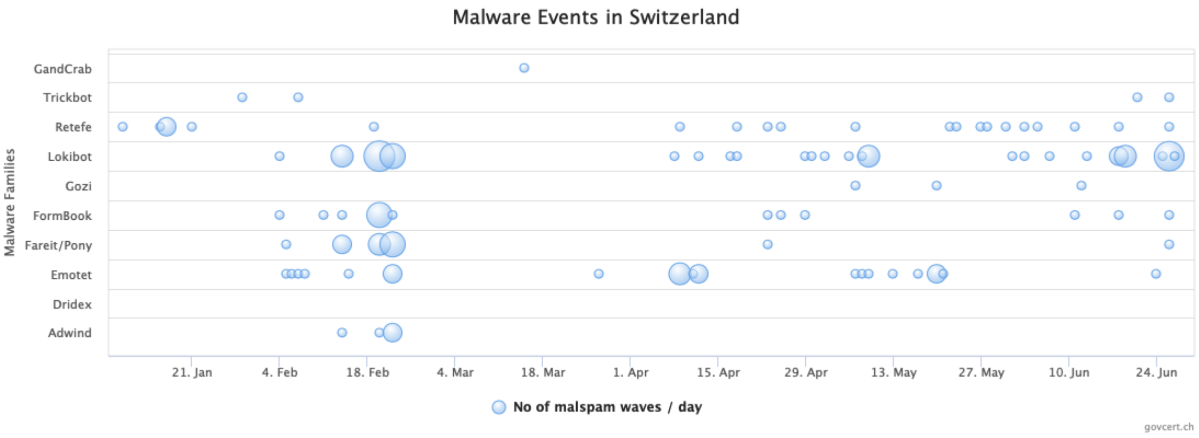


Figure 5: Observed malspam waves

The large number of LokiBot waves is clearly visible, as is the ongoing activity by Retefe. Emotet is somewhat underrepresented in this chart, as MELANI tracks the different waves en bloc rather than individually.

During the period under review, Emotet became a very significant threat, as the attackers had already begun to sell on infected bots in companies last year. Emotet thus serves as a gateway for targeted ransomware attacks (see also section 3.4.1). Trickbot might not have any Swiss banks in its configuration files, but it is often used in a second step following the initial infection by Emotet. Here, Trickbot's modularity comes in useful for the attackers. It has various

[90] In DNS sinkholing, traffic to domains being used for criminal purposes can be redirected to the infrastructure of security organisations by reregistering the domains.

modules, for example to steal access data or to spread using the EternalBlue vulnerability (vulnerability in the *SMB protocol*).

In the period under review, in addition to targeted ransomware attacks, there were also many cases of non-targeted attacks, often carried out using GandCrab. Files on the affected device were encrypted immediately after the malicious attachment was executed.

Retefe was also particularly active, and was spread by the attackers through waves of *malspam* with various subject lines. Sometimes the waves took the form of attacks against companies, and sometimes against end users.[91] Technically speaking, Retefe was mainly spread via an email with an attached Word file. The emails often used a well-known brand name in order to appear credible. By embedding active code in the Word files, various components were installed on the victim's device, such as a root certificate to prevent any certificate warning being generated during a "*man in the middle*" attack, a *SOCKS* to allow the use of proxy services, and a Tor client to redirect traffic to e-banking platforms. In addition, Retefe changed the browser settings (*proxy* settings) so that traffic could be redirected. At the first attempt to log in to the e-banking platform, Retefe tried to trick users into installing an additional app on their mobile device to intercept the second authentication factor.

MELANI collects information on infected devices in Switzerland and distributes it to ISPs and critical infrastructures. The chart below shows, for each *malware* family, the current number of infected devices rendered harmless using *DNS* sinkholing.

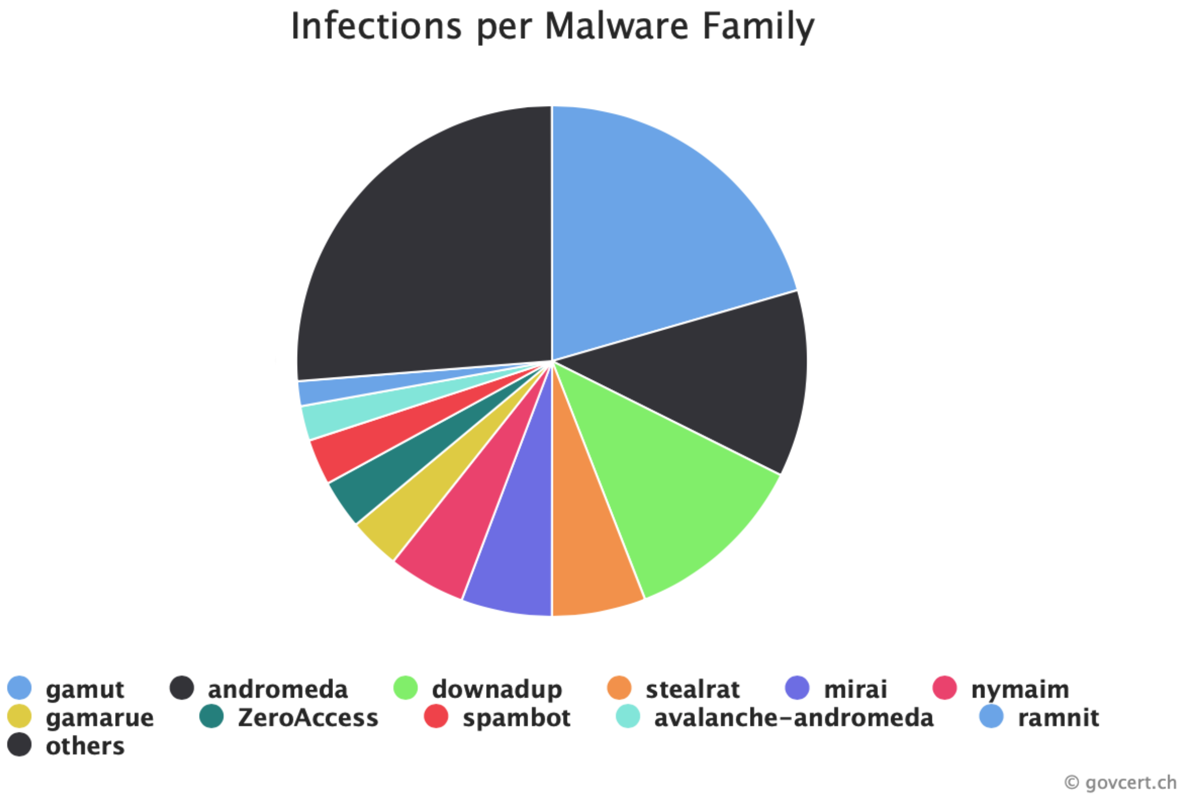


Figure 6: Breakdown of malware in Switzerland known to MELANI. The reference date is 30 June 2019. Current data can be found at: http://www.govcert.admin.ch/statistics/malware/

[91] Regarding the spread of malware via social engineering, see section 4.4.6 above.

It is interesting that around 20% of infections were caused by the Gamut spambot. In second place is Andromeda, a *malware dropper* (i.e. it can be used to install *malware*). A considerable number of infections continue to be caused by Downadup (also called Conficker), a *worm* that has been active since 2008.

5 Situation internationally

5.1 Espionage

5.1.1 Notable developments

In the first half of 2019, numerous cyberespionage attacks were uncovered, mostly through reports or analyses by security companies. The many reports, different targets, inventive attackers and new techniques mean it is not easy to maintain an overview of the situation.

As a result, frequent attempts are made to attribute attacks to specific groups of attackers or regions. This attribution[92] is difficult, as overlaps between groups and campaigns can often be observed. For example, recent Kaspersky analyses show that the Sofacy and Sandworm groups, which are known for separate attacks, have many similarities and sometimes work from the same infrastructure.[93] To complicate matters even more, false flags are used to cover attackers' tracks and misdirect the attribution of attacks. For example, false flags such as code parts written in Chinese are said to have been discovered in Muddy Water's activity, even though it is suspected that an Iranian group was behind Muddy Water. This group was very active during the period under review and, in addition to the usual targets in the Middle East, was interested in organisations in Asia and Europe.[94]

Finally, when making an attribution, the unique markers of an attacker come into play. Which element is so specific to an attacker that it makes an attribution possible? Increasingly, the technology used by attackers fails to answer this question. Many groups currently use a multitude of different, openly available tools, either to access a network or to move around within it. These include open source products such as Metasploit and the ID collector Mimikatz or leaked tools like the EternalBlue exploit. Due to the variety of instruments deployed during attacks, the groups remain agile and can deploy their technologies as and when required. One example is the arsenal used by the Emissary Panda group[95] in various attacks on governments in the Middle East in 2019. The group's own tools were used only for specific situations. It is difficult to identify a group based on the tools used if everyone uses the same ones.[96] In addition, the number of potential attackers has increased considerably due to the availability of tools.

It may come as a surprise that public attribution is so widespread, especially by governments,[97] when attribution based on technical elements is becoming increasingly uncertain. There are,

[92] This refers to the public attribution with official naming of an attacker.

[93] https://securelist.com/zebrocys-multilanguage-malware-salad/90680/

[94] https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

[95] https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

[96] Other technical elements such as the infrastructure used (IP, domains) can supplement the attribution.

[97] In recent years, for example, the United States and/or its allies have officially attributed NotPetya to Russia, WannaCry to North Korea and APT10 to China; see also section 4.1.4.

however, other elements on which attribution can be based, such as the answer to the question: "Cui bono? (for whose benefit?)". The political and economic goals of major powers are usually known (sometimes these are even part of public strategies) and the interests behind an attack are often apparent.

As fascinating and complex as these attributions may be, they are of little help to those who are targeted by an attack. At best, these companies and users can adjust their risk assessments in light of the known or suspected interests of the countries that carry out such attacks. However, an attacker's identity is ultimately irrelevant to the victim. The important thing is to identify one's own vulnerabilities and understand how these could be exploited by an attacker. In this respect, the number and variety of tools available are bad news; every attacker has a huge arsenal of tools at their disposal.

The protection and defence of targets are made more difficult by the fact that attacks are also carried out via compromised non-target elements. For some time now, the focus has been on supply chains.[98] The activities of the APT10 cyberespionage group, which is attributed to China and targets large managed service providers (MSPs), are one example of this.[99] During the period under review, further press articles appeared, most of which reported on developments which had already been made public.[100] The software used by companies can also be affected, as was the case with the German remote maintenance software TeamViewer. In May 2019, the company admitted that an attack took place in 2016, the effects of which are difficult to assess.[101] Another example of an attack on a supply chain is the attack which affected users of ASUS devices and which was discovered in March 2019.[102] It is believed that the malicious code was spread via ASUS' automatic update function. This affected an (unknown) number of devices that were identified from their MAC addresses. Users are powerless in such cases. Software company updates are urgently recommended for security reasons. During the period under review, further attacks via external infrastructure which involved compromising the *DNS* were carried out. A detailed report on this is provided in the following section.

5.1.2 DNS hijacking – a guide to ambushes

The *domain name system (DNS)* ensures that internet users are routed to the IP address of the associated server when accessing an internet domain (e.g. 162.23.128.232 for www.melani.admin.ch). In January 2019, US-CERT[103] warned against attempts to penetrate *DNS* infrastructure and modify *DNS* records so that domain visitor traffic was redirected through systems controlled by attackers.

Talos, Cisco's security division, reported on the first variant, known as DNSpionage.[104] It observed both the use of *malware,* which it also called DNSpionage, against Windows computer users, and redirections at network level against targets in Lebanon and the United

[98] Discussed in MELANI semi-annual report 2018/2, section 3 and in this report in section 5.3.1.

[99] MELANI semi-annual report 2017/1, section 5.1.1 and 2018/2, section 5.1.1.

[100] https://uk.reuters.com/article/uk-china-cyber-cloudhopper-special-repor/special-report-inside-the-wests-failed-fight-against-chinas-cloud-hopper-hackers-idUKKCN1TR1DC

[101] https://www.zdnet.com/article/chinese-cyberspies-breached-teamviewer-in-2016/

[102] https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

[103] https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign

[104] https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

Arab Emirates. By controlling *DNS* records, the attackers were also able to issue valid SSL certificates for their servers to redirect encrypted traffic.

A more comprehensive overview of *DNS* hijacking activity was presented by security service provider FireEye[105] in January 2019. Threat researchers cited three different variants of how *DNS* queries from destinations in the Middle East, North Africa, Europe and North America had been manipulated. The attackers mainly attempted to tap further access data from the redirected data stream for systems such as email and file servers. This was done in order to then be able to penetrate the systems while posing as seemingly legitimate users.

At the end of January 2019, the cybersecurity company CrowdStrike[106] confirmed the described attack methods and identified the targets of the attack campaigns, dating back to 2017, as the public administration and civil aviation sectors, and also internet service providers and network infrastructure service providers.

In April 2019, Talos reported another player by the name of Sea Turtle,[107] who they observed engaged in similar activity against *DNS* infrastructure. Its victims were national security organisations, foreign ministries and well-known energy organisations. They also attacked their *DNS* service providers, such as registrars or telecommunications providers, who served as stepping stones for attacks against their clients. In a follow-up report, Talos[108] mentioned the Greek registry, which manages the allocation of .gr domains, as one of the victims. The attacks broadened to include energy companies, think tanks, NGOs and at least one airport. Service providers and organisations in Switzerland must also be prepared for Sea Turtle attacks, either as a means to an end or as direct targets.

As a result of these attacks, ICANN, the highest internet regulatory body, called for the full deployment of Domain Name System Security Extensions (DNSSEC).[109] These are a series of internet standards that add security mechanisms to the *DNS* to ensure the authenticity and integrity of data and could be used to ward off such attacks.

The Federal Administration supports DNSSEC and has introduced such extensions for all its websites.

5.2 Industrial control systems

5.2.1 Energy supply control systems during armed conflicts always in focus

On 14 June 2019, Dragos, a security company specialised in industrial control systems, published a blog article on the activities of a group called Xenotime and its Triton/Trisis

[105] https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

[106] https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

[107] https://blog.talosintelligence.com/2019/04/seaturtle.html

[108] https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html

[109] https://www.icann.org/news/announcement-2019-02-22-en

malware that targets industrial security systems.[110] According to a report by FireEye on 23 October 2018, Russian players are said to be behind the *malware*.[111]

According to the Dragos report, increased activity by the group has been observed since mid-2018 in European countries and, above all, in the United Sates. Although supposedly no facilities were compromised, the group has continued to develop its reconnaissance activity. In particular, Xenotime has expanded its target range.[112] The Triton/Trisis *malware* was deployed in power supply and production facilities, for example, as well as in a gas and oil refinery.

On 15 June 2019, the New York Times published an article on possible *malware* incursions into the Russian electric power grid by the US Cyber Command (USCYBERCOM).[113] These operations, which have been developed in recent years, are intended not only to give the United States a head start in the event of conflict, but above all to act as a deterrent against Russian cyberoperations against the USA.

The referenced articles show that state interest in critical infrastructures continues,[114] above all in the energy sector, and that operators must continue to enhance their networks and expand their ability to respond to cyberattacks.[115] The minimum standard for guaranteeing ICT security in power supply distribution can be found on the website of the Federal Office for National Economic Supply (FONES).[116]

5.2.2 GPS spoofing troubles pilots in Israeli airspace

Since the vast majority of smartphones have been equipped with a GPS sensor as standard, most people rely on satellite-based orientation when navigating their way around on foot, by car or by other means. As indicated in section 4.2.2, GPS coordinates are also central to aircraft pilots' flight routes. In the course of June 2019, several pilots complained about unreliable GPS signals when approaching Ben Gurion Airport near Tel Aviv.[117] The Israeli Airline Pilots Association believed that a *spoofing* attack was the reason behind the problems with incorrectly displayed positions.

Israeli security authorities located the signal source at the Syrian air base Khmeimim and accused Russian electronic warfare (EW) systems of being behind the attacks. The base is located approximately 350km north of Ben Gurion and is used intensively by the Russian Air

[110] https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/, see also MELANI semi-annual report 2017/2, section 5.3.2.

[111] https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

[112] https://www.wired.com/story/triton-hackers-scan-us-power-grid

[113] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

[114] See also MELANI semi-annual report 2015/2, section 5.3.1 and 2016/2, section 5.3.1.

[115] See the Electrosuisse study referred to in section 4.2.1.

[116] https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/minimalstandard_strom.html (document available in German only)

[117] https://www.gpsworld.com/israel-accuses-russia-of-spoofing-in-its-airspace/

Force to support the Syrian regime. If the accusations are true, this shows how powerful the Russian EW systems must be in order to achieve the described effect over such a distance.

The Russian ambassador to Israel immediately denied the accusations and dismissed them as unreliable and fake news.[118]

5.2.3 An externally controlled remote control

Who has never stopped at a construction site to watch the crane operator down on the ground use a little joystick to steer a giant, heavily laden crane? Such radio controls are widely used in construction, logistics and manufacturing.

In its analysis,[119] the Japanese security company TrendMicro was able to demonstrate that attacks are possible via this radio interface and that control commands, for example, can be manipulated. The prerequisite for a successful attack in these cases is that the attacker is physically close to the target, so that the signals can reach the device under attack. In order to avoid the need to be in the vicinity, attackers can place a small transmitter close to the remote-controlled system and remotely access it via Wi-Fi or mobile radio. To demonstrate the plausibility of the threat, the researchers developed their own battery-powered RFQuack wireless hardware (see figure below), which fits into a trouser pocket.

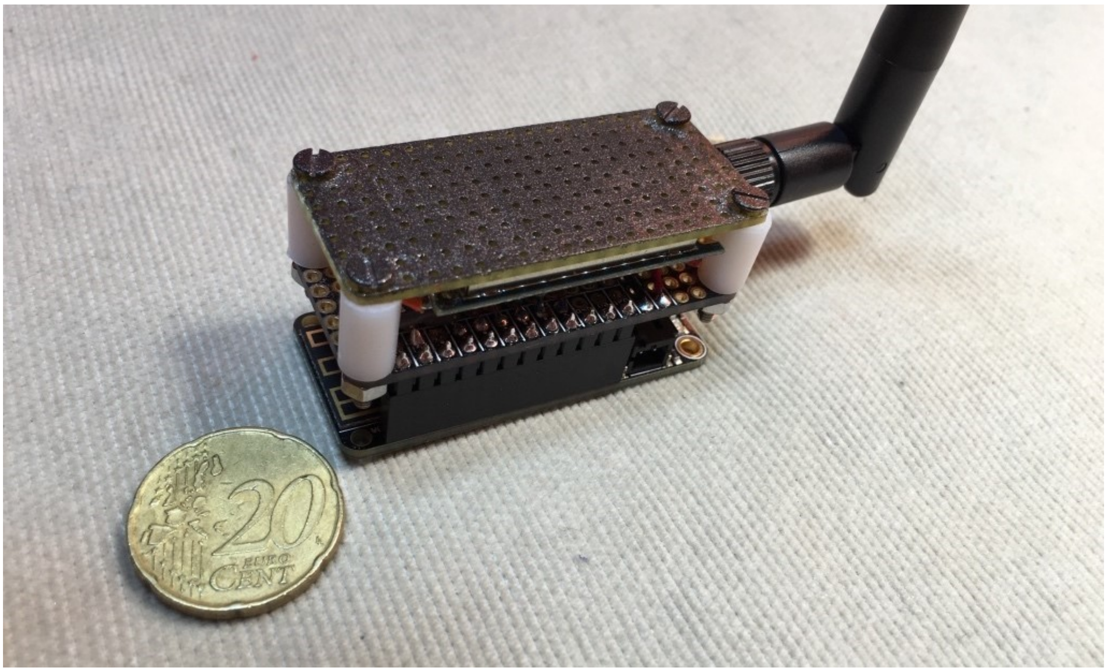


Figure 7: Size comparison of the RFQuack radio module

[118] https://www.bbc.com/news/technology-48786085

[119] https://blog.trendmicro.com/trendlabs-security-intelligence/demonstrating-command-injection-and-e-stop-abuse-against-industrial-radio-remote-controllers/

Recommendation:

In order to best protect yourself against such attack scenarios, analysts recommend that you carefully study the documentation for any remote control you are about to acquire. You should ensure that the devices offer a configurable pairing connection mechanism. Further measures are as follows: Operate the computer which is used to program the remote control separately from the network and, where possible, use well-researched standard protocols such as Bluetooth Low Energy.

Conclusion / recommendation:

The increasing computerisation and networking of all types of everyday objects (Internet of Things) offer many new and useful functions and conveniences. These also include consumer electronics and internet access in cars and aeroplanes. The associated risks should not be ignored. New possibilities always entail dangers as well, and these must be taken into account already during the development phase (security by design).

DOKU

Checklist with measures for the protection of industrial control systems:

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

5.3 Attacks (DDoS, defacements, drive-bys)

5.3.1 IT service provider WIPRO hacked

In April 2019, investigative journalist Brian Krebs reported that the multinational IT service provider WIPRO had been the victim of an attack.[120] In view of the activities of groups such as APT10, which mostly attack managed service providers (*MSPs*) to spy on their clients, experts feared that the situation would be bad. More recent analyses by RiskIQ[121] and Proofpoint[122] also indicate an attack on the company's clients, but with an alternative motive. The attacker seems to seek financial gain rather than espionage. The group is said to have been active since 2015 or 2016 and to have been targeting company gift cards to finance its activities.

The attackers largely gained access to their target's network via phishing. According to RiskIQ, they used templates from Lucy Security, an awareness-raising company based in Switzerland. This does not necessarily mean that this company was itself compromised. The attackers also used freely accessible attack tools and, after an initial compromise, used existing dual-use tools in the target's network.

[120] https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/

[121] https://cdn.riskiq.com/wp-content/uploads/2019/06/Gift-Cardsharks-Intelligence-Report-2019-RiskIQ.pdf

[122] https://www.flashpoint-intel.com/blog/wipro-threat-actors-active-since-2015/

This attack shows once again how real the risk of attacks via the supply chain is. It is not only in espionage attacks that attempts are made to get into the target system by compromising suppliers. Other perpetrator groups also seem to take advantage of this approach.

5.3.2 Botnet attempts to crack RDP server with brute force attacks

For years, attackers have been scanning the internet for open or poorly secured ports, which are then used as a gateway to networks. These ports are usually assigned to an internet service or protocol and are sometimes defined by default. There are now even search engines which can be used to find these "open doors" with little technical understanding. Some of these doors are more popular than others. In the last six months, MELANI once again observed an increase in *RDP*[123] port scanning activity. The default *RDP* port is 3389.

At the time of the SANS article,[124] the GoldBrute botnet, which is controlled by a single *Command & Control* server, scanned 1.5 million *RDP* servers exposed to the internet. And the botnet continues to grow. The infected system downloads the bot code and then starts scanning random IP addresses for *RDP* ports. Each time the bot finds a further 80 IP addresses with accessible *RDP* ports, it reports them to the command server. The command server then forwards to each bot a set of IP addresses, which it should then *brute-force*. However, atypically only one assigned username and ONE associated password is tried in order to remain under the radar and thus go undetected by common security programs. Systems compromised via *RDP* become bots themselves. In theory, attackers could also install other malicious software, such as ransomware or data acquisition software, which could have serious consequences for the owners of the hacked system.

5.3.3 Latest developments from Anonymous

Anonymous has claimed responsibility for very few campaigns in recent times. One reason for this could be the high-profile arrests of participants following previous actions. However, various events, especially relating to freedom of information, have continued to mobilise activists belonging to the movement; e.g. the arrest of Julian Assange in London, which triggered actions against UK and Ecuadorian interests. The WikiLeaks founder lived inside the Ecuadorian Embassy in London from 2012. In April 2019, shortly after his asylum was revoked and he was arrested, a group affiliated to Anonymous published stolen data from various UK police forces. However, this did not appear to include personal data. Another group, acting in the name of Anonymous, declared responsibility for *DDoS* attacks on UK government websites. The Ecuadorian authorities also reported *DDoS* attacks, notably on the websites of its Central Bank and Prime Minister.

5.3.4 DDoS attacks for bitcoins

It has been known for some time that the success of virtual currencies provokes virtual robberies. MELANI has already reported several times on attacks on users and platforms of such currencies.[125] The more popular a currency or service is, the greater the risk of an attack. This year, the bitcoin wallet service Electrum was hit. The users of the service were persuaded

[123] Remote Desktop Protocol: A Microsoft network protocol for remote access to Windows computers.

[124] https://isc.sans.edu/forums/diary/GoldBrute+Botnet+Brute+Forcing+15+Million+RDP+Servers/25002/

[125] See in particular MELANI semi-annual report 2017/2, section 5.4.3.

to download a manipulated version of the app. For this purpose, the attackers positioned a number of malicious nodes in the peer-to-peer network used to release the transactions. If a user reached one of these nodes (which acts as a server in the peer-to-peer network), they received an error message with a link to a supposed app update that had to be downloaded. It was, however, a malicious program that emptied the wallet.

That's not all. As a reaction to the countermeasures taken by Electrum's operators, *DDoS* attacks were conducted on the non-compromised network nodes. When the "real" nodes were inaccessible, it was easier to redirect users to the "fake" nodes with the harmful update. In April, the security company Malwarebytes estimated that 771 bitcoins had been stolen in this way (equivalent to approximately USD 4 million in April).[126]

5.4 Data leaks

5.4.1 Citrix hacked

The software company Citrix was informed by the FBI on 6 March 2019 that international cybercriminals had gained access to the internal Citrix network.[127] Citrix subsequently informed its customers that foreign hackers had infiltrated its internal corporate network and had obtained data. Investigations are ongoing to determine what data the intruders had access to. According to Citrix, however, there is no evidence that the hackers manipulated the official Citrix software or other products.

The incident may have been part of a sophisticated campaign that focuses heavily on governments, military-industrial companies, energy companies, financial institutions and critical infrastructure operators.[128]

5.4.2 Magento: Online shop security

Vulnerable third-party extension modules are now the main source of hacks into Magento online shop software. For example, a vulnerability in the MySQL database protocol, which has been documented for years, allows criminals to build malicious code into e-commerce shops. This example shows that it is difficult for online merchants to keep their websites clean from malicious code, as any third-party modules in use should also always be kept up to date. This leads to a conflict of interest between the stability of an e-shop and a continuous update policy, not least because Magento does not offer a standardised way of being notified of critical third-party releases.

5.4.3 Data leak in Panama

Security researchers discovered an unprotected Elasticsearch server that stores personal information on nearly 90% of the Panamanian population. The exposed data includes full names, dates of birth, passport numbers, health insurance numbers and other personal information. The database also contains 3.4 million records on Panamanian citizens referred

[126] https://blog.malwarebytes.com/cybercrime/2019/04/electrum-bitcoin-wallets-under-siege/

[127] https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/

[128] https://www.forbes.com/sites/kateoflahertyuk/2019/03/15/who-is-resecurity-the-mysterious-firm-that-blamed-iran-for-the-citrix-hack/; https://www.theregister.co.uk/2019/03/08/citrix_hacked_data_stolen/

to as "patients". Upon notification, CERT Panama immediately secured the database. However, it is no longer possible to determine whether anyone accessed the data during the period in which it remained unprotected.

5.4.4 Millions of Facebook records found on Amazon cloud servers

Security researchers again found countless Facebook user records that were publicly available on Amazon's cloud computing servers.[129] The most recent discovery shows that even a year after the Cambridge Analytica scandal, Facebook user data is still unsafe and widely available online. The fact is that Facebook data was relatively freely available contractually for years to anyone who had integrated the social network into their service. This practice only recently came to an end. Nevertheless, the findings show that some companies that gain access to Facebook data due to their contractual relationship are not active enough as far as data protection is concerned. After numerous scandals, it remains doubtful that user data on Facebook is secure and data handling traceability is probably not sufficiently transparent for individual users. However, this is not a problem specific only to Facebook. In times of big data and automation, this topic is more relevant than ever before, as significant conclusions can be drawn from analysing data records. Users are well advised to consider their digital appearance and the treatment of their personal data before any disclosure or publication. This latest example further illustrates how the problems of data security and data control are being exacerbated by another trend: the move away from companies running their operations and data storage predominantly within their own data centres towards cloud computing services provided by technology giants.

5.5 Vulnerabilities

5.5.1 BlueKeep – wormlike vulnerability in RDP protocol

In May 2019, a vulnerability in the Microsoft remote desktop protocol (*RDP*) became known (BlueKeep, also known as CVE-2019-0708). Shortly after Microsoft announced the vulnerability and released the security patch, attackers started automated scanning activity to find open *RDP* ports.[130] They then attempted *brute force attacks* (trying simple, weak or already known passwords) to gain access to the systems and subsequently exploit the vulnerability.

The vulnerability allows code to be executed remotely. Since the vulnerability can be found in all Windows versions from Windows 2000 to Windows 7, including Windows Server 2008 R2, it was classified as highly critical. Later versions (Windows 8 and 10) are not affected. Microsoft released a patch on 14 May 2019 which supports all versions, even those that are no longer supported by Microsoft because they have reached the end of their lifespans.

The special feature of this vulnerability is that it is *wormlike*. This means that *malware* can "automatically" spread to unpatched systems without human interaction. This could have devastating consequences, since many systems are vulnerable and are not always patched promptly.

[129] https://www.upguard.com/breaches/facebook-user-data-leak

[130] https://www.zdnet.com/article/intense-scanning-activity-detected-for-bluekeep-rdp-flaw/

There is currently some evidence that it is possible to exploit this vulnerability, but researchers have not made any how-to instructions available to the public and, as of yet, it has not been actively exploited by criminals. However, increased *RDP* port scanning activity has been observed for some time. Such port scanning can be used to create a list of vulnerable systems so that potential targets are already known when a working exploit becomes available. It is only a matter of time before someone writes an exploit that is then used "in the wild".[131]

Recommendation:

In order to protect yourself from BlueKeep, you are strongly advised to install the appropriate security patch. In addition, MELANI advises deactivating remote desktop services and the associated ports if they are not absolutely essential.

Increased *RDP* port scanning is worrying, as there are many ports that are more or less freely accessible from the internet. Studies indicate that the most common gateway for ransomware in the first quarter of 2019 was open or poorly configured *RDP* ports.[132] This is often because neither users nor administrators know that the service is enabled on their networks. This means that users are attacked via a vector whose existence they are unaware of and therefore they do not take any measures to protect themselves against this. It is thus indispensable that users and administrators know their networks and know what services and devices are available in order to effectively secure them.

The effects of ransomware, as described in chapter 3 above, are serious and can completely paralyse a company for several days. Attackers can also use the *RDP* gateway to move laterally within a corporate network and thus move on to more interesting targets. In this way, they can also steal, delete or encrypt important data and make it unusable. Unless a good, tried-and-tested backup solution is available, such data is usually lost until someone creates a so-called decryption tool that can be used to restore at least some of the data.

To avoid such an attack, McAfee gives the following tips:[133]

Recommendations:

- Do not allow *RDP* connections over the open internet; *RDP* should NEVER be open to the internet due to continuous scanning and because users are vulnerable to denial of service attacks or account takeovers.
- Use complex passwords because many *brute force attacks* are attempted on *RDP* ports.
- Use multi-factor authentication (e.g. security token, code received via message or biometric verification).
- Use *RDP* gateway to increase control (e.g. to enable logging).
- Block usernames and IP addresses that register too many unsuccessful login attempts.

[131] Between writing and publishing of this report, this prediction has come to pass and BlueKeep is now integrated in the open source penetration-testing tool Metasploit.

[132] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-security-explained/

[133] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-security-explained/

- Use a firewall to restrict access.
- Use encryption.
- Enable Network Level Authentication (NLA). This measure largely protects against the BlueKeep vulnerability, as an attacker would have to log in with a valid account before they can exploit the vulnerability.
- Restrict access rights for users who are able log in via *RDP* (usually not all administrators need access).

If you have implemented these measures correctly, you will have significantly reduced your risk of ransomware and other attacks via RDP.

5.5.2 Exim vulnerability in millions of mail servers

Exim is a mail transfer agent (MTA), i.e. an integral part of a mail server. It is the software that receives and sends emails. Most Unix-based systems use Exim components, and Debian systems have them installed as standard software.[134, 135]

Firstly, local attackers (insiders) can execute system commands with root access, and secondly, attackers who only have remote access can perform similar actions with certain non-default configurations.

This vulnerability was actively exploited by attackers a week after its release. There is disagreement in the reports about how many vulnerable systems were in existence worldwide at the time the vulnerability was released: According to Skybox Security more than 3.5 million servers are concerned. SecureZoo[136] estimates that more than 4 million devices (about 90% of all installations worldwide) use the vulnerable version of Exim.[137] The latest version of Exim is no longer affected by the vulnerability. All systems should urgently be upgraded to Exim version 4.92. As Exim software runs on 57% of all email servers, security researchers estimate the potential damage to be immense.[138]

Assessment:

A large number of vulnerabilities are published every day. For some, a security patch already exists at the time of release; for others not. Since a single company will usually have different systems and software, it can be difficult to manually track all vulnerabilities relating to the hardware and software in use. Updates should therefore be installed automatically whenever possible. Not all published vulnerabilities are effectively exploited by attackers. However, there are vulnerabilities which can be exploited relatively easily, be integrated into exploit kits after a short time and then have the according potential to cause damage.

[134] https://meterpreter.org/cve-2019-10149-exim-remote-code-execution/

[135] https://blog.skyboxsecurity.com/exim-vulnerability/

[136] https://www.securezoo.com/2019/06/critical-exim-vulnerability-discovered-and-patched/

[137] https://www.cisecurity.org/advisory/a-vulnerability-in-exim-could-allow-for-remote-command-execution_2019-061/

[138] https://www.securezoo.com/2019/06/critical-exim-vulnerability-discovered-and-patched/

5.5.3 How a smartphone becomes a bugging device

Reports of two vulnerabilities that would have allowed attackers to turn a smartphone into a bugging device were published in the first half of 2019. One was found in FaceTime and the other in WhatsApp.

The WhatsApp vulnerability was a buffer overflow vulnerability in WhatsApp's VoIP (Voice-over-IP) module, which is used to make phone calls with the application. It could be exploited by sending custom SRTCP[139] packets to the target smartphone. More precisely, all that was required was a manipulated WhatsApp call to the target smartphone. The callee did not have to answer the call, nor was there any trace of a missed call. Therefore, it was difficult to detect that the smartphone had been compromised. The vulnerability was discovered when a lawyer in the United Kingdom allegedly became the target of such an attack.[140]

The FaceTime vulnerability was discovered accidentally by a teenager. It concerned a software bug in the iPhone FaceTime app.[141] After only a few steps, it allowed you to listen to audio recordings of the person's surroundings and to see images from the front camera even before they answered the call. For this to work, the caller had to add themselves to the call as if they were an additional person. Shortly afterwards, Apple released a security patch for this bug which fixed the problem.[142]

5.5.4 Internet Explorer zero-day vulnerability: irresponsible disclosure

Security researchers regularly publish exploits for vulnerabilities to force software companies to immediately produce patches for vulnerabilities previously reported to them.

This was also the case with an Internet Explorer *zero-day exploit*.[143] A security researcher informed Microsoft about the exploit and when the company indicated that it did not currently have any patch planned, the researcher published the exploit together with a proof of concept. In this, he demonstrated that it was possible for attackers to exfiltrate local files and then conduct remote reconnaissance on locally installed program version information when a user opens a prepared MHT file[144] (automatically set to open in Internet Explorer as standard).

Cybercrime groups often use MHT files for *spear phishing* or *malware* distribution. The race between criminals to implement this method and Microsoft to release a corresponding patch has begun.

In such cases of "irresponsible" disclosure, it is generally impossible to say whether the researchers are simply impatient or whether there is a problem on the part of the software company. In any case, these companies should carefully examine all incoming vulnerability reports and provide security researchers with appropriate feedback, including a time horizon for resolving each vulnerability.

[139] Secure Real-time Transport Control Protocol: https://tools.ietf.org/html/rfc3711

[140] https://securityaffairs.co/wordpress/85477/breaking-news/whatsapp-zero-day.html

[141] https://www.buzzfeednews.com/article/nicolenguyen/facetime-bug-iphone

[142] https://9to5mac.com/2019/01/28/facetime-bug-hear-audio/

[143] https://www.zdnet.com/article/internet-explorer-zero-day-lets-hackers-steal-files-from-windows-pcs/

[144] MHT files store web pages including graphics and other embedded elements.

5.6 Preventive measures and prosecution

5.6.1 Dismantling the criminal network behind GozNym

The e-banking Trojan GozNym was operated by a criminal network which had a clear division of labour and whose members were spread across several countries (including Georgia, Bulgaria, Ukraine, Moldova, Kazakhstan and Russia). A complex police operation involving various countries and international organisations resulted in the arrest of several gang members. Among them were *malware* developers, a specialist in mass email distribution, hackers in charge of the actual online bank robberies, money laundering agents and other individuals working in support functions. In May 2019, ten members of the group were charged in Pittsburgh and further cases are pending in Georgia, Moldova and Ukraine. The provider of the bulletproof hosting service is also currently facing legal action in Ukraine. In addition to GozNym, its services were used for more than twenty other *malware* campaigns.[145]

5.6.2 Another success against fake Microsoft support

MELANI already reported on a police operation against computer support fraudsters in its last semi-annual report. In that case, the Indian police searched 26 call centres from where the calls, conducted in English, had been made.[146] Since then, the French police force has also reported a success after arresting three Frenchmen suspected of being the masterminds behind another group performing the scam.[147] In this case, difficult to remove pop-up messages suggested to the victims that their computers had been infected and that they should call "Microsoft Support" on the number displayed. The evidence first led to the Maghreb, where the alleged support agents were located. Investigations into cash flows eventually led to the identification of the French ringleaders.

The fake Microsoft support scam has been around for almost ten years now. MELANI regularly reports on and warns of this phenomenon.[148] Nevertheless, MELANI continues to receive reports of the scam on a regular basis. It can be assumed that it will continue to be used with success and is unlikely to disappear anytime soon. However, at the same time, law enforcement authorities are expected to be able to arrest more and more fraudsters of this kind.

[145] https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

[146] MELANI semi-annual report 2018/2, section 5.5.1.

[147] http://www.leparisien.fr/faits-divers/cybercriminalite-trois-chefs-d-entreprise-soupconnes-d-avoir-pirate-8-000-francais-31-01-2019-8001474.php

[148] https://www.melani.admin.ch/melani/en/home/meldeformular/form/meldeformularhaeufigefragen/mich-hat-eine-firma-angerufen-und-gesagt--dass-mein-computer-mit.html; https://www.melani.admin.ch/melani/en/home/themen/fake_support.html

6 Trends and outlook

6.1 Costs of cybercrime

The experts all agree that cybercrime is on the increase. The reasons for this are widely known: ever-increasing digitalisation of all our activities is opening up a wide range of criminal possibilities. Everyone agrees on that. It is more difficult to quantify this development and even more difficult still to estimate the damage for individual countries or worldwide. The greatest difficulty in obtaining reliable figures lies in the large number of unreported cases of cybercrime, be it because the crimes are not always signalled or reported, or because the victims do not detect them at all. Consequently, statistics on cybercrime costs should always be treated with caution, as they are often purely estimates or projections.

Despite these difficulties, quantitative data is important for those combating cybercrime and for the competent political authorities, especially when it comes to planning appropriate measures. This chapter summarises some studies on cybercrime published in the first half of 2019. The figures can provide information on the extent of the phenomena observed. It is also possible to identify trends by comparing the results obtained with the same method over different periods.

In the study "Measuring the Changing Cost of Cybercrime",[149] which was presented at the Workshop on the Economics of Information Security in Boston in June 2019, the authors compared the current figures and estimates with those of the first study they conducted in 2012. They systematically evaluated the costs of cybercrime, focusing on fraud. In the seven years between the studies, there has been a paradigm shift in ICT use: more and more data is being stored in the cloud, laptops have been replaced by smartphones, Android has replaced Windows, and people are increasingly living their lives online (as well) and on social media. This means that half of all property offences (in terms of number and the amount concerned) are now committed online. The authors also mentioned that business email compromise (BEC) incidents and offences involving cryptocurrencies have soared. Moreover, they found that cybercrime prosecution was not as efficient as that for conventional property offences and suggested that more money should be spent on prosecution than on prevention and anticipation. Although prevention and anticipation are very important, the total loss is still too high from a financial point of view.[150]

Regarding ransomware, the study revealed that criminals made a profit of approximately USD 16 million over a two-year period (2015-2017). However, the actual damage (including lost data, production downtime, recovery time, etc.) is estimated to be multiples of that.

According to the Internet Society's Online Trust Alliance (OTA),[151] cybercriminals are getting better at monetising their activities, and ransomware attacks alone caused USD 8 billion in damage last year. OTA suspects that the cost of ransomware attacks will rise to USD 20 billion

[149] https://www.repository.cam.ac.uk/handle/1810/294492

[150] https://www.inside-it.ch/articles/54646

[151] https://www.internetsociety.org/news/press-releases/2019/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-45b-in-2018/

by 2021 and estimates that cyberincidents resulted in more than USD 45 billion in total losses in 2018. [152, 153]

According to a Crowdstrike study, the Ryuk ransomware netted over EUR 3 million for its criminal users within four months. And this is despite the fact that Ryuk is not mass ransomware; instead, it is distributed in a targeted manner.[154]

Business email compromise (BEC) is another phenomenon that has generated quite a lot of money for the attackers. This form includes cyberattacks aimed at companies that involve invoices and payment instructions via email. Fake sender email addresses or compromised email accounts of the finance division of suppliers and business partners are used in most cases. Attempts were made to transfer money to US accounts in three quarters of all cases in the United States. Most of the cases observed in Switzerland involved foreign accounts to which transfers were to be made. The attempted and successful wire fraud cases reported to the FBI concerned an average of USD 301 million per month in 2018. Even if only a fraction of the recipients pay the bogus invoices or execute the fictitious transfer orders, it is good business for the attackers. According to the study, conventional CEO fraud (alleged CEO issues urgent payment order to the finance division)[155] is declining and bogus payment orders are increasingly being made on behalf of external persons (customers, suppliers, etc.). The email accounts of external persons are sometimes hacked, but other times their address is simply *spoofed*, i.e. used as a fake sender. BEC is a lucrative business, as the profits are quite high, but the risk and work involved are relatively minor.[156]

Another fascinating study was produced by the security company Positive Technologies.[157] This seeks to put a price on how much an *APT* attack costs the attackers. *APT* attackers can be state-sponsored players who can also serve states with rather weak finances. The researchers tried to estimate the costs necessary to procure or produce the tools based on those actually used for *APT* attacks. They concluded that a tool for *spear phishing* (targeted phishing) would cost around USD 2,000. On top of that, penetration testing software costs from USD 8,000 to USD 40,000. The tools needed for a banking attack would thus start at USD 55,000. A cyberespionage campaign, in contrast, would be at least USD 500,000 to start. These figures should be treated with caution, however, as the prices for attack tools vary considerably. If own tools are developed, the estimated price tag is generally higher, as the corresponding expertise of hackers and software developers has to be paid for. Otherwise, there are attack tools that are legally available commercially and are also used by hired penetration testers. These are usually cheaper and also make it more difficult to attribute the attacks to specific *APT*s, as the same tools are used by different groups or nations.

[152] https://www.hackread.com/cloud-hosting-provider-insynq-hit-by-megacortex-ransomware/

[153] https://www.finanzen.ch/nachrichten/aktien/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-$45b-in-2018-1028337623

[154] https://www.lemonde.fr/pixels/article/2019/01/14/le-rancongiciel-ryuk-a-rapporte-plus-de-3-millions-d-euros-a-ses-auteurs_5408807_4408996.html

[155] See section 4.4.5 above.

[156] https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

[157] https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/

Due to the incidents of recent years and greater awareness, more and more companies are increasing their cybersecurity budgets. An ESI ThoughtLab report[158] found that the losses from cyberattacks averaged USD 4.7 million per victim in the last financial year, with more than one in 10 companies losing over USD 10 million. The authors of the study conducted a survey of various companies to find out whether they had been attacked and whether they planned to invest more in cybersecurity in the future. Apparently, companies in most sectors will significantly increase their cybersecurity investments.

Conclusion:

Cybercrime is booming, as a lot of money can be earned by relatively simple means. The capital outlay for cybercrime newcomers is limited and the expertise does not have to be vast, as more and more attack methods are being sold as a service (Cybercrime-as-a-Service, CaaS). An example would be a hacker group that provides Ransomware-as-a-Service, which can be bought by criminals and used with relatively little expertise to make big profits or cause major damage.

One of the aims in the fight against cybercrime is to break cybercriminals' business model. This means increasing the outlay and making it more difficult to earn money, so that profits are smaller. Opportunistic cybercriminals try to penetrate networks with easily available resources. If the company is reasonably well protected and the use of standard attack tools is not immediately successful, they soon look for another target that is less well protected. Needless to say, this statement does not apply to state-sponsored attackers, as these are usually supposed to penetrate a specific network and can thus invest a lot of time and money in an attack on a specific target.

6.2 Personal data protection and social protective measures – finding the balance

We are increasingly using encryption technologies as a matter of course in our personal and business lives, something that was scarcely conceivable a few years ago. For example, many people use WhatsApp for communication, and the current version of this uses the Signal Protocol for end-to-end encryption of chats. This means that the messages written can be read only on the sender's and recipient's devices. The texts are encrypted when they are transmitted over the internet. Aside from interpersonal communication, websites are increasingly being viewed in encrypted form. Evaluations of the telemetry data of Chrome[159] and Firefox[160] show that connections established via these browsers are now secured with TLS certificates in around four out of five cases. The fact that website operators can obtain certificates free of charge via the Let's Encrypt[161] initiative of the non-profit organisation Internet Security Research Group (ISRG) has certainly contributed to this.

[158] https://www.helpnetsecurity.com/2019/07/15/boost-cybersecurity-investments/

[159] https://transparencyreport.google.com/https/overview?hl=en

[160] https://letsencrypt.org/stats/

[161] https://letsencrypt.org/about/

The move towards more and better encrypted connections will become more pronounced. For example, the Internet Engineering Task Force (IETF) released the transport layer security protocol version 1.3 (TLS 1.3) last year.[162] Likewise, *DNS* queries are increasingly being transmitted in encrypted form. Mozilla is planning to activate DNS over HTTPS (DoH) by default for its Mozilla Firefox browser.[163] DNS over TLS (DoT) is forced by the system in the current Android version 9 if available,[164] and the new 5G mobile phone generation offers better protection against fake mobile base stations.[165]

All of these advancements improve connection confidentiality for device users, but in some cases restrict established protection mechanisms against criminal content or law enforcement surveillance options. For example, encrypted *DNS* queries prevent attackers from modifying them on the network path, but, depending on the server queried, also make it impossible for internet providers to issue warnings concerning phishing sites or sites attempting to deliver *malware*. MELANI also supports blacklist operators, for instance, so that internet users do not end up on phishing sites[166] and unintentionally disclose their access data for e-banking, for example. A similar problem arises with SSL termination, where encrypted connections are broken on a *proxy* to filter out malicious content such as *malware*. TLS 1.3 severely complicates the established methods used by many companies or even makes them impossible.

Especially in the area of law enforcement, the shift towards more encryption has been the subject of vigorous discussion,[167] as the mechanisms used to protect against criminal content and to monitor criminals were dependent on certain design vulnerabilities in the infrastructure. The problem is that some government players reacted with new technology bans or regulations for the inclusion of backdoors instead of seeking ways in which protection and legal monitoring could be implemented without any loss of security in the personal use of the technology. It was often argued recklessly that these measures would not compromise user security. The United States Attorney General changed his argument only recently and admitted that the proposed measures for government protection of society are not possible without a loss of security for end users.[168]

Therefore, discussions can be held on a transparent basis in a company as well as in a state as a whole regarding which personal restrictions can be tolerated in order to reduce the overriding risks. An example of how SSL termination can be implemented in compliance with personal data protection is given in the Zurich Data Protection Commissioner's checklist for decrypting web connections.[169]

[162] https://www.ietf.org/blog/tls13/

[163] https://blog.mozilla.org/futurereleases/2019/04/02/dns-over-https-doh-update-recent-testing-results-and-next-steps/

[164] https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html

[165] https://www.zdnet.com/article/stingray-spying-5g-will-protect-you-against-surveillance-attacks-say-standards-setters/

[166] https://www.antiphishing.ch/en/about/

[167] https://www.theregister.co.uk/2019/06/25/andrew_sullivan_internet_society_interview/

[168] https://www.schneier.com/blog/archives/2019/07/attorney_genera_1.html

[169] https://dsb.zh.ch/internet/datenschutzbeauftragter/de/publikationen/anleitungen/_jcr_content/contentPar/form/formitems/kein_titel_gesetzt__0/download.spooler.download.1562593220478.pdf/Checkliste-Entschluesselung-Webverbindungen.pdf

All organisations should exploit the new technologies in their environment to boost the security of the infrastructure of the persons involved and introduce restrictions on these measures to protect against criminal content only in a very reflective manner. Holding on to absolutist positions will tempt those who disagree to circumvent them. Only with the right balance can the desired optimal security be achieved for everyone on the internet of the future.

6.3 Threat of supply chain deglobalisation?

Imagine the following scenario: in rare cases, a software error in a supplier's vehicle control component leads to malfunctions in the braking behaviour of the cars concerned. This may sound bad, but a quick recall of the affected models of various car manufacturers using this component can fix the problem with a 15-minute software update in your local garage. Only the new assumedly European car, which you bought after careful consideration of road safety in particular, is excluded from the update. This is because the vehicle supplier was placed under an export control regime in its home country due to alleged national security interests and unfortunately it is no longer allowed to transfer technology with companies whose parent company is headquartered in China.

This scenario may appear rather far-fetched, but something similar actually happened in the communications industry in the first half of 2019. On 16 May 2019, the Bureau of Industry and Security (BIS) of the United States Department of Commerce issued a so-called final rule which added the Chinese ICT manufacturer Huawei and its affiliates to an entity list that subjects the transfer of goods and know-how to these entities to an export control regime. This prohibits US companies from doing business with these entities without special authorisation. As a result, Google announced a few days later that it would no longer deliver Android updates to Huawei in the foreseeable future and that Huawei mobile phones would be banned from the Google ecosystem sooner or later. The chip manufacturers Intel, Qualcomm and Broadcomm made similar announcements shortly thereafter.

Huawei's response to the chip manufacturers' statements was primarily focused on assuring customers that enough hardware was already stockpiled to meet planned deliveries, such as supplying Sunrise with components for the 5G network infrastructure. Furthermore, alternative supply channels that are independent of US companies are set up. Faced with the threat of exclusion from the Android family, the Chinese mobile phone manufacturer announced the possibility of creating its own operating system and thus its own ecosystem.

With their intervention – even though postponed temporarily and slightly alleviated in the meantime – in the domestic ICT industry,[170] the US authorities ultimately escalated a fundamentally bilateral trade dispute to the global level and thus also exposed the vulnerability of highly globalised supply chains, especially with regard to the communications industry. While the biggest threat to non-US and Chinese companies and customers had been higher costs due to the mutual sanctions between China and the United States, Swiss users of Huawei products and components are now additionally faced with the issue of their preservation of vested rights, lifespan, maintenance and interoperability in the future. And more generally, there is the question of whether a state leveraging its de facto predominant market clout has created a precedent that will lead to similar actions in other contexts. The economic policy undertone of subjecting Huawei to the US sanction regime can hardly be ignored. Accordingly, there is the

[170] See also chapter 3 of the MELANI semi-annual report 2018/2.

question, at least hypothetically, of whether something similar could also be possible against an unpopular, non-Chinese manufacturer, irrespective of the planning uncertainties and costs that the current situation already entails.

Supply chains are a global phenomenon nowadays, not only in ICT but in virtually all industrial production. Suppliers are not limited to just a handful of countries. For example, the ETH spinoff u-blox, based in Thalwil, plays a leading international role as a supplier of high-precision positioning components for the development and manufacture of self-driving vehicles. These globalised supply chains are based on the core principle that technology and know-how can be traded, installed and used according to market principles in order to manufacture a wide range of end products whose success or failure is ultimately determined by the market.

Disruptions to this system first affect small, open economies such as Switzerland, which are dependent on foreign suppliers due to a lack of domestic alternatives and on foreign customers in view of their own supply industry, in a supply and demand market that is as open and globally interoperable as possible. This can be in terms of plannability, investment security or the possibility of opting for a mixture of (infrastructure) components from different spheres of state influence as part of risk management.

The momentum initiated in May bears the risk of a medium- to long-term regionalisation of the supply chains and may in extremis lead to the basic safety of certain products temporarily no longer being guaranteed. Or, following the introductory example: The brakes of the new car at home will continue to fail in 1:100,000 cases until a work-around from the car manufacturer becomes available, because the government intervention in the supply chain does not permit a prompt solution.

7 Politics, research, policy

7.1 Switzerland: parliamentary procedural requests

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Mo	19.3009	Incentive programme for the spread of innovative digitalisation projects in the education sector	National Council Science, Education and Culture Committee (SECC-N)	21.02.2019	NC	SECC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193009
Mo	19.3010	Launch of a digitalisation incentive programme for federal and cantonal universities, universities of applied sciences, vocational training and continuing professional development	SECC-N	21.02.2019	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193010
Ip	19.3051	Huawei and the challenges of 5G; risks and opportunities for Switzerland	Regazzi Fabio	06.03.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193051
Mo	19.3121	National procedure for dealing with data leaks	Buffat Michaël	14.03.2019	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193121

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Po	19.3135	Do we have cybersecurity under control when it comes to Armed Forces procurement?	Dobler Marcel	18.03.2019	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193135
Po	19.3136	Do we have the hardware and software components for our critical infrastructures under control?	Dobler Marcel	18.03.2019	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193136
Ip	19.3139	Minimise cyberthreats by means of cyberattachés	Müller Damian	18.03.2019	CS	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193139
Ip	19.3185	No digital backdoors for federal procurement	Vogler Karl	20.03.2019	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193185
Po	19.3199	Improve the security of connected products	Reynard Mathias	21.03.2019	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193199
Ip	19.3205	Digitalisation is losing momentum. What is the Federal Council doing?	Burkart Thierry	21.03.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193205
Ip	19.3255	Defend liberal democracy against the rise of antisemitism and extreme right-wing ideas	Wermuth Cédric	21.03.2019	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193255
Ip	19.3267	Is the PTSS practice in compliance with the law in terms of the obligations of providers of derived communications services?	Flach Beat	21.03.2019	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193267
Ip	19.3321	The launch of the new 5G mobile phone technology in Switzerland requires the Confederation to duly inform the population	Amman Thomas	22.03.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193321
Ip	19.3330	Should patient data be sold to the highest bidder?	Reynard Mathias	22.03.2019	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193330
Po	19.3342	Authorisation system for open government data	Badran Jacqueline	22.03.2019	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193342
Ip	19.3377	Cantonal differences in criminal proceedings for child pornography. Still no need for action?	Guhl Bernhard	22.03.2019	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193377
Mo	19.3428	Necessary expansion of the "digital transformation" advisory board	Kälin Irène	07.05.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193428

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Ip	19.3431	Economic advantages and health consequences of 5G?	Fiala Doris	07.05.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193431
Mo	19.3448	Provisional setting aside of objection – alignment with the changed business practice (digitalisation)	Dobler Marcel	08.05.2019	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193448
Ip	19.3461	Cybersecurity – tackling the future alone or together?	Béglé Claude	08.05.2019	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193461
Ip	19.3505	Allocation of 5G mobile licences without a corresponding basis for the licensing authorities	Töngi Michael	09.05.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193505
Ip	19.3534	5G: When a working group investigates the impact of electromagnetic radiation in Switzerland, the independence of the group members is at least as important as their skills	Borloz Frédéric	03.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193534
Ip	19.3535	Launch of 5G technology in Switzerland: What compensation from the Confederation in view of the additional burden for the cantons?	Gschwind Jean-Paul	03.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193535
Po	19.3574	Push for a digital public service	Marti Min Li	11.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193574
Po	19.3593	Digitalisation of scientific collections for the benefit of Swiss research	Germann Hannes	12.06.2019	CS	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193593
Mo	19.3649	Legal basis for a digitalisation fund	Savary Géraldine	18.06.2019	CS	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193649
Ip	19.3659	Swisscom launches data leech Beem: How is this compatible with the Confederation's owner strategy?	Marti Samira	19.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193659
Mo	19.3663	A digital council, in the name of the people!	Pardini Corrado	19.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193663
Ip	19.3686	Tallinn Declaration on eGovernment: Where does Switzerland stand at present and what has to be done?	FDP.The Liberals Group	19.06.2019	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193686
Ip	19.3693	Digital transformation – a major challenge	Fiala Doris	19.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193693

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Po	19.3759	Digital-compatible form requirements in the Consumer Credit Act	Dobler Marcel	20.06.2019	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193759
Po	19.3785	Digital illiteracy leads to social exclusion	Reynard Mathias	20.06.2019	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193785
Ip	19.3787	What is the Confederation doing to combat hate speech on the internet?	Seiler Graf Priska	20.06.2019	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193787
Po	19.3850	How can the private sector be efficiently involved in development projects and how can new technologies be promoted?	Béglé Claude	21.06.2019	NC	FDFA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193850
Ip	19.3865	International Geneva: How can Switzerland support international organisations and NGOs in the digitalisation process and at the same time guarantee the protection of war victims' data?	Derder Fathi	21.06.2019	NC	FDFA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193865
Ip	19.3866	A cybercommand for the Swiss Armed Forces?	Candinas Martin	21.06.2019	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193866
Po	19.3878	5G must not jeopardise net neutrality	Béglé Claude	21.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193878
Mo	19.3884	A strategy for Switzerland's digital sovereignty	Derder Fathi	21.06.2019	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193884
Ip	19.3919	Artificial intelligence (AI) and digital transformation – we need a holistic strategy	Ricklin Kathy	21.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193919
PI	19.417	Creation of a media promotion levy on digital platforms	Töngi Michael	21.03.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20190417
PI	19.418	For a model aimed at promoting electronic media	Töngi Michael	22.03.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20190418
QT	19.5274	5G technology – inform and explain to rebut some common misconceptions	Regazzi Fabio	05.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195274
QT	19.5286	5G antennas – what are the limits?	Schneider Schüttel Ursula	05.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195286

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
QT	19.5296	5G technology – alternatives?	Schneider Schüttel Ursula	05.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195296
QT	19.5315	Is 5G already in operation?	Hardegger Thomas	11.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195315
QT	19.5349	5G – what next?	Bigler Hans-Ulrich	12.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195349
QT	19.5355	5G – delay and costs for the economy?	Brunner Hansjörg	12.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195355
QT	19.5370	Beem	Masshardt Nadine	12.06.2019	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195370

7.2 CSS study compares national cybersecurity strategies – challenges for Switzerland

ETH Zurich's Center for Security Studies (CSS) published a comparative study on national cybersecurity strategies in Finland, France, Germany, Israel, Italy, the Netherlands and Switzerland in March 2019 and made the following findings.[171] The cybersecurity strategies generally have many conceptual similarities. These include in particular key aspects such as the holistic approach, which encompasses both national security and socioeconomic concerns; the importance of international cooperation; an emphasis on essential cooperation with the private sector; and the need for comprehensive awareness-raising, education and information. The main differences lie in the location of cybersecurity within state structures and the assignment of responsibilities. This applies especially to the extent of centralisation and the relationship between civil and military units. The reasons for the differences largely stem from the political culture and the organisation of political systems.

The CSS identified various challenges in the development and implementation of national strategies. Examples include the vertical integration of national cybersecurity into the national security framework and the horizontal coordination of the various bodies in charge of cybersecurity. Furthermore, in the future, countries will have to focus increasingly on promoting international cooperation and developing international codes of conduct in cyberspace. Appropriate situation analyses and efficient crisis management round off the future needs.

[171] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MELANI%20Studie_final_AW_18März2019.pdf

7.3 Implementation of the national strategy for the protection of Switzerland against cyber-risks (NCS)

The Federal Council has taken fundamental decisions to protect Switzerland against cyber-risks over the past two years. In April 2018, it adopted the "national strategy for the protection of Switzerland against cyber-risks (NCS)"[172] for the period 2018 to 2022. The overriding objective of the NCS is to ensure that Switzerland is appropriately protected against cyber-risks and resilient to them when exploiting the opportunities offered by digitalisation. Based on this vision, the NCS identifies seven strategic objectives which are to be achieved by means of 29 measures in a total of ten areas of action.

Unlike with the first NCS for the period 2012 to 2017, the area of cyberdefence is an integral part of the strategy. This refers to the role of the Armed Forces and the Intelligence Service regarding attribution, the prevention of cyberattacks and the assurance of military readiness. Further new features include the extension of the target group to the entire economy and society (the first strategy focused on the protection of critical infrastructures) and a stronger focus on standardisation and regulation, including the examination of a reporting obligation. With these adjustments, the NCS fulfils its function as an overall strategy, takes account of the growing importance of cyber-risks for all companies and provides the basis for the development of standards and regulatory measures.

7.3.1 Implementation plan and organisation of the Confederation in the area of cyber-risks

It is clear that the ambitious portfolio of the NCS can be successfully implemented only if the work of the various players involved is optimally coordinated and all existing expertise is used. All federal, cantonal, business and university bodies involved thus drew up the NCS implementation plan[173] together, and it was adopted by the Federal Council on 15 May 2019.[174] For each measure, the implementation plan sets out which organisation will implement which projects by when, thereby forming the basis for the strategic controlling with which the progress of NCS implementation will be checked.

The Confederation reviewed and adapted its own organisation while the implementation plan was being drawn up.[175] The key elements of this organisation in relation to NCS implementtation are illustrated in the figure below.

[172] https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie.html

[173] https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/umsetzungsplan.html

[174] https://www.admin.ch/gov/en/start/dokumentation/medienmitteilungen.msg-id-75046.html

[175] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73839.html

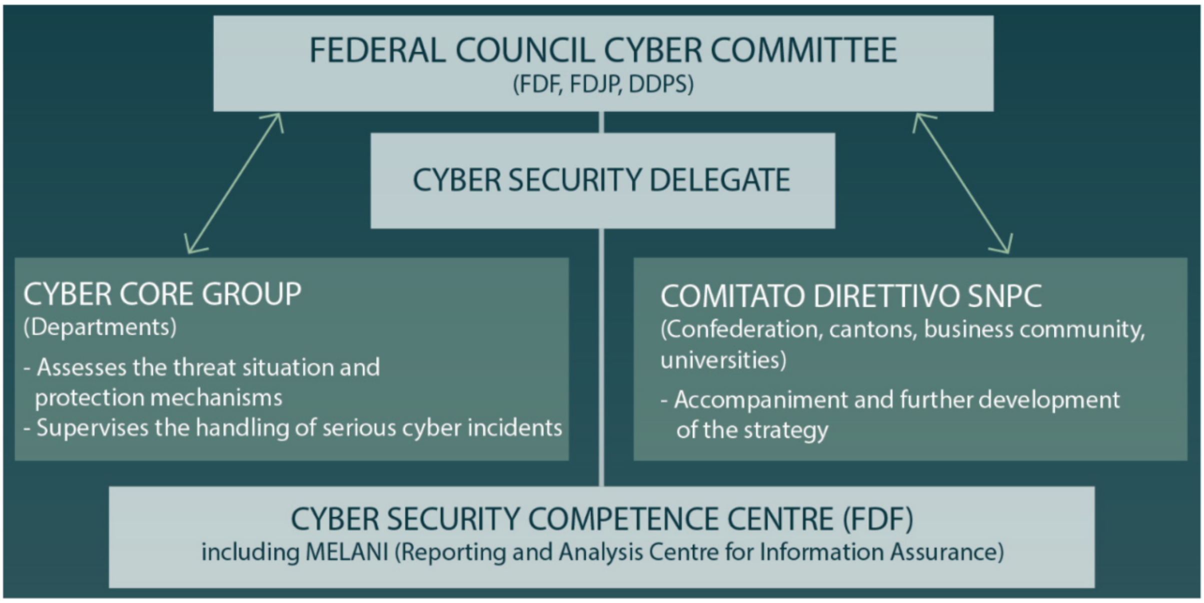

FEDERAL COUNCIL CYBER COMMITTEE
(FDF, FDJP, DDPS)
CYBER SECURITY DELEGATE
CYBER CORE GROUP
(Departments)
- Assesses the threat situation and protection mechanisms
- Supervises the handling of serious cyber incidents
COMITATO DIRETTIVO SNPC
(Confederation, cantons, business community, universities)
- Accompaniment and further development of the strategy
CYBER SECURITY COMPETENCE CENTRE (FDF)
including MELANI (Reporting and Analysis Centre for Information Assurance)

Figure 8: Federal cyber-risk organisation

The strengthening of interdepartmental coordination and cooperation with the business community, the cantons and universities are important elements of the new organisation. The following bodies have been created for these tasks:

- The **Federal Council Cyber Committee**, consisting of the heads of the Federal Department of Finance (FDF), the Federal Department of Justice and Police (FDJP) and the Federal Department of Defence, Civil Protection and Sport (DDPS), has the task of supervising the implementation of the NCS.
- The **Cybersecurity Core Group** boosts coordination between the three areas of security, defence and criminal prosecution, ensures a joint threat assessment and supervises the handling of serious and interdepartmental incidents by federal units.
- The **NCS Steering Committee (NCS StC)** ensures the coordinated and targeted implementation of the NCS measures and develops proposals for the further development of the NCS.

7.3.2 Cyber Security Delegate and National Cyber Security Centre

Aside from the coordinating bodies, central structures were created with the Cyber Security Delegate and the National Cyber Security Centre. The Cyber Security Delegate is in charge of the strategic management of cybersecurity in the Confederation, heads the National Cyber Security Centre, as well as the interdepartmental bodies appointed by the Confederation (with the exception of the Cyber Committee), and represents the Confederation in other bodies. Florian Schütz was appointed for this key position.[176] He took up his duties in August 2019 and reports directly to the Head of the Federal Department of Finance.

The National Cyber Security Centre in the FDF will be the national contact point for all issues relating to cybersecurity. It will build on MELANI's existing organisation and expand it so that

[176] https://www.efd.admin.ch/efd/en/home/dokumentation/nsb-news_list.msg-id-75421.html

it can offer services for the entire economy, and issue warnings and information on cyber-risks for the general public. Within the Confederation, it supports the offices with cyberexpertise in terms of prevention, standardisation and regulation. When dealing with cyberincidents, it receives the authority to issue directives vis-à-vis federal units.

With the adoption of the NCS implementation plan, the Federal Council also provided resources for the National Cyber Security Centre so that it can expand MELANI's existing operations accordingly from 1 January 2020.

A more detailed description of the National Cyber Security Centre and its tasks will be published in the next MELANI semi-annual report.

8 Published MELANI products

8.1 GovCERT.ch blog

8.1.1 Severe ransomware attacks against Swiss SMEs

09.05.2019 – As we have seen an ever-increasing number of ransomware cases with a rather sophisticated modus operandi, we are publishing a warning via the MELANI newsletter along with this blog post, documenting technical details about the recent ransomware attacks against Swiss small and medium-sized enterprises (SMEs). The aim of this blog post is to give you a better understanding of the various modi operandi of the most common ransomware families we have encountered hitting Swiss targets in the past months.

➔ https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

8.2 MELANI newsletter

8.2.1 Sextortion: numerous people in Switzerland affected – authorities launch "stop-sextortion.ch"

24.04.2019 – Blackmailers claim in an email to have access to computers and webcams and threaten to publish images and videos with sexual content if no ransom is paid. This scam is called fake sextortion and typically requires payment in bitcoins. With the help of this form of fraud, criminals have obtained bitcoins worth approximately CHF 360,000 over the past six months in spite of the small sums demanded. As long as the email recipients concerned pay the ransom, this procedure will be invigorated and will continue to be used. Help stop this scam and refrain from paying any ransom. You can find information and report fake sextortion emails on the website stop-sextortion.ch, which was launched by the authorities today.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/fake-sextortion.html

8.2.2 Encryption Trojans are increasingly targeting corporate networks

09.05.2019 – Since the beginning of 2019, there have been growing numbers of reports from SMEs and large companies in Switzerland and abroad that their data has been encrypted by encryption Trojans, so-called ransomware, and thus made unreadable. In some cases, backups were also encrypted during these attacks, making it impossible to restore the business activities of the companies concerned.

➔https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/verschluesselungstrojaner-greifen-vermehrt-gezielt-unternehmensn.html

9 Glossary

Term	Description
APT Advanced persistent threat	Various techniques and tactics are used in this attack. It is specifically targeted at a single organisation or country. Very significant damage can be done in most cases. Therefore, 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 an often intentionally incorporated software feature that allows users to gain remote access to a computer or protected function of a computer program by circumventing the usual access controls.
BGP Border Gateway Protocol	Border Gateway Protocol is the routing protocol used on the internet to determine the path of data packets between networks.
Bitcoin	Bitcoin is a decentralised payment system that can be used worldwide, as well as the name of a digital currency unit.
Bot	Comes from the Slavic word "robota" meaning work. Refers to a program that automatically carries out certain actions after receiving a command. Malicious bots can control compromised systems remotely and have them carry out any kind of arbitrary action.
Botnet	Several bots can form a network, which is controlled via a command & control infrastructure.
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.
C2 Command and control	Command and control infrastructure of botnets. Most bots can be monitored and receive commands via a communication channel.
CaaS Cybercrime-as-a-Service	Cybercrime as a service that can be purchased enables technically inexperienced criminals to carry out illegal activities on the internet with easy-to-use tools.
CEO fraud	CEO fraud occurs when perpetrators instruct the accounting or finance department in the name of the CEO to make a payment to the (typically foreign) account of the scammers.

Term	Description
CPU / processor	The CPU (central processing unit) is another term for processor, the central unit in a computer, and contains the logic 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. With a DoS attack, the victim's service or system is attacked simultaneously by many different systems, bringing it to a standstill and rendering it unavailable.
Defacement	Unauthorised alteration of websites.
DNS Domain name system	With the help of DNS, the internet and its services can be utilised in a user-friendly way, as users can utilise names instead of IP addresses (e.g. www.melani.admin.ch).
Drive-by infection	Infection of a computer with malware simply by visiting a website. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
Dropper / downloader	A dropper or downloader is a program that downloads and installs one or more instances of malware.
Exploit kits	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.
GPS Global Positioning System	Global Positioning System (GPS), officially NAVSTAR GPS, is a global navigation satellite system for determining position and measuring time.
Internet of Things	The term "Internet of Things" (IoT) describes the networking and collaboration of physical and virtual objects.
ISP Internet service provider	Internet service providers are providers of services, content or technical services that are required for the use or operation of content and services on the internet.

Term	Description
JavaScript	An object-based scripting language for developing applications. JavaScripts are program components integrated in HTML code enabling specific functions in internet browsers. An example could be checking user input in a web form. It is possible to verify that all the characters entered when a telephone number is requested are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the computer of the website visitor. Aside from useful features, unfortunately dangerous functions can also be programmed. Unlike ActiveX, JavaScript is supported by all browsers.
Malspam	Bulk emails with which malware is distributed.
Malware	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Malware	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Man-in-the-middle attacks (MITM)	Attacks in which the attacker infiltrates the communication channel between two partners unnoticed and is thereby able to spy on or even modify their data exchanges.
Metadata	"Metadata" and "meta-information" refer to data containing information about other data.
Monitoring and control systems (MCS)	Monitoring and control systems (MCS) 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 systems (ICS)" is commonly used.
MSP Managed service provider	A managed service provider is an IT service provider that supplies and manages a defined set of services for its clients.
NAS Network-attached storage	Hard disk storage or file server connected directly to a network.
Patch	Software which replaces the faulty part of a program with an error-free part, thereby eliminating a vulnerability, for example.

Term	Description
Peer to peer	Network architecture in which the systems involved can carry out similar functions (in contrast to client-server architecture). P2P is often used for exchanging data.
Phishing	Fraudsters phish in order to obtain 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' credulity and helpfulness by sending them emails with false sender addresses.
PowerShell script	PowerShell is a Microsoft cross-platform framework 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 then making a connection on the other side via its own address.
RaaS Ransomware-as-a-Service	Ransomware as a service that can be purchased enables technically inexperienced criminals to carry out attacks with easy-to-use tools.
Ransomware	Malware that typically seeks to persuade its victims to pay a ransom by encrypting data.
RDP Remote Desktop Protocol	A Microsoft network protocol for remote access to Windows computers.
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 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.

Term	Description
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. Phishing is a well-known form of social engineering.
Spam	Spam refers to unsolicited and automated mass advertising, a category into which spam emails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
Spear phishing	Targeted phishing attacks. The victims are led to believe that they are communicating via email with someone they know, for example.
Spoofing	Falsification of address elements or signals in order to deceive the recipient person or device.
Supply chain attacks	Attack that attempts to infect the actual target by infecting a company in the supply chain.
Take-down	Term used when a provider takes a website offline due to fraudulent content.
TCP/IP	Transmission Control Protocol/Internet Protocol is a suite of network protocols, also referred to as the internet protocol family because of its great importance for the internet.
TLD Top-level domain	Every name of a domain on the internet consists of a sequence of character strings separated by full stops. 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 item in the sequence (com) is the top-level domain of this name.

Term	Description
Two-factor authentication	Two-factor authentication is used to increase security. 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, scratch list, etc.); 3. A unique body feature (e.g. fingerprint, retinal 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. Serial communication 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. New devices are usually detected and configured automatically (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 with malware using websites which tend to be visited only by a specific user group.
Website infection	Infection of a computer with malware simply by visiting a website. The websites concerned often have 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.
WLAN	WLAN stands for Wireless Local Area Network.
Worm	Unlike viruses, worms do not need a host program to spread. Instead, they use vulnerabilities or configuration errors in operating systems or applications to spread independently from one computer to another.
Zero-day vulnerabilities	Vulnerability for which no patch exists yet.
ZIP file	ZIP is an algorithm and file format for data compression to reduce the storage space needed for archiving and transferring files.