5 May 2022 | National Cyber Security Centre NCSC

Semi-annual report 2021/2 (July – December)

Information assurance

Situation in Switzerland and internationally

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
National Cyber Security Centre NCSC

1 Overview/content

Management summary

This report deals with the most important cyberincidents of the second half of 2021 both in Switzerland and internationally. The focus topic concerns attacks on IT product supply chains.

Nowadays, various suppliers and third-party providers are involved in the production of goods and services. Attacks on these can lead to far-reaching problems in the entire supply chain and halt production, for example. The supply chain attack on the software company Kaseya hit the headlines internationally in mid-2021. Furthermore, in Switzerland, the websites of the city and canton of St Gallen were unavailable for a prolonged period due to a DDoS attack on a hosting provider.

Cases of fraud most frequently reported

During the period under review, the NCSC received a total of 11,480 reports on cyberincidents, most of which concerned various types of fraud. In particular, emails supposedly sent by law enforcement agencies were reported very often. Other reports concerned advance payment fraud, investment fraud, CEO fraud and classified ad fraud. A trend towards more elaborate, customised approaches has emerged among some perpetrators of fraud. They work on victims over a lengthy period of time in order to build up trust before actually attempting to defraud them.

Ransomware and data leaks

In the second half of 2021, there were also numerous attacks with encryption Trojans, so-called ransomware, during which data was encrypted and a ransom was subsequently demanded. The attackers are increasingly turning to double extortion. They copy the data before it is encrypted, which gives them additional leverage. If the victim is unwilling to pay the ransom, they threaten to publish the data.

Software component vulnerabilities

Existing components such as libraries or open source code are often used in software development. However, these can also have vulnerabilities. If such a vulnerability is discovered, it must be rectified in all products in which the component with the vulnerability was integrated. This problem became apparent in December 2021 with the critical vulnerability in the widely used Java program library Log4j.

Phishing still a trend

Since the start of the pandemic, many phishing attacks involving alleged parcel notifications or delivery problems have been reported to the NCSC. Aside from emails, the attackers also regularly send text messages in order to reach their victims. Other reports concerned phishing attempts in connection with webmail and Office365. The access credentials phished in this way are subsequently used for invoice manipulation fraud in many cases. Another perennial issue is phishing emails regarding bills from internet providers that have purportedly been paid twice.

2 Editorial

No man is an island

The English author John Donne coined the phrase "no man is an island" in his work Devotions, published in 1624. The poet wanted to illustrate that each of us is part of a larger ensemble and that we share our fate with that of our fellow human beings.

Roger Wirth, Head of Cyber Security (CISO), Swissgrid Ltd

Our economic environment is characterised by ongoing specialisation and the associated reduction of vertical production in order to increase efficiency and reduce costs through economies of scale. As a result, the value chain of companies is becoming increasingly dependent on suppliers, service providers and partners – even though the COVID-19 pandemic has shown us the limits and risks of this global division of labour.

In particular, when it comes to cyberattacks against companies, all stakeholders in a supply chain share a common fate: a cyberattack on a supplier can have repercussions for its customers and, in turn, for the users of their services. In February this year, for example, Toyota had to temporarily close its Japanese factories after a supplier went down due to a cyberattack. The metaphor "no man is an island" can also be applied to organisations.

The problem is compounded by the fact that cyberplayers have begun to attack supply chains directly. For example, when they backdoor the products of network equipment providers in order to later attack their customers through these backdoors (as recently happened in the case of the attack on the Texas-based company SolarWinds), they achieve a multiplier effect.

Not protecting yourself also means potentially putting others at risk.

In discussions, I often notice that many companies pay only scant attention to supply chain risk management.

If we consider the extent of our interconnectedness and interdependencies, we may be looking at the greatest systemic cyber-risk in modern society!

We might ask ourselves why this topic does not attract greater attention. One possible explanation could be that when companies outsource services, managers also try to pass on the responsibilities that go with them. This creates a blind spot: while they can outsource the responsibility for service performance, the accountability to their stakeholders remains with them. And how can they be accountable to their stakeholders if they cannot control the risks to their supply chain created by outsourcing?

In my view, supply chain risk management must be an integral part of every company's operational management.

Systematic supply chain risk management is based on identifying and understanding the relevant risks. An analysis of core processes can help to identify critical dependencies with third parties. Threat modelling methods such as STRIDE can also help to identify threats and vulnerabilities at system transition points.

Building a resilient organisation is also very important. If companies are able to maintain their core processes by alternative means, for example if the primary IT system fails (business continuity management), or if they have taken precautions to contain the effects of an attack and to rebuild an ICT or OT system in a short time after a failure (incident response and disaster recovery), then they are also making a direct contribution to the resilience of the entire supply chain in which their company plays a role.

These precautions must be regularly tested and practised with employees within the company if they are to be effective in the event of an emergency.

Industry-wide standards and product and service certifications can also make a positive contribution. To this end, it is necessary for the companies in a particular sector to join forces in order to be able to enforce such standards and specifications vis-à-vis their suppliers.

If we want to be able to effectively counter cyberplayers who are becoming more and more sophisticated, every company must adequately address the cyber-risks in their supply chains.

Roger Wirth, Head of Cyber Security (CISO), Swissgrid Ltd

3 Spotlight: Supply chain attacks

3.1 What is a supply chain attack?

Many companies work with a number of partners (suppliers, third-party providers) who deliver different products such as raw materials, services or technologies which in turn are used to create an end product or which are processed into offers or services. As a result, many companies are dependent on external goods and/or services in order to keep their operations going. In a broader context, this supply chain includes the entire value chain. Each link in this chain is integrated into the overall process and can potentially serve as an entry vector for hackers (attack *via* the supply chain). The chain may also be interrupted by individual malfunctions (attack *on* the supply chain). In order to prevent cyberattacks, the entire supply chain and all involved suppliers and service providers must therefore be appropriately protected, function reliably and, if possible, ensure continuity by means of redundancies.

An attack via a supply chain is a double-pronged attack. The first attack targets an individual supplier. Access to its systems and its privileged relationship with its customers are used to attack the actual target. In simple cases, this occurs via poorly protected remote access, network gateways or established data transfer connections. As part of complex operations, attackers have also manipulated the software development at companies and placed code there which was then delivered to the customer via regular updates.[1] Attacks on software or hardware during the manufacturing process are also conceivable. The product is then delivered with a vulnerability, a backdoor or preinstalled malware. Attacks via the supply chain can focus on a specific high-ranking target[2] or a limited number of persons[3] or can be broad-based so that individual targets can be selected subsequently.[4] Moreover, attacks against as large a number as possible of potential victims can also be carried out, e.g. by disseminating ransomware after compromising an IT service provider.[5]

Attacks on the supply chain that aim to disrupt the operations of specific end customers often cannot be clearly attributed. DDoS attacks on the DNS provider Dyn in 2016 resulted in various platforms (incl. Twitter, Spotify, SoundCloud) which used its services being unavailable for a large number of customers.[6] Companies in the supply chain typically have contracts with their customers that regulate the services or deliveries. Recently, there have been various ransomware attacks on service providers and suppliers. These are then under huge pressure to provide their services again or to produce their products, as they have to uphold their

---

1 See semi-annual report 2020/2 (ncsc.admin.ch), section 4.7.2 on SolarWinds

2 See semi-annual report 2010/2 (ncsc.admin.ch), section 4.1 on Stuxnet, which was used to deliberately sabotage Iranian uranium enrichment

3 See semi-annual report 2017/1 (ncsc.admin.ch), section 3 on NotPetya, which was spread via Ukrainian tax return software

4 See semi-annual report 2020/2 (ncsc.admin.ch), section 4.7.2 on the SolarWinds hack and semi-annual report 2017/1 (ncsc.admin.ch), section 5.1.1 on operation Cloud Hopper

5 See section 3.3 hereafter and section 4.2.2 below

6 See semi-annual report 2016/2 (ncsc.admin.ch), sections 3.2, 4.4.1 and 4.6

obligations in respect of their customers. The blackmailers hope that the victim will be prepared to pay the ransom.

3.2 Ransomware attacks on Kaseya's VSA software supply chain

Kaseya Limited is a software provider specialising in tools for remote monitoring and administration of systems. It offers its customers VSA software (virtual system/server administrator) for downloading, which also functions via its own cloud server. Managed service providers (MSPs) can use the VSA software locally or license Kaseya's VSA cloud server. MSPs in turn offer other customers a range of IT services. When software is updated, Kaseya can send remote updates to all VSA servers.

In mid-2021, attackers used a zero-day vulnerability in Kaseya's own systems (CVE-2021-30116)[7] in order to carry out malicious commands remotely on Kaseya customers' VSA appliances. On 2 July 2021, an update was distributed to Kaseya customer VSAs that carried out the attackers' code. This malicious code placed ransomware on the systems of customers managed by this VSA.[8]

The US authorities then issued guidance for MSPs and their customers affected by the ransomware attack on Kasey's VSA supply chain.[9]

3.3 Incidents in Switzerland

Several SMEs were affected by the BlackMatter ransomware in early September 2021, after attackers succeeded in compromising an Austrian IT provider and attacking its customers.[10] Several websites were temporarily disrupted by DDoS attacks on a hosting company which, among other things, hosts the website of the canton of St Gallen[11] (see section. 4.3.1 below).

3.4 Parliamentary procedural requests and measures

At the political level, at the end of 2021, the report[12] of the Federal Council – in response to Dobler postulates 19.3135[13] and 19.3136[14] – addressed the topic of supply chain risk management (SCRM) and provided an interpretation of the applicable national rules and international standards.

---

7 CVE – CVE-2021-30116 (mitre.org)

8 REvil ransomware hits 1,000+ companies in MSP supply-chain attack (bleepingcomputer.com); see also section 4.2.2

9 CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack (cisa.gov)

10 Hackerangriff auf 34 Firmen (orf.at)

11 Website des Kantons wieder online (sg.ch)

12 Produktesicherheit und Supply Chain Risk Management in den Bereichen Cybersicherheit und Cyberdefence (parlament.ch)

13 Haben wir die Cybersicherheit bei Beschaffungen der Armee im Griff? (parlament.ch)

14 Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff? (parlament.ch)

Furthermore, the legal basis for applying standards for critical infrastructures was examined. The report also mentions requirements brought up in the "Supply chain security"[15] discussion paper produced by a working group of the Cybersecurity Commission of ICTswitzerland, that calls, among other things, for test centres in Switzerland for hardware and software components. The Confederation is prepared to support private initiatives in this area with specialist expertise.[16]

Conclusion / recommendations:

A regular check of supplier and service provider relationships in respect of the developing risk profile is an urgent challenge for company managements in view of the continuing digitalisation of all business areas.

Virtually the only possibility for smaller organisations that do not have their own specialists is to hedge the risks with external support from associations or specialised advisers, including the right to have service providers independently checked. This additional effort inevitably entails higher costs and is worthwhile only if there is also a heightened risk for the organisation.

The UK NCSC (NCSC-UK) offers guidance[17] on its website and a list of questions[18] that can help in the prioritisation process and selection.

The US Cybersecurity and Infrastructure Security Agency (CISA) likewise offers lots of information[19] on risks related to the supply chain.

The NCSC website also provides recommendations for cooperation with IT service providers (ncsc.admin.ch).

3.5 Software component vulnerabilities

Most software products are not written from scratch and in their entirety. Software development often uses existing libraries or integrates open source code. Consequently, any vulnerabilities contained in these components are also unintentionally integrated and disseminated. Once a vulnerability is ascertained, it must be rectified in all products containing the component with the vulnerability. This became clear at the latest in 2014 when the Heartbleed bug aroused global concern.[20]

In December 2021, a vulnerability in the popular Java program library Log4j[21] was identified that was viewed as critical at the global level. Log4j is a programming framework used to log application reports and is a key component of current software development. Consequently, it

15 White_Paper_Supply_Chain_Security_2019_09_25_EN.pdf (digitalswitzerland.com)
16 See also semi-annual report 2020/2 (ncsc.admin.ch), section 4.5.2
17 Supply chain security guidance (ncsc.gov.uk)
18 Supplier assurance questions (ncsc.gov.uk)
19 Supply Chain (cisa.gov)
20 See semi-annual report 2014/1 (ncsc.admin.ch), section 4.1
21 Log4j – Apache Log4j Security Vulnerabilities (apache.org)

is widely used in many commercial and open-source software products.[22] The vulnerability makes it possible to execute arbitrary code remotely (remote code execution, RCE) and, shortly after it became public, it was exploited internationally on a wide scale by cybercriminals. See section 4.5.3.

4 Events/situation

4.1 Reports received on cyberincidents – overview

The NCSC received an impressive 21,714 reports in 2021, roughly double the previous year's number of 10,833. One reason for this sharp increase is likely to be the fact that the NCSC's reporting form was updated and simplified at the end of 2020, and that it was more prominently placed on the NCSC homepage. There was also a clear rise in other phenomena that likewise contributed to this increase.
Many of the reported cases were identified attempted attacks rather than successful attacks. Moreover, a substantial number of unknown cases must be assumed, especially in the case of unsuccessful attempts, as there is no general reporting obligation in Switzerland.

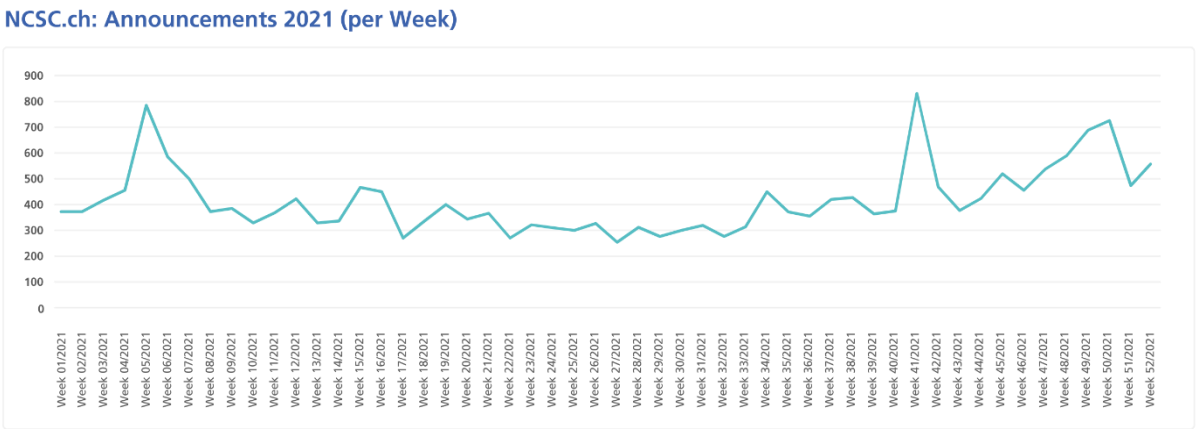

Fig. 1: Number of reports received per week by the NCSC from January to December 2021, see also Current figures (ncsc.admin.ch)

[22] New zero-day exploit for Log4j Java library is an enterprise nightmare (bleepingcomputer.com)

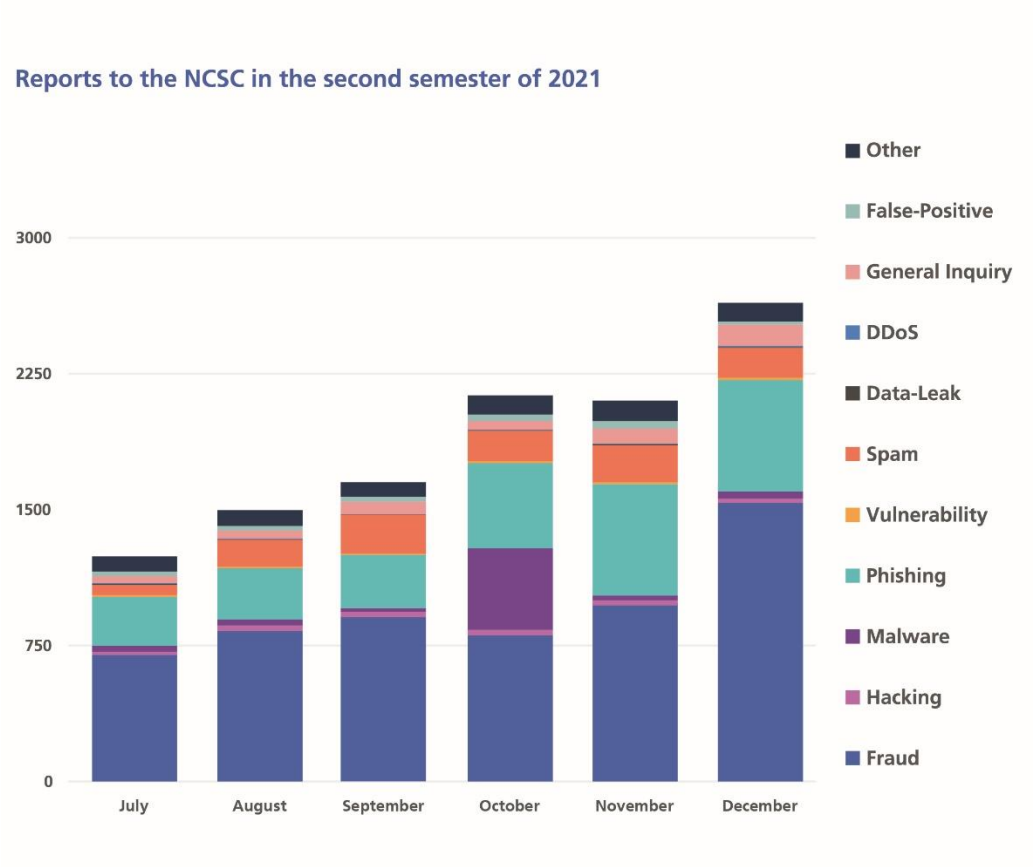

Fig. 2: Reports to the NCSC in the second half of 2021 by category, see also Current figures (ncsc.admin.ch)

4.1.1 Most frequently reported: fraud

As in the previous year, the incidents most frequently reported to the NCSC in 2021 were cases of attempted fraud. There was a total of over 11,300 reports. Whereas fake sextortion[23] dominated in the first half of the year and numerous waves of it were observed, reported cases of this phenomenon tended to decline in the second half of the year. From October on, there was then a sharp increase in reports of threatening emails purporting to be from the criminal prosecution authorities and demanding payment of a fine or deposit.[24] This phenomenon, which has been seen in France for some time and is related to fake sextortion, accounted for most of the reports in November and December 2021 and resulted in a sharp increase in the total number of reports. Other frequently reported categories in 2021 included advance payment scams (2,704), investment fraud (397), CEO fraud (394) and classified ad fraud (820). According to reports on classified ad fraud, the most common cases involved the vendor being required to pay an advance fee for transport despite the sale.[25]

---

[23] Fake sextortion (ncsc.admin.ch)
[24] Week 37 in review (ncsc.admin.ch)
[25] See also section 5.2 below

Aside from the classical examples[26], the cases of investment fraud also included giveaway promotions. If money was paid into a specific cryptowallet address, double the amount would be paid back. The specified website put pressure on the visitor by displaying a counter showing how much money and time was still available for the promotion.

4.1.2 Phishing reports

The number of reported phishing emails remained high in 2021 too. The main ones were emails with incorrect parcel announcements on behalf of the various parcel service providers or the Federal Customs Administration that demanded fees. There are numerous examples of these emails. In some cases, the recipient was asked to buy a paysafe card and send the code to the fraudster; in others, the link took the recipient to a subscription trap. But most of these emails lead the recipient to a phishing website where credit card details are to be provided.

One constant in the phishing category involves bills from internet providers that have purportedly been paid twice. Here, however, the attackers are not always very precise with the details provided. In some cases, the deadline by which the recipient was supposed to react, and which was intended to exert pressure, was almost six months in the past.

Phishing attempts against webmail and Office365 were also observed. This type of access data is often used for invoice manipulation fraud (BEC). This type of fraud refers to an existing email that contains a payment instruction or invoice. The fraudsters change the IBAN number to which the amount is to be paid. As the attackers obtain access to the sender's or recipient's email account in these cases, they also have access to the corresponding internal company communication or communication with customers which may include confidential information. This provides the attackers with further possibilities for fraud, and a victim may also be blackmailed with this data.

4.1.3 Malware reports

As regards malware, almost half of the reports concerned FluBot.[27] This was due to a wave of text messages in weeks 41 and 42, which tried to fool recipients into installing a malicious Android mobile app containing FluBot malware. This wave caused the year record for weekly reports to the NCSC in week 41.

There was also a disproportionately high rise in the number of reports of ransomware. The NCSC received 161 reports on ransomware in 2021, as opposed to 67 the year before. In spring, for example, the NCSC received numerous reports of the Qlocker ransomware being used in attacks on network attached storage (NAS), which is predominantly used by private individuals. A total of 44 reported cases were attributable to Qlocker last year.[28]

Attempted attacks using the Retefe malware are still an issue and are regularly reported. Corresponding emails are often accompanied by a telephone call from a company called Swiss

---

[26] See investment fraud (ncsc.admin.ch) and semi-annual report 2021/1 (ncsc.admin.ch), section 4.8
[27] See semi-annual report 2021/1 (ncsc.admin.ch), section 4.2.1 and section 4.2.1 below
[28] See semi-annual report 2021/1 (ncsc.admin.ch), section 4.1.3

Express Service (or similar), which wants the recipients to sign the shipping documents and informs them during the call that the papers will be sent by email. The link in the email or the attached PDF document then leads to malware – usually an e-banking Trojan.

4.1.4 Vulnerability reports

In the vulnerability category, aside from the Log4j vulnerability[29], reports last year mainly concerned exchange servers.[30] These vulnerabilities are used to distribute malware, for example. Links to malware are added to intercepted emails, which are then sent once again to the recipient. By using a trusted sender, the fraudsters hope to fool the potential victim into opening a document. The Office documents contain a malicious macro, including instructions on how to adjust the settings so that the macro is executed on the computer. The best protection against such attacks is therefore not to execute any macros, even if you are strongly and explicitly urged to do so.

4.2 Malware

4.2.1 General situation

In the second half of 2021, the media were especially interested in ransomware even though it constitutes only a small portion of all malware attacks. The reason for this was that numerous such attacks resulted in serious consequences for the victims both in Switzerland and abroad (see section 4.2.2). In order to use ransomware successfully, the attacker first needs to access the target system. This is usually done using other malware, which specialises in spreading and embedding itself in systems. One such type of malware is QakBot, which is described in more detail in section 4.2.3. The widely used Emotet malware suffered a setback in early 2021 when an internationally coordinated police intervention succeeded in disabling the Emotet infrastructure.[31] Emotet returned at the end of 2021, however.[32] This was made possible by the TrickBot malware, which had previously been used in connection with Emotet. Whereas in the past Emotet installed TrickBot, Emotet now used TrickBot to rebuild its infrastructure. This type of interaction is ultimately attributed to the development of the malware-as-a-service model.[33] Here, malware developers or botnet operators rent their infrastructure to other criminals. Then, each player can specialise in certain partial services and offer them on the underground market.

---

29 See section 4.5.3 below

30 See semi-annual report 2021/1 (ncsc.admin.ch), section 3.1.1

31 World's most dangerous malware EMOTET disrupted through global action (europa.eu); semi-annual report 2020/2 (ncsc.admin.ch), section 4.3.2

32 Emotet malware is back and rebuilding its botnet via TrickBot (bleepingcomputer.com)

33 Malware-as-a-service is the growing threat every security team must confront today (securitymagazine.com); Malware-as-a-service (MaaS) (kaspersky.com); Malware Has Evolved: Defining Malware-as-a-Service (zerofox.com)

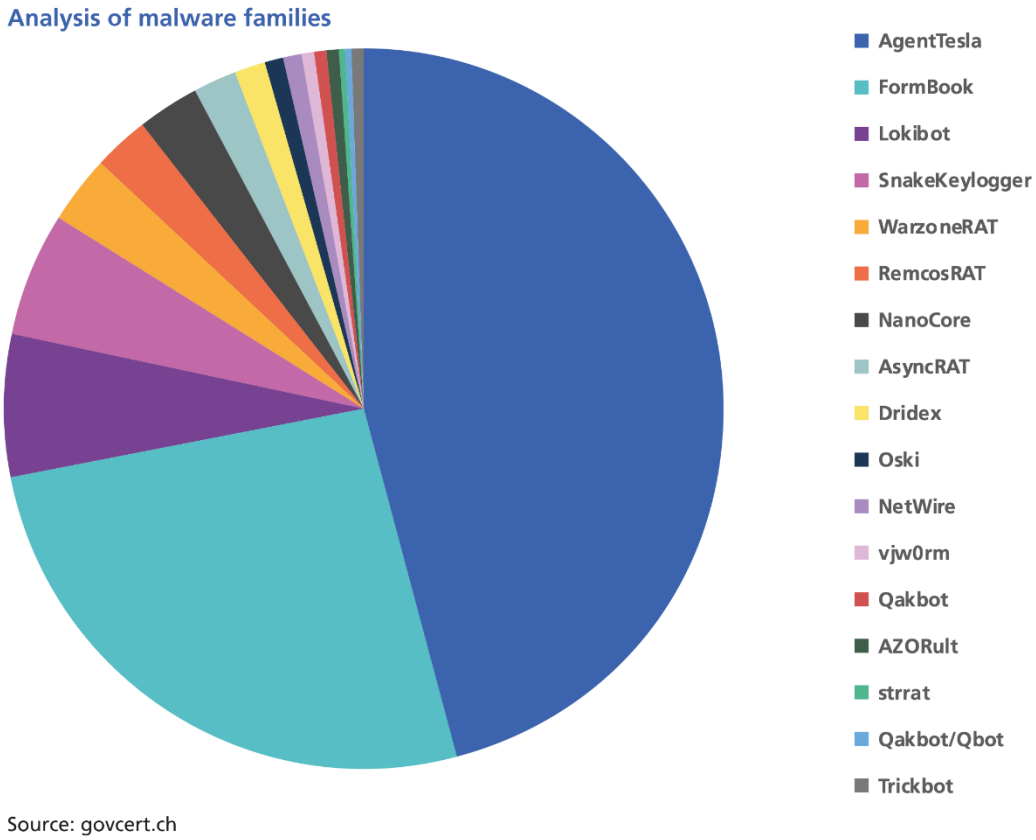

Fig. 3: NCSC analyses of malware families in Switzerland in the second half of 2021

The following chart shows the malware families identified in Switzerland by analysing DNS sinkhole data. DNS sinkholes are used to ward off malware by preventing the malware from accessing the intended domains and re-registering these domains with a security organisation. This makes it possible to identify infected devices which are now connected to the server of the security organisation instead of being connected to the server of the malware operator. The NCSC receives this data from different international partners for the entire Swiss address area and informs the owners of these devices about the infection via their providers.

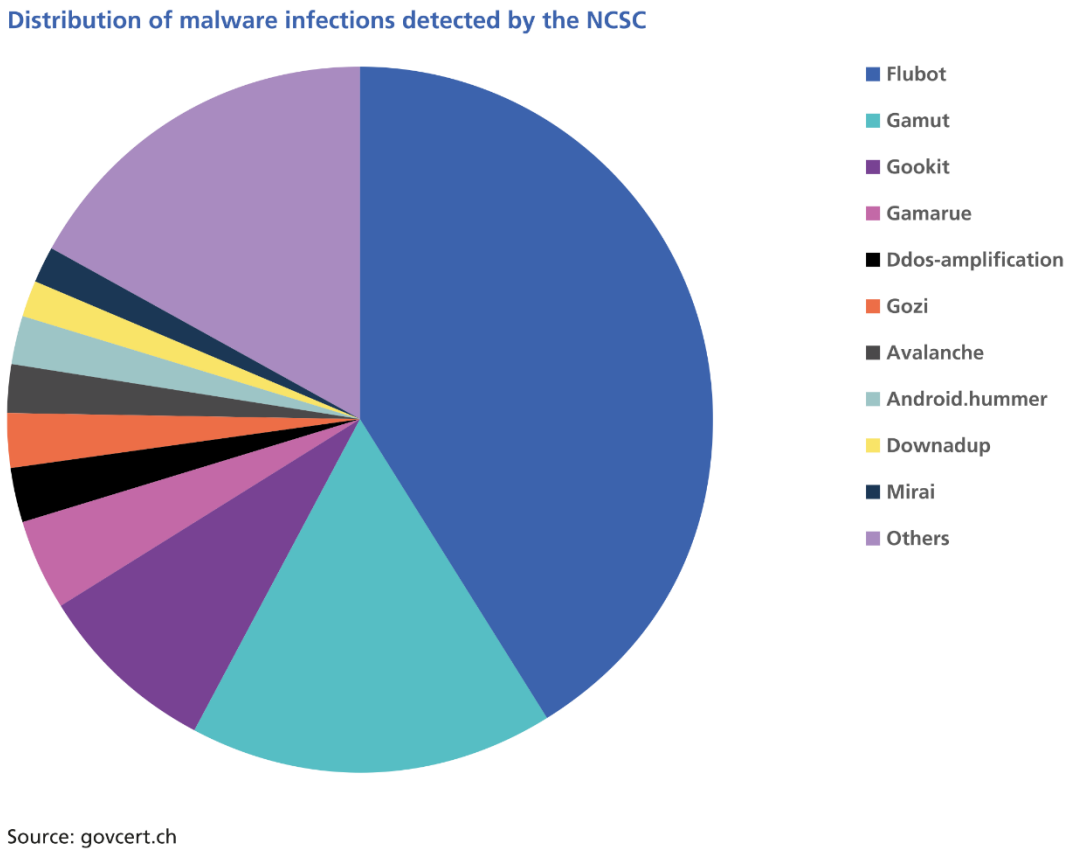

Fig. 4: Distribution of malware infections detected by the NCSC in Switzerland in the second half of 2021

Both in the first and second half of 2021, the most commonly disseminated malware was FluBot. In order to spread this malware for Android devices, the criminals send text messages with a link to a purported voice message. The link takes the user to a supposed app that has to be installed in order to call up the voice message. Instead of the voice message, however, the victims then download FluBot onto their devices. Then the attackers can steal data on the devices and, among other things, access applications protected with a second factor as soon as the second factor is sent via text message. However, the malware can also be used to spy on the victims' e-banking activities.[34]

Conclusion / recommendations:

- Do not install on your mobile phone any apps that are offered outside the official stores.
- In particular, you should not install any app received via a link in a text message or other messenger service (WhatsApp, Telegram, etc.).

[34] FluBot (Malware Family) (fraunhofer.de); Week 41 in review (ncsc.admin.ch)

- If you nevertheless installed such an app, you should have the device checked by a specialist and, in the meantime, you should not carry out any banking transactions or online shopping, or enter any passwords.
- Restoring the factory settings on the infected device is almost the only way to remove the malware.

The spambot Gamut ranked second. Devices infected with Gamut are integrated into a botnet and used to send spam emails, usually on topics such as intimate encounters, pharmaceutical products or job opportunities.[35]

The information stealer Gootkit was in third place. This malware specialises in stealing the victims' banking data. To reach its victims, it uses spam campaigns and compromised websites, which prompt users to download the malware.[36]

4.2.2 Ransomware

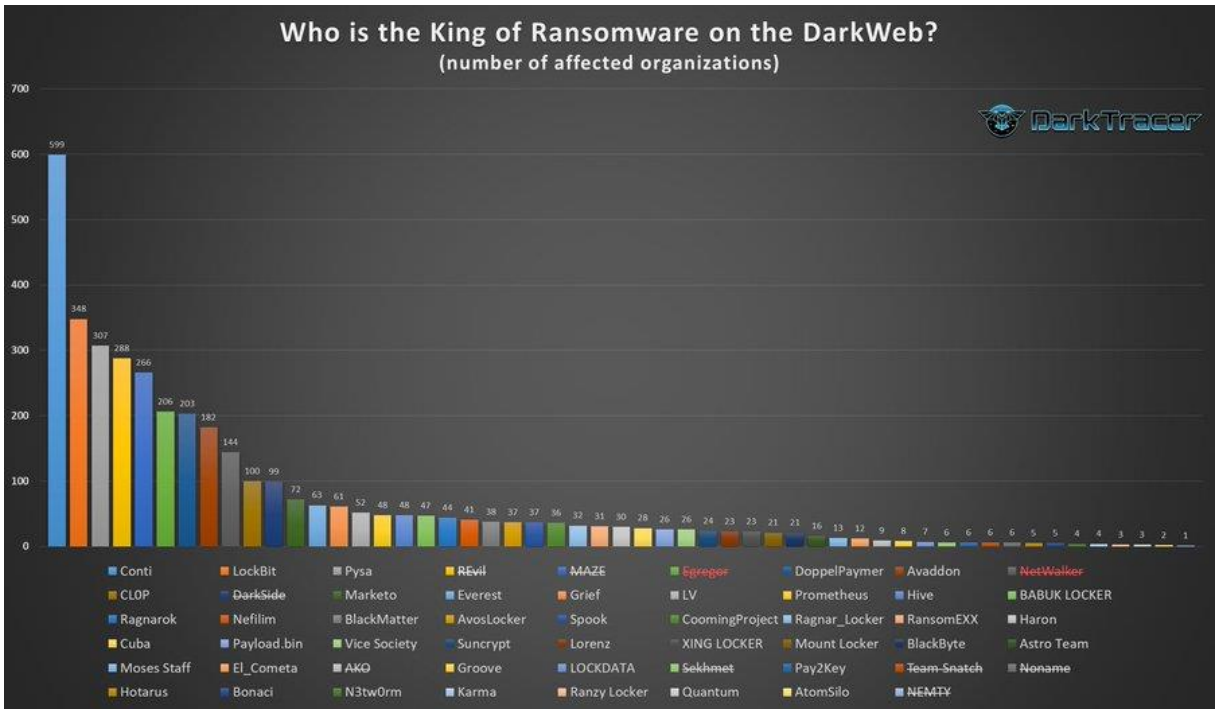

Fig. 5: Worldwide victims of ransomware by attacker according to data leak sites. The crossed-out groups were no longer active at the time the chart was created. (Source: darktracer.com)

35 ENISA Threat Landscape 2020 – Spam (enisa.europa.eu)

36 GootKit (malware family) (fraunhofer.de); "Gootloader" expands its payload delivery options (sophos.com); Gootkit: the cautious Trojan (securelist.com)

Ransomware infections remained the incidents with the gravest potential consequences for Swiss companies in the second half of 2021 too.

During the period under review, the NCSC recorded reports of over twenty different active ransomware variants in Switzerland. The already known REvil (alias Sodinokibi), LockBit 2.0, Conti and ech0raix were particularly active. The new ones included in particular BlackMatter and Grief, the successor to DoppelPaymer.

Although the number of ransomware attacks reported to the NCSC fell slightly from 91 to 70 compared with the previous six months, numerous attacks on private individuals and SMEs in various business sectors were still carried out in Switzerland in the second half of 2021. Critical infrastructure was also affected, including several communes[37], a bank[38] and a private clinic.[39] Other incidents that attracted attention throughout the country involved, among others, the national film archive[40], MCH Group (Messe Schweiz)[41], the well-known Swiss comparison portal Comparis.ch[42] and Matisa, a large company in the construction sector that provides machines for maintaining railway routes.[43] Swiss branches of companies based abroad were also impacted by encryption attacks. For example, all national companies of MediaMarktSaturn were affected by the Hive ransomware attack on the parent company Ceconomy.[44]

As described in previous editions of the report, various ransomware players use multi-stage blackmailing tactics.[45] Once the criminals obtain access to the victims' systems, they procure copies of as much data as possible before initiating the encryption. If the victim refuses to pay the ransom for decryption, the attackers threaten to publish the data. During the period under review, stolen sensitive information of Swiss companies and citizens too was sold or published on the dark web. This applies to tax data, for example, stolen from fiduciary companies using the ransomware LockBit 2.0[46], or data on residents of the commune of Rolle, exfiltrated by the Vice Society group as part of a ransomware attack.[47] Likewise, passports of Swiss travellers obtained from the German tour operator FTI using the ransomware Conti were published online by the perpetrators.[48]

IT service providers are attractive targets, as cybercriminals who have sufficient technical skills can infiltrate these networks to access the systems of their customers as well. The attacks described in sections 3.2 and 3.3 on Kaseya by REvil and an Austrian IT provider by BlackMatter illustrate this clearly. The pressure exerted on operators of ransomware by the

---

37 Montreux a été victime d'une cyber-attaque (watson.ch)
38 Hacker attack on Aquila (finews.ch)
39 20210823_MM_Pallas_Kliniken_Cyberattacke.pdf (pallas-kliniken.ch)
40 Cinémathèque suisse: Cyberattaque à la Cinémathèque suisse (cinematheque.ch)
41 Cyberattack: information and recommendations for our customers and partners (mch-group.com)
42 Ransomware attackers demand $400,000 from Swiss website (swissinfo.ch)
43 Matisa: les hackers Grief ayant piraté Comparis volent le géant du rail (watson.ch)
44 Cyberattack on Media Markt parent Ceconomy (inside-it.ch)
45 See semi-annual report 2020/2 (ncsc.admin.ch), section 4.3.1; semi-annual report 2021/1 (ncsc.admin.ch), section 4.3.2
46 48 heures pour payer la rançon de 200'000 francs en bitcoins (24heures.ch)
47 Cyberattaque contre Rolle: la commune appelle ses résidents à la vigilance (ictjourna.ch)
48 Hackers steal data of a large tour operator, including passports of Swiss citizens (inside-it.ch)

authorities and the resulting criminal proceedings at the global level intensified after the attack on the Colonial Pipeline.[49] European and US criminal prosecution authorities arrested several ransomware players in the autumn in several interventions.[50]

Conclusion / recommendations:

Ransomware can cause considerable damage, especially if data backups are also affected. Important aspects of incident management are described on the NCSC website: Encryption malware - What next?

As a rule, the NCSC recommends that victims do not pay a ransom. By paying, the criminals' business model is confirmed, they receive financial support and are motivated to continue and develop their activities. In the worst-case scenario, a victim loses both the data and the money. The NCSC advises reporting the incident to the police.

Considerations regarding how to insure against cyberattacks were made in the previous edition of the semi-annual report in section 4.2.3.

Furthermore, the US Cybersecurity and Infrastructure Security Agency (CISA) published a document geared to companies which aims to prevent data leaks via ransomware attacks and on how to react to them.[51] Another relevant article at the international level was provided by New Zealand's CERT, which created a diagram of the life cycle of ransomware, including checks for stopping infiltration.[52]

4.2.3 QakBot

QakBot (also known as Pinkslipbot, Quakbot or QBot) was originally a Trojan when it was discovered in 2007 and was mainly used to steal banking data and financial information from the victims. The malware has since been refined and enhanced with a range of additional modules. It can spread in the networks of the infected system, collect and extract data (especially email content used in later campaigns) or install other malware components (payloads) on the infected computer. These functions make QakBot a dangerous malware which had already been identified by the NCSC on several occasions as a vector for ransomware attacks in Switzerland.[53]

In an analysis, the QakBot attack chain was broken down into individual modules which, depending on the target of the campaign, can be compiled in different ways. This means that

---

49 See semi-annual report 2021/1 (ncsc.admin.ch), section 4.2.3

50 Five affiliates to Sodinokibi/REvil unplugged (europol.europa.eu); Ransomware gang arrested in Ukraine with Europol's support (europol.europa.eu); Arrest in Romania of a ransomware affiliate scavenging for sensitive data (europol.europa.eu); Joint global ransomware operation sees arrests and criminal network dismantled (interpol.int); Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (justice.gov)

51 Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches (cisa.gov)

52 How ransomware happens and how to stop it (cert.gov.nz)

53 QAKBOT – Threat Encyclopaedia (trendmicro.com); QakBot (malware family) (fraunhofer.de); QakBot, Software S0650 (mitre.org)

different attack chains are possible, which in turn makes it more difficult to identify a QakBot campaign in an infected network. Nevertheless, a QakBot infection almost always occurs via an email. In addition to the well-known methods using an attachment or a link, images that show a URL which the victim is supposed to enter manually in the browser are now being used.

Here too, an Office document with macros is finally used to install QakBot on the computer.[54]

The sent emails are frequently based on previous communication (thread hijacking), as the NCSC observed several times in the period under review.[55] Since the victims recognise the email, they are more likely to open the document and follow the instructions. Typically, the instructions say that the content cannot be opened because macros have not been activated. The user is then guided through the various steps to activate the macro function.[56]

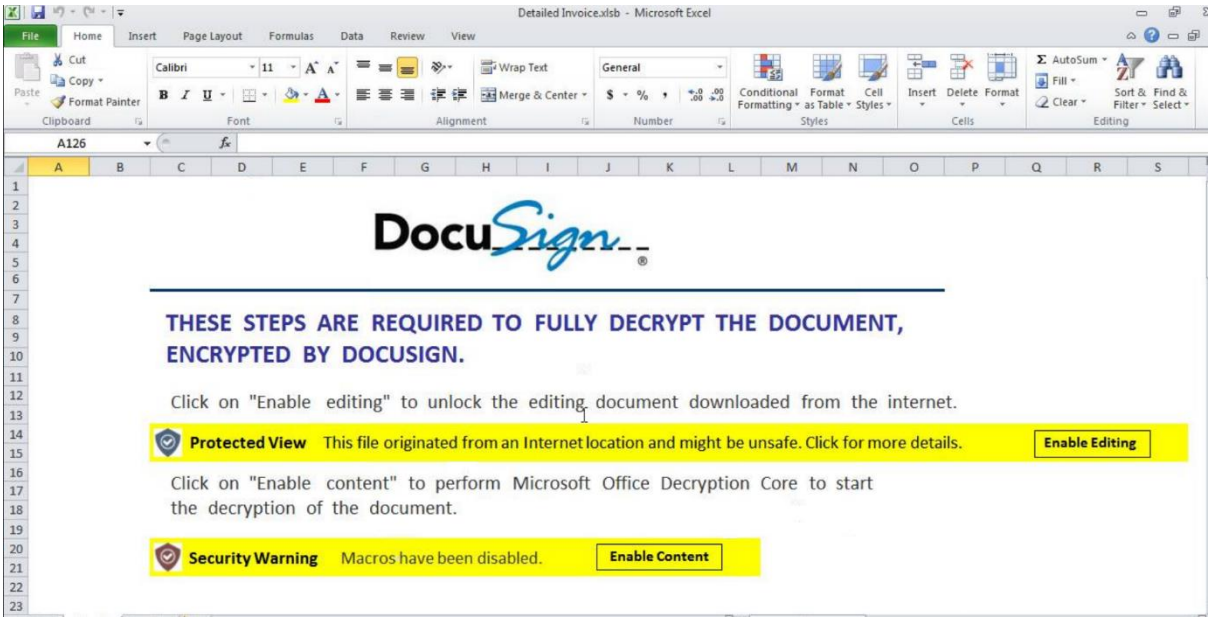

Fig. 6: Excel file with malicious macros

Since October 2021, it has been ascertained that Squirrelwaffle (a malware loader that also spreads via MS Office documents with malicious macros) likewise installs QakBot. Moreover, QakBot activities in the second half of the year featured the use of compromised Exchange servers.[57]

54 A closer look at Qakbot's latest building blocks (and how to knock them down) (microsoft.com)
55 Week 44 in review (ncsc.admin.ch); Week 50 in review (ncsc.admin.ch)
56 Week 20 in review (ncsc.admin.ch)
57 See section 4.1.4 above

Conclusion / recommendations:

- Malicious emails can also come from apparently known senders. Be careful if previous messages are suddenly used out of context.
- Malware is often distributed through Office documents. In most cases, the macro function is exploited. Never give permission to activate the macro function.
- The NCSC recommends as a matter of urgency that operators of Microsoft Exchange servers apply all appropriate patches and keep their servers up to date.
- Microsoft Exchange servers must not be directly accessible from the internet. Either place a WAF (web application firewall) upstream or place an SMTP filtering proxy in front of the Exchange Server.
- Websites used to spread QakBot should be blocked at the network perimeter. A list of these websites is provided free of charge by URLhaus (abuse.ch).

4.3 Attacks on websites and web services

4.3.1 DDoS

The impaired availability of websites caused by DDoS attacks (distributed denial of service) remains an issue both in Switzerland and abroad. 17 incidents of this type were reported to the NCSC in the second half of 2021.

The financial sector remains a popular target for extortionate DDoS waves. In the second half of 2021, however, IT service providers, authorities and educational institutions in Switzerland were also targeted. Using the name Fancy Lazarus, DDoS blackmailers attempted to blackmail a number of Swiss companies and cantonal authorities. However, the attacks of massive scale threatened by the attackers after demo attacks did not materialise. In July and October, the hosting provider of the city and canton of St Gallen fell victim to DDoS attacks, which led to temporary website disruptions.[58]

Several international VoIP (voice over IP) service providers such as Telnyx, Bandwidth and Twilio reported temporary malfunctions as a result of DDoS attacks.[59] In September, the online services of banks in New Zealand were disrupted.[60] And the Polish branch of T-Mobile warded off a major DDoS wave in December.[61]

In the context of the German parliamentary elections, the press reported politically motivated DDoS attacks.[62]

58 Homepages der St.Galler Behörden durch Hackerangriff lahmgelegt (tagblatt.ch)
59 DDoS attack takes yet another VoIP provider offline (techradar.com)
60 Government still gauging impact of Wednesday's denial-of-service attacks (stuff.co.nz)
61 Polish T-Mobile unit faces cyberattack, systems not compromised (reuters.com)
62 Bundestagswahl 2021: Hackerangriff auf Website des Bundeswahlleiters (businessinsider.de)

DDoS attacks are also combined with other types of attack: the ransomware families HelloKitty and Yanluowang use DDoS to increase the pressure on their victims.[63]

Conclusion / recommendations:

DDoS extortion is a large-scale business. Attackers try their luck with as many companies as possible in a relatively undifferentiated manner. If they do not succeed, they try elsewhere. However, if they succeed in disrupting a company's systems with a (demo) DDoS attack, the focus is on this company as a potential victim. The perpetrators step up their efforts in the hope that the company will pay the ransom. It is therefore a good idea to prepare for possible DDoS attacks.

For critical systems, the NCSC recommends subscribing to a commercial DDoS mitigation service. Many internet service providers offer such services.

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

The Inter-University Computation Center (IUCC) also recently published a detailed guide on best practices for DDoS mitigation strategies:

Best Practices for DDoS Mitigation Strategies (geant.org).

4.3.2 Attacks against VoIP systems

Telephony is now almost completely digitalised, and most voice communications occur via the internet (voice over IP, VoIP). Company VoIP systems are thus connected to the internet and constitute not only an attack target for DDoS (see section 4.3.1 above), but can also be misused if poorly protected. The VoIP systems of a Swiss organisation that was protected only by a standard password was misused by criminals for costly calls. By making calls to Tunisia, the perpetrators generated a bill of several hundred thousand francs.

4.4 Industrial control systems (ICS) & Operational Technology (OT)

Direct attacks against industrial control systems aimed at disrupting or affecting physical processes were the exception in the period under review. It is more often the case that the operational consequences are caused by links between the control system networks and the administrative IT systems via which the company's administration, such as the commercial relationships with customers and suppliers, is processed.

63 Kaspersky Q4 2021 DDoS attack report (securelist.com)

4.4.1 Fuel supply in Iran restricted after cyberattack

Last October, operations at numerous filling stations in Iran were restricted. The payment system for subsidised fuel was down[64], the result of a cyberattack by a foreign power[65] according to the Iranian authorities. The pumps were providing petrol, but the payment system for the subsidised purchase of petrol was not working. For most domestic customers, this was tantamount to a malfunction, as they could not afford the fuel without the subsidised discount.

The disruption occurred shortly before the second anniversary of the last major wave of protests in Iran, which also erupted because of the hike in petrol prices. At the same time, travellers on the main roads saw the message "Khamenei, where's our petrol?" on electronic displays. These messages were reminiscent of a similar cyberattack on Iran's railway system in July 2021, when a Wiper component[66] was also used. However, a direct link between the two incidents has not been established so far.

4.4.2 Operator blocked from controlling building automation

The consequences of unauthorised manipulation of industrial control systems were described by the computer security service Limes Security using the example of an attack on a building automation system.[67] An attacker succeeded in accessing KNX technology-based components and manipulating their configuration so as to block the regular operator from controlling the devices.

The attacker needed specific knowledge of how KNX works in order to turn a smart building into one that could only be partially controlled – manually and onsite – or one that could not be controlled at all. Forensic examinations of the device memories by specialists were required to prevent a complex exchange of devices, some of which were permanently embedded in the building's substance. The attacker's intentions could not be established.

Conclusion / recommendations:

It is a good idea to invest in protecting access to industrial control systems and to monitor the operation and any manipulations so that action can be taken quickly if abusive changes are suspected.

The NCSC recommends on its website Measures to protect ICS (ncsc.admin.ch).

64 Störung der Benzinversorgung - Schlangen vor Irans Zapfsäulen: «Khamenei, wo ist unser Benzin?» (srf.ch)
65 Iran says Israel, US likely behind cyberattack on gas stations (reuters.com)
66 MeteorExpress | Mysterious Wiper Paralyzes Iranian Trains with Epic Troll (sentinelone.com)
67 KNXlock – an attack campaign against KNX-based building automation systems (limessecurity.com)

4.4.3 OT threatened by clarification and collateral damage

Attacks as described in the previous section that disrupt the operation of industrial control systems through the dedicated abuse of their functionalities remain the exception in cyberincidents that impact physical processes. More frequently, IT systems used to operate control systems are infected with widely transmitted malware[68] or an attempt is made to use IoT devices for DDoS or crypto mining botnets[69].

Infections of this type usually do not affect the controlled processes. In cases where ransomware is subsequently installed on the systems, this unfortunately changes frequently. Six known ransomware families (Cl0p, MegaCortex, Netfilim, LockerGoga, Maze and EKANS) even attempt to terminate IT processes with a link to OT systems after the attack. For instance, in the fourth quarter of 2021, Dragos, a company specialising in ICS security, observed 176 published data leaks with an ICS link to dark net pages of ransomware groups.[70] The manufacturing industry was the most often affected, followed by the transport and food sectors.

68 https://ics-cert.kaspersky.com/publications/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/

69 Honeypot experiment reveals what hackers want from IoT devices (bleepingcomputer.com)

70 Dragos ICS/OT Ransomware Analysis: Q4 2021 (dragos.com)

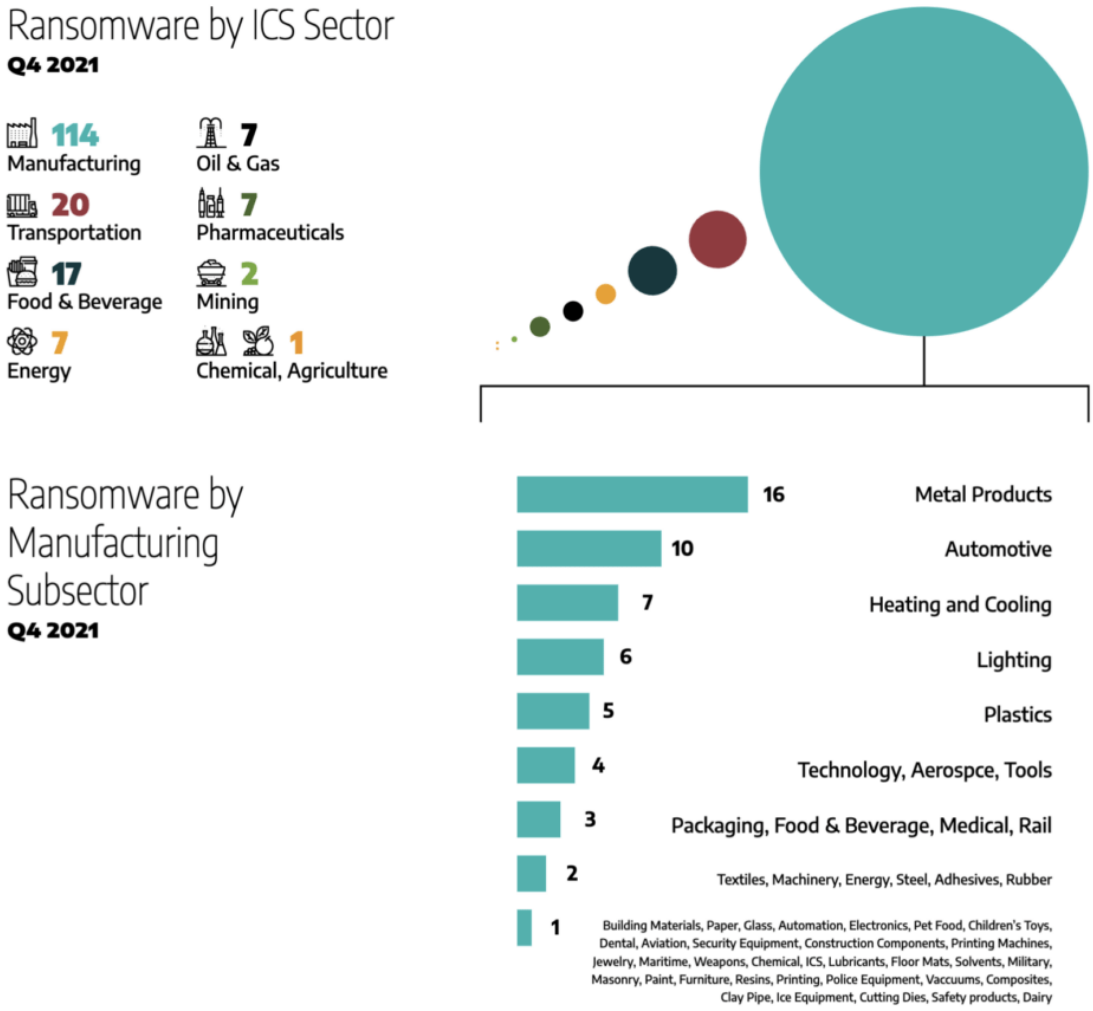

Fig. 7: ICS-related data published by ransomware groups by sector (Source: dragos.com)

A survey[71] conducted by Claroty, another company that specialises in the field of OT, confirmed the threat posed to systems by ransomware. 47% of the 1,100 operators surveyed registered consequences for OT systems caused by ransomware attacks.

According to Mandiant, if files procured via ransomware attacks are published, in one in seven cases they contain documents with information about OT systems (network architecture, hardware and software used, etc.) which could potentially be used for future attacks.

71 Ransomware Often Hits Industrial Systems, With Significant Impact: Survey (securityweek.com)

Actual sabotage attempts on industrial control systems are still most likely to be expected in the vicinity of existing conflicts. For example, Ukraine, aided by specialists in the United States and the United Kingdom, stepped up its defences[72] in view of the troop deployments at its border with Russia.

4.5 Vulnerabilities

4.5.1 Atlassian Confluence – CVE-2021-26084 – remote code execution

On 25 August 2021, the software provider Atlassian announced the publication of a patch for a critical vulnerability in the Confluence software.[73] Confluence is a collaborative tool for managing work areas and projects which is used by many companies worldwide and which often contains internal data. The vulnerability enables an attacker to execute arbitrary code remotely (remote code execution, RCE). The attacker can compromise the entire server on which Confluence is run. In several cases a cryptominer was installed[74] or companies were blackmailed via encryption of their data.[75]

According to Atlassian, only the on-premises solution of their product was affected; the cloud version was not in danger.

Conclusion / recommendations:

This vulnerability is evidently easy to exploit. In view of what is known about the details, the risk is considered to be very high.

Members of the public are indirectly affected if a company of which they are a customer is compromised. Companies using on-premises solutions should be particularly careful. Companies that maintain their Confluence servers themselves are strongly advised to apply the necessary patches.[76]

4.5.2 Azure – OMIGOD – privilege escalation, remote code execution

On 8 September 2021, Microsoft announced a patch for several critical vulnerabilities related to its Azure service. The group of vulnerabilities called OMIGOD concerns OMI, a tool for managing Linux and UNIX systems, used in various Azure services. The vulnerabilities facilitate escalation of user privileges (CVE-2021-38645, CVE-2021-38648, CVE-202138649) and remote code execution by a non-authenticated attacker (CVE-2021-38647). The vulnerabilities range between 7.0 and 9.8 on a severity scale with a maximum of 10. Six days

72 US and Britain Help Ukraine Prepare for Potential Russian Cyberassault (nytimes.com)
73 Confluence Security Advisory – 2021-08-25 | Confluence Data Center and Server 7.16 (atlassian.com)
74 Cryptominer z0Miner Uses Newly Discovered Vulnerability CVE-2021-26084 to Its Advantage (trendmicro.com)
75 New Atom Silo ransomware targets vulnerable Confluence servers (bleepingcomputer.com)
76 [CONFSERVER-67940] Confluence Server Webwork OGNL injection – CVE-2021-26084 (atlassian.com)

after the patches, the company that had discovered the vulnerabilities published an article on how they work.[77]

On 14 September 2021, Microsoft released a patch that was automatically deployed only to certain cloud services. Customers who operate their own Azure infrastructure have to install the patch themselves. Microsoft published a list of the affected services and described the process.[78]

Conclusion / recommendations:

Members of the public are indirectly affected by this type of critical vulnerability if personal details of the companies of which they are customers can be disclosed. The risk for companies operating their own Azure infrastructure is high. They are advised to check and follow the information from Microsoft.

4.5.3 Log4j – CVE-2021-44228 – Log4Shell

On 9 December 2021, the critical vulnerability in the open source library Apache Log4j was reported (CVE-2021-44228). The details required for exploitation were also published. Log4j is a popular Java library that provides a protocol infrastructure for third-party applications. The security vulnerability is classified as critical (10 out of 10), as arbitrary code can be executed remotely (remote code execution, or RCE).

Numerous products and open source software are based on the use of Log4j as a protocol framework. Many companies may thus be affected without realising it through the use of external products in parts of their infrastructure.

In the wake of CVE-2021-44228, a number of Log4j-related vulnerabilities were remediated. The NCSC published a detailed overview of the developments in the GovCERT blog.[79]

Conclusion / recommendations:

The NCSC urgently recommended that available security patches be installed as quickly as possible and that companies using Log4j or solutions with Log4j in their infrastructure closely monitor the situation.

As this vulnerability can also affect components of an infrastructure developed by a third party, it is also urgently recommended that an up-to-date inventory of these services be kept and that any affected services be updated regularly.

---

77 OMIGOD: Critical Vulnerabilities in OMI Affecting Countless Azure Customers (wiz.io)
78 Additional Guidance Regarding OMI Vulnerabilities within Azure VM Management Extensions (microsoft.com)
79 Zero-Day Exploit Targeting Popular Java Library Log4j (govcert.admin.ch)

Given that this vulnerability can easily be exploited and based on the published information, the risk for systems that have not yet installed the patch is still extremely high.

In addition to the indirect consequences for the general public if a company falls victim to an attack, this vulnerability also has direct consequences for private individuals. NAS (network attached storage) devices used both by companies and private individuals were also identified as susceptible to this type of attack. NAS manufacturer QNAP published recommendations and information on the products in question[80], and several successful ransomware attacks were reported.

4.5.4 Blacksmith – CVE-2021-42114

On 15 November 2021, researchers at the Federal Institute of Technology in Zurich (ETHZ), Qualcomm and the Free University of Amsterdam published a study on a hardware vulnerability called Blacksmith.[81] The vulnerability concerns devices with a RAM chip type and shows a new method for efficiently circumnavigating security systems implemented on DDR4 chips.
As the NCSC obtained recognition as a Numbering Authority for the assignment of CVE identifiers in September 2021, it acted as an intermediary between the research team and chip manufacturers. The CVE number for the Blacksmith vulnerability was the first CVE number issued by the NCSC.

Conclusion / recommendations:

The vulnerability concerns chips made by Samsung, SK Hynix and Micron, which are used by various technology companies. The vulnerability is viewed as critical, as the chips are used worldwide. The risk of exploitation is very low, however, as the related effort is considerable.

In this case, there are no patches from the manufacturers, and the RAM-DDR4 chips remain susceptible. For critical infrastructures, it is recommended to use a chip type that is better protected against row hammer attacks (ECC or DDR5).

80 Multiple Vulnerabilities in Apache Log4j Library – Security Advisory (qnap.com)
81 Blacksmith – Computer Security Group (ethz.ch)

4.6 Data leaks

4.6.1 Fortinet VPN credentials

A threat actor known as “Orange” published half a million sets of access data for Fortinet VPN accounts on a newly launched underground forum.[82] The access data was allegedly obtained in the summer via a vulnerability for which a patch is now available.

The NCSC identified around 400 entries with a link to Switzerland and informed the affected organisations accordingly.

Conclusion / recommendations:

Vulnerable remote access solutions are regularly used to launch ransomware. If criminals have currently valid access data for remote access, even patched systems are not safe.

If possible, protect access to data, accounts, systems and networks with two-factor authentication, and not only with a user name/password combination.

Access credentials should be changed regularly. This applies in particular after rectification of a vulnerability that entails the risk of a leakage of access data.

4.6.2 EasyGov

In August 2021, hackers apparently used automated bulk queries to access the web platform www.easygov.swiss operated by the State Secretariat for Economic Affairs (SECO) and obtain the names of up to 130,000 companies which had requested a COVID-19 credit. However, the hackers were unable to see the amount of the credit or other details of the companies in question. SECO was informed of the incident on 19 October and implemented measures immediately. The affected web interface was closed within minutes, the data was removed from the server and the process used on EasyGov was completely deactivated.[83] In this case, the NCSC provided SECO with support and advice. SECO launched an investigation.

Conclusion / recommendations:

Digitalisation simplifies administrative processes in a number of ways. This is reflected in the name of the SECO portal: EasyGov. During the pandemic, there was an urgent need to assist the business sector in an unbureaucratic manner. Companies were thus able to use their business identification number (UID) to open a form to apply for a credit.

82 Hackers leak passwords for 500,000 Fortinet VPN accounts (bleepingcomputer.com)
83 Cyberattack on EasyGov (seco.admin.ch)

If an application for a (first) credit had already been requested for a UID, no form opened. It was possible to exploit this and use bulk queries with the UIDs publicly available in the commercial register to see which companies had made use of this option.

The activation of query possibilities or content linked to a database always entails a risk of misuse. It is therefore important to consider in advance what results an unauthorised, inquisitive person can achieve through various queries – even a "negative" answer allows conclusions to be drawn. In any case, it is essential to prevent bulk queries so that unauthorised persons cannot obtain large volumes of data in a very short time.

4.7 Espionage

4.7.1 Pegasus

In the second half of 2021, the use of the surveillance software Pegasus became a major focus for the press, researchers, NGOs and the general public, after Amnesty International published a report in July 2021 on the global use of Pegasus against human rights activists and media representatives.[84] The Canadian research platform CitizenLab had already published information in 2018 on its use in 45 countries between 2016 and 2018.[85] A product of the Israeli company NSO, Pegasus is spyware for mobile devices which, according to the manufacturer, was developed to combat terrorism and is sold to government authorities. Solutions like this are used worldwide to investigate target persons as part of criminal investigations and intelligence service procurement. Security authorities choose this type of procedure mainly because the communication channels and applications used by suspected perpetrators increasingly use end-to-end encryption, which means that listening in or reading during transmission is no longer possible. Recent years have seen the emergence of an industry that offers surveillance products for government authorities which target end devices. The fact that these surveillance tools are used within the purchasers' local legal framework is cause for concern in some cases. In September 2021, Apple remedied a vulnerability in the iMessage chat service that had been exploited by Pegasus.[86]

4.7.2 Data theft via Slack API

The hacker group MuddyWater, which is purportedly supported by Iran[87], uses a newly discovered backdoor called Aclip to misuse the interface (API) of the web-based instant messaging service Slack for clandestine communication. Aclip is executed via a Windows batch script called aclip.bat, hence the name. The backdoor remains on the infected device by adding a registration key and is automatically launched when the system is activated. Aclip

84 Forensic Methodology Report: How to catch NSO Group's Pegasus (amnesty.org)
85 HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries (citizenlab.ca)
86 Analyzing Pegasus Spyware's Zero-Click iPhone Exploit ForcedEntry (trendmicro.com)
87 MuddyWater (Threat Actor) (fraunhofer.de)

receives PowerShell commands from the C2 server via Slack API functions and can be used to execute other commands, send screenshots of the active Windows desktop and exfiltrate files. The attacker used this technology to target airlines, according to an IBM report.[88]

4.7.3 Nobelium

The perpetrator behind the supply chain attack on SolarWinds was nicknamed Nobelium by researchers. Various bodies suspected that Nobelium was the APT29 group and hence the Russian foreign intelligence service.[89] In the second half of 2021, Nobelium remained active and, according to Microsoft, targeted IT-managed services and cloud service providers in the United States and Europe in particular in order to gain access to their customers. Microsoft observed that the perpetrator focused on accounts with privileged rights in order to spread out further in cloud environments and to exploit customer relationships.[90] The campaign underscores the relevance of trust-based and customer relationships for espionage risks, especially in the field of IT service providers.

4.7.4 Nickel/K3chang

Cyberespionage players continue to exploit unpatched remote access solutions: Microsoft reported a campaign by a perpetrator called Nickel who acted in this manner.[91] Nickel appears to operate from China and was attributed to the K3chang group.[92] The campaign described by Microsoft involved various targets such as government organisations, diplomatic representations and NGOs on several continents, including in Switzerland.

4.8 Social engineering and phishing

4.8.1 Phishing overview

In the period under review, 90,046 URLs were checked after being reported via the antiphishing.ch portal operated by the NCSC or via the form used to report incidents to the national contact point. This resulted in 3,991 confirmed phishing websites, which the NCSC then reported to the respective hosting providers, various browser manufacturers and anti-phishing working groups. There was a slight decline compared with the first half of 2021, when 4,682 phishing websites were detected.

88 Nation State Threat Group Targets Airline with Aclip Backdoor (securityintelligence.com)
89 APT29, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, Group G0016 (mitre.org)
90 NOBELIUM targeting delegated administrative privileges to facilitate broader attacks (microsoft.com)
91 NICKEL targeting government organizations across Latin America and Europe (microsoft.com)
92 Ke3chang, APT15, Mirage, Vixen Panda, GREF, Playful Dragon, RoyalAPT, Group G0004 (mitre.org)

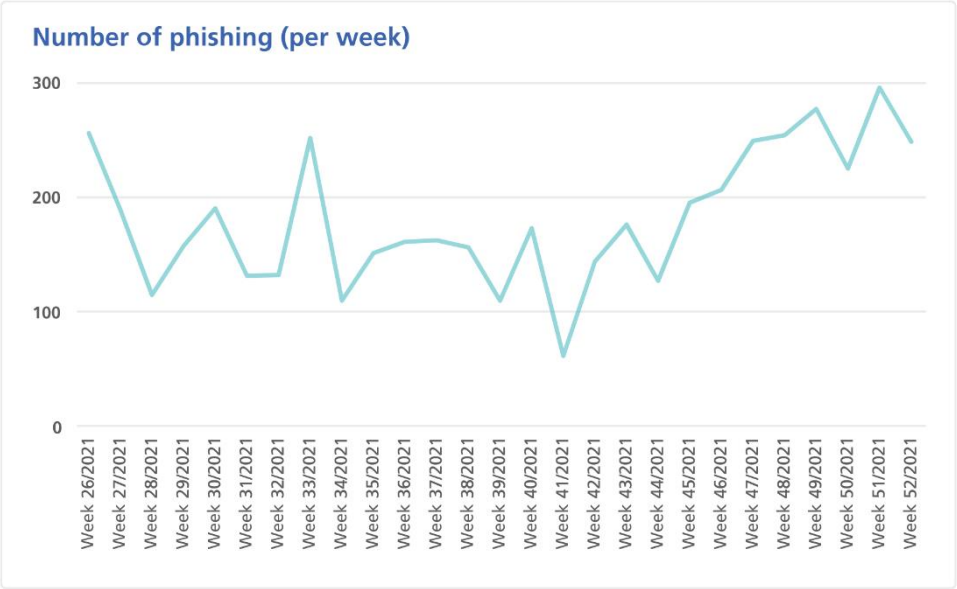

Fig. 8: Number of phishing URLs checked and confirmed by the NCSC per week in the second half of 2021
Current data can be found at: https://www.govcert.admin.ch/statistics/phishing/

The NCSC has seen a shift in the phishing attempts. Instead of big international brands, the identities of local companies, some of which operate solely on the Swiss market, are being misused. The targets still include access credentials for financial service providers and internet services. In order to obtain credit card data, the criminals use the logos of various companies and also use different pretexts.[93]

Phishing was originally a mass phenomenon. Now, however, the players tend to attack very specific targets in some cases. In the period under review, a phishing attempt was observed aimed at companies which are customers of Migros Bank. Anyone selecting the "Individuals" heading on the phishing website was forwarded to the genuine Migros Bank website. The phishers were targeting access data that can be used for access with companies' bookkeeping software.

[93] See section 4.1.2 above and section 5.2 below

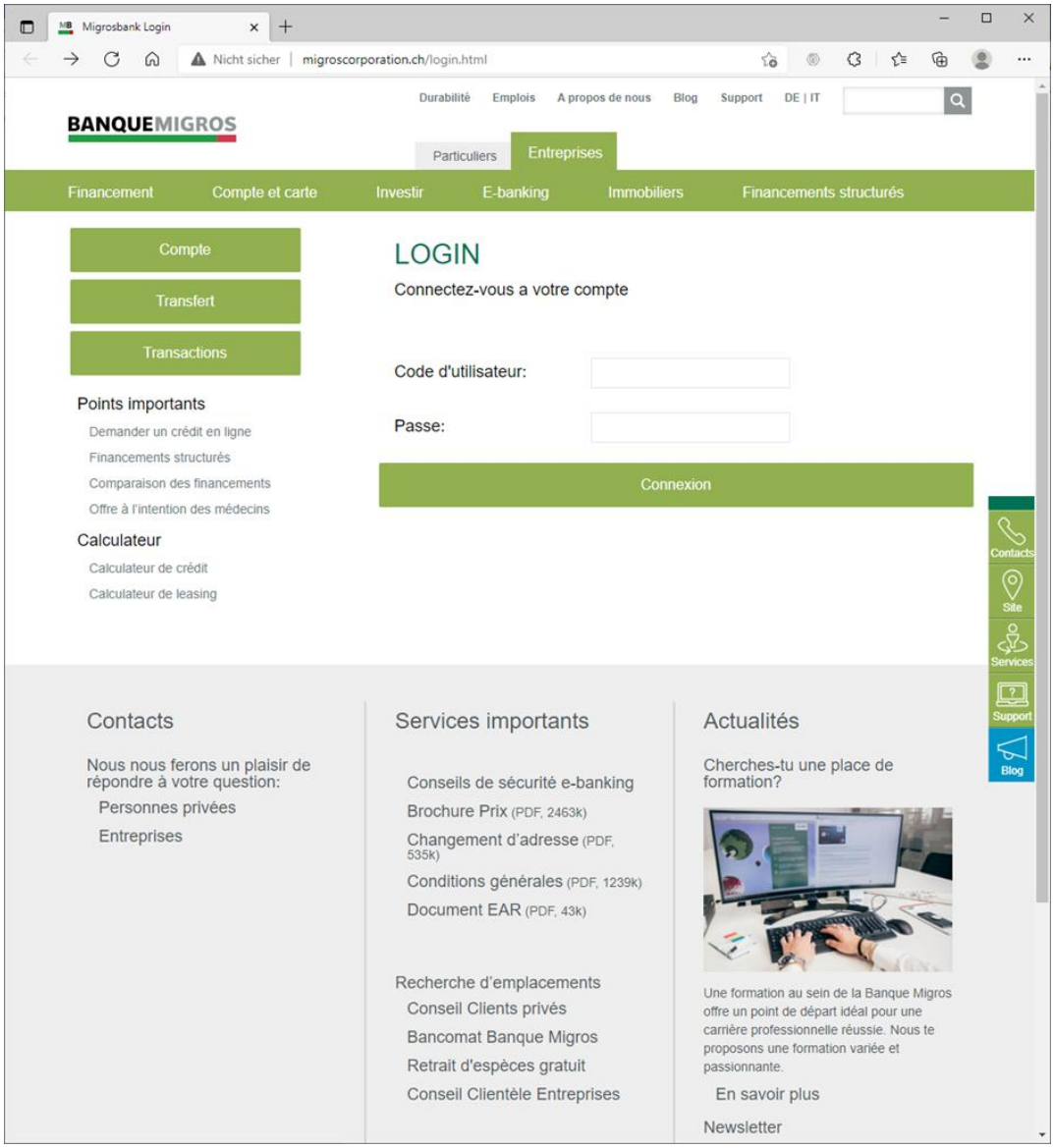

Fig. 9: Phishing website against corporate customers of Migros Bank

Moreover, in the second half of the year, real-time phishing aimed at customers of Swiss financial institutions was again observed, although the volume was extremely low compared with all other phishing attacks. This technique, which cancels two-factor authentication but requires a more active component on the part of the perpetrator – who has to log on to the e-banking system at the same time as the victim – was already described in the 2019/1 semi-annual report.[94]

[94] Semi-annual report 2019/1 (ncsc.admin.ch), section 4.4.2

Social networks can also be used for phishing attacks. For example, in mid-November, the Facebook function that displays pages on which a person has been tagged was exploited for targeted phishing attacks.[95]

4.8.2 Smishing

Text messages and other short message services are increasingly being misused for phishing (known as smishing). These messages typically appear to be from trustworthy senders, e.g. well-known retailers or logistics companies. In some cases, the messages pretend that there's a competition. A link in the message usually takes the recipient to a website created by the criminals on which the person is asked to enter personal data or credit card details.

In the period under review, for instance, Coop published a warning on social media about a phishing message that was circulating on WhatsApp and which claimed that the recipient was the winner of a competition organised by Coop.

Fig. 10: Warning from Coop regarding fraudulent competitions in their name:[96]

4.8.3 SIM swapping

SIM card swapping is a technique used to reroute network traffic from a mobile subscriber without having access to his device.[97] In SIM swapping (or SIM hijacking), an attacker persuades a mobile phone operator to issue a new SIM card and to link it to an existing telephone number and an account. In this way, the perpetrator, who has had this new SIM card issued, can receive text messages with codes for two-factor authentication, for example,

95 Week 45 in review (ncsc.admin.ch)
96 coop_ch on Twitter: "#Phishing message on WhatsApp." (twitter.com)
97 Network Effects, Tactic TA0038 – Mobile (mitre.org)

in order to access certain services or can reset an account password, as this action often requires the entry of a code sent in a text message.[98]

One possibility for criminals to trigger the issuing of a new SIM card is social engineering against a mobile phone company's employees. Helpful information here may come from data leaks at this type of company. The US subsidiary of Deutsche Telekom, T-Mobile US Inc., reported several data leaks in recent years. T-Mobile publicly announced the last incident in December 2021 after receiving several reports from users who had been affected by SIM swapping.[99]

Another tactic involves persuading employees of telecommunications companies to install remote access software or to disclose the registration details of an operational remote access service. In this way, the perpetrators can gain external access to the computer and can initiate the issuing of a new SIM card and its dispatch to any address.[100]

4.8.4 E-banking fake support via Google ad link

The phenomenon of fraudulent support calls[101] in which it is claimed that the computer has been infected has been known for some time. The criminals usually claim to be employees of an IT company and attempt to infect the victim's system or say they want to sell a service to obtain the person's credit card details. In the case observed by the NCSC[102] and the cantonal police authorities[103] between the end of August and the end of September, the fraudsters posted Google ads which appeared first in a search for the e-banking platforms of certain Swiss banks. Clicking on the link in the ad takes the user to a phishing page. However, if you enter your login details and password, an error message appears telling you to call a Swiss telephone number. The call is taken by an alleged bank staff member. The victim is persuaded to download remote access software so that the employee can access the computer and rectify the "problem". The supposed employee acquires control of the PC, initiates a "test payment" and then disappears with the money.

98 SIM Card Swap, Technique T1451 – Mobile (mitre.org)
99 T-Mobile says new data breach caused by SIM swap attacks (bleepingcomputer.com)
100 Hackers Are Breaking Directly Into AT&T, T-Mobile, Sprint to Take Over Customer Phone Numbers (vice.com)
101 Fake support (ncsc.admin.ch)
102 Week 32 in review (ncsc.admin.ch); Week 34 in review (ncsc.admin.ch)
103 Raiffeisen message "Owing to suspicious activities, your account has been blocked" is fraud (cybercrimepolice.ch)

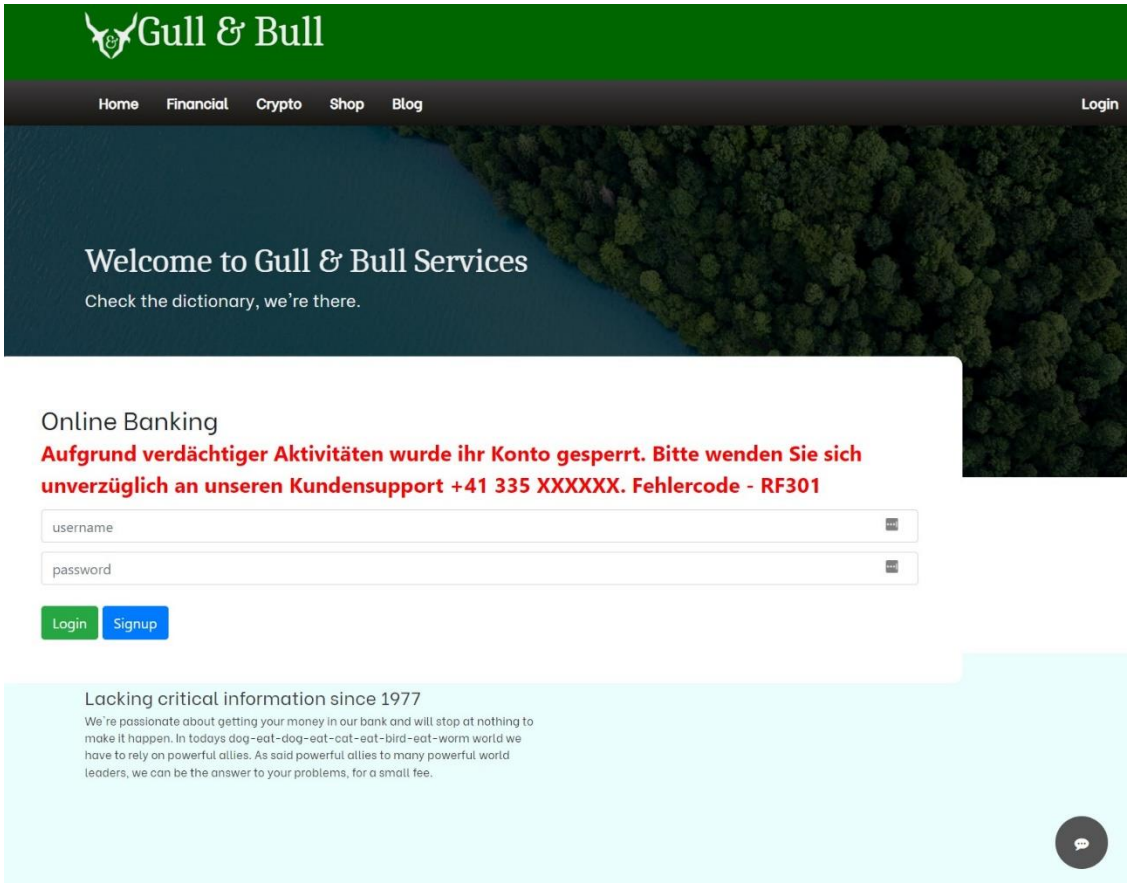

Fig. 11: Imitated e-banking login screen

5 Combined social engineering phenomena

5.1 Trend: Customised attacks instead of mass business

Advance payment scams, fake sextortion or fake support. This is just a fraction of the phenomena observed by the NCSC in the past year. An overview of the phenomena, which now nu mber over 45, can be found on the Cyberthreats[104] page of the NCSC. In more and more cases, however, it is not possible to make a clear categorisation. The fraudsters are increasingly attempting to combine different phenomena. The background to this trend is that it is becoming more difficult for the fraudsters to deceive their victims with "normal" fraudulent emails; they have to go to greater lengths to achieve their goal.

In recent years, attempted fraud was a mass business. Fraudsters send hundreds and thousands of automated emails to any number of recipients in the hope that a certain percentage will fall into the trap. The effort involved for the fraudsters is low, but the success

[104] Cyberthreats (ncsc.admin.ch)

rate is also very low. Nevertheless, this business model appears to have paid off in recent years. Numerous bulk mailings of this type are still being observed.

Internet users are becoming increasingly aware of the problem, though, and the success rate is shifting steadily away from the fraudsters. Clumsy attempted attacks are usually recognised. The fraudsters thus have to come up with different ways of persuading potential victims to do something that they would not normally do. The idea is to build up trust over a certain period. Contact is established via platforms that the recipients are familiar with, for instance, and with which they have already had a positive experience. This reduces scepticism and increases the likelihood that a victim will still take the bait in what is actually a simple case of fraud.

For instance, people advertising on classified ad platforms are diverted to phishing sites. Adverts on property websites are suddenly answered by someone claiming to be a soldier, who wanted to invest his assets in Switzerland. And on classical dating sites, scammers try to convince their victims to "invest" their money on dubious platforms.

5.2 After a classified ad comes phishing

Classified ad platforms are teeming with fraudsters. Classified ad fraud is thus one of the most frequently reported crimes. In addition to the classical variants where non-existent goods are sold or goods are not delivered after payment, the NCSC is seeing more and more combinations involving persons placing classified ads being robbed of their credit card details. The fraudsters go to some lengths by setting up official-looking parcel delivery websites. However, these are not generic webpages. The websites are personalised and contain not only the supposed name of the recipient, but also a description and picture of the item for sale. In other words, the attackers set up a personalised website for each seller! This is of course all designed to dispel the victims' doubts and persuade them to finally provide their credit card details.

5.3 An inheritance instead of a house purchase

Advance payment scams are a classic among fraudulent emails and are sent in large numbers. Apparent inheritances and lottery prizes aim to arouse the recipients' curiosity and persuade them to react to the email. However, these emails are now recognised by most recipients as fraud and are deleted. Fraudsters are thus testing new variants that promise greater success. One such new variant involves fraudsters reacting to a property ad. In this case, a supposed soldier who had been stationed in Afghanistan and is now looking for a new home in Switzerland expresses interest in a property. After sending numerous confidence-building emails in connection with the future sale, the purported soldier steers the discussion towards assets he supposedly possesses and which he wants to invest in Switzerland. The real estate owner is promised a large sum if he helps him with the investment. As with other variants, the victim will sooner or later be expected to pay fees. As the story is fictitious, neither the soldier nor the money exists.

5.4 Investing instead of lending

The digital form of marriage fraud, so-called "romance scam" or "love scam", has been around for many years. In this type of fraud, fake profiles are created on social media and online dating sites in order to make other people believe the fraudster is in a romantic relationship with them and ultimately to obtain financial benefits from the "partner". Here, too, it is becoming more difficult for the fraudsters to persuade victims to pay money, whether for an allegedly sick mother or to pay off a debt that the supposed partner urgently needs to pay to avoid becoming homeless. These variants are well known and trigger alarm bells among potential victims. The attackers are looking for new possibilities in this context as well. The fraudsters often attempt to persuade the victim to invest via an investment platform. A "partner" or "acquaintance" of the fraudsters either works in this field or the fraudsters claim to have already earned a lot of money on the platform. The tactics are clear: the fraudsters deflect attention from themselves and claim to be well-off. Instead of begging for money, they allow the victims to share in their "knowledge" and raise the hope of a substantial profit. It is virtually impossible for the victims to know that the operators of the alleged investment platform and the "bait" are all in it together.

Conclusion / recommendations:

In some cases at least, fraudsters are shifting their sphere of activity from mass business to individualised attacks. What all these variants have in common is the fact that the fraudsters initially use subliminal contact to try and gain the victim's confidence. It is therefore important that people remain cautious, even if they have the feeling that they know who they are dealing with. The internet is – and will remain – a place where anyone can acquire an identity. This also applies to profiles on well-known platforms. Even if someone has been communicating online with another person for some time, this does not mean that the person is trustworthy.