Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

National Cybersecurity Centre NCSC
Federal Intelligence Service FIS

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

INFORMATION ASSURANCE

SITUATION IN SWITZERLAND AND INTERNATIONALLY

Semi-annual report 2020/1 (January – June)

29 OCTOBER 2020

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

1 Overview/contents

2 Editorial

Swiss cyberdiplomacy in the context of digital geopolitics

Special Envoy for Cyber Foreign and Security Policy, Jon Fanzun

Jon Fanzun, Special Envoy for Cyber Foreign and Security Policy

Just a few years ago, cybersecurity was a niche topic that, at an international level, was almost only discussed in technical expert circles. Today, cybersecurity has become an elementary part of international politics and a hotly debated topic. The issue is also sensitive because digital technologies play a central role in our highly developed information society. Key technologies are therefore becoming the focus of global conflicts.

The current dispute between the United States and China on 5G is an example of how security policy, economic and social issues are merging into a new form of geopolitics. In this context, we can talk about "digital geopolitics", which is not only a race between technologies, but also an ideological race between a liberal and a state-centred model.

Against this background, Switzerland must also actively represent its interests in cyberspace. The FDFA cyberoffice assumes this task in cooperation with the various partners in the Federal Administration – in particular with the National Cybersecurity Centre (NCSC). The current national strategy for the protection of Switzerland against cyber-risks (NCS 2.0) and the 2020-2023 foreign policy strategy provide the strategic framework for this.

Switzerland is committed to a free, secure and open cyberspace, which is used for peaceful purposes and based on clear rules and mutual trust. In doing so, it adheres to the principle that international law must also be applied and implemented in cyberspace. In addition, we are committed to the inclusion of relevant stakeholders from international civil society and business. We promote our interests and values in international forums such as the UN, the OSCE and also the OECD. Bilateral cyberdialogues are equally important. In the coming years we want to intensify and expand these dialogues with selected countries, in line with NCS 2.0.

However, in view of the increasing formation of blocs, the dramatic decline in trust between countries and the resulting fragmentation of cyberspace, progress in international cyberdiplomacy will be hard to achieve. It will be difficult enough to consolidate the international consensus already achieved as set out, for example, in the 2015 report of the "United Nations Group of Governmental Experts" (GGE).

As confidence wanes and debates become more intense, the need for bridge-builders will grow. This is where Switzerland can bring its diplomatic strengths and credibility to bear. It can apply its offline experience to the online world. International Geneva plays an important role here as Switzerland can provide a trustworthy framework for discussions on cybersecurity and new technologies. The "Geneva Dialogue on Responsible Behaviour in Cyberspace" is a good example of how Switzerland is making a pragmatic contribution to cybersecurity by involving global companies such as Microsoft, Kaspersky and Huawei in the discussions on cybersecurity.

Cyberdiplomacy is a team sport. It is essential to include the relevant stakeholders and their know-how in order to represent Swiss interests effectively on the international stage. In this respect, the bundling and coordination of forces within the NCSC also creates added value for Switzerland's international cybersecurity. My thanks therefore go to all those involved from the various departments for their commitment to a free, secure and open cyberspace.

Jon Fanzun

On our own behalf:

This is the last time that the MELANI semi-annual report will appear in this guise. In the future, it will be published by the National Cybersecurity Centre (NSCS) as MELANI became part of the NCSC when the Ordinance on Protecting against Cyber-Risks in the Federal Administration came into force on 1 July 2020.

To enable us to continuously improve our products and respond to readers' needs, we invite you to send us **your views on this report**:

https://www.melani.admin.ch/melani/en/home/dokumentation/reports/evaluation-halbjahresbericht1.html

3 Key topic: COVID-19

3.1 Opportunity for social engineering

Cyber threat actors regularly adapt social engineering attacks to current major events such as natural disasters and sporting events. This was also the case with the current pandemic. A new type of virus, about which little is known and which can potentially affect everyone, is ideally suited for such attacks as they exploit feelings of insecurity, fear and curiosity. Attackers have tried to secretly install malware on people's computers, or they have tried to trick individuals into revealing personal information by promising to provide information about the virus. These promises of information ranged from the latest findings concerning infection vectors, infection figures and information about the current spread of the virus. They also offered news regarding protective measures and treatment methods. The initially limited availability of personal protective equipment (PPE) such as face masks and disinfectants also provided the attackers with an opportunity to attract attention with relevant offers.[1] After governments adopted measures to support their citizens and companies, fraudulent emails about these followed.[2] This was especially the case where exceptional and therefore unfamiliar processes were introduced. Contact tracing also brings new opportunities for social engineering. Finally, leisure parks and attractions advertised special offers after their reopening, which criminals used as an opportunity to spread bogus offers.[3] Criminals are likely to use the development and launch of vaccines as a next front for this type of attack.

One scenario that gained momentum as a result of shop closures and the resulting increase in online orders was a supposed issue with an alleged parcel delivery.[4] Often these messages were accompanied by a request to take action: the recipients of such emails or text messages were asked to pay missing postage or a customs clearance fee. These types of emails, sent under the name of delivery companies such as DHL, FedEx and UPS, but also national postal services or customs, are often used to spread malicious software, or to carry out phishing or fraud, as well as to set subscription traps (see chapter 3.1.3 and Overview of reports received in chapter 4).

3.1.1 Spread of malware

Almost all common malware families were sooner or later disseminated using the pretext of coronavirus or COVID-19. The most common vector for spreading was emails with a malicious attachment or a link to an infected website. In addition, unofficial app stores offered apps that

---

1 https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/

2 https://www.cisa.gov/sites/default/files/publications/Avoid_Scams_Related_to_Economic_Payments_COVID-19.pdf; https://www.proofpoint.com/us/blog/threat-insight/ready-made-covid-19-themed-phishing-templates-copy-government-websites-worldwide

3 https://www.cybercrimepolice.ch/de/fall/wieder-betrug-mit-themenpark-tickets-zoo-zuerich-nein-abofalle/; https://www.srf.ch/news/schweiz/abzocke-mit-abofalle-betrug-im-namen-des-zueri-zoo

4 https://www.cybercrimepolice.ch/de/fall/sms-angeblich-im-namen-der-post-betrueger-verteilen-spionage-app/; https://www.cybercrimepolice.ch/de/fall/angebliche-paketlieferung-mit-code-per-sms-freischalten/; https://www.kaspersky.com/blog/covid-fake-delivery-service-spam-phishing/35125/

were supposed to show the spread of the virus on a map and warn of infected people nearby.[5] Copies of official tracing apps that had been infected with malware were also discovered.[6] The increased interest in video conferencing solutions was also exploited: bogus websites using typo domain names, i.e. domain names that are so similar that they could be mistaken for each other, provided installation files for conferencing software that were infected with malware.[7]

On 13 March, there was a wave of malware emails specifically targeted at Switzerland.[8] Here, the English abbreviation "FOPH" (Federal Office of Public Health) was used as the alleged sender. The emails were sent via the Kenyan Embassy in Paris, whose IT infrastructure had been hacked. The attached Excel file contained the AgentTesla Trojan, which records keyboard entries and can create screenshots.

Fig. 1: Email sent in the name of the FOPH with a malware attachment.

In most cases, these coronavirus and COVID-19 decoys were used to spread malware that could steal information (*infostealer* or *spyware*).[9] This *spyware* often contains modules that

5 https://www.cybercrimepolice.ch/de/fall/vorsicht-vor-falscher-corona-virus-mapping-app/; https://symantec-blogs.broadcom.com/blogs/threat-intelligence/android-apps-coronavirus-covid19-malicious; https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/

6 https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data; https://www.bleepingcomputer.com/news/security/new-f-unicorn-ransomware-hits-italy-via-fake-covid-19-infection-map/; https://cert-agid.gov.it/news/campagna-ransomware-fuckunicorn-sfrutta-emergenza-covid-19/

7 https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/; https://blog.trendmicro.com/trendlabs-security-intelligence/zoomed-in-a-look-into-a-coinminer-bundled-with-zoom-installer/

8 https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/gefaelschte-emails-im-namen-des-bag.html

9 https://blog.checkpoint.com/2020/05/11/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/; https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/; https://www.bleepingcomputer.com/news/security/microsoft-warns-of-covid-19-phishing-spreading-info-stealing-malware/

allow any other type of malware to be installed later on. In some cases, ransomware was distributed directly via such emails.

Recommendations:

If you have clicked on links or opened attachments in suspicious emails, your device may be infected with malware. You should examine your device and clean it if necessary, or better still, reinstall it completely. If you are unable to do this yourself, contact a specialist. Antivirus programs do not provide any guarantee that they will detect all infections and remove them completely. After reinstalling, change all passwords used on the device concerned.

3.1.2 Phishing

Current events and unfamiliar situations are often used by cybercriminals for social engineering to make people perform an action out of curiosity, fear or lack of knowledge. In such cases, the actual event is often referenced in order to lend credibility to the scenario. For example, shortly after lockdown was imposed, emails were sent in the name of Netflix promising free access during the coronavirus crisis.[10] Credit card details had to be provided to register for this offer. Phishing via supposed conference platforms was another example of how the extraordinary situation was exploited to carry out attacks. Many users were using such conferencing and collaboration software for the first time. This meant that many users found it difficult to tell whether a message actually came from the platform or whether it was a fake.[11] The attackers exploited these uncertainties in such a way that users were directed to manipulated login screens where they were asked to enter their passwords.

Recommendations:

A healthy degree of scepticism should always be shown when you receive new or unusual messages. Instead of using the links in such messages, you should sign in to your user account in the usual way if possible. Before entering any personal data, passwords or credit card information, always check that you are actually on the page you want to visit.

3.1.3 Subscription traps

During the lockdown in March, messages circulated via WhatsApp in Switzerland promising a food voucher giveaway. Retailers who "wanted to support the nation during the Corona pandemic" were listed as the supposed senders. To this end, the perpetrators misused well-known brands such as Migros, Coop and Denner.[12] The linked website asked for credit card

---

10 https://www.cybercrimepolice.ch/de/fall/corona-phishing-mail-im-namen-von-netflix/

11 https://www.darkreading.com/cloud/fake-microsoft-teams-emails-phish-for-credentials/d/d-id/1337717; https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/; https://abnormalsecurity.com/blog/abnormal-attack-stores-zoom-phishing-campaign/;

12 https://www.cybercrimepolice.ch/de/fall/whatsapp-fake-kettenbrief-im-umlauf-migros-verlost-kostenlose-lebensmittel-im-wert-von-250-euro-um-die-nation-waehrend-der-corona-pandemie-zu-unterstuetzen/; https://www.cybercrimepolice.ch/de/fall/weiterer-whatsapp-fake-kettenbrief-angeblich-von-denner-im-umlauf/;

information – allegedly for identity verification and so that each person could claim only one voucher. The small print on the site, however, concealed an expensive subscription, for which a monthly fee was charged to the credit card.

Recommendations:

Always check your credit card statements carefully so that in the event of irregularities or unjustified charges, you can contact the issuer and have the cards blocked if necessary. Fraudsters not only use data disclosed to make payments themselves, they may also sell the information to other parties.

3.2 Attacks on websites and web services

In several countries, websites of hospitals and authorities that provided information or services related to the pandemic were at times unavailable.[13] Some of those responsible for the websites attributed these disruptions to DDoS attacks. While this is certainly a plausible explanation and generally true, in some cases the increased public interest in content and services may well have led to server overloads.

Recommendation:

In companies that are heavily dependent on the availability of IT systems, absolute priority must be given to securing the relevant channels. Identify which services are so central that their failure could have far-reaching consequences for your organisation. You should also consider the basic systems without which your critical business applications could not function. Develop a strategy for dealing with DDoS attacks. The relevant internal and external bodies and other individuals who can intervene in the event of an attack must be known. Ideally, as part of its general risk management, a company should address the DDoS issue at management level before an attack occurs and ensure a certain level of DDoS defence readiness at operational level. Any organisation can be hit by a DDoS attack. Talk to your internet provider about your needs and appropriate precautions.

Checklist with measures to counter DDoS attacks

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

[13] https://www.cybercrimepolice.ch/de/fall/wieder-whatsapp-fake-kettenbrief-diesmal-im-namen-von-coop/; https://www.cybercrimepolice.ch/de/fall/neuer-whatsapp-kettenbrief-migros-verlost-gutscheine-in-hoehe-von-chf-180-/ https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response; https://hungarytoday.hu/coronavirus-govt-website-attack-shutdown/; https://www.lesechos.fr/tech-medias/high-tech/laphp-victimes-dune-cyberattaque-1188022; https://news.trust.org/item/20200401133925-o6wx4/

3.3 Attacks on hospitals

Before the pandemic, hospitals were already on the target lists of cybercriminals and were particularly affected by ransomware.[14] Due to the feared overload of health care institutions caused by the pandemic, every incident in this area received a lot of attention. The international outcry was huge when it became known on 16 March that a hospital in the Czech Republic, which is also an important corona testing centre, suffered restrictions in its operations due to a ransomware incident. Various governments vehemently condemned attacks on the health system and called for international cooperation to stop them. Some ransomware players promised to refrain from attacks on hospitals. Nevertheless, several hospitals continued to suffer ransomware attacks even afterwards.[15] Several security service providers offered to help affected health care institutions free of charge.[16]

3.4 Cyberespionage

In normal times, spies gather information according to the priorities set by their governments, which can vary greatly between continents and countries. During the pandemic, governments were interested in the same information about the virus and the resulting disease. Although it is a global problem affecting the whole of humanity, not all parties are cooperating unconditionally. Various countries do not trust each other or the World Health Organization (WHO) and believe that information is being withheld from them. Accordingly, they deploy their spies to obtain such information. While the disclosure of potentially modified case numbers in a country can be used for better risk assessment or political propaganda, information on the suitability of protective measures, treatment methods and remedies is directly helpful for a country's own measures. When it comes to potential vaccines, the matter becomes somewhat more complicated: although many academic institutions and other organisations are conducting research in this area and exchanging information with each other, there are also various private companies active in this field that hope to make big profits by manufacturing their own products or patenting them. The challenge of finding an effective product and then supplying it to one's own population or even to the whole world is a scientific and logistical, but also economic and political matter. See also section 4.6.1 for more on espionage in the time of COVID-19.

Conclusion:

All those involved in research and development in the field of pandemics must be prepared for espionage attacks from various sides. Both public and private organisations are interested in relevant data, research results and commercial secrets.

---

[14] See MELANI semi-annual reports 2016/1, section 5.4.3; 2017/1, chapter 3; 2019/1, chapter 3; 2019/2, section 4.6.1

[15] https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/; https://securityaffairs.co/wordpress/100548/malware/ryuk-ransomware-hospitals-covid19.html;

[16] https://www.coveware.com/blog/free-ransomware-assistance-to-healthcare-coronavirus; https://cybersecurity.att.com/blogs/labs-research/a-surge-in-threat-activity-related-to-covid-19; https://coronahelp.isss.ch/

3.5 Working from home – but secure!

The pandemic gave digitalisation in our everyday work a major boost. Many companies introduced or extended working from home. Meetings were increasingly held via telephone or video conference. In some cases, however, organisations switched their IT infrastructure to working from home at short notice without adequately implementing security measures, thereby exposing their networks.[17] Attackers intensified their scanning activities to identify vulnerable remote access solutions and to find existing weaknesses or insufficiently protected implementations of *remote desktop protocol (RDP)* solutions and *virtual private network (VPN)* servers in order to penetrate corporate networks. Phishing attacks were also targeted at this changed way of working. Many users were using conferencing and collaboration software for the first time and were unfamiliar with messages sent from such platforms. This made it difficult for them to easily detect forgeries.[18] For more on working from home see also section 6.1.

Recommendations:

The use of private IT infrastructure when working from home, especially private computers, increases the attack surface for cyberattacks. This is because private networks and personal devices are often less well protected than corporate infrastructures managed by professionals. Employees working from home are also often on their own when it comes to detecting *social engineering* attacks, as they cannot discuss suspicious activities directly with colleagues. Awareness campaigns as well as setting up and announcing reporting channels to the company's IT security officers can help here.

MELANI checklists on working from home:

For companies: https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff.html

For users: https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff-enduser.html

3.6 Proximity tracing apps

In order to track the spread of the coronavirus and to take appropriate protective measures, many countries introduced so-called proximity or contact tracing apps. This new technology is used to trace potential chains of infection and to inform affected persons of the relevant risks. These technical tools can make an important contribution to limiting the spread of the virus by providing information on when someone has been exposed to a risk of infection. Those affected are informed so that they can have themselves tested and take temporary measures to prevent any unwitting spread of the virus.

17 https://blog.shodan.io/trends-in-internet-exposure/

18 https://www.darkreading.com/cloud/fake-microsoft-teams-emails-phish-for-credentials/d/d-id/1337717; https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/; https://abnormalsecurity.com/blog/abnormal-attack-stores-zoom-phishing-campaign/

Although everyone wants the pandemic to end, not everyone is equally willing to disclose data, or accept restrictions or obligations. The launch of tracing apps led to criticism in various countries regarding their respective design, either because of a lack of data protection or due to potential security vulnerabilities. It is challenging to weigh up the different interests and find a solution that is acceptable to the respective population. This is a new technology which first needs to be tried and tested and which will continue to mature over time.

Note:

Within the framework of the Swiss COVID-19 proximity tracing project, the NCSC set up a security & privacy task force to assess issues related to cybersecurity and privacy. A public security test is being conducted by other experts and interested individuals to thoroughly test the security of the entire system. The public security test has been running since 28 May 2020.

https://www.melani.admin.ch/melani/en/home/public-security-test/infos.html

4 Events/situation

Overview of reports received

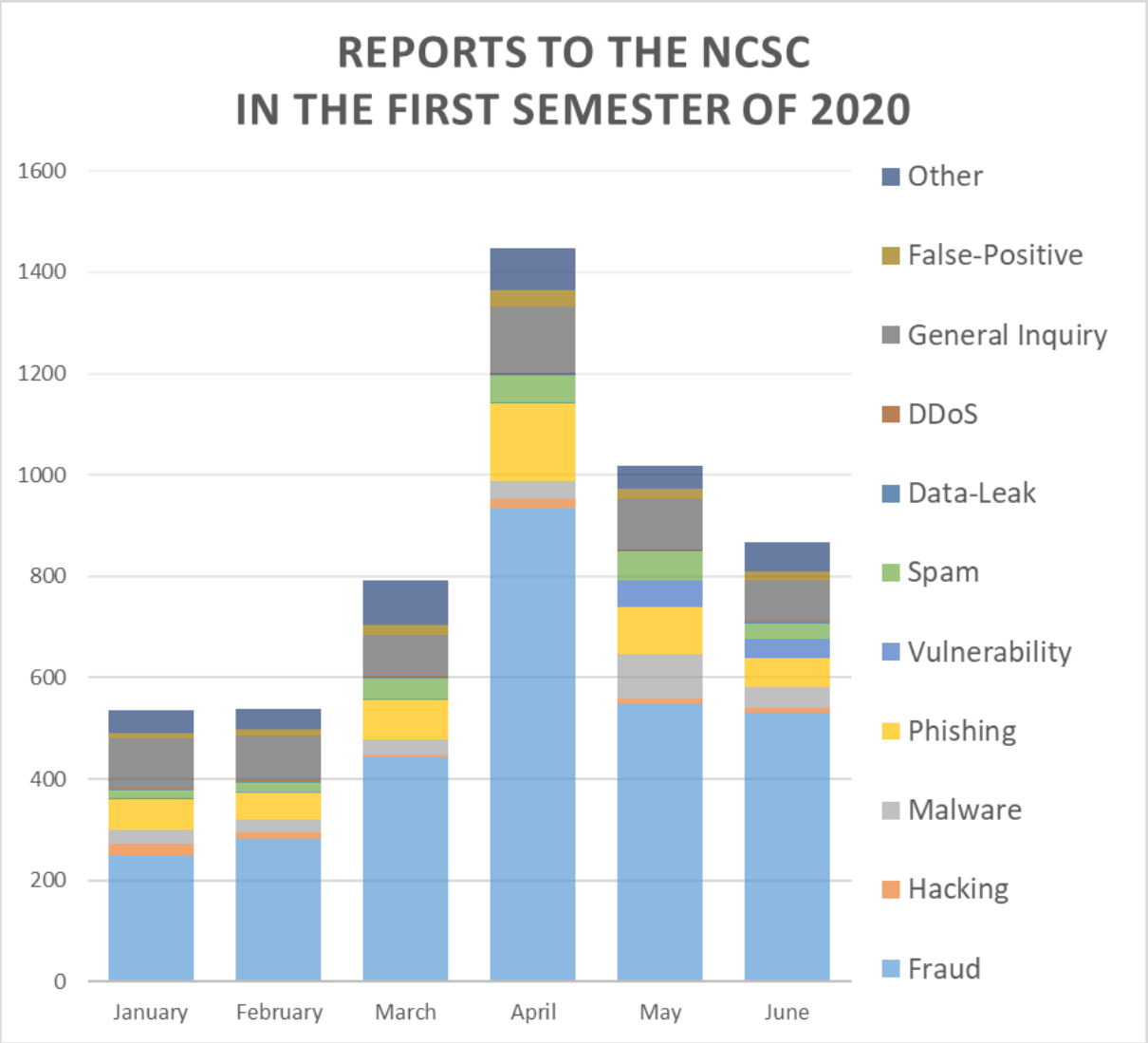

Fig. 2: Reports received by the NCSC in the first half of 2020.

In the first half of 2020, a total of 5,152 reports were registered at the NCSC's national contact point for cybersecurity. Attempts to commit fraud accounted for the largest share with more than half of all reports (2,938), 825 of which alone concerned emails containing advance payment scams.

With 270 reports, so-called parcel subscription scams were frequent. This type of fraud is a modification of the long-known subscription trap, where supposedly free offers are promoted which are then converted into paid subscriptions after a few days. This change is intentionally only mentioned in the small print. In the versions circulated in summer, a small fee was to be charged for the purported delivery of a parcel. However, here too, a subscription was unwittingly taken out. Credit card details had to be provided or a code sent to a short number.

Fraudsters specialised in this new variant during the coronavirus crisis because many people were placing online orders and thus waiting for their parcels to be delivered (see section 3.1).

Large numbers of blackmail emails were also sent out. *Fake sextortion*[19] emails made up the largest share of these, with 578 reports. In this type of fraud, it is claimed that the victim's computer was hacked. Allegedly, the webcam has been accessed and compromising images have been captured. This is usually not the case and therefore an empty threat. The first half of 2020 also saw blackmail attempts against web administrators. These emails claimed that the website had been hacked and underlying databases stolen. The message ended by threatening to publish this data. Again, the threat did not correspond to the facts (see chapter 4.7.5). The fact that fraudsters do not shy away from wilder stories was shown by two bomb threats sent to companies by email, which also turned out to be false.

An old scam celebrated its comeback in the first half of 2020. 63 cases of so-called domain name scams were reported. In this type of fraud, an alleged domain management company contacts a website owner of a .ch domain and claims that another company is interested in the corresponding .com domain. However, the purchase could be prevented by the website owner buying that .com domain. These domains are heavily overpriced and it is not certain that they will actually be registered.

So-called CEO fraud was frequently reported by companies (94 reports). The perpetrators usually gather information in advance about email addresses and employees' roles from a company's website. This information is then used to invent a story tailored to the company. The fraudsters then give instructions to the accounting or finance department to make an urgent payment by order of the pretend CEO.

There were 232 reports of malware incidents. Of note are 42 reports of cases involving encryption software (ransomware). Although this number is small compared to the number of fraud attempts, the potential damage is far greater (see chapter 4.1.1).

4.1 Malware: current overview

The statistics below show which malware affects Swiss internet users the most. These statistics come from various sources and are aggregated and filtered for the entire Swiss IP space known to the NCSC. The detailed technical information is made available to Swiss ISPs so that they can inform affected customers about infections and recommend measures. The different malware families are sometimes difficult to distinguish, as there is no common naming system. It is important to note that these figures represent only the tip of the iceberg, as the database contains only data from a few individual command and control servers.

[19] https://www.melani.admin.ch/melani/en/home/ncsc/form/meldeformularhaeufigefragen/FakeSextortion.html

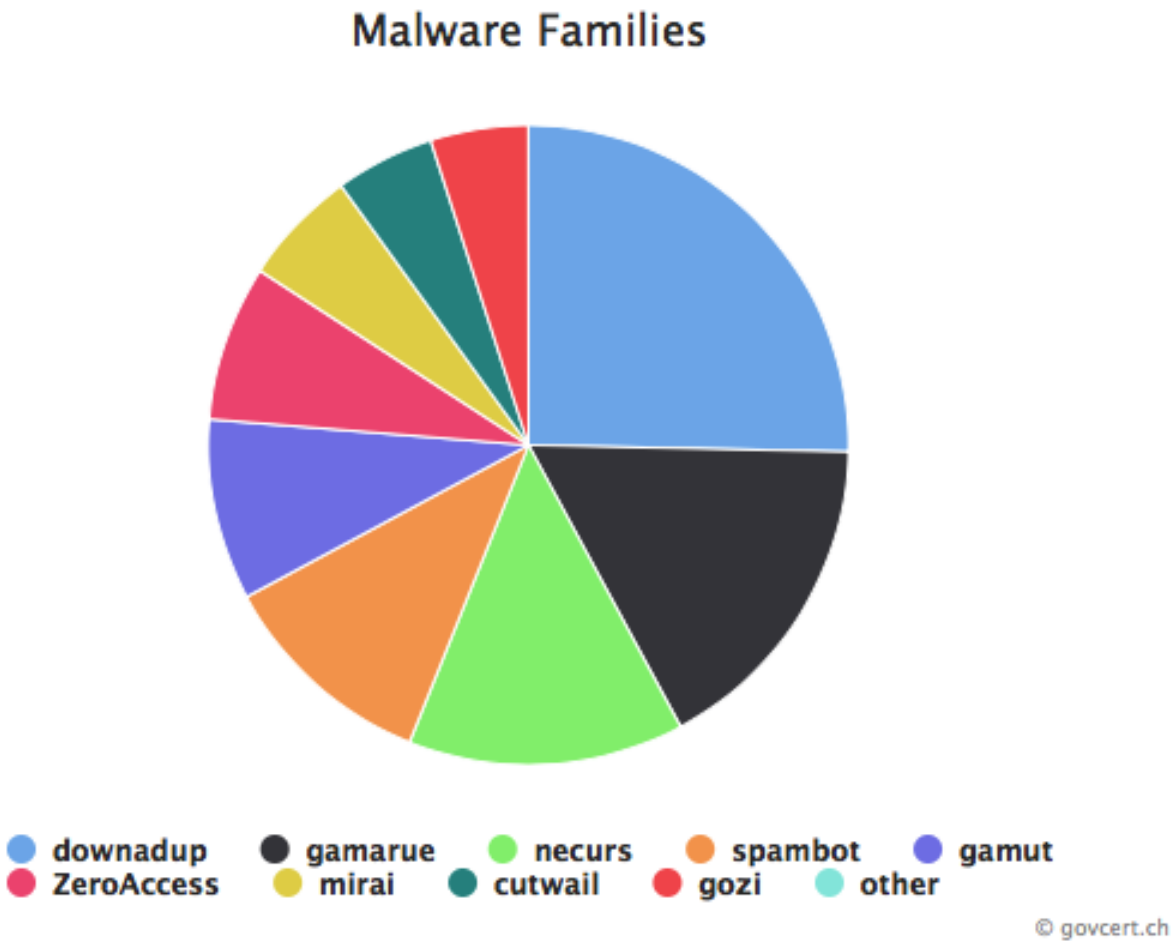

Fig. 3: Breakdown of malware in Switzerland known to the NCSC. The reference date is 30 June 2020. Current data can be found at: https://www.govcert.admin.ch/statistics/malware/

4.1.1 Ransomware Update

MELANI has been following the ransomware phenomenon for many years.[20] According to Trustwave's statistics,[21] this ever-growing threat quadrupled in 2019 and now ranks first in the list of the most frequent cybersecurity incidents. It is not just the number of infections with ransomware that is increasing; so too is the number of attack vectors and the services that provide the tools to carry out an attack and handle the ransom payment (*Ransomware-as-a-Service*, *RaaS*). A report by Coveware,[22] a company dedicated to curbing ransomware attacks, notes that ransom demands in the first quarter of this year increased by 33% compared to the last months of 2019.

---

[20] See MELANI semi-annual reports 2011/2, section 3.5; 2013/2, section 3.1; 2014/2, sections 3.6 and 5.3; 2015/1, section 4.6.1.5; 2015/2, section 4.5.1; 2016/1, sections 4.6.3, 4.6.4 and 5.4.3; 2016/2, sections 4.6.3 and 6.1; 2017/1, chapter 3; 2017/2, section 5.4.2; 2018/2, sections 4.5.4 and 5.3.5; 2019/2, section 4.6.1

[21] https://www.zdnet.com/article/Ransomware-is-now-the-biggest-online-menace-you-need-to-worry-about/

[22] https://www.coveware.com/blog/q1-2020-Ransomware-marketplace-report

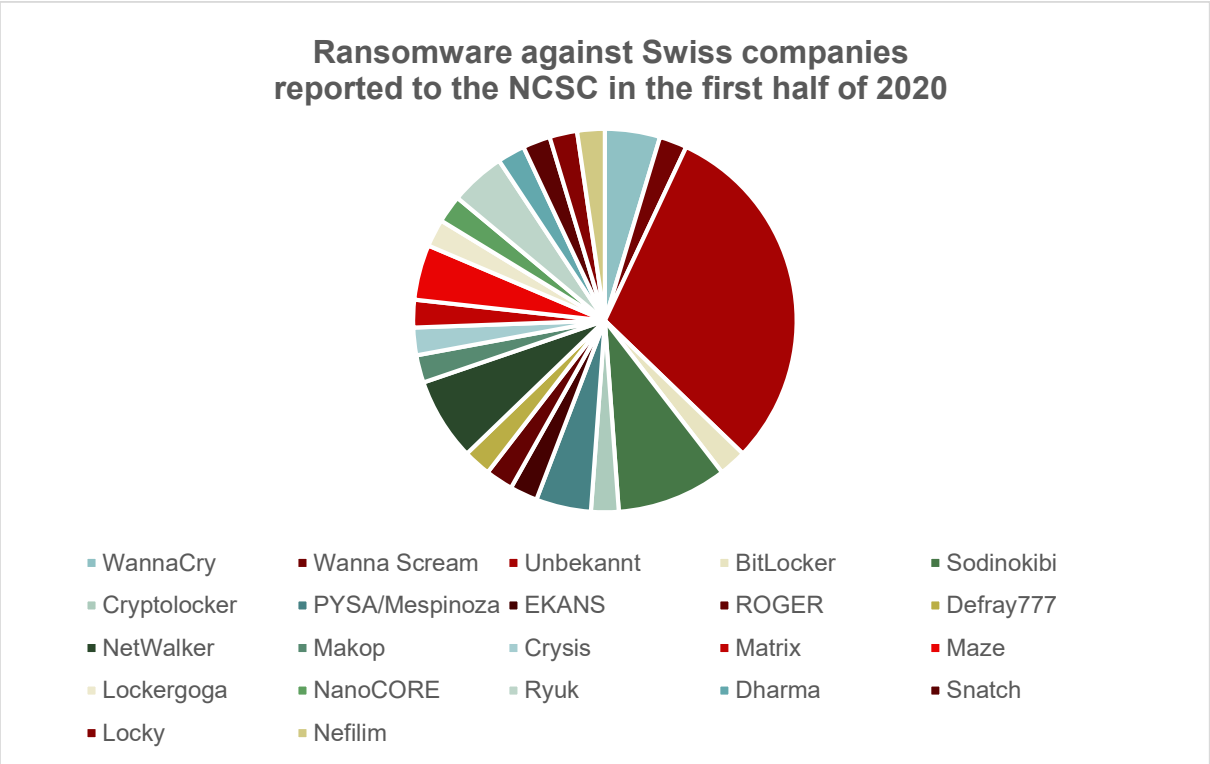

Fig. 4: Ransomware against Swiss companies reported to the NCSC in the first half of 2020.

Swiss companies were again targeted by ransomware attacks in the period under review. In total, 42 cases of ransomware attacks against companies were reported to the NCSC. Unfortunately, not all reports contained information about the malware used in the attacks. As illustrated in Figure 4, various types of ransomware attacks were reported during the reporting period. Although the majority of reports to the NCSC concern SMEs, larger companies were also affected. The attack in January on Bouygues Construction, the French construction group, attracted considerable media attention. In this case, following an attack using the Maze ransomware, the company was forced to temporarily halt production in all its subsidiaries, including those in Switzerland, in order to remedy the situation.[23] At the beginning of May, the rolling stock manufacturer Stadler Rail was attacked with ransomware. The company was blackmailed with the threat that data stolen during the attack would be published if it did not pay a CHF 5.8 million ransom.[24] In order to increase the likelihood that a ransom will actually be paid, criminals adjust the amounts demanded to what they believe the victims have the financial means to pay. Private victims therefore have to pay much smaller amounts – often less than CHF 1,000. The amounts demanded also vary greatly from campaign to campaign. Ryuk, known for its high ransom demands, for example, demanded a ransom of around CHF 300,000 from an SME, while WannaCry demanded only CHF 1,500 from a comparable company, although only part of the data was actually decrypted after payment.

23 https://www.itnews.com.au/news/bouygues-construction-it-taken-out-by-Ransomware-537516

24 https://www.srf.ch/news/cyberAngriff-auf-stadler-rail-solange-es-etwas-zu-holen-gibt-wird-schindluder-getrieben; https://www.swissinfo.ch/eng/cyberattack-_hackers-demand-millions-in-ransom-for-stolen-stadler-rail-documents/45794036

Changes in the methods used

As early as November 2019, a group using Maze ransomware adapted its business model: they began downloading the victim's data before the actual encryption attack, only to extort money by threatening to publish it on a blog created especially for this purpose if the encryption blackmail did not lead to the desired success. This approach has the potential to be very successful because, apart from reputational damage and publication of business secrets, it may also entail legal consequences in connection with the processing of personal data. Moreover, the published data can be used for further attacks. In the first half of 2020, the number of groups applying this strategy rose sharply. The cybersecurity company Coveware lists, in addition to Maze, six other ransomware families that have been identified in connection with data publication attacks: Sodinokibi/REvil, DoppelPaymer (successor to BitPaymer), Mespinoza/PYSA, NetWalker, CLoP and Nefilim[25] (as well as its new version Nemty).[26, 27] All of these malware programs are also active in Switzerland, but not all infections reported to MELANI involve a data breach. But any ransomware attack that is part of one of the aforementioned campaigns should always be considered to likely be linked to data theft. Regarding Switzerland, the operators of Maze claim to have not only encrypted Stadler Rail and stolen its data, but also to have done the same to Zurich based Chubb Insurance, which has not confirmed the infection.[28]

In its last semi-annual report,[29] MELANI predicted that cybercriminals would find other ways to make a profit from stolen data (depending on its value). This could be done, for example, by not limiting themselves to using the data to exert pressure. This has now happened: recently, the cybercriminals responsible for the distribution of the Sodinokibi/REvil ransomware have been auctioning stolen data when the victims refused to pay the ransom for decryption.[30] Other groups might even demand a double ransom, first to recover the encrypted documents and second to ensure that the stolen data is permanently destroyed.[31] The amounts demanded vary according to the victims and the campaign, but in some cases they virtually skyrocket. To give just one example: in July, Sodinokibi/REvil demanded a USD 42 million ransom payment from the celebrity law firm Grubman Shire Meiselas & Sacks to prevent the stolen data from being published and to obtain the decryption code. Because the victim refused to pay, the blackmailers began to auction off a number of documents about celebrities from the entertainment industry, with initial prices ranging from USD 600,000 to USD 1 million.[32] The sale of stolen data through criminal forums is not a new phenomenon, but its publication and

---

25 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigation-into-a-nefilim-attack-shows-signs-of-lateral-movement-possible-data-exfiltration/

26 As a further illustration of the fact that this scheme is becoming increasingly popular with cybercriminals, a platform has been set up by another ransomware on which stolen data is published, but without any data breach being previously published. The name of the platform is Sekhmet, see also: https://www.bleepingcomputer.com/news/security/three-more-Ransomware-families-create-sites-to-leak-stolen-data/

27 There is also the RagnarLocker ransomware (also known as Ragnarok), which has not yet been seen in Switzerland: https://www.securityweek.com/ragnar-locker-Ransomware-uses-virtual-machines-evasion

28 https://www.bankinfosecurity.com/insurer-chubb-investigating-security-incident-a-14023

29 MELANI semi-annual report 2019/2, section 4.6.1

30 https://www.bleepingcomputer.com/news/security/revil-Ransomware-creates-ebay-like-auction-site-for-stolen-data/

31 https://krebsonsecurity.com/2020/06/revil-Ransomware-gang-starts-auctioning-victim-data/

32 https://www.scmagazine.com/home/security-news/cybercrime/lebron-james-among-the-1st-stars-to-have-their-stolen-law-firm-files-put-up-for-auction/

use as a means of exerting pressure is a new variant that is causing more and more victims to give in and pay ransoms. See also section 4.5 on data breaches.

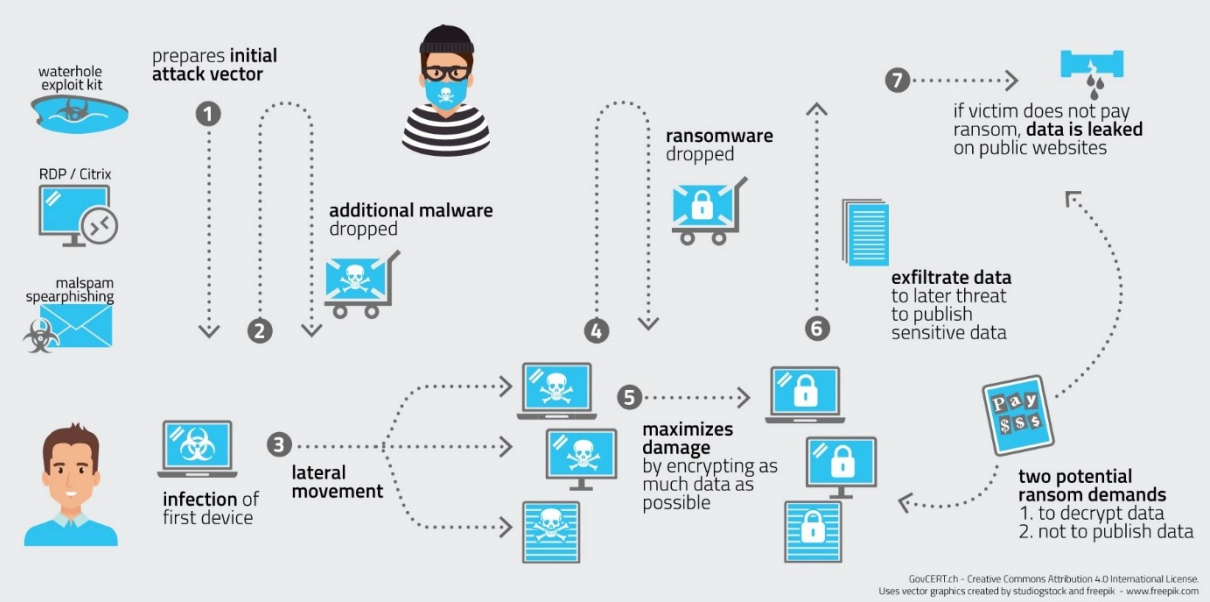

Fig. 5: Current modus operandi of ransomware

The possibility of making sizeable profits and the complexity of multi-level attacks have led to the emergence of more and more collaborative models between different groups and between group members and freelancers. According to FireEye, for example, Maze ransomware is not used by a single group, instead different players are organised as a partnership network (affiliate network). In other words, ransomware developers work together with other parties who, for example, are responsible for spreading malware, establishing network access, scouting out infected networks or other specific aspects. They either operate as employees or receive a commission once the victim has paid the ransom.[33]

Maze was initially spread mainly by means of infected emails; in the first half of 2020, there was an increase in infections with this ransomware as part of structured attacks. These use a pre-existing infection with another malware and allow extensive data theft through a more finely crafted infiltration of the network before encryption. Security service provider FireEye found large differences in how the attacks were carried out, for example in the time between the initial infection and the use of the ransomware or in the intrusion vector used (for instance, open RDP ports or other services that were poorly configured and accessible via the internet, those with weak passwords or via access data that had previously been leaked and was now offered on the darknet). There are also major differences in strategies for greater network persistence or the ability to interact with a victim's systems in the various stages of scouting and lateral movement. This diversity is interpreted as a further indication of the involvement of several players. Maze operators also published on their website data that was stolen from an

33 https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-Ransomware-incidents.html

architecture firm by LockBit operators. A member of the Maze group had indicated that they were prepared to establish a working relationship with a third group in the near future.[34]

Maze is not the only ransomware where the operators rely on the strategy of "joint forces". Since March 2020, the operators of NetWalker have also been building affiliate networks which promote their ransomware at conferences that take place on underground blogs. In order to recruit partners, huge payments of 70% of a ransom are promised; this translates into earnings of anything from USD 487,000 to as much as USD 1 million. In addition, a platform was also created for NetWalker to publish the stolen data. This enables their partners to publish information themselves about the victims in order to optimise the profits from the various attacks.[35]

Technical developments

In the last semi-annual report,[36] it was already mentioned that in many cases a ransomware infection does not require interaction by the users. This, together with other features such as the possibility of using the same malware for a large number of victims, explains the success of this phenomenon. One of the most common attack vectors exploited in ransomware campaigns to infiltrate a corporate network between January and June 2020 was the insufficiently protected RDP ports,[37] whose permissions can be purchased on the black market at very low prices. Servers with security vulnerabilities can also be exploited as gateways to IT infrastructure. In the first half of 2020, the Sodinokibi/REvil malware, which had already been placed in company networks via a security vulnerability in VPN products from Pulse Secure, was the first ransomware to be placed in a company network by exploiting the CVE-2019-19781 Citrix vulnerability (see section 4.4). In addition to Sodinokibi/REvil, two other ransomware variants were observed in the reporting period, Maze and RagnarLocker, to be delivered via this vulnerability.[38] In Switzerland, too, it cannot be ruled out that infections may have occurred via vulnerable Pulse Secure VPN and Citrix servers.

In recent months, the NCSC has noted a sharp increase in attacks on remote desktop protocol (RDP) as an initial attack vector for targeted ransomware attacks. There are a large number of scans against RDP ports where attackers try to exploit weak passwords (through dictionary and brute force attacks). Another tactic is to exploit unpatched and therefore vulnerable servers. The NCSC observed the same procedure with other exposed protocols for remote access, such as Pulse Secure VPN and Citrix NetScaler vulnerabilities, which REvil, for example, searches for and uses as the initial vector. The NCSC assumes that such access data is also traded by criminals in relevant forums and in this way different groups of attackers can gain access to their victims' networks.

---

34 https://www.scmagazine.com/home/security-news/Ransomware/new-Ransomware-trends-spotted-auctioning-stolen-files-cybergangs-joining-forces/

35 https://www.bleepingcomputer.com/news/security/Ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/

36 MELANI semi-annual report 2019/2, section 4.6.1

37 The FBI also takes this view; at the RSA cybersecurity conference in February 2020, it stated that in 70% to 80% of ransomware attacks, access via the RDP port is used as an attack vector: https://www.bleepingcomputer.com/news/security/Ransomwares-big-jump-ransoms-grew-14-times-in-one-year/

38 https://www.zdnet.com/article/hackers-target-unpatched-citrix-servers-to-deploy-Ransomware/

Recommendation:

The following measures should be implemented as soon as possible:

- All remote accesses (RDP, Citrix, VPN) must be protected with two-factor authentication.
- In addition, they can be placed on a non-standard port, making them more difficult to find (caution: this alone is not a sufficient security measure).
- Introduce and implement a password policy that prevents simple passwords.
- If possible: only allow single or specific IP addresses or only IP addresses from Switzerland.
- Monitor log files for failed and successful logins.

During the six months under review, a number of ransomware attacks were observed which used innovative techniques to circumvent security measures and stay longer on the victims' networks. RagnarLocker, for example, installed its own 280MB Windows XP virtual machine (VM) on the victim's system to operate without any interference from the host's monitoring programs. All of the affected computer's drives were also made accessible within the VM and could thus be encrypted by the ransomware.[39] NetWalker, on the other hand, developed a technique already used by other types of malware, known as "reflective DLL injection". It allows a DLL file (dynamic-link library) to be injected whose execution code for the malware is only stored in the RAM. This means that the ransomware's binary code cannot be detected by monitoring instruments that only examine the hard disk.[40] As a further measure, NetWalker also blocks security program processes.

Refining targets

One worrying global trend is ransomware attacks against industrial control systems. A separate chapter of this MELANI semi-annual report is devoted to the phenomenon (see section 4.3.1).

Another recent development concerns the Maze infection announced by Cognizant, one of the world's largest managed service providers (MSP), on 18 April.[41] This incident is part of a long series of attacks against service and IT providers in the second half of 2019,[42] which, according to the CrowdStrike Global Threat Report published in March, is a real trend.[43] Among the ransomware particularly active against service providers, Ryuk stands out; its victims include Data Resolution (December 2018), CloudJumper (May 2019), CorVel (July 2019) and TSM

39 https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
40 https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-Ransomware-injected-via-reflective-loading/
41 https://www.bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-Ransomware-cyber-attack/
42 https://www.zdnet.com/article/at-least-13-managed-service-providers-were-used-to-push-Ransomware-this-year/
43 https://www.channelfutures.com/mssp-insider/msps-under-heavy-Ransomware-attack ; https://www.crowdstrike.com/press-releases/crowdstrike-global-threat-report-reveals-big-game-hunting-tele-communication-targeting-top-adversary-trends/

Consulting (August 2019), and potentially others as well. In March 2020, Ryuk also infected the financial technology service provider Finastra, which provides software and services to over 8,500 clients, including 90 of the world's 1,000 largest banks. In order to prevent the infection from spreading, Finastra quickly deactivated part of its servers, which resulted in a temporary interruption for the service's many clients.[44] The infection of an MSP or cloud service provider has the potential to cause huge damage, as it can act as a gateway into the companies whose IT infrastructure is operated by such providers, for example using remote monitoring and management (RMM) software. For this reason, Cognizant informed its clients immediately and provided them indicators of compromise (IoC) so that they could detect any possible infections in their own networks.

In order to be less conspicuous, some ransomware attackers have specialised in using the programs used by the MSPs as gateways, such as desktop sharing or remote management software. In this way, the Energias de Portugal (EDP) group, one of Europe's largest energy producers, was attacked with RagnarLocker in April. Some ransomware groups, e.g. Sodinokibi/REvil, are taking the opposite approach: according to Coveware, after attacks on various small MSPs, including PerCSoft (August 2019), Complete Technology Solutions (December 2019) and Synoptek (January 2020), the group appears to be more interested in large companies with vulnerable VPNs since early 2020.

Recommendations:

The following measures have proven to be effective for companies to protect themselves against ransomware attacks: observe complete data backup practices. This can increase the certainty that all data can be restored after a ransomware attack. This also includes testing the data recovery process. Document your IT infrastructure, install software updates as soon as they are released and keep your security policies up to date. Create concepts for incident management, communication and business continuity management. Determine the effectiveness of these concepts through regular testing. For effective prevention against cyberattacks, technical security measures should be accompanied by regular employee awareness programmes. A company's management bodies have the responsibility to ensure that these measures are implemented, and this cannot be delegated.

Almost no company is able to fend off every cyberattack with absolute certainty. Therefore, it is important to build response and recovery capabilities to mitigate the effects of an unavoidable incident.

In the second half of 2019, MELANI published updated security measures for protection against the new approach to ransomware attacks:

https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

[44] https://www.bloomberg.com/news/articles/2020-04-08/how-finastra-survived-a-Ransomware-attack-without-paying-ransom

4.1.2 Gozi active again

The Gozi malware,[45] developed for ebanking attacks, has been present in Switzerland for over ten years, but has only been sporadically active in recent time.

In March of this year, it was discovered that Gozi had been spread by emails that made reference to the victims' genuine previous email correspondence (so called *thread hijacking*). This method is already used by other banking Trojans, including Emotet. The email contained a password that allowed the user to open a .zip file, which was not attached but stored on Google Drive. The archive supposedly contained a presentation. In fact, it was a JavaScript file that downloaded and executed Gozi. In April, Gozi was then sent in an attached infected .xls file. The emails, written in Italian, all referred to an invoice.

The Gozi malware and its variants, which were offered on illegal online trading platforms and therefore used by various cybercriminals, have been distributed in various ways for years. These include compromised websites of newspapers and manipulated software publicised in advertisements explicitly created for this purpose. In addition to ebanking systems, Gozi also targets payment software and cryptocurrency wallets.[46]

4.1.3 Previously hidden Emotet module

In early 2020, security researchers from Binary Defense discovered a Wi-Fi module in the Emotet malware.[47] This module, on which little research has been conducted to date, is used to query the wireless networks (Wi-Fi or Wireless Local Area Network, WLAN) to which the victim is connected. In addition, Emotet tries to access all other wireless networks that are within range using a predefined list of common passwords. Emotet can access a Wi-Fi if it is completely unprotected or secured with a password on the predefined list. Starting from the first victim, the malware will then infect and spread to the computers on the network it has infiltrated.

According to initial findings, the module appears to have been in existence since 2018. However, since malware analyses are mostly carried out on virtual machines without Wi-Fi, it was not noticed for a long time. This discovery illustrates that attackers are always looking for new ways to spread malware and are not lacking in creativity.

Emotet is often a gateway for further malware such as Ransomware.[48]

---

45 GovCERT blogs on Gozi: https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature; https://www.govcert.ch/blog/when-gozi-lost-its-head/

46 MELANI semi-annual report 2018/1, section 4.7.3

47 https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

48 See also MELANI semi-annual reports 2019/1, section 3.4.1 and 2019/2, section 4.6.1

Conclusion:

The spread of malware is a constant cat and mouse game between attackers and defenders. When the methods used prove less successful because a propagation vector has been better protected, malware developers invent new infection variants or revive old ones that security experts pay less attention to. As the first network component for connecting to the internet, Wi-Fi as a vector is locally limited and does not scale in the same way as attacks via email and the web. Nevertheless, Wi-Fi as an attack vector should not be underestimated.

You can find recommendations on Wi-Fi / WLAN security on our website:

https://www.melani.admin.ch/melani/de/home/schuetzen/sekundaere-grundschutz.html

4.2 Attacks on websites and web services

4.2.1 HPC supercomputers

In mid-May 2020, the security team at the EGI (European Grid Infrastructure, an association of universities with high-performance computing centres) reported an attack affecting several EGI members.[49] High-performance computing centres (HPCs) are an important tool for solving complex calculations such as aerodynamic modelling and currently COVID-19 propagation models. The computing power can also be used to mine cryptocurrencies or to decipher encrypted data. The centres also enjoy significant bandwidths. HPCs are therefore interesting targets for attacks. Thanks to the EGI security team's report, many data centres worldwide, including several in Switzerland,[50] have been able to detect unauthorised access to their systems and ward off attackers. The attackers' motivation and goal could not yet be determined.

4.2.2 DDoS update

The aim of *distributed denial-of-service (DDoS)* attacks is to reduce the availability of an IT system in order to extort money from the organisation concerned or to damage it by making its websites and services inaccessible. In recent years, there has been a general decrease in the number of successful DDoS attacks. This drop is thanks to the players specializing in mitigation and containment of DDoS attacks. At Link11, a DDoS containment service provider, the largest attack fended off in the first quarter of 2020 was 406Gbps, while Cloudflare experienced a DDoS attack with a peak of over 550Gbps.[51]

These services noted an increase in the complexity and volume of such attacks compared to the previous year. In the first three months of this year, Link11 recorded as many as 51 attacks

49 https://csirt.egi.eu/academic-data-centers-abused-for-crypto-currency-mining/

50 https://www.rts.ch/info/suisse/11329094-soupcons-de-hacking-du-plus-gros-superordinateur-de-suisse-.html; https://www.tagesanzeiger.ch/eth-supercomputer-gehackt-370887112689

51 https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

with a volume of more than 50Gbps, while the average bandwidth reached 5.0Gbps (an increase of 0.7Gbps compared to the same quarter last year).[52] Cloudflare reported an increase in small-scale attacks of short duration, with 92% of these not even reaching 10Gbps. In addition, 79% of the attacks lasted between 30 and 60 minutes, an increase of 19% compared to the second half of 2019 for short attacks.[53]

The number of DDoS attacks recorded by Cloudflare seems to have increased, especially since March, in parallel with the COVID-19 pandemic. This finding was confirmed by other IT security companies, including Netscout, which noted that it had never recorded such a high number of DDoS attacks over a 31-day period as between 11 March and 11 April 2020 (over 864,000).[54] Cybercriminals had expected a possible increase in the impact of such attacks due to the shift of daily activities such as work and school to online solutions (working from home and home schooling) and the resulting dependence on connectivity and services. The policy of social distancing in various countries has increased the dependence of their economies on the internet and the importance of some online information channels. This is the case, for example, with the websites of government public health organizations. They were consulted on a daily basis by a large number of citizens seeking information on the coronavirus. In this context, the website of the US Department of Health and Human Services was the target of a DDoS attack in mid-March, but this did not significantly slow down the government agency's systems.[55] The existence of DDoS-as-a-service providers allows such attacks to be carried out quickly and cost-effectively. However, the NCSC did not record a significant increase in DDoS attacks in Switzerland during the extraordinary situation. In general, some unspecific waves of attacks were observed in Switzerland in the first half of 2020, most of them without a ransom demand. This indicates that the actors were simply testing the affected infrastructure or looking for vulnerabilities.

However, amidst all these weak and short attacks, two attacks took place, which are among the largest attacks of this kind ever recorded. The first attack, in mid-February, was halted by the protection provided by Amazon (AWS Shield). It lasted for three days and reached a traffic peak of 2.3Tbps. The attack was directed against a specific client who was not named by Amazon.[56] The second attack, which was directed against a European bank and took place at the end of June, was not primarily characterised by a high bandwidth intensity (almost 418Gbps), but rather by the most intensive packet flow per second (pps) ever recorded: 809 million pps.[57] Before this attack, which was contained by the infrastructure service provider Akamai, the strongest DDoS attack ever recorded had reached around 580 million pps.[58] The two attacks in the first half of 2020 can claim to be the largest DDoS incidents ever recorded. The difficulty in determining which of the two attacks was larger is that the attackers used different methods to hit their target: bits per second (bps) in the first case and packets per second (pps) in the second case. High bps attacks aim to paralyse the internet pipeline, while

52 https://www.helpnetsecurity.com/2020/04/20/ddos-attacks-increasing/
53 https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q1-2020/
54 https://www.netscout.com/blog/asert/measuring-cruellest-month
55 https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
56 https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
57 https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html
58 https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

high bps attacks aim to hit network devices or apps in data centres or in a cloud.[59] The February attack reached a packet volume of 293 million pps, which is much lower than in June. A third attack with a peak of 754 million pps was registered between 18 and 21 June. The four-day attack was executed from over 316,000 IP addresses against one Cloudflare address.[60]

Recommendation:

In companies that are heavily dependent on the availability of IT systems, absolute priority must be given to securing the relevant channels. Identify which services are so central that their failure could lead to far-reaching consequences for your organisation. You should also consider the basic systems without which your critical business applications could not function. Develop a strategy for dealing with DDoS attacks. The relevant internal and external bodies and other individuals who can intervene in the event of an attack must be known. Ideally, as part of its general risk management, a company should address the DDoS issue at management level before an attack occurs and ensure a certain level of DDoS defence readiness at operational level. Any organisation can be hit by a DDoS attack. Talk to your internet provider about your needs and appropriate precautionary measures.

Checklist with measures to counter DDoS attacks:

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

4.3 Industrial control systems

Increasing digitalisation and networking in the area of basic services means more efficient management of services such as electricity and water supply, but also poses risks in terms of vulnerability and thus reliability. While such systems were traditionally limited to local or regional areas and were often operated via their own physical networks, they can now increasingly be controlled remotely via the internet. Ideally, however, the corresponding control elements are not directly accessible from the internet, but rather are protected against unauthorised access by various protective measures.

4.3.1 Industrial control systems (ICSs) targeted by ransomware

As shown in chapter 0, the number of ransomware attacks continued to increase worldwide. Up to now, ransomware attacks have targeted the IT infrastructure of the victims and have usually only affected control systems collaterally. In the first half of 2020, a ransomware was discovered which had been specially designed to attack process control systems. EKANS, as it is known, has been active since December 2019, but the ransomware only became known at the beginning of 2020.[61] It has specific capabilities to attack processes related to industrial control systems. EKANS, which is mainly used for targeted attacks, checks after penetrating

59 https://www.bleepingcomputer.com/news/security/european-bank-suffers-biggest-pps-ddos-attack-new-botnet-suspected/

60 https://blog.cloudflare.com/mitigating-a-754-million-pps-ddos-attack-automatically/

61 https://www.bloomberg.com/news/articles/2020-01-28/-snake-Ransomware-linked-to-iran-targets-industrial-controls; https://www.otorio.com/blog/snake-industrial-focused-Ransomware-with-ties-to-iran/

the network whether the internal domains and IP addresses match the target. Before the ransomware encrypts files, it steals data and then forces a whole series of processes to stop, although this is done without manipulating them or sending commands. These processes not only affect industrial control systems (ICS), but also security or management software, databases and data backup solutions. Security services provider Dragos published a detailed report on this threat, named among the attacked ICS products the Proficy Historian software from General Electric and the licensing servers from GE Fanuc ma. Other targets included the HMIWeb application from Honeywell and the FLEXNet, Sentinel HASP and ThingWorx Industrial Connectivity Suite licence managers.[62] After encrypting the files, EKANS displays a ransom demand.

EKANS was initially seen as a forerunner for this type of attack. However, during the analysis of the malware, Dragos found significant analogies to a variant of the MegaCortex ransomware, which had been targeting industrial control systems since last summer. By discovering these similarities, the significance of EKANS was somewhat relativised. This is due in part to the fact that the list of processes targeted by MegaCortex (over 1,000) is longer than that of EKANS (64). While the same industrial control processes are affected by both ransomware, MegaCortex also blocks countless security processes. The only significant development made by EKANS would be the concealment of the program code by obfuscation to make detection more difficult.

Both of these ransomware pose a threat to the industrial sector and to many critical infrastructures. Ransomware, which principally targets IT infrastructure, can usually only affect Windows-based control systems that are also accessible via the network, and must therefore have a certain propagation capacity. EKANS and MegaCortex, on the other hand, were developed to specifically target industrial automation systems. To date, however, none of the publicly known victims of EKANS has confirmed that ICSs have been compromised due to an attack. For instance, Honda[63], the major car manufacturer, admitted to having been the victim of an infection that affected its IT network but had no impact on production or sales and had no consequences for its customers. Energy multinational Enel[64] discovered an intrusion into its IT system on 7 June, but the antivirus programme was able to stop the ransomware before it could have any effect. As a precaution, the company's network was briefly isolated. Again, the control systems were not damaged and no data leaks were detected. Among the publicly known victims of EKANS is Fresenius Medical Care, a large private European hospital provider. After the ransomware attack, highly sensitive information such as the results of medical examinations, notes on treatments and allergies, but also names, professions, telephone numbers and addresses of patients were published on the internet.[65] According to the internet security company Kaspersky, vehicle and car manufacturers are also among the victims of EKANS; moreover, they suspect that in at least one case it was not just the office network that was infected, as the malware was detected and blocked on the video surveillance system of an organisation in China.[66]

---

62 https://www.dragos.com/blog/industry-news/ekans-Ransomware-and-ics-operations/

63 https://www.bleepingcomputer.com/news/security/honda-investigates-possible-Ransomware-attack-networks-impacted/

64 https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-Ransomware-attack/

65 https://www.bleepingcomputer.com/news/security/snake-Ransomware-leaks-patient-data-from-fresenius-medical-care/

66 https://ics-cert.kaspersky.com/media/Kaspersky_ics_cert_alert_Snake_EN.pdf

Apart from the ransomware which mainly targets industrial control systems, a significant number of attacks against critical infrastructure in the energy sector were recorded in the first half of 2020. Such attacks also pose risks for companies' productivity. On 18 February, for example, the US cybersecurity agency CISA registered an attack on the operational technology (OT) network of a natural gas compression plant. The threat actor, who was not publicly named, entered the company's IT network via a link in a targeted email. He subsequently succeeded in using lateral movement within the network and was able to penetrate the OT network. The threat actor then initiated the encryption on both networks. The infected OT processes include human machine interfaces (HMIs), data chronology and so-called polling servers. The victim was forced to interrupt operations to delete all traces of the malware, resulting in a corresponding loss of productivity and profit.[67]

Below is a summary of successful and publicly known ransomware attacks against organisations in the energy sector during the six months under review.

Date	Ransomware	Victim	Consequences
1 April	Maze	Berkine, a group comprising the Algerian state-owned oil company Sonatrach and its American trading partner Anadarko	More than 500MB of documents were published, containing strictly confidential information (including salaries and coordinates of employees, information on production volume, budget and objectives).[68]
14 April	RagnarLocker	Energias de Portugal (EDP), Portuguese energy multinational (electricity and gas)	After encrypting the company data, the ransomware operators demanded a ransom of USD 11 million. In addition, the cybercriminals are alleged to have stolen 10TB of sensitive documents, threatened to publish them, and actually published part of the data as a warning. It is said that the attack did not affect the power supply.[69]
30 April	NetWalker	Northwest Territories Power Corporation NTPC, Canadian electricity company	According to the electricity company, there was no interruption in the operation of the electricity systems. The website was hit and defaced and a message from the cybercriminals could be seen.[70]

67 https://us-cert.cisa.gov/ncas/alerts/aa20-049a

68 https://www.inter-lignes.com/des-documents-hyper-confidentiels-de-sonatrach-derobes-par-des-hackers/

69 https://www.bleepingcomputer.com/news/security/ragnarlocker-Ransomware-hits-edp-energy-giant-asks-for-10m/

70 https://www.cbc.ca/news/canada/north/ntpc-apparent-Ransomware-attack-1.5551603

4 May	Unknown, Taiwanese authorities suspect Chinese involvement.[71]	Taiwanese state oil refinery CPC Corp	CPC's website was hit and several petrol stations were temporarily closed as no more payments could be processed with the CPC Corp card.[72] The attack had no impact on CPC's energy production.
14 May	REvil/Sodinokibi	Elexon, a major intermediary in the UK electricity grid	The incident affected the internal IT network and shut down the email server. No damage was caused to the power transmission systems.[73] At the beginning of June, those responsible published a folder containing 1,280 files stolen from Elexon on the darknet.[74]

Security measures:

Operators of industrial control systems (ICS) should, wherever possible, keep operational IT systems separate from the OT network. A multi-level structure should be used for the OT network, in which the less critical processes are separated from the truly critical ones. In order to limit both virtual and physical access to the critical systems, it should also be ensured that only authorised personnel have access to the ICSs.

DOCU

The NCSC published on its website a checklist of "Measures for the protection of industrial control systems (ICSs)":

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

The US Cybersecurity and Infrastructure Security Agency CISA recently issued recommendations:

https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

71 https://www.cyberscoop.com/cpc-Ransomware-winnti-taiwan-china/

72 https://www.taiwannews.com.tw/en/news/3927869

73 https://www.elexonportal.co.uk/news/view/27108?cachebust=ebf1vtjsp0

74 https://www.theregister.com/2020/06/01/elexon_Ransomware_was_revil_sodinokibi/

4.3.2 Sabotage attacks linked to the conflicts in the Middle East

On 3 January 2020, an American air strike[75] at Baghdad airport killed Iranian general Qassem Soleimani, commander in the Islamic Revolutionary Guard Corps (IRGC) of the Quds Force, and Jamal Jafaar Ibrahimi, the long-time leader of Kata'ib Hizballah and deputy chief of the Popular Mobilisation Forces (PMF). This kinetic attack must be seen in the broader context of the Middle East conflict that is not only limited to physical confrontations. For years, the conflicting parties have also been regularly fighting each other in cyberspace and have no qualms about the physical effects their cyberattacks may have. Sometimes these effects are even intentional.[76]

At the end of 2019, the national oil company of Bahrain, Bapco, faced the effects of cyberattacks that were intended to cause destruction.[77] Malware was used to render several devices in the system landscape unusable. Although never confirmed by Bapco, a connection is suspected with a warning[78] from the Saudi cybersecurity authority about the *wiper* malware Dustman.[79] The original entry point appears to have been a remote access system. In a report on the Fox Kitten[80] attack campaign, the cyberintelligence company Clearsky described successful access to company networks via poorly protected *RDP* accesses or non-updated and thus vulnerable VPN servers from Pulse Secure, Fortinet or Palo Alto. The attackers are mainly active in the Middle East, and have an arsenal that also includes the PowDesk[81] script, which compromises systems using the LANDesk Management Agent software. Attacks via the HOLMIUM group's cloud were discovered by Microsoft, for example.[82] Other specific tools such as POWERTON[83] were also used. According to the security service provider Yoroi, APT34/Oilrig attacked an email server of the Lebanese government with the help of the Karkoff implant.[84] Once such attack attempts are successful and access to the network is established, control systems are also targeted. In April, for example, the Israeli government warned[85] against attacks against SCADA systems in the water supply system. Later, further attempts to attack water management systems in Israeli agricultural facilities became public[86] and it is suspected that cyberattacks against the Iranian port on the Strait of Hormuz[87] were in retaliation for such actions.

---

75 https://www.defense.gov/Newsroom/Releases/Release/Article/2049534/statement-by-the-department-of-defense/

76 See MELANI semi-annual report 2019/2, section 5.2

77 https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/

78 https://www.scribd.com/document/442225568/Saudi-Arabia-CNA-report

79 https://malpedia.caad.fkie.fraunhofer.de/details/win.dustman

80 https://www.clearskysec.com/fox-kitten/

81 https://www.clearskysec.com/powdesk/

82 https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/

83 https://attack.mitre.org/software/S0371/

84 https://securityaffairs.co/wordpress/98802/apt/karkoff-malware-lebanon.html

85 https://www.gov.il/he/departments/publications/reports/scadaalert

86 https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

87 https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

If the attempt to attack the target directly is unsuccessful, the attackers move along the supply chain to find a more distant entry point. In February, the FBI warned[88] against attacks on software suppliers involving the remote access Trojan Kwampirs.[89] The attacks focused in particular on companies that work with industrial control systems in the field of energy production, transmission and distribution.

Note:

Organisations that do business with companies active in such conflict areas should be aware that there is a possibility of being directly or collaterally affected by such attacks.

4.3.3 Continued reconnaissance attacks on electricity suppliers

The transmission system operators (TSOs) for power utilities in Europe collaborate in the ENTSO-E association, to coordinate electricity provision across Europe. In spring 2020, it emerged that the association had had to deal with a cyberintrusion into its office network last year. In a short press release issued in March 2020, ENTSO-E emphasised that "the ENTSO-E office network is not connected to any operational TSO system".[90] Many of the 42 members from 35 European countries (see fig. 6), including Switzerland's Swissgrid, have confirmed the association's assessment on the impact of the attack.[91] It was therefore not possible for this attack to cause direct disruption of the power supply in Europe.

This incident highlights the existence of players who are interested in knowing how electricity provision works in different parts of the world. More references to this can be found in the previous semi-annual report.[92] This current example shows that Europe is not immune. The specialised journalists at Cyberscoop[93] have linked an analysis by Recorded Future[94] to the incident at ENTSO-E. The malware employed, Pupy RAT, has previously been used by groups that are not averse to launching destructive wiper attacks. To date, destructive attacks of this kind have been observed only on the periphery of existing conflicts, such as those described in section 4.3.2 on tensions in the Middle East. In view of possible geopolitical developments, every country and every power supply company needs to have adequate risk mitigation measures in place against attacks of this nature. In addition to the reconnaissance attack observed in Europe, there were also intrusion attempts at American energy utilities,[95] in which Flowcloud[96] malware was used.

88 https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/
89 https://malpedia.caad.fkie.fraunhofer.de/details/win.kwampirs
90 https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/
91 https://www.swissgrid.ch/en/home/about-us/newsroom/newsfeed/20200309-01.html
92 MELANI semi-annual report 2019/2, section 4.2.1
93 https://www.cyberscoop.com/europe-grid-pupy-rat/
94 https://www.recordedfuture.com/pupyrat-malware-analysis/
95 https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new
96 https://www.proofpoint.com/us/blog/threat-insight/flowcloud-version-413-malware-analysis

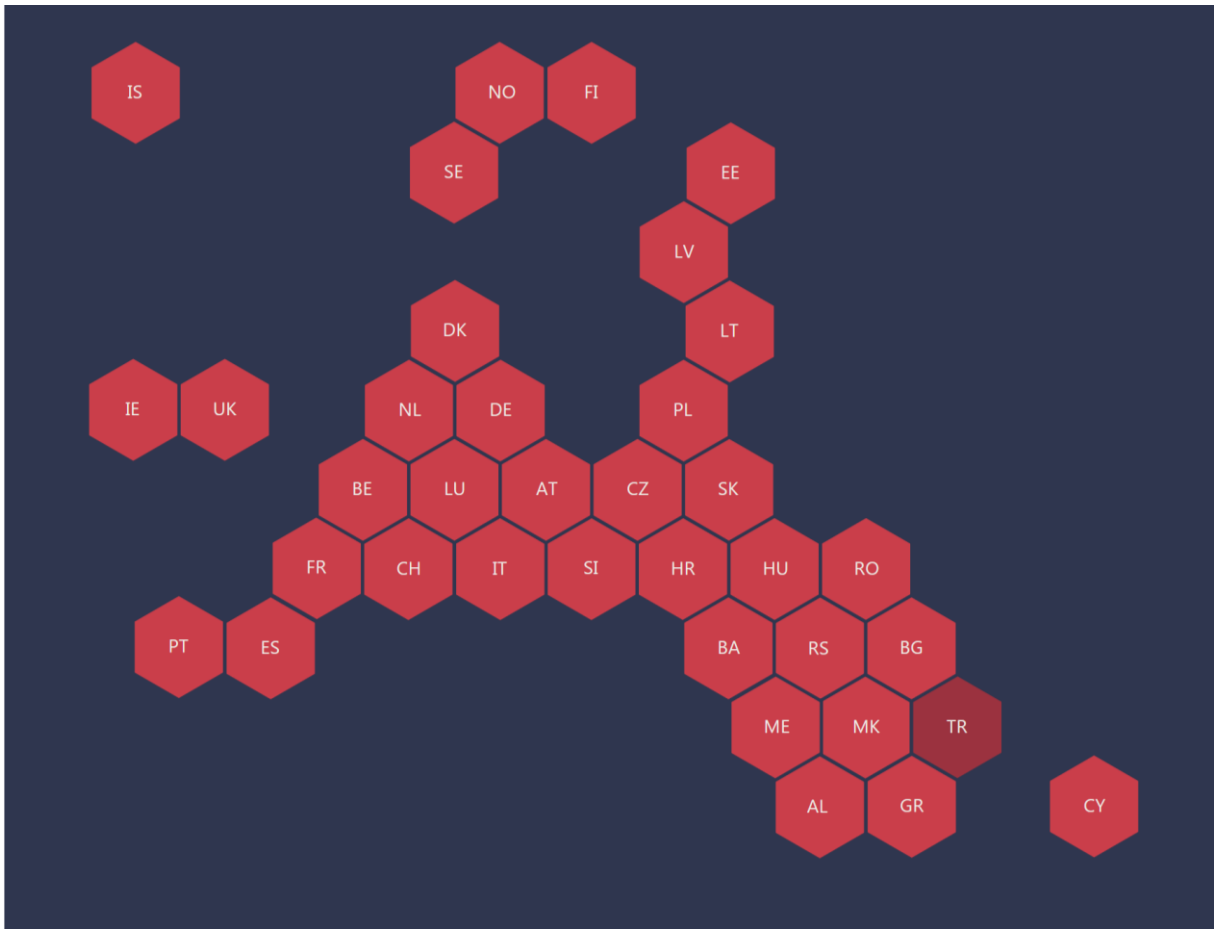

Fig. 6: ENTSO-E members[97]

A recent ransomware incident, which also had no impact on operational control systems, targeted the British power grid intermediary Elexon. After Elexon refused to give in to ransom demands from the Sodinokibi/REvil blackmail group, the criminals published the data they had abstracted.[98] For the moment, Elexon appears to have got off lightly. However, it should be borne in mind that the published information could be used for future attacks by players who are not interested only in financial gain. Section 4.3.1 describes similar attacks, such as the RagnarLocker incidents in Portugal or the ransomware used against CPC Corp's refinery in Taiwan. Such ransomware attacks are currently the more serious threat, especially those that also attempt to disrupt operational control systems for physical processes.

Note:

The NCSC is in regular contact with Swiss energy utility representatives within the closed constituency of MELANI. The participants collaborate to ensure that such attacks in Switzerland can be prevented or detected early, and their impact can be minimised as far as possible.

97 https://www.entsoe.eu/about/inside-entsoe/members/

98 https://www.theregister.com/2020/06/01/elexon_ransomware_was_revil_sodinokibi/

4.4 Vulnerabilities

In the first half of 2020, a number of vulnerabilities were published that proved critical in the context of lockdown. Specifically, many companies made working from home more widely available during lockdown. The requisite infrastructure is complex and tricky to set up securely even in normal circumstances, i.e. when there is no extreme time pressure.

Many Swiss companies, including some critical infrastructures, were affected by the CVE-2019-19781 vulnerability, published on 17 December 2019 and involving Citrix's *application delivery controller* (ADC) and *gateway* products. This vulnerability allows attackers to run code on devices for which they are not authorised. As these Citrix products are frequently installed at a network's outer perimeter, attackers can use this vulnerability to gain unauthorised access. Despite Citrix's security announcement and urgent recommendation to its customers, not all of them mitigated the vulnerability. On 10 January 2020, several *exploits* for this vulnerability were published, and in a matter of hours there was a surge in searches for Citrix products that were exposed to the internet and still vulnerable. Over the next few days, attackers used the exploits to compromise corporate networks and extort money by means of ransomware attacks. After the exploits were published, the NCSC issued urgent information to more than 50 operators of critical infrastructure on the potential danger and the requisite protective measures.

Areas targeted by hackers include routers or VPN servers whose software versions contain vulnerabilities and have not been protected by additional measures. Their strategy is to find a gateway into the corporate network and, once inside, deploy ransomware. In recent years, increasing numbers of organisations have suffered major losses after not mitigating exposure to the internet of an application or product containing a vulnerability that had been revealed a short time earlier.[99]

Recommendations:

Companies should keep an up-to-date inventory of their IT infrastructure. Top priority should be given to products that are exposed to the internet. In a second step, vulnerabilities and updates should be monitored by means of real-time risk management in which relevant announcements from manufacturers are obtained, analysed and ranked according to priority. Finally, areas and procedures should be planned for urgent updates of key components (especially perimeter components).

Published vulnerabilities are listed in the *Common Vulnerabilities and Exposures* (CVE) database. Available at: https://nvd.nist.gov.

[99] See MELANI semi-annual reports 2019/2, section 4.6.1, and 2020/1, section 4.1.1

4.5 Data breaches

Data breaches are not a new phenomenon, but the frequency of such incidents increased over the period under review, and it can be expected that this trend will continue. Leaking or selling corporate data is very popular with some cybercriminals. According to one study, over the next two years, one in four companies will fall victim to a data breach.[100]

In May this year, EasyJet was forced to announce that it had been the victim of a highly sophisticated cyberattack, involving the theft of data of around 9 million customers, including email addresses, travel dates and credit card details. According to EasyJet, it would take time to gauge the scale of the attack and identify who had been affected. The airline gave no details about the type of attack or the motives behind it, although it did say that its investigations suggested that the hackers had been after the company's intellectual property, rather than information that could be used for identity theft. Nonetheless, the airline warned its customers of the possibility of phishing attacks and advised increased vigilance. Under the European Union's General Data Protection Regulation (GDPR), EasyJet could face a fine of up to 4% of its global annual turnover if it is found that customer data was improperly handled. If negligence can be proved, damages claims from customers are also possible, which would substantially increase the airline's costs.

In February 2020, the Marriott International hotel chain also announced a data breach involving the personal data of up to 5.2 million guests. Marriott suspects that the attack began in mid-January 2020. Yet the incident was not discovered until the end of February, when an unexpected amount of guest data was retrieved using the login data of two franchisee staff members. In response, Marriott launched an investigation, strengthened its monitoring and organised information and support resources for customers, including a portal for potential victims which provided information about data protection infringements upon request. This is already the second incident reported by Marriott in the last two years. In November 2018, the company announced that the reservation database of Starwood Hotels had been hacked.

According to a new survey, nearly 80% of companies reported at least one breach of their cloud data during the past 18 months and around 43% reported ten or more breaches.[101] The 300 chief information security officers (CISOs) who took part in the survey stated that incorrect security configurations (67%), a lack of transparency over access settings and activities (64%) and errors in granting identity and access management permissions (61%) were their greatest concerns in connection with cloud-hosted data.[102] Excessively broad permissions also pose a problem, and can remain undetected for a long time, because they are often granted as the default when a new resource or service is added to the cloud. They are a prime target for attackers, as they can be used for malicious activities such as stealing sensitive data or introducing malware. As a result, the top priorities with regard to cloud access are: maintaining the confidentiality of sensitive data; compliance with statutory requirements; and ensuring that access levels are correct.

---

100 https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan

101 https://www.helpnetsecurity.com/2020/06/03/cloud-data-breach/

102 https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan; https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Data breaches are not only financially motivated; sometimes, the reason can be ideological. For example, on 19 June 2020, a group called Distributed Denial of Secrets (DDoSecrets) circulated a 269GB data dump revealing more than 24 years of police files from over 200 US police departments.[103] Their aim was free access to data that was allegedly in the public interest, as well as collective transparency. The probable motive for the breach was retaliation, in view of the current anti-racism protests against police in the US. There has never before been a data breach of this magnitude targeting law enforcement authorities. Among the countless documents such as FBI reports and bulletins containing personal data, there are also bank details, photos of suspects, phone numbers and email addresses of victims and perpetrators. Obviously, hacktivists and cybercriminals will be able to exploit this data in the future. In this particular incident, the authorities are above all concerned about the danger to the victims. The authenticity of the data has since been confirmed. The source of the breach was apparently a vulnerability at Netsential, a software development company based in Houston, Texas. It is not yet clear how this hack will impact Netsential's other clients.

As described in section 4.1.1, ransomware incidents now also tend to involve a data breach. A major driver of this development is the Maze group, which has created a special Maze News website to publish data stolen from victims who did not give in to ransom demands. This blackmail technique was rapidly adopted by other groups, including Nefilim, Sekhmet and Sodinokibi/REvil. With the average ransom payment exceeding USD 100,000 and some victims apparently paying millions, certain groups have already enjoyed huge success just from blackmailing companies. Recently, however, there have been reports of a collaboration between Maze and LockBit, and the operators of Sodinokibi/REvil, in which the stolen data of non-paying victims is not simply published; instead, it is sold to the highest bidder. Owing to an organisation based on the division of labour, the sharing of tips and tactics, and a centralised platform for data breaches, blackmail groups can focus more on developing sophisticated attacks and successful blackmail attempts. This division of labour has already been observed in a number of cases. For instance, data breaches occurred in which the information did not come from a ransomware attack by Maze, but instead from another incident for which LockBit is thought to be responsible.

Trends in ransomware and data breaches are clearly moving in the direction of "services". Encryption by ransomware and data breaches can be bought as-a-service on the darknet. Also new is the fact that data is not simply published but also sold on or even put up for auction.

Conclusion:

The careful and conscientious handling of data is a major risk area that companies would do well not to neglect. Firstly, the company's reputation is on the line and the resulting costs are considerable. In addition, the public or customers are entitled to expect that companies and organisations will handle their personal data safely and conscientiously. A data breach response plan is a key measure in this regard. The mere preparation of such a plan will help identify specific risks and how to minimise them.

[103] https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Recommendations:

The description above shows just how varied the methods are for achieving a data breach. Every company should make preparation for a data breach scenario. Relevant measures include the following: system inventory, threat and vulnerability analysis, risk assessment, evaluation and mitigation, ongoing refinement of control mechanisms, and monitoring.

A data breach response plan enabling a fast and coordinated response should in any case be available, in case the company nonetheless suffers a data breach. In addition to classic incident management measures, the plan should also contain processes to identify the extent of the damage (i.e. which data was leaked, and how much), inform victims and report the incident. If external services (advice, operational support, etc.) are required, it is important that these partners are well known to the company beforehand and that the services are contractually defined. Communication (with victims and the media) is another key aspect that should be mapped out, not just in terms of content but also as regards the availability of resources (e.g. support in dealing with a flood of phone calls and emails). Moreover, in addition to the technical analysis and assessment of the incident, an early assessment of the situation and the possible legal and financial consequences is likely to be needed. Last but not least, there should also be a focus on reputation management.

4.6 Espionage

Espionage continues to be a very real threat, as the events of recent months have once more shown. State, or state-sponsored, groups continue to play a leading role, but a number of private companies already exist that can be hired to perform targeted espionage (see section 4.6.3).

4.6.1 Espionage in the time of COVID-19

According to Kaspersky, in the first half of 2020, APTs such as Kimsuky, APT27, Lazarus or ViciousPanda, along with other cyberplayers, exploited the coronavirus crisis for their own ends.[104] Although the pandemic had no impact on the tactics, techniques and procedures used by these groups, it was the main topic in a variety of attack scenarios (see section 3.1 on social engineering).

During a pandemic, the desire for information inevitably focuses on health services in the broad sense. For example, one of the key players worldwide during the crisis, the World Health Organization (WHO), was targeted a lot more often than usual. As its CISO explained to Reuters, the espionage attempts were the work of elite hackers.[105] Besides the WHO, the espionage activities targeted a number of organisations conducting research into a COVID-19 vaccine. There is stiff competition to find a vaccine. The US, Canada and the UK have all

[104] https://securelist.com/apt-trends-report-q1-2020/96826/

[105] https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

accused the Russian secret service of spying on organisations in their countries.[106] The US has also filed charges against two Chinese citizens, who are accused of having carried out espionage operations on behalf of China's Ministry of State Security.[107] The attacks were aimed at US biotech firms searching for a COVID-19 vaccine.[108] The accused hackers appear to be part of a criminal gang that has carried out espionage in a number of areas since at least 2009, and has made a substantial amount of money from stealing intellectual property in particular.

4.6.2 Industrial espionage also a reality in Switzerland

Industrial espionage involves obtaining industrial, scientific or technological information or data that has been deliberately kept secret (commercial secrets). Owing to the sensitivity of this topic and the scarcity of publicly available data, the scale of industrial espionage in Switzerland is difficult to quantify. To highlight the problem, the Federal Intelligence Service (FIS) commissioned a study on industrial espionage in Switzerland. In January 2020, the University of Bern published a qualitative and quantitative study by its Institute for Penal Law and Criminology on industrial espionage aimed at Swiss companies of different sizes in various branches of industry.[109]

The results of the study show that between 15% and 33% of Swiss companies are affected by industrial espionage, irrespective of their size. The industries most at risk are IT, telecoms, life sciences, machinery and equipment, manufacturing and pharmaceuticals. In 40% of cases, former or current employees were involved. In other areas, the targets are predominantly companies that make niche products or special security products. The companies taking part in the study noted the difficulty in distinguishing between attacks aimed directly at financial gain and those aimed at obtaining data for espionage purposes. It also appears to be difficult to categorise the cases: 38% of incidents could not be categorised. As regards types of damage suffered, the following were cited most often: loss of competitive advantage (18%), IT failures (14%), and loss of customers and orders (11%). In 11% of cases, the company's existence was threatened.

4.6.3 Espionage for hire

In June 2020, the Canadian research laboratory Citizen Lab published a report on large-scale "hack for hire" espionage activities by a group called Dark Basin.[110] Since 2017, Dark Basin has targeted journalists and activists, but also banks and hedge funds as well as companies operating in other sectors. According to Citizen Lab, the group is in all probability linked to an Indian firm named BellTroXInfoTech Services, and has worked for various unidentified clients.

---

106 UK: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development;
US: https://us-cert.cisa.gov/ncas/current-activity/2020/07/16/malicious-activity-targeting-covid-19-research-vaccine-development; Canada: https://cse-cst.gc.ca/en/media/2020-07-16

107 https://www.courtlistener.com/recap/gov.uscourts.waed.91446/gov.uscourts.waed.91446.15.0.pdf

108 https://www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations;
https://www.nytimes.com/2020/07/21/us/politics/china-hacking-coronavirus-vaccine.html

109 https://boris.unibe.ch/139072/

110 https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

One of these operations involved a large phishing operation aimed at different non-profit organisations whose common feature was their participation in the #exxonknew campaign. The campaign accused the US oil company Exxon of having deliberately played down the impact of climate change for decades. Another Dark Basin operation targeted employees at the German fintech company Wirecard AG, as well as journalists investigating suspected fraudulent activities within the company.[111]

4.6.4 Latest news about Winnti

The security service provider FireEye uncovered a large-scale espionage operation by Chinese group APT41.[112] Between 20 January and 11 March 2020, APT41 attempted to exploit vulnerabilities in the Citrix NetScaler/ADC, Cisco Router and Zoho ManageEngine Desktop Central applications at 75 FireEye customers. The attack targeted a number of countries, including Switzerland. Various branches were affected, including government and finance. APT41 is a highly sophisticated player that regularly diversifies its activities. This group is also known as Winnti, and was the subject of a report in the last semi-annual report.[113]

4.6.5 Sandworm targets popular Linux mail server

On 28 May 2020, the US intelligence service NSA issued an advisory on fending off intrusion attempts via vulnerabilities in the Exim *mail transfer agent* (MTA).[114] In its release, the NSA accuses a group called Sandworm of responsibility for the attacks and associates the group with the Main Centre for Special Technologies (GTsST) of the Russian military intelligence service GRU. Sandworm is suspected of at least some kind of involvement in the attacks on the Ukraine power supply at the end of 2015[115] and 2016[116].

The vulnerability (CVE-2019-10149) had already been known for a year and patches for the affected systems had been available for some time.[117] Nonetheless, at the time of the advisory, the dedicated search engine Shodan managed to still locate around 2.5 million vulnerable systems.[118] Use of the Exim MTA is common because many Linux distributions include this software by default for email functionality. System vulnerabilities allow attackers to remotely insert and run any code of their choosing.

---

111 https://www.ft.com/content/19c6be2a-ee67-11e9-bfa4-b25f11f42901

112 https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

113 MELANI semi-annual report 2019/2, section 4.1.2

114 https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/

115 MELANI semi-annual report 2015/2, section 5.3.1

116 MELANI semi-annual report 2016/2, section 5.3.1

117 https://www.qualys.com/2019/06/05/cve-2019-10149/return-wizard-rce-exim.txt

118 https://www.bleepingcomputer.com/news/security/nsa-russian-govt-hackers-exploiting-critical-exim-flaw-since-2019/

4.6.6 Ongoing threat from Berserk Bear

Since spring 2018, when the US warned about reconnaissance attempts targeting mainly American energy utilities[119], the attackers have hit the headlines repeatedly.[120] Most recently, it was discovered that San Francisco Airport's website had been compromised;[121] the attackers had attempted to obtain access data from unsuspecting visitors to the site.[122]

On 27 May 2020, the day after the journalists at Cyberscoop had reported on a warning issued by German authorities,[123] the German Tagesschau news programme broadcast the somewhat more sensationalist story "Russian bears suspected of hacking".[124] In a document not intended for public distribution, Germany's Federal Intelligence Service (BND), Federal Office for the Protection of the Constitution (BfV) and Federal Office for Information Security (BSI) reported ongoing attacks by the group known as Berserk Bear.[125] The threat is of concern specifically for companies in the power, water and telecommunications industries.

The BfV had already issued a warning about attacks by Berserk Bear,[126] in which German companies were also targeted, back in summer 2018. According to research by Bayrischer Rundfunk, Bavaria's public broadcasting service, the German authorities felt obliged to reiterate their warning about the danger, in light of continuing, and in some cases successful, attempts to compromise systems.

Note:

In the past, Berserk Bear has managed to infiltrate networks repeatedly, getting in as far as systems connected to process controls, such as the power supply. From there, it is only a small step to cybersabotage with a physical impact.

4.6.7 Australia - target of cyberattacks

According to the Australian authorities, in recent months the country has been the target of a spate of highly sophisticated attacks against a number of institutions of government, politics, education, healthcare, manufacturing and operators of critical infrastructure. Australia has often found itself in the attackers' sights, but this wave was conspicuous for its high frequency, scale, technical sophistication and potential impact.

The Australian Cyber Security Centre reported[127] that the attackers had used a copy-paste compromise tactic to infiltrate their victims' systems. In other words, the attackers mainly used

---

119 https://us-cert.cisa.gov/ncas/alerts/TA18-074A

120 https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

121 https://www.bleepingcomputer.com/news/security/russian-hackers-tried-to-steal-san-francisco-airport-windows-accounts/

122 https://attack.mitre.org/techniques/T1187/

123 https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

124 https://www.tagesschau.de/investigativ/br-recherche/hacker-angriff-infrastruktur-101.html

125 https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

126 https://www.wirtschaftsschutz.info/SharedDocs/Kurzmeldungen/DE/ITSicherheit/Cyberbrief_1_18_dow.html

127 https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf

existing *exploits* and other open source tools, which they were able to simply copy and paste. For example, in order to gain entry to the target networks, vulnerabilities in out-of-date versions of Telerik UI, Microsoft Internet Information Services (IIS), SharePoint and Citrix (see section 4.4) were exploited. Where this was not possible, the attackers resorted to *spear phishing*. They gained legitimate remote access by means of stolen identities. Via *web shells* and *HTTP/HTTPS* traffic, compromised websites were used as *command & control servers*. Once inside the target network, open source or bespoke tools were used to ensure persistence and interaction within the network.

The Australian government reckons that the attacks are state-sponsored, although Prime Minister Scott Morrison named no names. Later on, the word in government circles was that China was probably behind the attack.[128] The Chinese government immediately issued a denial, and accused the Strategic Policy Institute of deliberately making false accusations.[129]

Less than a month after the attacks were made public, a group of experts commissioned by the Australian government published a report containing recommendations for the 2020 Australian cybersecurity strategy.[130] The recommendations cover five areas:

- Deterrence: deterring malicious actors from targeting Australia;
- Prevention: preventing people and sectors in Australia from being compromised online;
- Detection: identifying and responding quickly to cybersecurity threats;
- Resilience: minimising the impact of cybersecurity incidents;
- Investment: investing in essential cybersecurity enablers.

To implement the new strategy, Australia is planning to spend an unprecedented AUD 1.35 billion (around CHF 900 million). Roughly one third will go towards employing some 500 cybersecurity specialists within the Australian administration.[131]

4.6.8 Austria in the cross hairs

Austria was the target of two espionage attacks reported in recent months. An attack at the beginning of 2020, apparently by a state actor, targeted the Austrian Foreign Ministry. No details of the incident are publicly available.[132]

In June 2020, Austria's largest telecoms provider, A1 Telekom Austria, confirmed an attack after a whistleblower close to the company contacted a security expert.[133] The operation appears to have taken place as far back as November 2019 and to have been discovered in December. It took six months for A1 Telekom to finally get rid of the attackers.[134] According to A1, the malicious actors had compromised only a limited part of its network, and the complexity

128 https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison
129 https://www.abc.net.au/news/2020-06-19/china-responds-to-accusation-of-australia-cyber-attack/12375324
130 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf
131 https://www.itnews.com.au/news/govt-reveals-135bn-investment-into-cybersecurity-over-next-decade-549856
132 https://www.bbc.com/news/world-europe-50997773
133 https://blog.haschek.at/2020/the-a1-telekom-hack.html
134 https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/

of its systems had prevented worse damage. As it turned out, however, the attackers had been able to make considerable inroads by first obtaining permissions of a local administrator and then of a domain administrator, thereby gaining access to the Windows network.[135] A1 insists that the intruders did not abstract any data, although the whistleblower claims that the attackers gained access to sensitive customer data. A1 was unable to name the perpetrators, unlike the anonymous witness, who attributed the attack to a Chinese state actor, specifically the Gallium group, which specialises in telecoms companies.

4.7 Social engineering and phishing

4.7.1 Phishing

Systems such as Google reCAPTCHA v3 have revolutionised the way CAPTCHA works. CAPTCHAs allow a website to rule out the possibility that the ostensible user is actually a robot with the help of puzzles that must be completed or distorted words that need to be interpreted. This can, for example, prevent large numbers of forms being filled out automatically. reCAPTCHAs facilitate this process by only asking the website's visitors to click a box to confirm that they are not a robot.

Researchers at the IT security firm Barracuda have discovered that cybercriminals were using Google reCAPTCHAs to make it more difficult to detect their attacks.[136] This measure means that automatic security systems designed to check links in emails are unable to access the actual phishing site, and thus do not recognise it as a phishing site. Inserting a reCAPTCHA in front of the phishing site gives the attackers an additional advantage, because users will recognise it as a security feature, which reinforces their mistaken belief that the website is genuine. In the attack monitored by Barracuda, cybercriminals sent an email with an apparently lost voicemail attached. When the mail recipient clicked on the attachment, they were directed to an internet page that contained only the reCAPTCHA. After confirming that they were not a robot, users ended up on a page that appeared to be a Microsoft login page.[137]

Attacks using CAPTCHAs have also been observed in Switzerland, but they were not aimed at Swiss companies; they targeted international payment systems that are also used by Swiss citizens (e.g. PayPal).

Phishing-as-a-Service

Cybercrime-as-a-Service (CaaS) has been a widespread concept in all areas of cybercrime for many years. A wide range of attack tools are offered on the darknet. According to the Singaporean IT security firm Group-IB, phishing kits are increasingly being requested and the available range has doubled compared to last year. Prices of these products have also risen. A "phishing kit" is a set of scripts that can be used to run a phishing website. In 2019, Amazon, Google, Instagram, Office 365 and PayPal were among the most popular names used for phishing. In other words, most requests are for phishing kits for well-known brands with a large

135 https://www.heise.de/hintergrund/Massiver-Angriff-auf-A1-Telekom-Austria-4775451.html

136 https://blog.barracuda.com/2020/04/30/threat-spotlight-malicious-recaptcha/

137 https://hotforsecurity.bitdefender.com/blog/cybercriminal-are-using-google-recaptcha-to-hide-their-phishing-attacks-23156.html

number of users. These attack tools are, so to speak, sold off the peg to cybercriminals with limited technical skills, allowing countless phishing sites to be set up.[138]

Situation in Switzerland

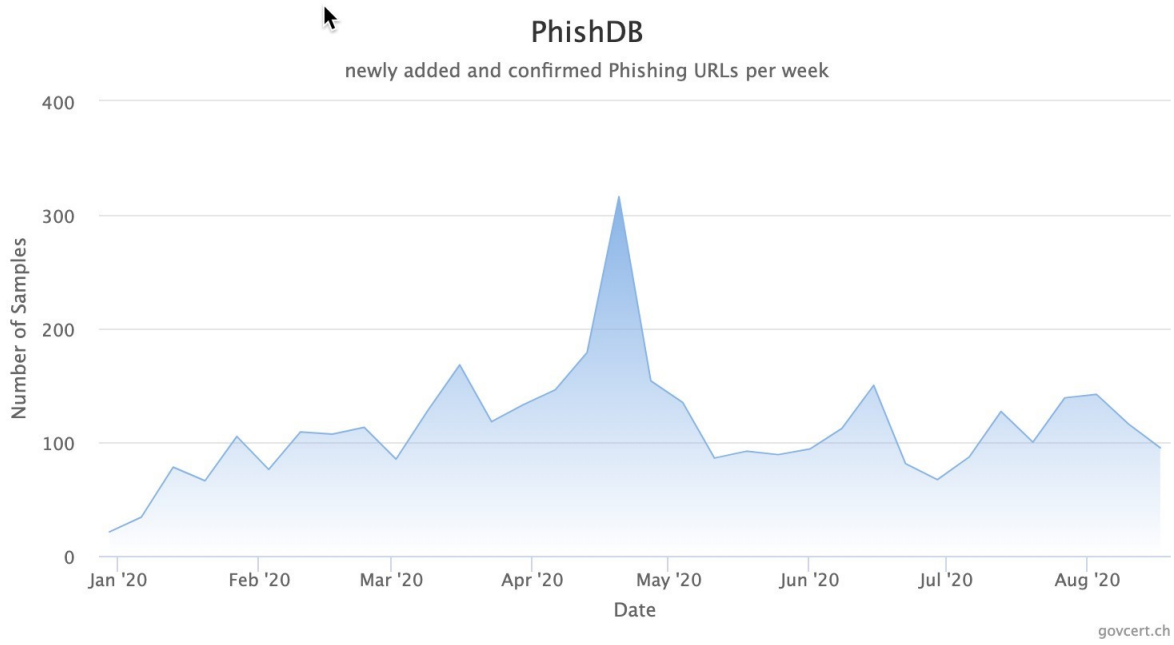

Fig. 7: Reported and confirmed phishing sites per week on antiphishing.ch in the first half of 2020

In the first half of 2020, the several ten thousand reports to the antiphishing.ch portal operated by the NCSC led to a total of 3,029 verified unique phishing sites. Figure 7 shows identified phishing sites per week in the first half of 2020.

From April 2020, the NCSC recorded an increase in phishing attacks on website operators and domain owners. In order to obtain access data for website administration, the cybercriminals sent phishing emails to the website operators and domain owners; these mails ostensibly came from their hosting provider(s). Most of the mails contained a personal link which directed the recipient via an infected website to the final phishing site, where the domain name and/or the name of the hosting provider had already been entered and the victims were requested to enter their access data.

Recommendations:

INFO

GovCERT has published an entry on its blog, describing the attacks on webmasters in detail, together with general recommendations for users and specific advice for hosting providers.

138 https://securityaffairs.co/wordpress/101616/cyber-crime/underground-market-phishing-kits.html

4.7.2 Spoofing – bogus senders

In IT, *spoofing* is the tactic of taking on a false identity, especially by changing address elements such as the email sender ID or phone numbers. Websites, IP addresses, MAC (media access protocol) addresses or ARP (address resolution protocol) messages can also be spoofed.[139] Spoofing is used to give the recipient the impression of credibility and ultimately persuade them to behave in a certain way. It is thus a social engineering technique.

Spoofing methods are constantly being refined and improved in line with changing digital possibilities. As a result, spoofing is widespread, despite some protective measures being available. Both criminals and state actors successfully use a variety of spoofing methods in different contexts. For this purpose, they falsify email addresses, phone numbers, text message sender IDs, logos and company names in order to exploit people's trust and the recipient's need for information. During the COVID-19 pandemic, for example, malware was sent to members of the public in Switzerland, with the Federal Office of Public Health (FOPH) as a false sender (see section 3.1.1).

Spoofing of email addresses: email addresses are easy to spoof, as the protocol used (Simple Mail Transfer Protocol, SMPT) does not verify the sender's address. If a mail server is openly available and unprotected online, any user can connect to it and send emails. The sender's display name can be freely chosen. Where no restrictions are configured on the email server, the sender's address can also be freely defined and may contain a domain name that is not associated with the server, for example invoice@ncsc.ch.

However, it is possible to set up technical protective measures:

- Servers that are entitled to send mails with a specific domain as the sender address can be entered in the Sender Policy Framework (SPF). Sending, transferring and receiving servers can use the SPF to verify emails and filter messages accordingly.

- Domain Keys Identified Mail (DKIM) assigns a digital signature to an email. The receiving system can use this to verify that the domain mentioned in the mail sender's address is correct and that the mail has not been changed somewhere along the delivery chain. If verification fails, the email delivery can be rejected.

- Domain-based Message Authentication and Conformance (DMARC) is based on authentication of the sender (SPF) and verification of the integrity (DKIM), and signature verification is a prerequisite.

Spoofing of phone numbers and text message senders: thanks to internet telephony (voice over IP, or VoIP), numbers are now relatively easy to spoof or conceal. There is even a market for services offering caller ID spoofing. Text messages can also be sent via online services. As no mobile phone and no associated number are needed, some services allow the display name to be freely chosen. International efforts are under way to prevent the spoofing of phone numbers.[140] Currently, however, providers do not have a common technical measure that could be implemented to stop phone number spoofing. It is likely to be some time before a

[139] See, for example, https://www.cybersecurityintelligence.com/blog/beware-spoofing-attacks-4890.html

[140] e.g. STIR/SHAKEN, see https://www.metaswitch.com/knowledge-center/reference/what-is-stir/shaken

correspondding standard is introduced. In most countries, phone number spoofing is not prohibited by criminal law; instead, it falls under private law where only the person whose identity is abused can sue the sender, not a recipient of a spoofed message – this is also the case in Switzerland. However, the planned revision of the Data Protection Act should introduce a new provision which will make identity theft, and hence certain forms of phone number spoofing, a criminal offence.

Spoofing of websites: websites can be copied and operated from another web address. Spoofed websites can also achieve a recognition effect by incorporating the original logos. If users do not check the domain name in the address line and do not notice that, say, a false certificate is being used, they could be fooled by such websites. Often, fraudsters register so-called typo domains, that vary only marginally from the original address, such as: svvisscom.ch instead of swisscom.ch. Typo domains can also be used for sending emails and thus for phishing, fraud or spreading malware.

Some attackers also successfully use combinations of spoofing methods: the Retefe group employs phone calls from spoofed numbers, using a pretext to convince their victims to open a PDF file that has been emailed to them before, during or after the phone call (see chapter 4.7.4). If the victim clicks on the enclosed link, the computer is infected with the Retefe ebanking Trojan. To protect Swiss businesses and the population, the NCSC supplies internet providers with information to help them block attempts by their customers to access websites through which Retefe is spread. In order to conceal malicious links, *shortener services* such as bit.ly or goo.gl are used.

Note / recommendations:

In principle, the sender ID on any message can be spoofed.

It is always a good idea to cultivate a healthy scepticism, especially if you receive new or unusual messages. Instead of following the links in these messages, you should log into your user account via the usual channels wherever possible. Before entering personal data, passwords or credit card details, verify that you really are on the intended website.

Do not click on links in suspicious messages – not even out of curiosity. Otherwise, you risk infecting your device with malware or being diverted to dubious websites. In case of any doubt, contact the supposed sender using the contact details you already have or those indicated on the sender's website, to check with them what the message is about exactly and whether or not it actually comes from them.

4.7.3 Smishing

Smishing is a portmanteau of "SMS" and "phishing", and generally refers to the misuse of SMS, but increasingly also of instant messaging apps like WhatsApp, as an attack vector for stealing sensitive data such as access data, passwords, credit card details and account information. Frequently, the sender's number and name are spoofed (see section 4.7.2 above on spoofing). Criminals also employ smishing to misuse mobile payment services, capture an *mTAN* or circumvent two-factor authentication, for example with an *SMS stealer*. In Switzerland and abroad, it has also been observed that criminals are combining social engineering techniques: victims are sent a text message requesting them to forward an authentication code they have just received in another text message; it is claimed that the code was sent accidentally or that there is an emergency. Theoretically, this method can be used to

compromise all services protected by two-factor authentication, so long as the attacker has already obtained the victim's login, password and phone number. In the case of WhatsApp, under the default setting an authentication code alone can be used to take control of someone's entire user account.[141]

Mobile phone payment services were a particular target for fraudsters in the first half of 2020. These services allow people to pay invoices via their phone bill. The service provider sends an SMS code to the mobile phone; this code must then be entered as confirmation on the website. In one case, the victims were tricked into thinking that a package could not be delivered. In order to release the delivery, they were supposed to provide their phone number and then download an app. The app was an *SMS stealer*. The fraudsters subsequently initiated payments with the victim's mobile phone and the app forwarded the authentication code directly to the criminals.

Increasingly, the dissemination of links to malware such as Emotet or EventBot via text message has been observed; these malware are used to steal access data for ebanking and financial applications.[142] In smishing, false senders and, as mentioned above, social engineering techniques are used to prompt the target to behave in a certain way. To do this, the attackers make use of major current events and their effects, such as the COVID-19 pandemic: in March 2020, the South Korean authorities warned of smishing related to information on the spread of the new coronavirus. By mid-February already, nearly 10,000 messages had been sent to South Koreans, claiming to come from companies offering free face masks.[143]

Smishing represents a growing threat to both private citizens and businesses: in the US in the first quarter of 2020, companies alone recorded a 37% increase in phishing on mobile devices.[144] In Switzerland, there are still relatively few publicly known cases: by July 2020, a total of 16 smishing cases had been reported to the NCSC; of these, nearly half were recorded in June. For the next half-year, however, the NCSC is expecting an increase in this phenomenon.

Scams are also circulating via SMS and messaging services: messages spoofing the sender IDs of well-known Swiss firms (Coop, Migros, Swiss Post) trick the recipients into signing up to premium paid services, for example in the guise of a competition or voucher (see chapter 3.1.3).

---

[141] In this regard, see also https://www.20min.ch/story/mit-diesem-code-bist-du-dein-whatsapp-8203-8203-konto-los-252382069481 and https://www.mimikama.at/allgemein/vorsicht-wenn-ein-whatsapp-kontakt-einen-verifizierungscode-verlangt/

[142] As regards EventBot, see https://www.zdnet.de/88379272/cybereason-warnt-vor-neuem-mobilen-banking-trojaner/; as regards Emotet, see: https://threatpost.com/sms-attack-spreads-emotet-bank-credentials/153015/

[143] https://www.zdnet.com/article/south-korea-sees-rise-in-smishing-with-coronavirus-misinformation/

[144] https://blog.lookout.com/global-mobile-phishing-encounters-surged-by-37-percent-amid-wfh-shift

Note / recommendations:

In principle the sender ID in any message can be spoofed.

Over the years, email infrastructure has developed very efficient methods to filter out spam mail in particular. This technology is not easily transferable to the text message context. It will not be possible to introduce a similar mechanism for messaging services like WhatsApp or Threema because the messages are sent in encrypted form between the sender and the recipient, and the content cannot be checked by an intermediary.

Do not click on links in suspicious messages – not even out of curiosity. Otherwise, you risk infecting your device with malware or being diverted to dubious websites. In case of any doubt, contact the supposed sender using the contact details you already have or those indicated on the sender's website, to check with them what the message is about exactly and whether or not it actually comes from the sender.

Before entering personal data, passwords or credit card details, always check that you really are on the intended website.

4.7.4 Dial "M" for malware

Fraudsters can go to great lengths to install malware in a victim's systems, as illustrated by the 64 cases reported to the NCSC in numerous variations in the first half of 2020. The common denominator in all the variations was the fact that the victim was also called as well as being sent an email. Either the fraudsters started by phoning and announcing an email with a PDF attachment, or they would phone once the mail had been sent, to make sure that the victim had seen the mail, opened the attachment and clicked on the link it contained. When the link was clicked, malware would be installed.

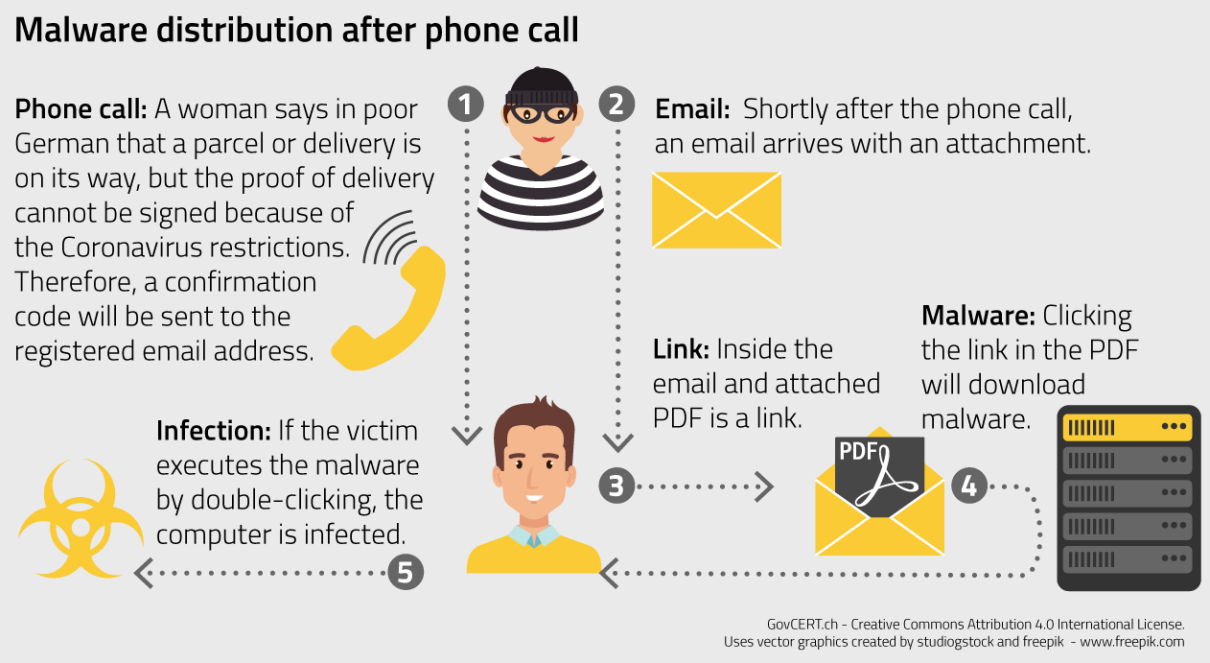

Fig. 8: Procedure following an infection with the Retefe Trojan. The scenario used in the call can vary infinitely.

Names often used by the callers (which claimed to be a delivery service in each case) were CH-Express, Delivery Experts or Delivery Schweiz. Attacks were aimed predominantly at small companies such as architects' offices, landscape gardeners or carpentry businesses. The emails usually related to requests for quotes. In many cases, the perpetrators claimed to be a university and sent the emails using a domain name that could easily be mistaken for the real thing (a so-called *typo domain*). Latterly, however, the attacks have also targeted private individuals.

The current pandemic was also used to persuade victims to install malware. It was claimed, for example, that the danger of infection prevented delivery of a package that needed to be signed for; instead, a confirmation code was being sent by email, which the recipient would then have to give to the courier. Here too, the callers pretended that the code was in the mail's PDF attachment, which the recipient only needed to click on. See also chapter 4.7.2 on spoofing.

Detailed information is provided on the cybercrimepolice.ch website.[145]

Conclusion / recommendations:

It is astonishing that the attackers will go to the effort of calling each individual victim. Apparently, it is no longer that easy for the attackers to get malware onto a device, so the criminals have to go to greater lengths. It is also astonishing that the malicious link is not inserted directly into the mail, but instead into the PDF attachment. It is doubtful whether this is worth the effort. This approach is likely to be counterproductive, as it makes the attack more complicated and gives the victim time to reflect about the story's plausibility. More than a few would-be victims became suspicious after opening the PDF and did not follow through. It is therefore all the more important to exercise caution when opening links and attachments, and above all not to allow yourself to be coerced into doing something.

4.7.5 Website operators blackmailed

In the period under review, numerous website operators received fraudulent ransom mails, in which criminals claimed to have exploited a vulnerability to hack into a website and steal its entire database.[146] They threatened to inform customers, publish or sell the stolen data and thus damage the victim's reputation, unless a ransom was paid in Bitcoins. In Switzerland, emails in both English and German were observed. In one case, the sender claimed that the attack had been commissioned by a rival company, with the aim of sabotaging the mail's recipient. However, the company allegedly ordering the attack now wanted to renegotiate the agreed price, which had annoyed the criminals and prompted them to contact the apparent victim with an offer to give back the stolen data – in return for a substantial compensation payment, of course. In this variation, further pressure is applied by mentioning the legal problems that the victim would face with regards to the European General Data Protection Regulation (GDPR). See also section 4.5 on data breaches.

145 https://www.cybercrimepolice.ch/de/fall/online-betrueger-aufforderung-packetsendung-freischalten-nicht-nur-per-mail-sondern-neu-auch-per-telefon/

146 https://www.watchlist-internet.at/news/website-betreiberinnen-aufgepasst-erpressungsmails-im-umlauf/

As part of this type of fraud, the cybercriminals exploit the website operators' fears over the consequences of a data breach, in the hope that this will cause them to pay the ransom. Yet the websites are not really compromised, or at least not in most of the cases that the NCSC is aware of. These emails are strongly reminiscent of the fake sextortion wave, which MELANI has described in a number of previous semi-annual reports. In these attacks, the fraudsters claim to have hacked the victim's webcam and to have caught the victim watching pornography.[147] In these cases too, the computer had not really been hacked and the cybercriminals did not have any material with which they could cause damage for the blackmail victim. Even so, the attackers used social engineering methods to persuade the victim to nonetheless pay a certain amount in Bitcoins.

Recommendations:

If you receive a ransom demand, keep calm. Do not allow yourself to be put under time pressure. Often, the blackmail claims are baseless and have been sent to a large number of people in the hope that a few of them will be intimidated and will pay over-hastily. Blackmail attempts are in any case prosecutable offences and can be reported to the police.

If you suspect that there could be some substance to the claims, you should contact your local cantonal police without delay (see https://polizei.ch), so that they can start investigating the perpetrators.

4.8 Preventive measures and prosecution

4.8.1 Charges brought against German bulletproof hoster

Bulletproof hosters are data centres designed to evade intervention by the authorities, especially law enforcement agencies. They are often located in countries where the justice system does not function very effectively; moreover, the administrative and technical online setup conceals the location using a variety of false information and straw men. Bulletproof hosters are used by various kinds of criminals.

Last autumn, after a four-year criminal investigation, the German authorities managed to access such a bulletproof hoster; it had been operating for many years out of a decommissioned NATO bunker in Germany, providing a platform for various cybercriminals. For example, the Wall Street Market drugs hub, the Flugsvamp darknet marketplace (which handled 90% of the online drugs trade in Sweden) and the Mirai botnet were all managed on the cyberbunker's servers. In autumn last year, over 700 officials searched the bunker compound in Traben-Trarbach and took down more than 800 servers. The attorney general's office has now filed charges against eight people for conspiracy to commit a number of offences, including possession of stolen data, botnet attacks and drug dealing. Links to child pornography and contract killings were also uncovered. This complex case involves data

[147] See MELANI semi-annual reports 2018/2 section 4.4.2 and 2019/2 section 4.4.3; MELANI Website: https://www.melani.admin.ch/melani/en/home/ncsc/form/meldeformularhaeufigefragen/FakeSextortion.html

memories with a total capacity of 2 petabytes, and is pushing the investigating teams to the limits of their capacity.

Under German law, a conspiracy charge also requires the existence of a main crime. This means that the investigators first had to clear up the offences committed through websites hosted by the cyberbunker. Accessing the cyberbunker's internal email system (used for hoster/client communications) was a challenge. These communications are crucial for proving that the accused operators did not only act as technical service providers with no liability, but were instead willing participants in the offences and thus laid themselves open to a conspiracy charge.[148]

4.8.2 Swiss prosecutors arrest cybercriminals

In April 2020, Swiss and Polish law enforcement authorities, supported by Europol, broke up the InfinityBlack hacking group in April 2020. InfinityBlack was a group of cybercriminals involved in distributing stolen user credentials, creating and distributing malware and hacking tools, and fraud.

The police confiscated electronic equipment, external hard drives and hardware cryptomoney wallets worth some EUR 100,000. Two platforms with databases containing over 170 million entries were also seized and closed down by the police.

The hacking group's business model involved creating online platforms for selling user login credentials (so-called combos). The group was efficiently divided into three teams, with the developers creating tools to test the quality of the stolen databases, while the testers analysed the suitability of authorisation data. The project leaders then sold the data against payment in cryptocurrency. In this way, the hackers gained access to a large number of Swiss customer accounts. Although the losses are estimated at only EUR 50,000, the hackers had access to accounts from which more than EUR 610,000 in total could have been abstracted. The hacking group drew its main source of income from stealing credentials for the loyalty programme of a Swiss wholesaler and selling them on to other, less technically savvy criminal groups. The buyer groups then exchanged the loyalty points for expensive electronic equipment. The fraudsters and hackers, some of whom were minors or young adults, were unmasked when they tried to exchange the stolen points for goods in Swiss shops. Following the arrests, the police discovered links to a hacking group in Poland. The transmission of the data from the seized computers to the Polish authorities subsequently led to further arrests of InfinityBlack members in Poland.[149]

[148] https://www.heise.de/newsticker/meldung/Cyberbunker-Staatsanwaltschaft-erhebt-Anklage-gegen-Betreiber-4698785.html

[149] https://www.europol.europa.eu/newsroom/news/hacker-group-selling-databases-millions-of-user-credentials-busted-in-poland-and-switzerland; https://www.blick.ch/news/cyberkriminalitaet-treuepunkte-hacker-nach-polizeioperation-in-waadt-in-polen-gefasst-id15877097.html; https://www.watson.ch/!158091108

5 Research and development

5.1 SCION: high-performance secure internet

Ilona Wettstein, Adrian Perrig, ETH Zurich, Network Security Group

The increasing digitalisation of all areas of life and industry requires a secure internet. Every day, billions of people rely on it to send data without it getting lost, diverted or analysed during transmission. At the same time, security should not come at the expense of performance, i.e. the security mechanisms should not reduce network capacity or result in additional delays in delivering data.

The internet is based on the *Border Gateway Protocol (BGP)*, which routes data packets through the internet and has remained practically unchanged for the last 30 years. At each network node, it decides which route a data package should take. Owing to the massive expansion of the internet, this protocol now has numerous vulnerabilities and it is becoming clear that the internet is built on a crumbling foundation: data traffic is diverted by state or criminal actors and can be spied on or disrupted by them.

SCION is a new kind of internet architecture.[150] The acronym stands for **S**calability, **C**ontrol, and **I**solation **O**n **N**ext-Generation Networks. The architecture was developed at the ETH Zurich; it replaces BGP with a more secure and efficient protocol and resolves many of the current internet's other security problems, such as false security certificates or *Distributed Denial of Service* (DDoS) attacks. In contrast to the current internet, in which all routing decisions are performed by the network nodes, SCION offers users transparency and control over network paths. The data packets are already assigned the exact path for their route through the internet at the time they are sent, so they cannot go astray. Moreover, through smart routing choices, this approach can be used to optimise the transfer time for data packets. By using several paths, SCION can also switch to a new path in a matter of milliseconds, in the event of a disruption in communication.

150 https://www.scion-architecture.net/

The developed architecture is already being used by the federal higher education institutes and several banks. A SCION connection offers a number of clear advantages:

- Guaranteed communication and sovereignty on the internet: communications cannot be disabled by an attack from abroad or by lone attackers (no *"kill switch"*).
- Possibility of setting organisational or geographical boundaries for data traffic. This prevents confidential information travelling via non-trusted networks.
- Simultaneous use of several connections to optimise communications and increase reliability, even in the event of the connection dropping (business continuity).
- Higher capacity through the use of multiple network paths.

The next-generation internet thus promises both greater security and better performance than the existing set-up. A number of internet service providers have formed a consortium to act as integrators and providers of connections in Switzerland and abroad. SCION is currently being commercialised and implemented by Anapaya Systems, a spin-off of the ETH Zurich.[151]

6 Outlook and trends

6.1 Working everywhere – not only in the office anymore

As already discussed in the key topic (section 3.5), the COVID-19 pandemic has changed the world of work, especially for office employees. Lots of them were able, or were forced, to work from home. As a result, many companies and employees have gained experience with working from home and other models that involve people working from any location they choose, rather than in the office. This will result in greater general acceptance of – and perhaps even demand for – location-independent working. It is still unclear when the current pandemic will be over and when people might be able to revert to the previous normality. It must be borne in mind that a return to pre-pandemic working situations may be neither possible nor desirable. While some companies have long had a stable and secure infrastructure for location-independent working, others have so far only hastily installed and somewhat makeshift solutions. It is worth taking advantage of the experience gained and reviewing the solutions adopted, in order to improve them or launch a comprehensive overhaul project so that, in addition to the required infrastructure capacity, the security of devices, networks and data can be adequately factored in from the outset (security by design).

Remote access infrastructures offer an attack vector for compromising corporate networks. Both VPN and RDP connections must be securely configured and adequately protected. For some time now already, threat actors have been scouring the internet for vulnerable implementations of remote access solutions. After the pandemic-related increase in the use of remote access solutions, corresponding scanning activity also increased significantly (see section 3.5). Sooner or later, each vulnerable system will be found and attacked. After all, remote access can be used to i.a. steal company data or infect a company's network with ransomware (see section 4.1.1 on ransomware and section 4.4 on vulnerabilities).

Cloud collaboration platforms and conference software are important tools for location-independent working. Here too, appropriately secure configurations must be selected and staff must be trained in the safe use of such tools.

---

[151] https://www.anapaya.net/

Working on private devices (bring your own device, BYOD) that are not maintained by the company's IT department reduces the company's control over the security of its data and increases the onus on employees. In order that they can appropriately meet their obligations, they need to know and understand the company's rules and receive regular training in threats and dangers.

Recommendations:

Given the wide variety of risks inherent in location-independent working, a clear strategy and a comprehensive implementation concept should be drawn up. In addition to technical security measures, user-related aspects must also be considered, as good user behaviour can make a substantial contribution to reducing risks.

Take your cue from MELANI's checklists on home working:

For companies:
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff.html

For users:
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff-enduser.html

6.2 The geopoliticisation of the internet

Anyone who has looked into the origins of the internet will soon get the impression that they are in a world consisting solely of technically adept researchers, highly bureaucratic standardisation bodies and IT-savvy early users. This world focused on many things, but concepts such as international security policy, geopolitics, power politics, the UN and diplomacy were not among them. Organisations such as the Advanced Research Projects Agency (ARPA), the International Telecommunication Union (ITU), the Internet Corporation for Assigned Names and Numbers (ICANN) and the Geneva-based European Organization for Nuclear Research (CERN) were the main creators of the current internet, and remain its guardians to this day. A worldwide infrastructure which, in 2020, most of us take for granted and, as the names of the organisations involved suggest, was initially regarded simply as the next technical step in the area of communications and technology, and best managed by non-political technical specialists.

Now, the internet is at the heart of almost all economic and sociopolitical developments, especially digitalisation of course. For example, it enables the remote management of power stations, the Internet of Things (IoT), industrialisation 4.0 and – particularly in the COVID-19 age – the maintenance of productivity by means of working from home. What was once thought of as redundant technology, which allowed information to be shared easily and continued to function even in the case of partial system failure, has become the global backbone for critical processes in all areas of life. Of course, this realisation has not come about only in 2020; it reached the international security policy echelons much earlier. However, the COVID-19 crisis has reminded us in no uncertain terms that the high degree of interconnectedness and digitalisation can make critical infrastructures such as hospitals a target for cyberattacks.

The resolution brought before the UN by Russia in 1998 on "Developments in the field of information and telecommunications in the context of international security" put this advancing

interconnectedness and digitalisation centre-stage internationally. The resolution proposed that the UN member states engage in regular exchanges in the future on how potential abuse and exploitation of information and communication technology could be prevented at international level. In response, the UN set up a first Group of Government Experts (GGE) in 2004, drawn from 15 member states. Among other things, the group examined the question of whether, for information and communication technology, the focus should extend to the content, or concentrate on the infrastructure that enables content to be exchanged. Given such a controversial starting position, it is hardly surprising that the first GGE was unable to produce a consensus report when winding up its mandate in 2005.

The debate surrounding what the definition of information and communication technology should encompass, what a critical infrastructure actually is, and how international law applies to cyberspace, runs like a leitmotif through the discussions of subsequent GGEs. The 2015 iteration of the GGE was able to report the establishment of generally applicable but non-legally binding standards for the UN member states on good practice in the use of information and communication technology. For example, the standard specified that cyberattacks should not be carried out on critical infrastructures. Moreover, the applicability of international law in cyberspace was confirmed. Similar efforts and discussions are under way at regional level, for instance within the Organization for Security and Co-operation in Europe (OSCE).

What began as a purely technical project to set up resilient and redundant IT networks has today, with its global outreach, become a bargaining chip for partly contradictory security policy interests. Indeed, in the current international climate of hardened attitudes, international progress in this regard is rare. Since the GGE's 2015 report, practically no concrete progress has been made. The 2017 GGE ended without consensus. A new GGE was launched in 2019. Also in 2019, an Open Ended Working Group (OEWG) began discussions and consultations under Swiss chairmanship. Despite the current difficulties, it is vital to keep the various processes and dialogues going – these efforts at diplomatic level are in everyone's interest. Some time ago, Switzerland recognised the need to tackle the topic of cyberspace in the context of international and security policy. As a small, open economy that is highly interconnected internationally, Switzerland has to rely on predictability and order in international security policy. For this reason, Switzerland was also a member of the 2017 and 2019 GGEs and the OEWG, and plays an active part as well in drawing up standards and confidence-building measures within the OSCE. This is definitely an opportunity because Switzerland is well positioned internationally to lead the debate on digitalisation, cyberspace and its governance; as an international centre, Geneva would be the perfect location for such activities. There have been concrete contributions, such as the Geneva Dialogue on Responsible Behaviour in Cyberspace, which Switzerland launched in 2018 and that has been successfully continued in 2020 with the participation of numerous international business representatives. In more than ten virtual meetings, good cyberspace practices have been developed that reflect a worldwide consensus between globally active IT firms and IT-related industries. In this way, Switzerland is making an important contribution to drawing up more precise international standards and principles in cyberspace, for example the GGE standards and the principles under the "Paris Call for Trust and Security in Cyberspace".[152] This will also reinforce Geneva's position as a centre for global digital and technology policy.

[152] https://pariscall.international/en/

7 Published MELANI products

7.1 GovCERT.ch Blog

7.1.1 Analysis of an Unusual HawkEye Sample

20.02.2020 - Currently, we are observing HawkEye samples being distributed by large mal-spam waves. HawkEye is a keylogger which has been around quite a long time (since 2013) and has evolved since then and gained more functionality. There are several good blog posts about HawkEye in general. Recently we observed an interesting obfuscation method in a Hawk-Eye binary, which we are going to describe in this blog post.

➔ https://www.govcert.admin.ch/blog/analysis-of-an-unusual-hawkeye-sample/

7.1.2 Phishing Attackers Targeting Webmasters

22.04.2020 - Since the beginning of April 2020, we are seeing an increase in phishing attacks against webmasters and domain owners in Switzerland. Unknown threat actors are phishing for credentials for accounts on web admin panels of at least three major hosting providers in Switzerland.

➔ https://www.govcert.admin.ch/blog/phishing-attackers-targeting-webmasters/

7.2 MELANI newsletter

7.2.1 Beware: Ransomware continues to pose a significant security risk for SMEs

19.02.2020 - In recent weeks, MELANI / GovCERT has dealt with more than a dozen ran-somware cases in which unknown perpetrators encrypted the systems of Swiss SMEs and large companies and rendered them unusable. The attackers made ransom demands of sev-eral tens of thousands of Swiss francs, in some cases even millions.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/sicher-heitsrisiko-durch-ransomware.html

7.2.2 Warning against false emails purporting to be from the FOPH

14.03.2020 - Since Friday lunchtime (13 March 2020), cybercriminals have been exploiting public anxiety related to the coronavirus. They are attempting to spread malware using emails purporting to be from the FOPH. The Reporting and Analysis Centre for Information Assurance MELANI is therefore warning the public. Delete such emails immediately.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/gefaelschte-emails-im-namen-des-bag.html

7.2.3 Kritische Verwundbarkeit in Microsoft Windows Server (SIGRed) (not available in English)

15.07.2020 - Am vergangenen Dienstagabend (14. Juli 2020) hat Microsoft ein Sicherheitsupdate für eine kritische Verwundbarkeit im Windows Domain Namen System (winDNS) veröffentlicht. Microsoft stuft die Verwundbarkeit mit 10.0 Punkte im CVSS (Common Vulnerability Scoring System) ein, was dem Maximum auf der verfügbaren Skala entspricht.

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

7.2.4 Trojaner Emotet wieder aktiv (not available in English)

23.07.2020 - Nach mehrmonatigem Unterbruch beobachtetet MELANI erneut verschiedene Malspam-Wellen mit infiziertem Word-Dokumenten im Anhang. Dabei handelt es sich um einen bereits länger bekannten Trojaner namens Emotet (auch bekannt als Heodo). Ursprünglich als E-Banking-Trojaner bekannt, wird Emotet heute vor allem für den Versand von Spam sowie das Nachladen von weiterer Schadsoftware (Malware) verwendet.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner-Emotet-greift-Unternehmensnetzwerke-an.html

7.3 Checklists and instructions

7.3.1 Home Office: Securing Remote Access

24.03.2020 - Based on the increased use of Remote Access solutions, we would like to remind you about a few best practices in order to minimize the risk associated with these technologies. We be-lieve that the risks are increasing with the number of Remote Accesses into an organizations network. Attackers know about the current situation and may try to use different ways of getting access into an organization's network.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff.html

7.3.2 Home Office: End User Guideline

02.04.2020 - In addition to the document “Home-Office: Securing Remote Access” we would like to provide you corresponding information for the end user on how to secure his own environment and therefore help to reduce the risk for the employer.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff-enduser.html

8 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.

Cryptomining	Using computing power to find and validate new units of a cryptocurrency, e.g. Bitcoin.
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	A program, a script or a line of code with which vulnerabilities in a computer system can be used to advantage.
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.
Infostealer	Malware that can harvest keystrokes, screenshots, network activity, and other information from systems where it is present.
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.

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.

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.
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.
Spyware	Spyware collects information about the user's surfing habits or system configuration without his knowledge and transmits it to a predefined address.
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.
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).
VPN	Virtual Private Network. Provides safe communication between computers in a public network (e.g. the internet) by encrypting the data flow.
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.