11 May 2021 | National Cybersecurity Centre NCSC

Semi-annual report 2020/2 (July – December)

Information assurance

Situation in Switzerland and internationally

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
National Cybersecurity Centre NCSC

1 Overview/contents

2 Editorial

The Swiss healthcare system is ailing

By Kim Rochat, Cofounder and Head of Digital Health at Medidee Services

Kim Rochat, Cofounder and Head of Digital Health at Medidee Services

The healthcare sector is evolving rapidly, driven by the introduction of cutting-edge technology. The digitalisation of applications and services, the increasingly granular treatment of data, the use of mobile IT and artificial intelligence, and the leveraging of increasingly interconnected systems has allowed significant progress as regards healthcare provision and the personalisation of medicine for the benefit of the population. The healthcare sector is increasingly connected; this is at once a necessity, an inevitable development and a huge opportunity.

This sector has strategic importance for our country, for two reasons. Firstly, hospital capacity is a critical resource requiring permanent availability in order to meet the population's healthcare needs. In this regard, the pandemic has served as a reminder of the importance of this capacity. At the same time, healthcare is a major driver of our economy. Switzerland has long been among the world leaders in pharmaceuticals. Now, we can add medical equipment providers as key players. The medtech industry, located between two renowned federal institutes of technology and benefiting from a close-knit network of specialist technology institutes, universities and professional training centres, currently employs nearly 60,000 people and brings in over CHF 15 billion in revenue, representing 2.3% of Swiss GDP.

Moreover, a number of medtech manufacturers are key contributors to the cybersecurity of our healthcare system. European lawmakers are well aware of this and, on 26 May this year, new legislation – Regulation (EU) 2017/745 on medical devices, which was passed in 2017 – will enter in force. Manufacturers are now required to ensure that their devices are not just safe for patients and users, but also secure as regards data protection and prevention of misuse.

Even though Switzerland, with all the to-and-fro on the bilateral agreements, has not signed up to the mutual recognition agreement (MRA) with the EU on medicial devices, it has nonetheless decided to remain aligned with European law through its new Medical Devices Ordinance (MedDO). This ordinance, which enters into force on 26 May 2021, makes direct reference to European law in Article 6. It is therefore useful to remember that Swiss manufacturers must now ensure the cybersecurity of the devices they bring to market, and it would be advisable to ensure that they are able to respond rapidly to this new requirement.

In addition, Switzerland has been more creative, by including in Article 74 of the MedDO the requirement for healthcare facilities to "take all necessary state-of-the-art technical and organisational measures to protect networkable devices from attacks and electronic access."

Quite apart from the fact that this article is yet further confirmation that the legislators are lagging behind the technology, this presents difficulties for our healthcare facilities as it only partly addresses the underlying problem. While it is indisputable that healthcare facilities must provide robust and efficient protection for their IT systems, they are often unable to take precautions against the risks they face from some medical devices. Indeed, either a large number of devices are not designed to ensure an appropriate level of security or the healthcare facilities do not have the funds to replace obsolete equipment. I participated in a project at a regional hospital, where over 30 systems were known to be using obsolete technology, including respirators and infusion pumps; this represents an unacceptable risks to patients.

In Switzerland, as in Europe, the healthcare sector urgently needs to adapt its infrastructures. At the same time, the regulatory changes under way and the growing pace of digitalisation in healthcare offer a fantastic opportunity to our industry. Our French neighbours are well aware of this challenge. On 18 February, France's president announced a new strategy for developing the cybersecurity sector, involving the allocation of EUR 1 billion for cyber-issues, in particular the creation of a cybercampus. Under this plan, EUR 515 million have been allocated to developing sovereign solutions and EUR 176 million to public sector needs, especially those of hospitals and authorities.

In Switzerland, the SNPC 2.0 strategic plan is a significant step forward in this regard, and sets appropriate objectives. We also benefit from the excellent work by players such as the National Cybersecurity Centre (NCSC) and participation in promising initiatives like the cyberdefence campus, but our digital strategy needs to be a lot more ambitious and aggressive on the subject of security, and our country needs to acquire tools that are up to the challenge we face. Governments must provide sound leadership, while ensuring a more structured and systematic inclusion of the various players in the implementation of these information systems by more actively supporting research, manufacturing and healthcare systems to arrive at common solutions. As we are regularly reminded by hospitals facing ransomware attacks (France has suffered several recently), critical public services can be put out of action by criminal gangs. This risk is known and it is unacceptable that it can materialise in a democracy such as ours.

Identifying the next national cybersecurity unicorns by leveraging our university expertise and our national infrastructures to help our healthcare system arm itself against proliferating risks: this challenge needs to be taken up without delay by our politicians, and it will need more than baby steps to meet it.

3 Focus: Digital healthcare

3.1 Introduction

As elsewhere, digitalisation is advancing inexorably in the healthcare sector, with all the advantages and disadvantages that this entails. Globalised supply chains and computer-controlled logistics are the order of the day. Patient records are kept digitally, which, in addition to saving storage space and offering low-effort data backup, makes it easy to pass on medical records to consulting doctors. As in other areas, growing digitalisation increases the potential attack surface.

3.2 Patient data

According to the Data Protection Act, data about a person's health is "sensitive personal data" and should therefore be particularly well protected against unauthorised access. Patient data is unique and, unlike passwords, cannot be easily changed in the event of misuse. However, health data must also be protected from destruction. Results of earlier tests cannot be collected retrospectively. Digitalisation can mitigate this risk. In addition, the protection of patient data against unauthorised modifications must also be ensured. Transfusions with the wrong blood group can end tragically. Incorrect information about drug intolerances or allergies can have devastating consequences. Only authorised persons should be able to access such data and the number of people who can modify this data must be restricted as far as possible.

3.3 Digital medical devices

Medical devices are now often small or large networked computers. X-ray images are digitally recorded and test results are more or less fed directly into the network of the practice or hospital, or uploaded to a cloud service. Test results from imaging procedures such as computed tomography (CT) scans or X-ray images have been found several times on insufficiently secured cloud servers and on data storage devices accessible from the internet – including the corresponding patient data.[1] The larger and more complicated the analysis device, the more likely it is to have an interface to its manufacturer, which monitors its operation and can also carry out remote maintenance on the device if necessary.

The healthcare sector must continue to establish a risk-weighted approach to total networking and remote access to digital data, as well as an appropriate sector-specific culture. Germany's Federal Office for Information Security (BSI) wrote in its final report[2] on the ManiMed (Manipulation of Medical Devices) project that vulnerabilities were found in every product. In almost all cases, IT security was affected and not patient safety directly.

---

1 See section 4.6.3 and MELANI Semi-annual report 2019/2, section 4.5.1

2 ManiMed final report (bsi.bund.de)

3.4 Data traces from medical products

In addition to medical devices, there are a large number of other medical products.[3] These include a wide variety of consumables for tests and operations. For example, various disposable invasive products are tracked for quality assurance reasons. In the case of expensive products that do not have an unlimited shelf life, each use is also recorded because large stocks are not kept and replacements have to be ordered shortly before use. Medical implants such as hip and knee prostheses are registered in the Swiss Implant Registry (SIRIS).[4] This also contributes to quality assurance. The registry is intended to make it possible to assess the long-term quality of implants and treatment. In addition, it serves as an early warning system for product and process errors.

The traceability of products used for tests and treatments undoubtedly increases the safety of patients' health. At the same time, however, attention must be paid to the confidentiality and integrity of the stored data; access to and processing of the data must be traceable.

3.5 Cyberthreats

Hospitals and other healthcare providers are exposed to the same cyberthreats as all companies that have an internet connection and work with computers. For this reason, access to data and systems in the healthcare sector must also be secured with multi-factor authentication, if possible, and malware infections must be prevented or at least detected and remedied promptly. Another important protective measure is to raise employee awareness regarding the secure use of IT resources and to highlight cyberthreats such as social engineering.

While the threats are very similar or even the same in most sectors, the consequences of successful attacks in the healthcare sector do have some specific characteristics. On the one hand, data leaks usually affect unalterable and sensitive personal data, and on the other hand, functional failures of IT systems or even temporary unavailability of data can endanger people's health or even their lives.

3.6 Example: Extortion with patient data

For several years now, encryption Trojans (ransomware) have proliferated as a successful criminal business model that is also used against hospitals. Nowadays, the perpetrators download as much data as possible before encrypting the files on the victims systems in order to have an additional means of extortion. At a psychotherapy company in Finland, extortionists unsuccessfully tried to get money from the company to prevent the publication of patient data and details of therapy sessions. The criminals subsequently tried to blackmail the patients in question directly.[5]

---

[3] Medical Devices Ordinance (MedDO, SR 812.213), Art. 1.

[4] Swiss Implant Registry SIRIS (siris-implant.ch)

[5] Vastaamo fires CEO for hiding another data breach in March 2019 (foreigner.fi); Cyberblackmailers in Finland: Welcome to dystopia (sueddeutsche.de)

3.7 In times of the pandemic

During a pandemic,[6] cases of illness can soar in a short period of time, stretching the healthcare system to its capacity limits. If cyberincidents then occur that lead to functional restrictions for healthcare providers, this may have life-threatening consequences. The case of Düsseldorf University Hospital, which was affected by ransomware in September 2020, attracted worldwide attention.[7]

The Hirslanden Group fell victim to ransomware in the summer of 2020. However, it was possible to restore the encrypted data with the help of backups, and patient care was reportedly not at risk at any time.[8] At two other hospitals in Switzerland, infections with the Emotet[9] Trojan were detected and remedied at an early stage.

During a pandemic, healthcare workers are under extraordinary strain and often overworked. People are more likely to fall for social engineering methods when they are already under pressure due to external circumstances. A key feature of social engineering involves creating a sense of urgency. The accumulation of real and artificially created pressure increases the chances of such attacks succeeding. The risk of clicking on a malicious link in an email or opening a harmful attachment rises when people are in a hurry. In addition to implementing technical measures, all employees should be made aware of the dangers of social engineering. Administrative processes should be established to detect fraud attempts and other social engineering attacks.

Recommendation/conclusion:

Supporting technical solutions that are to be newly introduced in the course of digitalisation must firstly be designed as securely as possible and, secondly, the individuals who are to work with them must be trained in their correct and secure use. It is hard to imagine healthcare and everyday life without digital aids and they will continue to gain in importance.

---

6 See also the key topic in chapter 3 of the MELANI Semi-annual report 2020/1

7 Düsseldorf University Hospital: "DoppelPaymer" ransomware is said to be behind the attack (heise.de)

8 Hirslanden hit by cyberattack: Threat remains high (nzz.ch)

9 See section 4.3.2

4 Situation

4.1 Overview of reports to the NCSC

In the second half of 2020, the NCSC contact point received a total of 5,542 reports from private individuals and companies.[10]

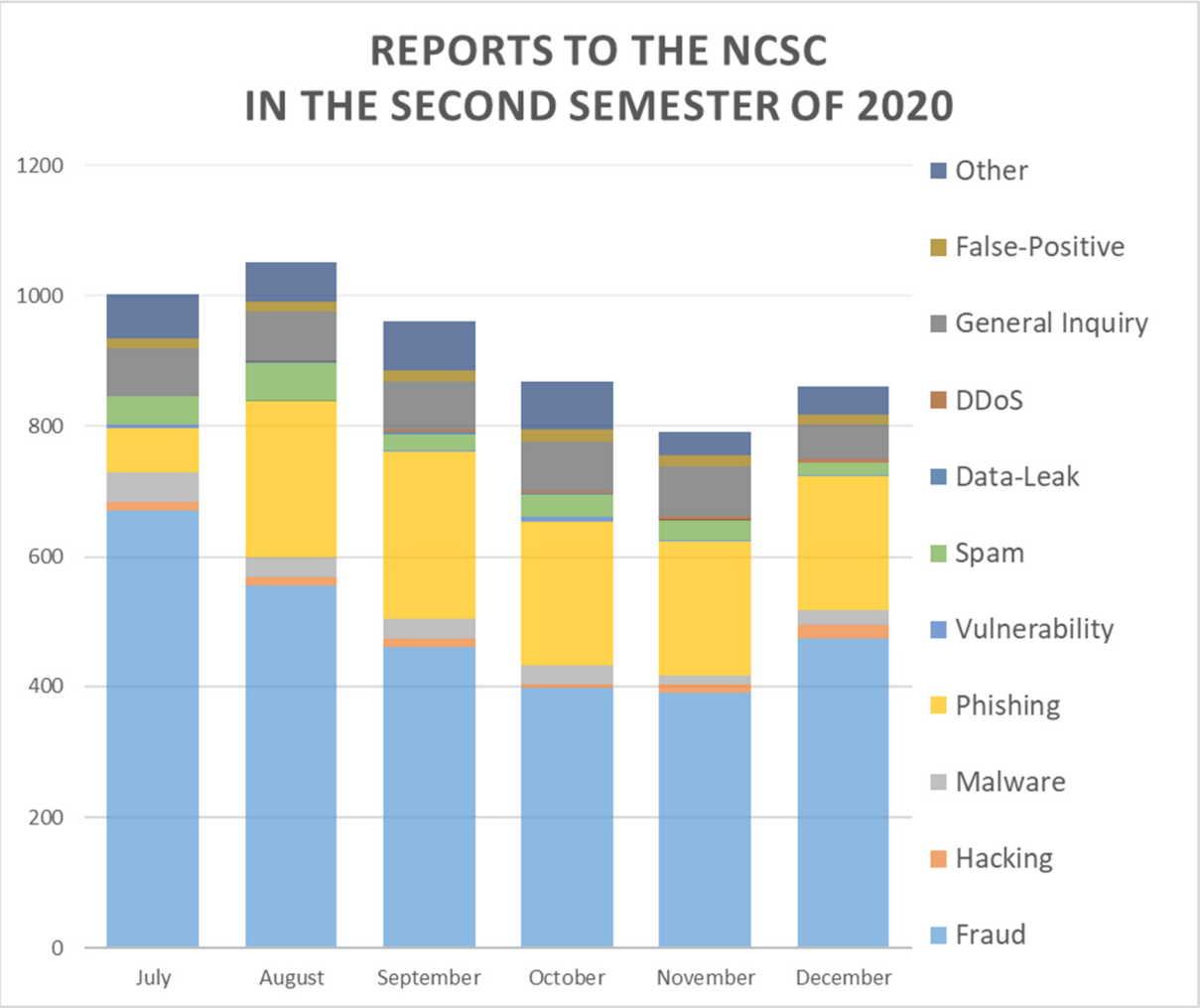


Fig. 1: Reports to the NCSC in the second half of 2020

Reports of fraud continue to account for the largest share, with 2,917 reports. Types of online fraud include the following:

Advance fee scams:

Advance fee scams remain the most frequently reported type of fraud, with 1,120 notifications.[11] Emails of this type are still being sent in large numbers, although their success is likely to be low. Only in one reported case was the recipient actually deceived and a financial loss suffered.

---

[10] Statistics can be found on our website: Current figures (ncsc.admin.ch)

[11] Information on our website about Advance-fee scam (ncsc.admin.ch)

Fake sextortion:

With 353 reports, reports of fake sextortion emails[12] also stand out. These emails claim that photographic or video material has been created showing the recipient during an alleged visit to pornographic websites. The blackmailers use a variety of methods to try to convince the victims that these claims are true. In one variant, the recipient's address is used as the sender. This suggests that the attacker has control of the email account. In actual fact, the sender is simply spoofed and hence bogus. In another variant, a password belonging to the victim is cited as "proof". However, these are passwords from old data leaks.[13]

Fee scams:

210 reports were received in relation to supposed fees to be paid. Most of these were emails announcing a parcel delivery. The most common (180 reports) were emails claiming to be from the Federal Customs Administration (FCA) and requesting payment of customs fees, usually in the amount of CHF 75.00. Recipients are told to buy "Paysafe" cards and send the card number by email. The same category of emails includes the numerous messages supposedly from parcel service providers such as Swiss Post, DHL or DPD, which claim that additional fees should be paid by credit card for the dispatch of a parcel.[14]

Classified ads, fake support, CEO fraud:

In addition to 145 reports of classified ad scams[15] and 130 on fake support calls,[16] cases of so-called CEO fraud[17] stand out, with 111 reports. In these cases, the attackers obtain information about a company or association from various public sources and then try to persuade the person contacted by email, using a fake sender, to trigger a supposedly urgent payment.

4.2 New reporting form

The NCSC's new reporting form went live on 21 December 2020. By answering a maximum of four questions, anyone who reports an incident will receive an initial automated assessment and helpful information. This user interface allows quick and uncomplicated reporting and at the same time allows each incident to be classified. The possibility to enter further information on a voluntary basis at the end enables the NCSC to provide even better support to those who report cyberincidents, if required. Reports from the public make an important contribution to the NCSC's ability to quickly identify trends, take appropriate countermeasures and obtain a complete picture of the cybersituation.

---

12 Information on our website about Fake sextortion (ncsc.admin.ch)

13 See Have I Been Pwned: Check if your email has been compromised in a data breach (havibeenpwned.com)

14 See section 4.8.2

15 Information on our website about Classified ad scam (ncsc.admin.ch)

16 Information on our website about Fake-Support (ncsc.admin.ch)

17 Information on our website about CEO-fraud (ncsc.admin.ch)

4.3 Malware

4.3.1 Ransomware

Encryption Trojans (ransomware) are among the incidents with the greatest potential for damage. In the second half of 2020, the NCSC received 34 reports on these from various economic sectors in Switzerland. Around 80% of the reports concerned small and medium-sized enterprises (SMEs).

As already discussed in previous semi-annual reports, ransomware is used to encrypt a victim's data and render it unusable. In order to decrypt the data, the victims are required to pay a ransom to the blackmailers. Since backups of the data are often available and victims do not comply with demands for payment, criminals have begun to implement a double blackmail tactic. Before the encryption attack, the victim's data is siphoned off. If the encryption blackmail does not achieve the desired success, they threaten to publish the data or sell it on the underground market.

Ransomware incidents can significantly disrupt business operations. The threat is particularly existential if backups have also been encrypted. The costs of system downtime and information unavailability, as well as incident response, are immense. In such incidents, communication from the victims to customers and business partners varies in practice; ranging from complete silence to transparent disclosure.

Recommendations:

Ransomware can cause considerable damage, especially if data backups are also affected. In the event of such an incident, remain calm and act with caution. Important aspects of incident management are finding the infection path and preventing a reinfection. Reboot the affected systems and restore data with existing backups.

If the necessary expertise is not available in your company, seek support from a specialised company.

Further information on the NCSC website: Ransomware (ncsc.admin.ch)

Incidents in Switzerland and internationally

In Switzerland, ransomware incidents at the helicopter manufacturer Kopter,[18] the electrical company Huber + Suhner[19] and also at the Hirslanden Group[20] became public knowledge in the second half of the year.

Internationally, for example, the IT service provider Sopra Steria[21] was affected, and it estimated the damage caused by the failure of its IT to be as much as EUR 50 million. A notable case occurred in the health sector in Germany: the data of the Düsseldorf University

[18] Ransomware hits helicopter maker Kopter (zdnet.com)
[19] Huber + Suhner crippled by cyberattack (inside-it.ch)
[20] Hirslanden hit by cyberattack: Threat remains high (nzz.ch)
[21] Cyberattack costs Sopra Steria up to EUR 50 million (inside-it.ch)

Hospital[22] was encrypted. However, the extortion demand was sent to the university, which the cybercriminals actually wanted to attack. In the United States, various educational institutions were also affected in this way. The ransomware actors also stole confidential student data and threatened to publish it if the institutions did not pay a ransom.[23]

A further escalation in ransomware extortion tactics

In order to put pressure on victims, some ransomware perpetrators now also pick up the phone and call affected companies. For example, they threaten to inform journalists about a security vulnerability within the victim's company or to publish sensitive documents on so-called data leak sites (DLSs).

Ransomware operators improve resilience

Many ransomware operators are already using the dual extortion tactic of encryption and data leaks. With this tactic, it is essential for the criminals to protect data leak sites (DLSs) against "takedowns" by law enforcement. Operating DLS infrastructures in countries where relationships with law enforcement in other countries may not be coherent can significantly complicate the takedown process. In addition, the stolen data is often replicated across multiple servers. An intervention on a single server will therefore not remove the data from the network.

New ransomware group Egregor follows in the footsteps of Maze

The group appears to have been active since September 2020. In October 2020, it attacked a few individual targets, particularly in the United States, including the American bookseller Barnes & Noble[24] and the video game developers Ubisoft and Crytek.[25] This was followed by a massive increase in attacks, which also disrupted Metro Vancouver's operations, for example.[26] Egregor appears to have filled the gap left by the apparent termination of the Maze ransomware gang's activities in October 2020. In Switzerland, no incident involving Egregor had been reported by the end of 2020.

Ransomware gang hacks Facebook account to post extortion ads

The Italian spirits company Campari Group was the victim of a ransomware attack. Using a hacked Facebook account, the perpetrators then took out ads warning Campari that its data would be made public if it did not pay the ransom. The Facebook ad was titled "Security breach of Campari Group network by Ragnar Locker team" and warned that more sensitive data would be released.

This new tactic of advertising attacks on Facebook illustrates the continued evolution of ransomware extortion.[27]

---

22 Düsseldorf University Hospital: "DoppelPaymer" ransomware said to be behind attack (heise.de)
23 K12 education giant paid the ransom to the Ryuk gang (securityaffairs.co)
24 Cyber-Attack on Major US Bookseller (infosecurity-magazine.com)
25 Ubisoft, Crytek data posted on ransomware gang's site (zdnet.com)
26 Vancouver Metro Disrupted by Egregor Ransomware (threatpost.com)
27 Ransomware Group Turns to Facebook Ads (krebsonsecurity.com)

4.3.2 Emotet

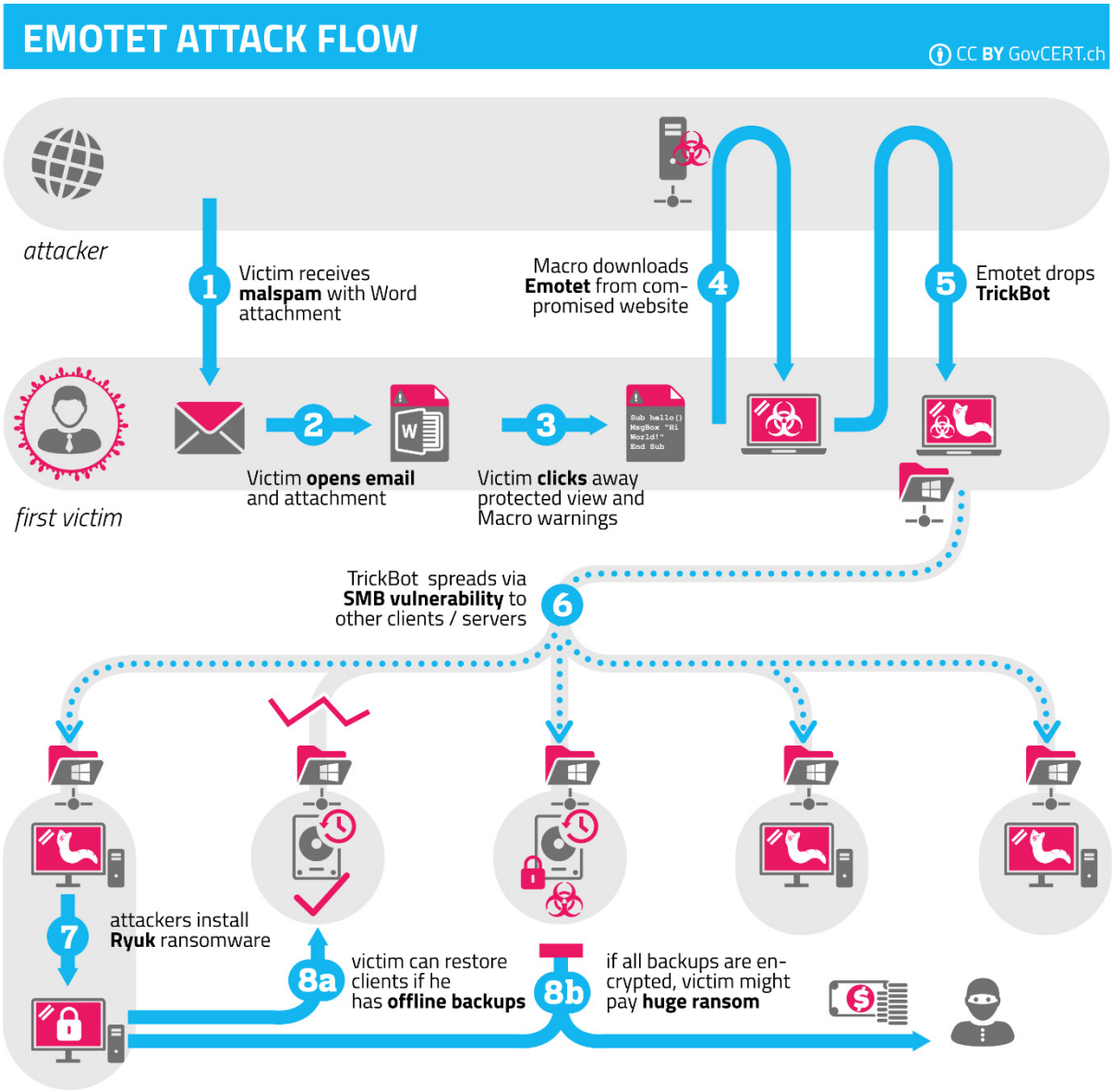


Fig. 2: Emotet infection sequence

After a lull of several months, the NCSC again observed various spam waves involving Emotet malware from July 2020 onwards. Although Emotet was less active overall in the second half of 2020 than in the first, it was again among the most widespread types of malware in Switzerland and abroad at the end of the year.[28] Originally known as an e-banking Trojan, Emotet was more recently used primarily for sending spam and subsequently loading other malware.

In November 2020, the NCSC warned[29] in particular of increasing Emotet activity, as this malware is specifically used to infect computers and servers in networks with ransomware such as Ryuk. Only Windows computers and servers are affected.

---

28 See URLhaus statistics (abuse.ch)

29 Emotet Trojan active again (ncsc.admin.ch)

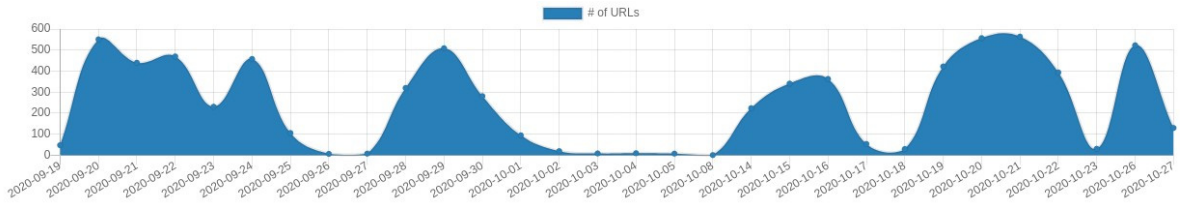


Fig. 3: Number of URLs observed in connection with Emotet; wave-like progression of Emotet activities

The Emotet infrastructure was successfully seized during the international law enforcement operation LADYBIRD, which was made public on 27 January 2021. The Netherlands, Germany, France, Lithuania, Canada, United States, United Kingdom and Ukraine participated in the operation.[30] Operation LADYBIRD seems to have been successful so far, and the operability of the botnet has been permanently disrupted. Emotet is, however, known for dynamic further developments following longer breaks in activity. It is possible that those behind Emotet will succeed in building new infrastructures and resume their criminal activities.

Recommendations:

- The execution of unsigned Office macros should be blocked by technical means. Office documents with macros should already be recognised on the email gateway or spam filter and not be delivered to the recipients at all. Password-protected ZIP files should also be recognised on the email gateway and delivered only after verification.
- Websites that are actively used for spreading Emotet should be blocked at the network perimeter. A list of these websites is provided free of charge by URLhaus (abuse.ch), for example.
- Servers that are used to control devices infected with Emotet must be blocked. A list of IP addresses that can be attributed to Emotet is published at Feodo Tracker (abuse.ch), for example.

Further measures and detailed information can be found on our website:

Information security checklist for SMEs (ncsc.admin.ch)

Update ransomware: new procedure (ncsc.admin.ch)

4.3.3 Trickbot

In the second half of 2020, Trickbot remained a major threat to businesses and organisations. Since its emergence in 2016, this malware has become specialised as a propagation vector for various types of attacks, most notably ransomware attacks.[31] In mid-October, several security actors attempted to dismantle the Trickbot control network.[32] However, the operations had only a limited effect and could not permanently shut down Trickbot.

---

30 World's most dangerous malware EMOTET disrupted through global action (europol.europa.eu)

31 See MELANI semi-annual reports 2018/2, section 4.5.4; 2019/1, sections 3.4.1 and 4.6; 2019/2, section 4.6.1 and blog post Trickbot - An analysis of data collected from the botnet (govcert.admin.ch)

32 Attacks Aimed at Disrupting the Trickbot Botnet (krebsonsecurity.com);
Cyber Command, Microsoft take action against Trickbot botnet before Election Day (cyberscoop.com);
Microsoft and others orchestrate takedown of TrickBot botnet (zdnet.com)

4.4 Attacks on websites and web services

4.4.1 DDoS attacks

A common approach used by criminals is to first carry out what tends to be a short demonstration DDoS attack on a target to demonstrate their basic skills. In an extortion email, the perpetrators then demand payment in a cryptocurrency (e.g. bitcoin). The blackmailers claim that they have a significantly stronger attack capacity than they used for the demonstration attack and threaten follow-up attacks. However, these usually fail to materialise. In exceptional cases – especially if the demonstration attacks have already led to significant restrictions – the follow-up attacks are actually carried out. However, these never reach the threatened capacity. As was already the case in the first half of 2020,33 such attacks continued to increase internationally in the second half of the year. Analysts at Nexusguard34 reported an overall 287% increase in DDoS attacks in the third quarter relative to the same period a year earlier.

Since August, a global DDoS extortion attack campaign has been detected in various sectors of the economy. The FBI even warned US companies that thousands of organisations around the world from a wide range of industries would be threatened with DDoS attacks within six days.

The NCSC did not detect a significant increase in DDoS attacks in Switzerland in the first half of the year, although this changed in the second half. Switzerland was not spared from the global DDoS wave mentioned above. In this country, too, various economic sectors, especially the financial and energy sectors, were affected by DDoS attacks and respective extortion demands in August. During the period under review, 19 DDoS attacks were reported to the NCSC. The maximum traffic volumes were between 150Gbit/s and 200Gbit/s. In the extortion demands, the attackers often adopted the names of notorious state groups such as Lazarus or FancyBear in order to scare the victims and make them pay. In November, the attackers returned and tried to blackmail some of the same companies again (once again unsuccessfully).

Conclusion/recommendation:

DDoS extortion is a large-scale business. Attackers try their luck with as many companies as possible in a relatively undifferentiated manner. If the defence works, they typically move on in search of more promising targets. However, if they are able to successfully disrupt a company's systems with a (demonstration) DDoS attack, it becomes their focus of attention as a potential victim and the attackers intensify their efforts in the hope that a ransom will be paid. Accordingly, it is beneficial to be adequately prepared for any DDoS attacks.

For business-critical systems, the NCSC recommends subscribing to a commercial DDoS mitigation service. Many internet service providers (ISPs) offer such a service for a corresponding surcharge.

Various preventive and reactive measures to deal with DDoS attacks can also be found on our website: Attack on availability (DDoS) (ncsc.admin.ch)

33 See MELANI semi-annual reports 2020/1, section 4.2.2

34 DDoS Threat Report 2020 Q3 (nexusguard.com)

4.4.2 Compromised websites

Attackers can access the website administration with stolen access data or via unpatched security vulnerabilities and place arbitrary code there.

The effects of compromised websites are manifold. The essential point is that, as a result of a compromise, the confidentiality and integrity of the data entered and stored can no longer be guaranteed.

Since the underground market is organised according to the division of labour, we also observe the regular phenomenon of the use of compromised websites by different actors: access to a website administration can be sold and passed on several times. If the attack vector is a security vulnerability, different actors can also compromise a website independently of each other. This places high demands on website administrators to truly remove all malicious code during clean-up.

Recommendations:

If a website has been hacked, a systematic clean-up is required involving the localisation and removal of the malicious code on the website. Furthermore, the latest versions of the content management system (CMS) and the plug-ins must be installed. All computers used for website administration must be scanned for malware and cleaned if necessary. Finally, all access passwords must be changed. Further information can be found on our website:

Hacked website – what next? (ncsc.admin.ch)

After cleaning up the website, additional measures are recommended to prevent cybercriminals from gaining access again in the future. On our website, you can find

Measures to secure content management systems (CMS) (ncsc.admin.ch)

4.4.3 Crypto scams

The hype surrounding cryptocurrencies is flourishing in a wide variety of ways – including many fraudulent ones. The term "crypto scam" covers a broad range of phenomena: fraudulent investment offers, bogus trading platforms (including the relevant app) and even completely fictitious cryptocurrencies. A scam can also start with a compromised social network account. This is what happened in July 2020: in a spectacular attack, 130 Twitter accounts of prominent people and companies were hacked.[35] Tweets were sent using the accounts of Barack Obama, Joe Biden, Elon Musk, Mike Bloomberg and Bill Gates, promising rewards for money transfers to a specific bitcoin address:

[35] 2020 Twitter bitcoin scam (en.wikipedia.org)

Fig. 4: Example of a message on a hacked account

The attack lasted only a few minutes, during which around USD 180,000 were transferred to bitcoin accounts held by the hackers.

4.5 Industrial control systems (ICSs)

The digital control of physical processes plays a large part in the standard of living to which society has become accustomed, especially in industrialised nations. The smooth operation of such systems therefore presents a worthwhile target for attackers. In parallel, the increase in the degree of automation and networking of these systems poses an ever greater challenge for operators to meet the requirements to secure them.

4.5.1 Threats against ICSs are becoming more diverse

Many previous semi-annual reports highlighted threats that also target industrial control systems (ICSs). In recent months, there have been new insights into some of the responsible actors, but at the same time new threat forms and actors have emerged.

The US Department of Justice charged six members of a unit of the Russian military intelligence agency GRU in October 2020.[36] The group, dubbed Sandworm by private security contractors, is blamed for the power outages in Ukraine in late 2015 and 2016, as well as the destructive malware NotPetya, among other things. A few days later, the US Department of the Treasury sanctioned a Russian research institute that had been involved in the attacks with the Triton/Trisis malware.[37] These attacks attempted to undermine industrial process safety systems (safety instrumented system, SIS), which are supposed to guarantee that neither people nor machines are harmed in the event of a plant malfunction. In a joint alert,[38] the American FBI and the cybersecurity agency CISA warned about incidents associated with the

---

36 Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (justice.gov);
US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit (wired.com)

37 US Treasury sanctions Russian research institute behind Triton malware (zdnet.com)

38 Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets (cisa.gov)

Berserk Bear group. Although the US authorities did not observe any sabotage attempts by the intruders, they suspect from the modus operandi that these could at least have been prepared.

Several attacks on water supply systems in Israel were attributed to Iranians.[39]

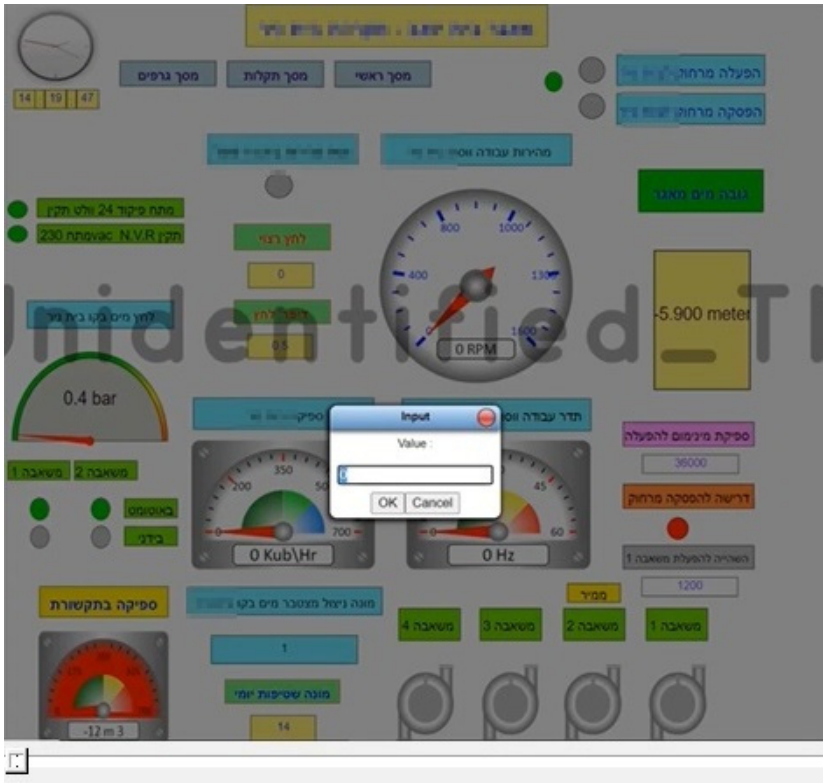


Fig. 5: Excerpt from the demonstration video of the open water supply control

In addition to water, electricity remains at risk from cyberincidents. Indian authorities suspect a cybersabotage attempt was behind a power outage in Mumbai on 13 October 2020.[40]

Politically and militarily motivated attacks against critical infrastructures continue to be observed mainly in the context of conflicts that have already escalated.

However, ransomware attacks that also involve industrial processes continue to pose a threat to operators of critical control systems, as the EKANS[41] malware has demonstrated several times.

4.5.2 Challenge of securing the supply chain during the digitalisation of industrial processes

Control systems consist of various components from different manufacturers or open source projects. If a vulnerability appears high up in the supply chain (e.g. in a basic component that is embedded in another product), it is often difficult for system operators to assess whether

39 Two more cyber-attacks hit Israel's water system (zdnet.com);
What We've Learned from the December 1st Attack on an Israeli Water Reservoir (otorio.com)

40 October Mumbai power outage may have been caused by a cyberattack (securityaffairs.co)

41 This is how EKANS ransomware is targeting industrial control systems (zdnet.com)

their controls, sensors and actuators are affected by the vulnerability, let alone how the vulnerability can be fixed in their specific implementation.

This problem was exemplified when various vulnerabilities were discovered in open source projects that allow the use of network protocols in a wide variety of devices. The group of vulnerabilities, dubbed AMNESIA:33[42] by those who discovered them, affected over a hundred component and device manufacturers. The NCSC was involved in working with affected manufacturers in Switzerland to facilitate the coordinated disclosure of the vulnerabilities and the provision of updates.

To help critical infrastructure operators address these multi-layered challenges, the NCSC is lending its expertise to the canton of Zug's initiative to establish a National Test Institute for Cybersecurity (NTC).[43]

4.6 Data leaks

Data leaks remain a common phenomenon and occur in a wide variety of contexts. In some cases, stolen data is reused by the attackers themselves. Much more often, however, it is sold on the underground market or published in hacker forums. Many data leaks are not noticed until the corresponding offers appear. Certain players also try to blackmail the victims by threatening to publish the data. In the case of ransomware, this has become part of the players' business model, in addition to the encryption of data.

The high monetary value of certain types of data, such as medical data, client or identity data, and to a lesser extent banking data, make them prime targets. Intellectual property data is likewise highly coveted and the target of advanced espionage campaigns.

4.6.1 Swiss citizens' data stolen in Argentina

At the end of August 2020, tens of thousands of sets of personal data, including those of around 11,000 Swiss citizens, were stolen in a ransomware attack on the Argentine immigration authorities.[44] After the affected authority failed to pay a ransom, the thieves published the data on the dark web. The data included the surname, first name, date of birth, passport number and destination of those affected, but no copies of passports.

4.6.2 Access data in the hands of hackers

In August 2020, it was discovered that hackers had stolen IP addresses, user names and passwords for more than 900 Pulse Secure VPN enterprise servers[45] and subsequently published them on a Russian hacker forum. The data is used for attacks by ransomware groups that frequent these forums. Following this data theft, the NCSC contacted the Swiss

---

42 AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices (forescout.com)

43 Canton of Zug plans national test centre for IT hardware (netzwoche.ch); Confederation participates in the establishment and operation of the National Test Institute for Cybersecurity (parlament.ch)

44 Argentina hack reveals data on thousands of Swiss travellers (swissinfo.ch)

45 Hacker leaks passwords for 900+ enterprise VPN servers (zdnet.com)

companies concerned and informed them of the situation so that they could change the affected access credentials.

4.6.3 Unintentionally exposed data

The disclosure of sensitive data does not have to be the result of a cyberattack; it can also come from a configuration error by organisations themselves. According to a report by security firm Risk Based Security, data leaks are unintentional in 69% of cases with internal involvement.[46] For example, the UK security firm Sophos was made aware that its customer data was visible online.[47] The intensive use of cloud platforms reinforces this phenomenon, as these require error-free configuration. The US pharmaceutical giant Pfizer, for example, made an error in the configuration of a Google cloud platform, exposing patient data, notably concerning cancer treatments.[48] In an investigation of internet resources, the cybersecurity firm CybelAngel found more than 45 million openly accessible medical images, including patient data, distributed across more than two thousand unprotected servers.[49]

Conclusion/recommendations:

The careful and responsible handling of data is an important topic for companies. In addition to appropriate security measures, every company should also prepare for a data breach scenario and draw up a corresponding response plan in advance. This will enable rapid and coordinated action in the event of an incident.

Further information on the NCSC website: Data leak (ncsc.admin.ch)

4.7 Espionage

4.7.1 COVID-19 and espionage

The COVID-19 pandemic led to an international race in medical research into the virus and in particular with regard to the development of vaccines. While warnings of espionage attempts in the field of vaccines had already been published in the first half of 2020,[50] the second half of 2020 saw several publicly confirmed cyberespionage attacks on medical research institutions and pharmaceutical companies. However, no new techniques and tactics have yet been observed. In addition, public authorities also remained reconnaissance targets for COVID-19-related espionage campaigns, especially in the area of medical treatments, such as the approval of medical products.

The UK National Cyber Security Centre (NCSC UK), together with the Canadian Communications Security Establishment (CSE) and the US Cybersecurity and Infrastructure

46 2020 Year End Data Breach QuickView Report (riskbasedsecurity.com)
47 Sophos notifies customers of data exposure after database misconfiguration (zdnet.com)
48 Pharma Giant Pfizer Leaks Customer Prescription Info, Call Transcripts (threatpost.com)
49 More Than 45 Million Unprotected Medical Images Accessible Online (cybelangel.com)
50 See MELANI semi-annual report 2020/1, section 4.6.1

Security Agency (CISA), published a document on 16 July that attributed cyberespionage attacks on COVID-19 vaccination research to APT29 and specifically referred to the Wellmess malware.[51] APT29 is also known as Dukes or CozyBear and is often associated with Russia.[52]

Microsoft warned in September about reconnaissance campaigns against research institutions and companies in the area of vaccine development[53] and published observations of cyberattacks on seven vaccine research companies in November.[54]

In November, the European Medicines Agency (EMA) was the victim of a targeted cyberattack. The origin, extent and consequences of this are not yet known for certain due to the ongoing investigations.[55] Pfizer and Moderna published media releases confirming that intruders stole documents related to their vaccine development from the EMA's systems.[56] At the beginning of 2021, stolen data concerning the Pfizer/Biontech COVID-19 vaccine was published on the internet.[57] The perpetrators are not yet known and the case is still under investigation.

In December, Kaspersky Lab published a report that claimed the North Korean hacker group Lazarus was responsible for cyberespionage attacks on a pharmaceutical company in September and an attack on a health ministry in October, in which various types of malware were used.[58]

Conclusion:

All those involved in COVID-19 research and especially in vaccine development must expect espionage attacks from various sources. Both public and private sector organisations are interested in corresponding data, research results and trade secrets.

4.7.2 Supply chain attack: SolarWinds Orion IT

On 13 December, US authorities reported that an attacker group had infiltrated their network via a compromised update of the Orion IT software. A backdoor had been built into the official program update in March 2020. Around 18,000 users of this software had downloaded the update. The attackers chose targets of interest among them to continue their attack, and closed the backdoor again for the collateral victims.

According to US sources, this operation was part of a larger espionage campaign that hit other companies, and the procedure showed similarities to that of APT29.

---

51 Advisory-APT29-targets-COVID-19-vaccine-development.pdf (ncsc.gov.uk)

52 APT 29 (Threat Actor) (fraunhofer.de)

53 Microsoft report shows increasing sophistication of cyber threats (microsoft.com)

54 Cyberattacks targeting health care must stop (microsoft.com)

55 Cyberattack on the European Medicines Agency (europa.eu)

56 Statement on Cyberattack on the European Medicines Agency (modernatx.com); Statement Regarding Cyber Attack on European Medicines Agency (biontech.de)

57 Hackers leak stolen Pfizer COVID-19 vaccine data online (bleepingcomputer.com)

58 Lazarus covets COVID-19-related intelligence (securelist.com)

Conclusion/recommendation:

By compromising a service provider, the attackers gained upstream access to their targets. This so-called supply chain attack strategy has become increasingly common in recent years (see AVAST CC Cleaner, ASUS, Cloud Hopper). It is particularly interesting because it allows access to several targets at the same time and conceals the intrusion better in the initial phase. The final targets of such campaigns are typically significant for the attackers and this selection influences which supplier is chosen as a means to an end. In the future, however, the supply chain attack method is likely to be used by opportunistic attackers to generate as many victims as possible.

Aside from a reference base for permissible communication in your own network to detect anomalies, it is advisable when concluding service contracts to define the information and messages that a service provider must communicate in the event of an attack.

4.7.3 Backdoors in Chinese tax software

In the summer of 2020, security firm Trustwave uncovered two malware programs called GoldenSpy[59] and GoldenHelper[60] in tax software introduced for Western companies established in China. The programs allow remote access to the client system. Among the Trustwave clients, a company active in the field of new technologies and a large financial institution were affected.

Conclusion/recommendations:

To protect themselves from spyware, companies should install officially prescribed software on a computer separate from the rest of the network.

Concrete measures for this case:

- Include the indicators of compromise (IOCs) in the FBI flash in the threat monitoring system (and observe any new IOCs).
- If companies have already installed this software, treat this as a potential incident and follow Trustwave's recommendations.

4.8 Social engineering and phishing

The variety of content tactics used in phishing and other social engineering attacks is almost endless and very wide-ranging. They involve more or less original stories with alleged incidents that appear to be related to everyday life.

59 'GoldenSpy' Malware Hidden In Chinese Tax Software (securityweek.com)

60 Researchers Find More Malware Delivered via Chinese Tax Software (securityweek.com)

4.8.1 Phishing overview

In the second half of the year, 4,498 phishing websites which had been reported via the antiphishing.ch portal operated by the NCSC were deactivated. Compared to 3,029 phishing websites in the first half of the year, this represents an increase of over 30%.

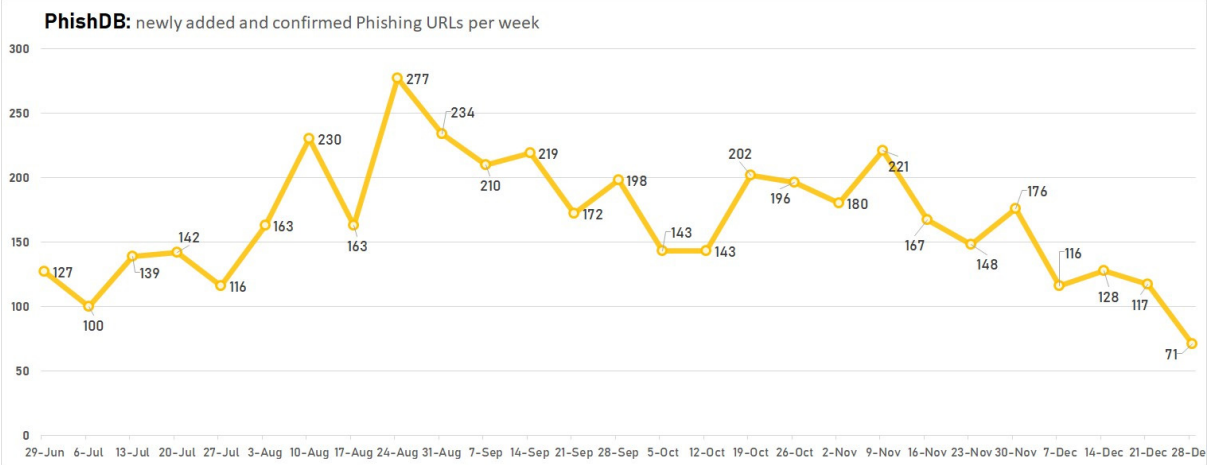


Fig. 6: Number of phishing URLs checked and confirmed by the NCSC per week in the second half of 2020.
Current data can be found at: https://www.govcert.admin.ch/statistics/phishing/

Some campaigns used fake messages from telecommunication companies, purporting to refund a duplicate payment. Other campaigns used fake logos from financial institutions and public transport companies. The aim of phishing is typically to obtain login details to the relevant online portal, credit card details, mobile phone numbers and other information.

In numerous campaigns, attempts were made to intercept security codes if sent via text message in order to overcome two-factor authentication.

Note:

Further information on our website on phishing (ncsc.admin.ch)

4.8.2 Parcel delivery phishing scenario

As a result of the pandemic, there was an increase in online shopping also in the second half of 2020. Therefore the probability that people were expecting parcels was high. Various phishing campaigns via email and text message picked up on this situation and exploited it.

Bogus fee for parcel redelivery (via email)

Emails from a well-known parcel delivery service advised that a parcel could not be delivered due to a problem. A fee was due for redelivery, so that the parcel could be delivered again, usually very shortly afterwards (within 24 hours). A link directed recipients to a fake website, which could barely be distinguished from the original. In order to make the payment, people had to give their name and credit card details. Visually, the impression was given that the entire payment process had been carried out correctly. Entering these details enabled the criminals to use the credit card for their own purchases.

Bogus fee for retained parcels (via text message)

In another variant, a text message purporting to be from a parcel delivery service claimed that a parcel had been retained due to insufficient postage. In order to confirm the delivery, the recipient had to click on the link in the text message. The link, however, led to a website designed by cybercriminals, on which personal details and credit card details had to be entered. As a result, monthly charges were made to the victim's card or, in some cases, the entire account was plundered.

4.8.3 Theft of Apple ID or installation of spyware (via text message)

Text messages with the message: "You have a SWISS POST consignment" and a link led to different websites depending on the type of mobile phone. Apple users were asked to enter their Apple ID on a phishing page. Android users were asked to install an app. The app was spyware that spied out data and also contained a backdoor. The numbers used to send the messages came from infected mobile phones or were bogus numbers.

4.8.4 Misuse of Google services for phishing

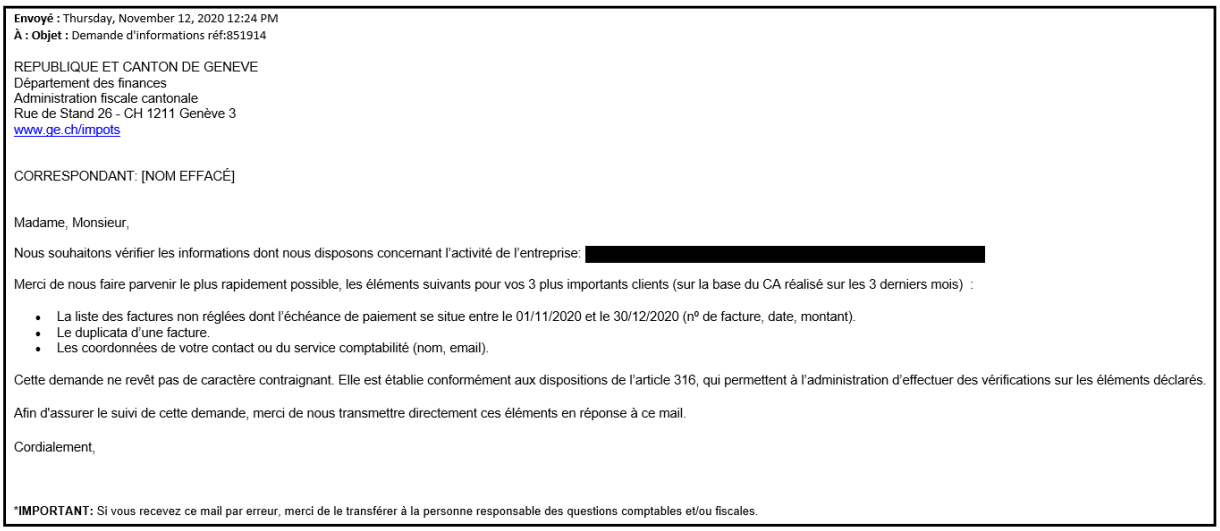
The security firm Armorblox[61] recently analysed how cybercriminals misuse a number of Google services for phishing or scam campaigns. In most cases, the attackers' goal is to steal sensitive data (login details, banking information and personal data). Very few companies block Google services, which has proven to be an efficient way for attackers to bypass security mechanisms. This is especially true when they combine this tactic with advanced social engineering methods to convince victims to download a file or fill out a form, for example.

4.8.5 Misuse of tax authority identities

Familiarity and urgency are essential mechanisms of social engineering. As a result, cybercriminals regularly make use of the identity of public authorities and, in particular, tax authorities to obtain sensitive information. In November 2020, several dozen companies received emails purporting to be from employees of the Geneva cantonal tax authority. The emails requested client data and payment of outstanding invoices. This was most likely in preparation for wire fraud. The Geneva tax authority warned the public on its website and in a newsletter.[62] 37 companies reported receiving fraudulent emails of this type.

---

61 OK Google, Build Me a Phishing Campaign (armorblox.com)
62 The AFC warns companies of phishing attempts (ge.ch)



Envoyé : Thursday, November 12, 2020 12:24 PM
À : Objet : Demande d'informations réf:851914

REPUBLIQUE ET CANTON DE GENEVE
Département des finances
Administration fiscale cantonale
Rue de Stand 26 - CH 1211 Genève 3
www.ge.ch/impots

CORRESPONDANT: [NOM EFFACÉ]

Madame, Monsieur,

Nous souhaitons vérifier les informations dont nous disposons concernant l'activité de l'entreprise: [redacted]

Merci de nous faire parvenir le plus rapidement possible, les éléments suivants pour vos 3 plus importants clients (sur la base du CA réalisé sur les 3 derniers mois) :

- La liste des factures non réglées dont l'échéance de paiement se situe entre le 01/11/2020 et le 30/12/2020 (nº de facture, date, montant).
- Le duplicata d'une facture.
- Les coordonnées de votre contact ou du service comptabilité (nom, email).

Cette demande ne revêt pas de caractère contraignant. Elle est établie conformément aux dispositions de l'article 316, qui permettent à l'administration d'effectuer des vérifications sur les éléments déclarés.

Afin d'assurer le suivi de cette demande, merci de nous transmettre directement ces éléments en réponse à ce mail.

Cordialement,

*IMPORTANT: Si vous recevez ce mail par erreur, merci de le transférer à la personne responsable des questions comptables et/ou fiscales.

Fig. 7: Example of a social engineering email

Recommendations:

Be careful when you receive unexpected messages. The sender and the legitimacy of the request should be checked. Take special care when passing on sensitive data and during financial transactions. In particular, raise awareness among employees in finance departments and key positions. If an erroneous payment has been made, contact your bank immediately. They may be able to stop or reverse the payment.

4.8.6 Spear phishing

Spear phishing is a sophisticated and targeted method of duping people into doing what the attacker wants them to do. This approach requires resources and time, which is why its use often points to state actors or well-organised gangs of perpetrators.

For example, Microsoft[63] reported on the activities of Phosphorus. This group, which is believed to be Iranian, attempted to get around 100 security experts to disclose their email account credentials. To do this, they set up bogus platforms for international security conferences taking place in Munich and Saudi Arabia. Once they had identified the security experts, they sent them invitations to the conferences. The targets were to enter their personal details with login and password on the supposed conference websites. With these details, the perpetrators could then access the victims' email accounts and steal data.

In other spear phishing attacks, attackers posed as recruiters and contacted their victims via the professional network LinkedIn and talked of the prospect of an interesting position. Various groups of players such as North Korean Lazarus[64] use this tactic. In operation “Dream Job”, this state group of perpetrators proceeded as follows:

1. A fake LinkedIn account is created posing as a recruiter for a large well-known company.

63 Cyberattacks target international conference attendees (microsoft.com)
64 Dream-Job-Campaign (clearskysec.com)

2. Exploratory phase: The perpetrators collect as much information as possible about their target person for later use.
3. Preparing the “dream job”: A false job offer is created that matches the target's wishes.
4. Contacting the victim: The bogus recruiter contacts the target person via their LinkedIn contact network; correspondence about the job offer follows via WhatsApp or email.
5. The details of the job offer are sent in a Word or PDF file enriched with malware, which the victim downloads via DropBox or OneDrive. Care is taken to send the file at a tactically favourable time so that the victim is at work and opens the file there.
6. Infection ensues and the perpetrators start spreading throughout the targeted network.
7. The bogus LinkedIn profile is deleted and the conversation is ended.

Once inside the corporate network, the attackers carry out espionage or business email compromise (BEC)[65] activities.

This tactic is highly cunning because it can assume that the parties involved will remain discreet. The current COVID-19 context, in which interest in secure jobs in large well-known companies has increased, seems to further favour this tactic.

5 Other topics

5.1 Reporting duty for critical infrastructures in the event of cyberattacks

In December 2020, the Federal Council took the fundamental decision that a general reporting duty should be introduced for operators of critical infrastructures in the event of cyberattacks and the discovery of security vulnerabilities.[66]

The exchange of information on cyberincidents has so far been on a voluntary basis with the NCSC. According to the national strategy for the protection of Switzerland against cyber-risks (NCS), the introduction of a reporting duty for critical infrastructures is to be examined. The Federal Council has now instructed the Federal Department of Finance (FDF) to draft a corresponding bill by the end of 2021. Taking into account existing reporting duties, criteria are to be defined as to who must report which incidents and within what time frame. No data about the individuals who submit reports is to be passed on. At the same time, the Federal Council wants to create a central reporting office.

The data collected from the reports will be used to systematically issue early warnings. The aim of this exchange of information is to detect attack methods at an early stage, to further improve the assessment of the threat situation and to further strengthen Switzerland's security.

---

65 On our website, you can find information on BEC (ncsc.admin.ch)

66 Federal Council supports a reporting duty for critical infrastructures in the event of cyberattacks (admin.ch)

5.2 Cantons want to better coordinate the fight against cybercrime

The police commanders of the cantons want to better coordinate the fight against cyber and paedophile crime. To this end, the Conference of Cantonal Police Commanders of Switzerland (CCPCS) and the Conference of Cantonal Justice and Police Directors (CCJPD) reached an agreement regulating the organisation and financing of the Network for Investigative Support in the Fight against Cybercrime (NEDIK). The agreement entered into force on 1 January 2021.[67]

NEDIK was established back in 2018 by the Conference of Cantonal Police Commanders of Switzerland (CCPCS). The administrative agreement that has now been concluded regulates the organisation and financing of services provided by the investigation network. The aim of NEDIK is, among other things, to ensure the mutual transfer of knowledge, the preparation of the national case overview and the triage of intercantonal cases. Furthermore, NEDIK contributes to prevention and cooperates with Swiss Crime Prevention (SCP) and with the National Cybersecurity Centre (NCSC). NEDIK will use specific analytical tools and operate a central knowledge database to efficiently combat cybercrime. Finally, within the NEDIK investigation network, the Federal Office of Police (fedpol) will take on the supra-cantonal and transnational coordination role and ensure international case coordination with partner authorities such as Europol and Interpol.

5.3 Federal Council's digital foreign policy strategy

Digitalisation opens up new opportunities for Switzerland and its foreign policy. This is because Switzerland has excellent research institutions, and numerous international organisations are based in Geneva. This mix allows Switzerland to play a special role in the field of digital governance. This role is important because the increasing geopolitical tensions are also evident in the digital world, as data is now a central source of power. There are also signs of a global technology race, especially in the field of artificial intelligence. This is why the Federal Council has made digitalisation a thematic priority in its foreign policy strategy and defined the fields of action in its digital foreign policy strategy:[68] digital governance, prosperity and sustainable development, cybersecurity and digital self-determination.

In the area of digital governance, Switzerland advocates moderate regulation and wants to make international Geneva the leading global hub for digitalisation and future technologies. Non-state players are particularly important in this regard and will be involved in the search for solutions. Prosperity and sustainability are about promoting good international framework conditions for the digital economy and new technologies. In cyberspace, Switzerland is committed to international law and promotes dialogue with the private sector on standards of conduct on the internet. Finally, the main goal of digital self-determination is to promote the responsible use of data and to ensure greater digital self-determination for citizens.

---

67 Increased cantonal commitment against cybercrime and paedophile crime (kkjpd.ch)

68 Digital foreign policy strategy (eda.admin.ch)

5.4 First EU sanctions against cyberattackers

In 2020, the EU made use, for the first time, of the cyberdiplomacy toolbox[69] adopted in 2019, and issued sanctions against suspected cyberattackers.

A travel ban and an asset freeze were imposed on two individuals and an entity linked to the Russian military intelligence service (GRU). They were involved in the 2015 attack on the German parliament in which parliamentary data was stolen. Third parties were also banned from providing funds to the sanctioned individuals and entity.[70]

Similar sanctions were imposed on six individuals and three entities of Chinese, Russian and North Korean nationality for involvement in the Wannacry, NotPetya, Cloud Hopper campaigns, as well as the attacks on the Organisation for the Prohibition of Chemical Weapons (OPCW) and the Ukrainian electricity grid.[71]

69 COUNCIL DECISION (CFSP) 2019/797 concerning restrictive measures against cyber-attacks (europa.eu)

70 Malicious cyberattacks: EU sanctions two individuals and one body over 2015 Bundestag hack (europa.eu)

71 EU imposes the first ever sanctions against cyberattacks (europa.eu)