11 May 2023 | National Cyber Security Centre NCSC

Semi-annual report 2022/II (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

Focus: cybersecurity for SMEs

Digitalisation is also progressing in small and medium-sized enterprises. Numerous computers are connected to each other via network interfaces. Processes such as order processing, planning, production and logistics are increasingly interlinked and digitally managed. This increases the number of systems that are accessible from the internet and therefore need the best possible protection. However, SMEs in particular often pay too little attention to cybersecurity. For this reason, the current semi-annual report focuses on cybersecurity in SMEs and highlights the most important aspects of protection against cyberthreats.

Most frequently reported: fraud

In the second half of 2022, the number of reports received by the NCSC remained very high at 17,341, which was practically identical to the first half of the year. In total, the NCSC received 34,527 reports last year. Of these, 85% came from the public and the remaining 15% from businesses, associations and authorities. The reports concerned various forms of fraud, with fake extortion emails, i.e. threatening emails in the name of prosecution authorities, accounting for almost one third of the reports. Other frequently reported forms of fraud included CEO fraud and invoice manipulation scams.

Unchanged amount of ransomware

Ransomware reports remained constant and accounted for almost half of all reports in the malware category. About one third of the 76 reports concerned private individuals, two thirds involved businesses. The LockBit ransomware is often used in attacks targeting businesses. This malware is known for the fact that not only is data encrypted, but it is also stolen and posted on the internet if the ransom is not paid. Such double extortion approaches are being observed more and more frequently. Since many businesses have recognised the threat of ransomware and now have backups, pure encryption is no longer lucrative enough for attackers. The initial infection in ransomware incidents is often due to a vulnerability or poor configuration, as well as emails with malicious attachments and links.

Hacking reports continued to rise sharply

Compared to the previous half-year period, the number of reports regarding hacking almost doubled in the second half of the year, with 276 reports. In particular, social media accounts are a popular target for hackers, for example to blackmail users or to use the hacked accounts to distribute advertising for investment fraud.

Editorial

I am often asked: "Are SMEs less secure than large companies?" Which rather begs the question: What does a typical SME look like? A free-market company is considered an SME if it employs fewer than 250 people. In Switzerland, 99.7% of all companies fall into this category. Most SME staff are employed in goods manufacturing, trade, maintenance and repair of motor vehicles, and health and social work activities.

As these facts alone suggest, there is no such thing as a typical SME. Consequently, there is no one-size-fits-all approach to cybersecurity for SMEs either. As with large companies, the conditions required for SMEs to protect themselves against cyberattacks can vary enormously. For example, a high-tech business in the pharmaceutical industry has completely different requirements from a regional trading company. Significant factors at play here include available finance, the company's technological capabilities, its business model, workforce composition, corporate structures and culture and, last but not least, the economic and political environment.

So the question posed at the start cannot be answered that easily. However, what this SME-focused semi-annual report makes clear is that SMEs are far from immune to cyberattacks, be they indiscriminate and opportunistic or targeted at specific SMEs with valuable intellectual property, for example.

This report aims to illustrate the threat situation, including specifically for SMEs, and to explain what safeguards can be deployed depending on the nature of the company. At the NCSC, we see it as our responsibility to create conditions whereby SMEs in Switzerland are even more effectively supported in protecting themselves. So please take the opportunity to give us your feedback on this report and to share any ideas you have about SMEs and cyber-risks.

For all their differences, one thing that SMEs have in common is that their often small headcounts do not allow for huge IT security departments. However, cybersecurity requires an integrated and business-oriented approach. Ultimately, this means that both management and employees need cyberknowledge within their areas of responsibility. If they are able to build up this knowledge without losing economic clout, SMEs could soon have a considerable advantage in an increasingly digital economy. But leveraging this opportunity for SME-rich Switzerland will require cooperation between public authorities, the business community, academia and society. So let's join forces and do it together!

Florian Schütz, Federal Cyber Security Delegate

2 Focus: cybersecurity for SMEs

2.1 Digitalisation is continuing apace

Digitalisation is an inescapable reality for almost all of us. Many people can no longer imagine life without the internet. Computers have found their way into virtually every sphere of business and society, at least when it comes to communication and administration. Manufacturing too is heavily reliant on them. Many of these devices are connected through network interfaces to each other as well as to administrative office networks in one form or another. Ordering, planning, production, logistics and billing are increasingly intertwined in partially or fully automated processes.

Recommendations:

Take a cautious approach to digitalisation, considering not only opportunities and benefits, but also new dependencies and risks. At every stage of digitalisation, factor in cybersecurity from the outset.

2.2 Core business and support tools

For businesses that only offer digital services, cybersecurity should be a matter of course – after all, they can operate only if their systems are working properly. In most companies, however, IT is primarily used in a supporting capacity. The priority is the core business, be it manufacturing products or providing services. As long as IT is working, little attention is paid to it, and it is often possible to find workarounds if systems are not behaving as they should. Nevertheless, total IT failures in particular can have massive consequences: if planning and billing activities are no longer possible, this can result in loss of working time and delays, which may impact the bottom line. Moreover, theft of intellectual property (industrial espionage) or a wrongly triggered payment can also cause major financial damage.

Conclusion/recommendation:

IT resources are work tools that need to be maintained and looked after. Seek advice and support from experts. Developed by the Federal Office for National Economic Supply (FONES) in collaboration with the business community, the ICT minimum standard and ICT minimum standards by sectors serve as recommendations and points of reference.

2.3 IT operations and cybersecurity

In SMEs, responsibility for cybersecurity is often included in running the company's IT. In many cases, this is not a full-time role. But with IT maintenance alone being an expensive and time-consuming business, there is a risk of cybersecurity being neglected. Typically, firms cannot afford cybersecurity as an independent function until they have reached a certain size. While, in the case of IT, clear requirements are set for functionalities and these are also measurable, cybersecurity is part of risk management and has to be controlled by management in this

context. In particular, it is advisable to treat cybersecurity as a separate budget item so that resources are explicitly available for the relevant measures.

Conclusion/recommendation:

While they are related, the operation and security of IT infrastructure are different fields of action. The allocation of resources to cybersecurity measures needs to be decided in the context of risk management.

2.4 Outsourcing

Every office has computers, but not all companies have their own enterprise network. However, firms that need to work across multiple devices but do not have their own network now have the option of outsourcing data storage and running programs in the cloud. Of course, this can also be useful for easing pressure on the enterprise network or boosting flexibility. Last but not least, as specialised IT service providers, cloud service providers are also likely to have a good understanding of cybersecurity. Another option is to hire an external cybersecurity service provider specifically to take care of security issues.

Conclusions/recommendations:

Contracts with external service providers should include appropriate provisions on security. Aside from any specific measures to protect and defend against cyberattacks (e.g. DDoS, data leaks and ransomware), data backups and reporting obligations in the event of incidents should also be addressed.

2.5 Incident prevention and preparedness

In addition to technical protective measures, training staff about cyber-risks is key, as employees are an important link in the chain of defence. While employees cannot be guaranteed to reliably and independently detect malicious emails, raising awareness of the danger is already a helpful step. If, in the event of suspicion or uncertainty about an email, recipients do not immediately follow the instructions given in the message, or do not click on the link or open the attached file, and instead have the email verified internally or confirm its authenticity with the (purported) sender, the risk of a successful attack is reduced.

However, even with the best prevention and awareness, an incident can never be ruled out. In order to be prepared for such eventualities, the company should draw up emergency plans, with processes and escalation paths that have been defined and tested. Thinking in advance about crisis communication, both internally and externally, relieves pressure in the event of an incident, helps to avoid mistakes, and thus contributes to the successful management of an attack. It is also advisable to establish contacts with potential service providers who could assist with incident response, so that you do not need to hunt around for them in an emergency.

Conclusions/recommendations:

Cybersecurity is not a state to be achieved. Rather, it is a process requiring ongoing care and attention and consisting of technical, organisational and HR measures.[1] Employee training is a key part of this.

Even if a business invests heavily in prevention, the possibility of a cyberincident can never be entirely ruled out. In addition to incident response plans, consideration should also be given in advance to appropriate internal and external communication.[2]

3 Guest articles: cyberattack experiences

3.1 Cyberattack at Verkehrsbetriebe Luzern

By Franz Theiler, Head of IT at VBL AG

On the night of Friday 13 to Saturday 14 May 2022, Lucerne's public transport company Verkehrsbetriebe Luzern (VBL) was the victim of a targeted cyberattack. Early in the morning, control centre staff alerted the IT on-call team to a malfunction. The IT team quickly recognised the extent of the problem and classified it as an exceptional incident. The IT systems were taken offline and VBL's IT network was disconnected from the internet.

The Head of Emergency and Crisis Management convened a meeting of the emergency team. Once the facts had been confirmed, the Lucerne police were notified and the incident was reported to the National Cyber Security Centre (NCSC). That same morning, the Head of Emergency and Crisis Management and the company's senior management briefed key stakeholders, including public authorities, transport and related companies, employees and the media, about the cyberattack that had taken place.

By Saturday lunchtime, VBL's IT team and staff from its external IT service provider had arrived at the company's premises to coordinate and start the work. VBL-Informatik operates critical and high-availability public transport systems for internal and external customers throughout Switzerland. It has a very sophisticated ICT system landscape operating in a Windows and Linux environment. Containment and analysis of the crisis got under way immediately. The malware was identified and removed. Necessary basic systems were rebuilt and isolated. It was possible to gradually restore the systems from the last backup, test them and transfer them to productive operation in a controlled and proven process. Flawless teamwork between employees, suppliers and specialist experts enabled rapid containment of the crisis and a successful recovery, while expert forensic support was provided by the Lucerne police. During the reconstruction process, targeted steps were taken to enhance specific aspects of security.

Passengers were not affected by the cyberattack. Only the departure screens were switched off for security reasons. Looking back, the company was well prepared for the crisis situation. The business areas were able to keep operating throughout, in a well-organised, albeit

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

2 Incident – what next? (ncsc.admin.ch)

reduced, form. The internal emergency and crisis management team met on a daily basis for several weeks, including a follow-up meeting with senior management, which acted largely as a bridge to the specialist departments.

The NCSC gave VBL prompt and customer-oriented support in this difficult situation, supplying it with valuable and reliable information about perpetrators and possible patterns of action. We would also like to thank the NCSC for the two impressive talks given during the management and staff briefings to raise awareness of cyberattacks among VBL's employees. As a public transport operator with critical infrastructures, VBL is able to participate in the exchange meetings organised by the NCSC and benefits from its regular updates on security developments.

3.2 A ransomware incident as seen by the police

By the Digital Crime Unit, Bern Cantonal Police

A ransomware attack involves the encryption of data and the issuance of a ransom demand, usually in cryptocurrency. The attack is automated and initiated by an organised criminal group. If the targeted company refuses to pay the ransom, the attackers threaten to disclose or sell sensitive customer information on the dark web. This would have a direct impact on the firm's reputation.

In a recent case, the company in question reported the attack via the police switchboard. It was passed on to the relevant Digital Crime Unit, which assigned the responsible investigators and called in specialists from the Digital Forensics Department, with whom the first measures were planned. A ransomware case always requires interdisciplinary cooperation between multiple players. As in this case, talking to the affected company is key in order to gather the necessary information and decide what course of action to pursue. Good collaboration is crucial in many respects, bearing in mind that the company's main concern in a ransomware case is not the enquiries and investigations but data recovery and the resumption of business activities.

In this case, aside from the police, a private security service provider was called in very early on to help rebuild the infrastructure. Collaboration with this particular provider was good, but this usually depends on the company, how much they want to contribute to the investigation and how much of a priority it is for them.

As a ransomware attack is technically sophisticated, discussion and meetings take place to try to pinpoint the vulnerabilities that allowed an unauthorised intrusion in the first place.

Given that an attack of this kind can bring to light other injured parties and affect sensitive data, the firm concerned wanted us to provide advice on how to proceed and, above all, some legal guidance, in addition to our investigative work.

Generally speaking, the company in this case did exactly the right thing by reporting the incident to the police as quickly as possible and calling in a security service provider. This enabled work to proceed smoothly between the specialists from the Digital Crime Unit and the Digital Forensics Department. We always advise not to consider paying a ransom, as this helps to fund organised crime. Willingness to pay often depends not only on the degree of data encryption and the likelihood of data recovery, but also on the amount demanded. Here, too, the company acted in an exemplary fashion and never considered paying the ransom. To avoid

getting into a similar situation, it is advisable to raise employees' awareness of risks in cyberspace and to invest in training and a secure infrastructure. The affected firm was able to resume its business activities after a short time, but it took several weeks to fully deal with the incident.

4 Reports from businesses and the public

4.1 Reports received on cyberincidents – overview

The total number of reports rose sharply once again this year. Although the total of 34,527 reports was not double the previous year's figure of 21,714, the increase of 12,813 reports in absolute terms still significantly exceeds last year's rise (increase 2020/21 +10,881). This can be partly attributed to the growing public awareness of the NCSC and its reporting form. However, there are other reasons for the further rise, linked mainly to the increase in reports of fake threatening emails allegedly sent from the police (see section 4.2.1) and phone number spoofing (see section 4.5.1). That said, the fact that a total of 17,341 reports were received in the second half of 2022, around the same number as in the first six months of the year, suggests that future increases will not be as large as in the past three years.

85% of reports came from the public, with businesses, associations and authorities accounting for the rest. Typical phenomena reported by businesses include CEO fraud (190 reports in the second half of 2022), business email compromise (45 reports), attacks involving encryption malware (54 reports) and distributed denial of service, or DDoS (13 reports). Moreover, fake extortion attempts do not only affect private individuals. There are also variants that directly target companies, as illustrated by the examples involving web administrators in section 4.4.2. Likewise, phishing attempts are no longer limited to private individuals, with company employees also being targeted increasingly frequently. Office 365 login credentials are the primary focus in such cases, as highlighted in section 4.3.2.

Reports to the NCSC in the second half of 2022 (per week)

Fig. 1: Number of reports received per week by the NCSC from July to December 2022, see also Current figures (ncsc.admin.ch)

Reports to the NCSC in the second half of 2022 (per category)

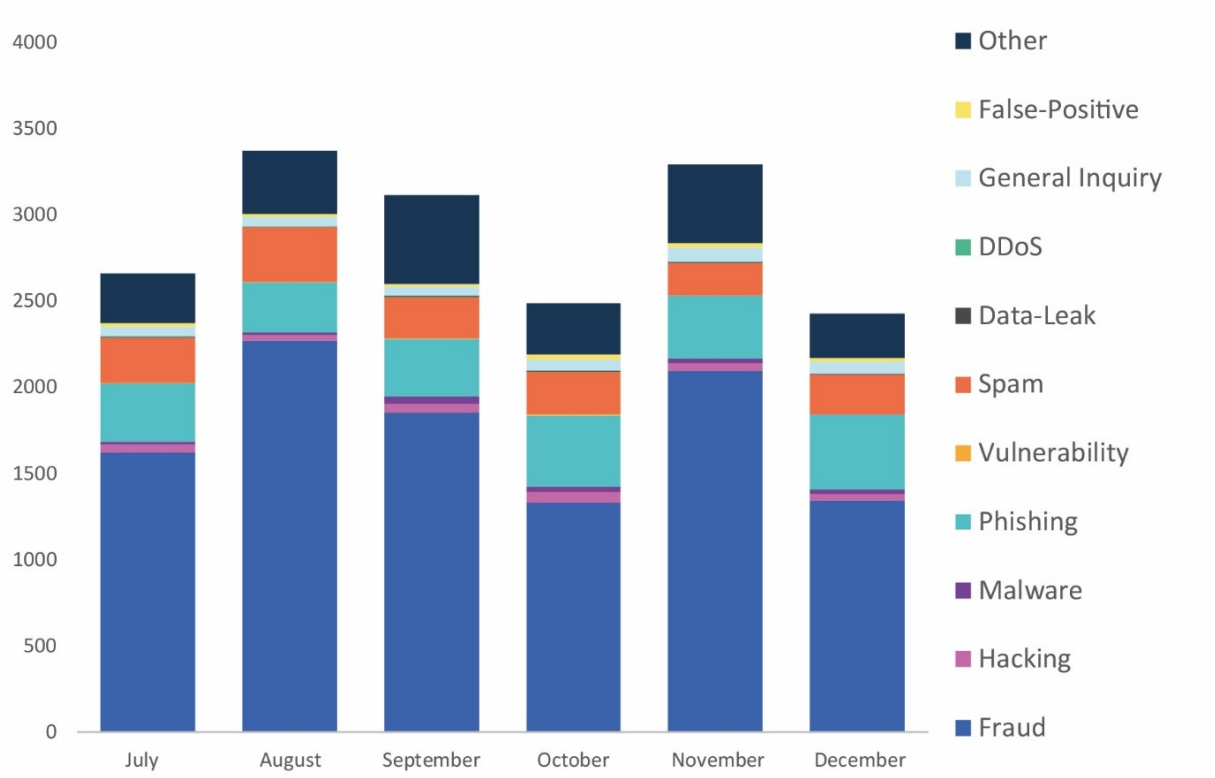

Fig. 2: Reports to the NCSC in the second half of 2022 by category, see also Current figures (ncsc.admin.ch)

4.2 Most frequently reported: fraud

4.2.1 Threatening emails allegedly sent from the police (numerous variants)

In the second half of 2022, the phenomenon with the highest number of reports (5,179) was once again fake threatening emails purportedly sent by law enforcement authorities. Consequently, it is hardly surprising that even in the record-breaking week 36, which saw the biggest number of reports for 2022, with 954 in total, threatening emails supposedly from the police accounted for the largest share, with a total of 418 reports. These threatening emails claim that the people contacted have been found guilty of significant misconduct (typically in connection with child pornography) and that the charges against them can be dropped only if they pay money. In total, 11,051 reports fell into this category in 2022, of which 5,179 were received in the second half of the year. This was approximately a third of the total number of reports received.

To make the extortion emails look official, the fraudsters combine the names and logos of a wide range of law enforcement authorities in Switzerland and abroad, more or less at random. Alleged senders in the second half of 2022 included the cantonal police authorities of Valais, Vaud and Geneva. Europol, Interpol and the French, Belgian and Dutch police were among the international names used. The NCSC was not spared either, with some of these extortion emails bearing its name. However, the attackers mistakenly used the logo of the UK cybersecurity authority of the same name. Emails claiming to be from the Federal Office of Police (fedpol) remain the most common variant. The attached documents appear to be signed by fedpol Director Nicoletta della Valle or the former Head of the Federal Department of Justice and Police (FDJP), Federal Councillor Karin Keller-Sutter.

Fig. 3: Variants of spurious threatening emails supposedly sent by law enforcement authorities and featuring a mix of senders and logos. Bottom right: the scammers made fraudulent use of the NCSC's name, albeit with the wrong logo.

4.2.2 Web administrators targeted

There were also fake extortion attempts targeting web administrators in the second half of 2022. The NCSC received a total of 114 reports of this type of fraud. The extortion message, usually sent via the contact form on the website, but sometimes by email, claims that the website has been hacked and the underlying databases have been stolen. It ends with a threat to publish the data. All the demands have a structure and wording similar to so-called fake sextortion emails. These forms of blackmail typically use the same Bitcoin addresses in the emails sent to different companies, so if someone were to make a payment, it would be impossible for the blackmailers to find out which victim paid the ransom. This is a classic type of bluff.

A subvariant of this type of fraud, observed for the first time in the period under review, saw security officers being contacted by purported researchers and alerted to supposed vulnerabilities in their systems. The email ended with an explanation that, as part of the "responsible disclosure" process for vulnerabilities, a corresponding reward was expected. However, the notification was not about an actual security vulnerability, but merely pointed out that the HTTP Strict Transport Security (HSTS) function was not enabled on the company's website.[3] Although it is of course highly recommended to implement HSTS, its lack can hardly be considered a classic security vulnerability. There are numerous sites on the internet that allow even people with no specialised IT knowledge to check websites for common security features. The scammers take advantage of these sites and web administrators' insecurity in the hope of getting a reward.

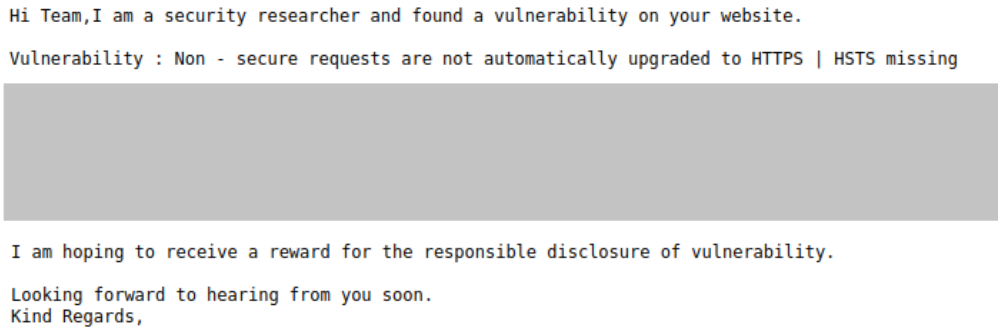

Fig. 4: Email reporting an alleged security vulnerability of the web server and requesting a reward.

4.2.3 Investment fraud

With 219 reports and total losses of more than CHF 4 million, investment fraud remained one of the most financially damaging phenomena reported to the NCSC in the second half of 2022. This amount is only the total of the sums actually reported. As not all cases are brought to the NCSC's attention and a considerable number presumably go unreported, the actual losses are likely to be much higher. Various scams are used to trick victims into investing their money on dubious sites. The best-known scam involves fake advertisements in which well-known figures explain how to make a lot of money quickly. Fake interviews with Roger Federer were doing the rounds a few years back, followed by fictitious advertising sites referring to the German-language version of the TV show Dragons' Den (Höhle der Löwen). Now, even the names of federal councillors are regularly exploited for such advertising. In the second half of the year, the NCSC received a total of 469 reports of fraudulent advertising promising big money fast. However, this number was slightly down on the previous half-year period, when 619 reports were received. Although the NCSC also receives reports from victims who have fallen for such fraudulent advertising, the success rate of this technique is likely to be low. Attackers are therefore increasingly looking for other tricks to convince victims to invest their money. One frequently observed method involves making seemingly innocuous contacts on social media or dating sites. The scammers spend a lot of time gaining the victims' trust before persuading them to make a supposedly lucrative investment. The fraudsters claim to have had their own experience of getting rich through such investments.

[3] If HSTS is activated for a website, an additional header is used in the HTTPS protocol that strictly instructs the browser to use only encryption from the first time the website is accessed.

4.3 Phishing reports

In the second half of 2022, the NCSC received a total of 2,177 phishing reports via its reporting portal. This was slightly fewer than in the previous half-year period, when 2,544 reports were received. While phishing emails targeting credit card details continue to dominate, the attackers often focus on other data such as email logins. Company email accounts are particularly valuable to attackers, as described in section 4.3.2, but private individuals' email accounts are also highly prized. The email account is now the linchpin of all online shops and services. If users forget their password for an online service provider, they can usually reset it via their email account. This means that, with this email password, attackers can gain access to multiple accounts. If online store accounts are hacked in this way, goods and services can be obtained fraudulently. However, scammers are now also using hacked email and social media accounts to lend weight to their fake extortion attempts (see section 4.4.2).

Number of detected phishing URLs per week

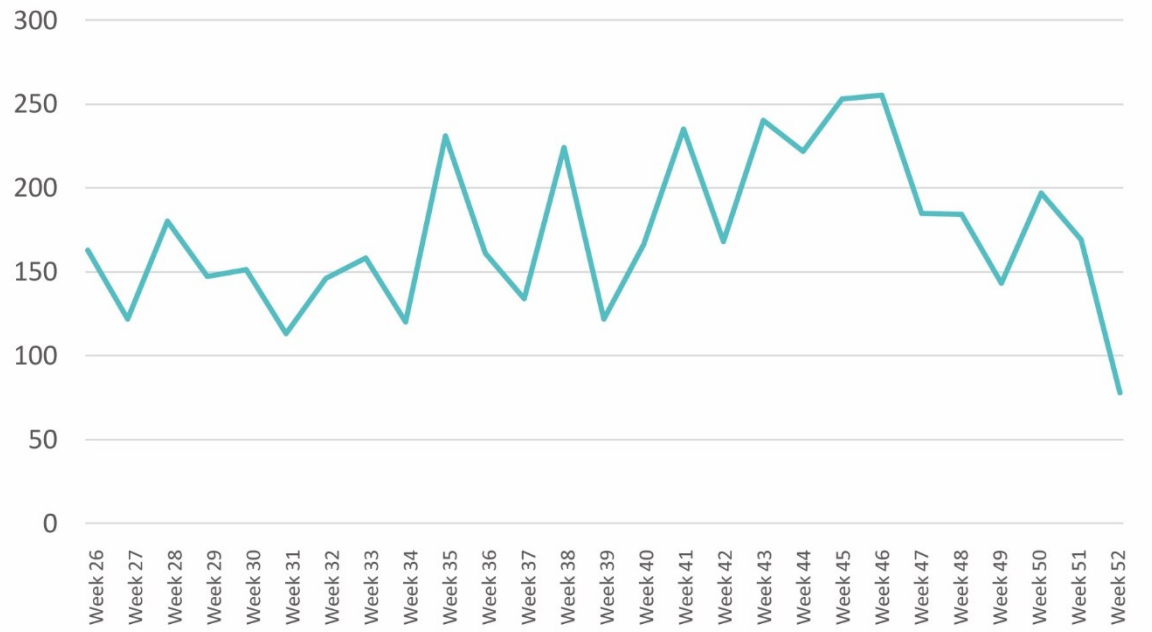

Fig. 5: Number of phishing URLs checked and confirmed by the NCSC per week in the second half of 2022; current data can be found at: https://www.govcert.admin.ch/statistics/phishing/

4.3.1 How phishers exploit probability

Emails claiming that Swisscom or Sunrise bills have been paid twice, text messages with purported ticket refunds, or fake parcel delivery notifications: what all these have in common is that there is a relatively high probability that the story invented by the attackers will seem plausible to the victim. Many people will be expecting a parcel, have direct debits with Sunrise or Swisscom, or have actually submitted a refund claim to SBB, the Swiss Federal Railways. In such cases, the attackers use probability theory to their advantage, basing their stories on transactions frequently carried out by members of the public. A classic example of this concerns the fake notifications from parcel service providers, which trick the victim into opening a page where credit card details need to be entered. Fake parcel notifications accounted for 532 phishing reports, almost a quarter of the total. Since the COVID-19 pandemic, there has been a sharp increase in people ordering goods online, so the probability that someone will actually be expecting a parcel is high. Assuming that 10% of the population places an online

order in a given week, the story will fit 10,000 people if the attackers send out 100,000 emails per week. The attackers also exploit probability in phishing attempts involving alleged double payment of telecoms bills. If messages about Swisscom bills that have supposedly been paid twice are sent to bluewin.ch addresses, or similar messages relating to Sunrise bills are sent to sunrise.ch addresses, there is a high probability that the bogus story will fit and the recipients will fall for the phishing attempt. In late 2022, attackers focused on purported refunds from the rail operator SBB. Here, too, the story seems to have been plausible in many cases, as shown by numerous reports from people who were actually awaiting a refund from SBB.

Fig. 6: Phishing attempt involving the alleged refund of an SBB ticket.

4.3.2 Increasingly professional Office 365 phishing targets employees

Office 365 login credentials are of particular interest to attackers, as these accounts can be used as the launchpad for further attacks, such as business email compromise. With 45 reports and losses of almost half a million francs notified to the NCSC in the period under review, this type of fraud is among the phenomena entailing great potential for damage. Here too, it can be assumed that many cases go unreported. Hacked accounts are searched for previously issued invoices. The fraudsters change the IBAN on the invoice to that of their own account, then resend the invoice under some pretext or other, asking the client to use the new IBAN. With access to Office 365 company accounts, the attackers can also exploit internal data to launch social engineering attacks against other employees or to blackmail the company. Attackers will often also set up email forwarding rules which send them a copy of all the emails the victim receives. That way, once the victim realises they have been phished and changes their login details, the attackers will continue to receive all their emails. It is therefore not surprising that phishers pull out all the stops to gain access to employees' credentials. These attempts are becoming increasingly professional and thus harder to detect. Employees should therefore receive regular training, and it is advisable to implement two-factor authentication whenever possible. This offers an additional layer of protection to prevent Office 365 accounts from being hacked.

Fig. 7: Purported project proposal to be downloaded from a server. A blurred document is shown in the background. To open this document, the user is told that they must first enter their Office 365 password.

4.4 Malware and hacking reports

4.4.1 Unchanged amount of ransomware

A total of 155 reports in connection with malware were registered in the second half of 2022, representing a sharp decline on the previous half-year period. The number of reports received in that period was 592, almost four times as many. The reason for this reduction is that there were no major waves. A year ago, the FluBot malware alone triggered 405 reports, whereas not a single FluBot case was reported in the current period.

Ransomware reports remained at much the same level. There were 76 of these, accounting for almost half of all reports in the malware category. Around a third of the reports concerned private individuals and two thirds businesses. The LockBit ransomware is often used in attacks targeting businesses. This malware is known for the fact that not only is data encrypted, but it is also stolen and posted on the internet if the ransom is not paid. Such double extortion approaches are being observed more and more frequently. This trend is likely to continue in 2023. Many businesses have recognised the threat of ransomware and responded with an adapted backup strategy. Consequently, pure encryption is no longer lucrative enough for attackers. They try to secure a ransom by threatening to publish the data. Other reported ransomware families targeting businesses in the last half-year period include Play, MedusaLocker, BlackCat, Magniber and Makop. In most cases, the infection vector is not yet

known at the time of reporting. However, the initial infection is usually due to a vulnerability or misconfiguration. This is also confirmed by a Microsoft study, according to which 80% of ransomware attacks can be traced to common configuration errors in software and devices.[4] Timely patch management, regular checking of the system configuration and consistent use of two-factor authentication for access can effectively reduce the risk of a ransomware attack.

When it comes to attacks against private individuals, network-attached storage (NAS) devices remain the primary target for attackers. The most notable example is the DeadBolt malware, which accounted for seven reports. Devices that are directly accessible from the internet are particularly exposed. These are systematically scanned for vulnerabilities or for misconfigurations such as weak passwords. It is therefore particularly important to always keep these systems up to date and to protect access appropriately.

QakBot continues to be the most active of the malware families, with a total of 20 reports to the NCSC in the second half of 2022. This malware is spread via emails. A special feature of QakBot is that it uses and connects to existing email threads hijacked in previous attacks. The attackers use the fact that the recipients are familiar with the thread and the alleged senders to try to build up trust, with the aim of tricking the victim into clicking on the link.

4.4.2 Another sharp rise in hacking reports

Reports in the hacking category increased sharply, reaching 276, almost double the figure for the previous half-year period. Social media accounts were the primary target, with 108 reports. Hacked social media accounts are now being used to lend credence to fake sextortion attempts (see below). Another common use of hacked social media accounts is to promote investment scams. Especially with accounts that have many followers, this is a popular way of getting information about dubious investment opportunities to as many potential victims as possible.

4.4.3 Fake extortion with real attacks

Up to now, fake sextortion emails have always been bluffs. The perpetrators claim in each email that they have collected photo or video material which shows the email recipient allegedly visiting pornographic websites. The extortionists threaten to publish the photo or video material if the ransom demanded is not paid by a certain deadline. During the period under review, 1,138 fake sextortion emails were reported to the NCSC. Normally, the scammers are bluffing. They do not have access to the victims' computer and hope that they will be intimidated into paying the ransom. In the last half-year, however, there were also reports where the victims' email account and various social media accounts were hacked shortly before or after the blackmail message was sent. In a total of 33 cases, the fraudsters uploaded pornographic material, resulting in an immediate blocking of the social media accounts and a notification to this effect. This was an attempt to scare the victims into paying up. The credentials are likely to have been obtained from either old data leaks or old phishing attacks. However, cases involving hacked accounts still make up only a very small proportion of the total number of reported fake sextortion emails. This suggests that the login/password combinations used are not very up to date and so do not work for every victim. This is likely to be a secondary use of login/password details that can be bought cheaply on the dark web.

---

4 Cyber Signals (microsoft.com)

4.5 Miscellaneous reports

4.5.1 Powerlessness in the face of phone number spoofing

Reports of spoofed telephone numbers have also skyrocketed. This is where attackers manipulate the phone number displayed so that a victim's phone shows a number that is not the attacker's, with a view to instilling a false sense of security. The NCSC received a total of 781 such reports in the second half of 2022 alone, compared with just 26 in the whole of 2021. This is due to a new approach taken by dubious foreign call centres. In order to ensure that those called actually answer as many of their advertising calls as possible, the attackers use inconspicuous Swiss numbers. This approach is seemingly innocuous at first glance, but it has far-reaching consequences for the person to whom the number belongs. In the event of a missed call, many return the call if the number is displayed, causing the owner of the number to be inundated with calls. Since the call centres use the same number for weeks or even months, this is extremely trying for the victims.

Unfortunately, little can be done about such calls. Since the calls from the call centres originate abroad, the Swiss telephone providers' obligation to verify number use is not applicable. It applies only if the call originates from the provider's network. If the calls do not stop, the only solution is to change number.

5 Situation

5.1 Initial access

Cyberplayers are organised according to a division of labour and specialise in individual stages of cyberattacks. Obtaining access to user accounts or remote access to computer systems is the first step in most types of cyberattack. Such initial access can be gained in various ways, and once obtained can be passed on to other players for them to exploit.

5.1.1 Username/password

Login details are usually obtained through phishing (see also section 4.3). In other words, it is users themselves who unwittingly provide them to the attackers. Login details can also be recorded by malware (keyloggers) when they are entered on an infected device.

Credentials for remote access via Remote Desktop Protocol (RDP) or virtual private networks (VPNs) are often exploited to penetrate enterprise networks.

Recommendation:

Two-factor or multi-factor authentication, for example, offers protection against this threat. This is where a username/password combination is not enough to access the secure system or user account, but additional information is required, such as a unique code sent to a mobile phone, or the access must be approved by an authentication app.

5.1.2 Malware (Trojans)

Malware that, once installed, creates a backdoor to the system remains a commonly used method to establish initial access.

The most popular vector for spreading such Trojans is still email. The text in the emails often refers to everyday things such as offers, deliveries, invoices or bills. Sometimes, exclusive information on current events such as the war in Ukraine, natural disasters or sporting events is provided in the hope of arousing curiosity. In many cases, urgency is feigned in order to trick recipients into acting rashly. In one scenario, such emails are sent in bulk to a large number of recipients (malspam). In another, old email threads previously obtained from compromised email user accounts or hacked email servers are used to target participants in these conversations (thread hijacking) and send them a Trojan.

Another way in which users are tricked into installing malware is malvertising, where fraudsters purchase online advertising space or infect sponsored search engine results. This makes it look as if the software that users are searching for, e.g. a browser, a communication app or a video player, is available via the ad in question. However, a Trojan is installed at the same time as the (often free) software. A similar method involves users clicking on an advertising link and being taken to a page claiming that their browser needs to be updated. The page is dynamically adapted to the browser used, which the website can recognise. Clicking on the update button then downloads a file that installs the Trojan when run. Such fake updates can also be spread via hacked websites.

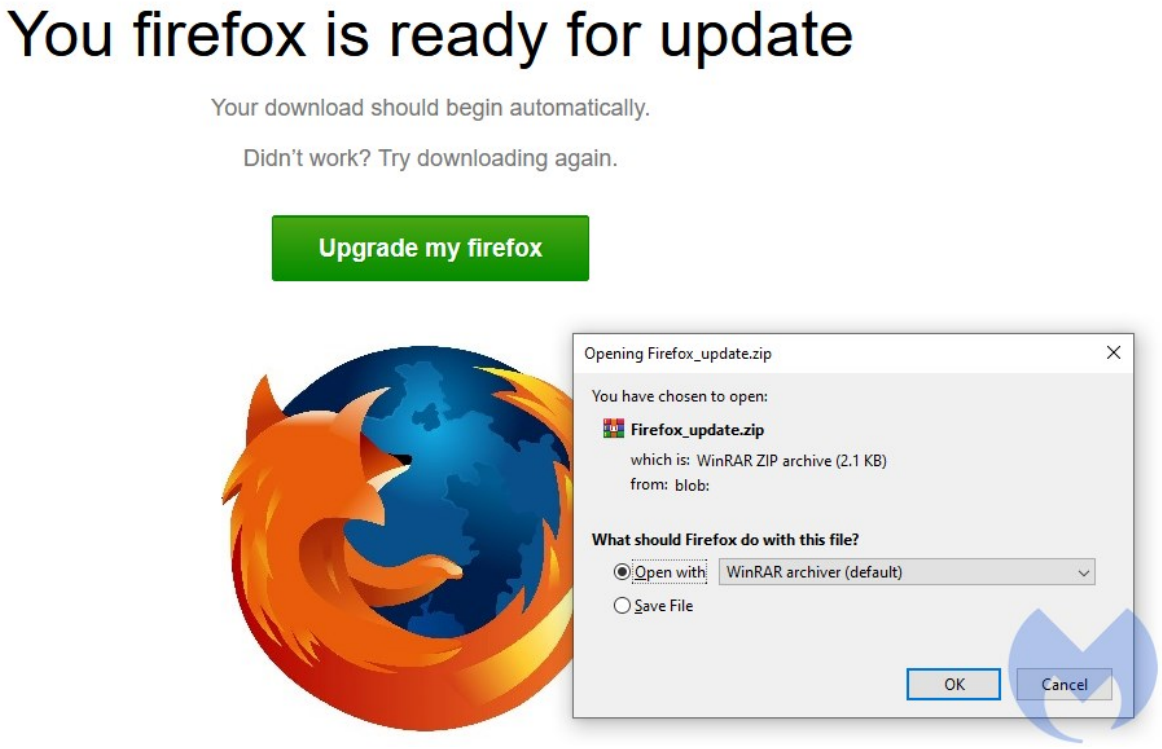

Fig. 8: Fake update (source: Malwarebytes.com)

Conclusion/recommendation:

Do not open any attachments or click on links in suspicious emails. If in doubt, check with the alleged sender whether the email is really from them.

When searching for software on the internet, check that you are on the manufacturer's website or another trustworthy website (e.g. a well-known computer magazine) before downloading it. Be wary whenever a download window pops up. If possible, let programs update automatically. Otherwise, always use the integrated update function or download the latest version directly from the manufacturer.

5.1.3 Exploitation of vulnerabilities

As soon as a product vulnerability becomes known, various players begin to scour the internet for vulnerable systems. After a few hours or days, the vulnerability starts to be exploited. However, vulnerabilities that have been known for some time and for which a patch is available are also regularly exploited. The Known Exploited Vulnerabilities Catalog kept by the US Cybersecurity & Infrastructure Security Agency (CISA)[5] regularly lists old vulnerabilities that could have been fixed by users with effective update management.[6]

As well as bugs resulting from developer error, which can be patched, vulnerabilities can also be caused by the configurations selected when implementing products. Various manufacturers provide configuration instructions for hardening their products.

Recommendations:

When using new products, check their security and data protection configuration. Make sure that only those features you actually need are enabled.

Both private individuals and businesses should always keep software up to date on all devices, preferably by means of an automatic update function.

End-of-life software for which the manufacturer is no longer providing updates should be replaced.

The NCSC regularly informs organisations that are vulnerable because of outdated systems.[7] It receives corresponding tips from security researchers who search the internet for such systems. Criminals can search for vulnerable systems in the same way and subsequently attack them. Therefore, system operators should not wait to be notified by the NCSC. It is strongly recommended to have your own effective software management with inventory and update processes.[8] However, prompt action is required at the latest when an organisation receives a registered letter from the NCSC.

---

5 Known Exploited Vulnerabilities Catalog (cisa.gov)

6 Adobe, Apple, Cisco, Microsoft Flaws Make Up Half of KEV Catalog (darkreading.com)

7 High time to fix the security vulnerabilities in Microsoft Exchange Servers (ncsc.admin.ch);
MS Exchange vulnerabilities still not patched (ncsc.admin.ch);
Over 2,800 vulnerable Microsoft Exchange servers in Switzerland once again (ProxyNotShell) (ncsc.admin.ch);
Microsoft Exchange servers still vulnerable in Switzerland (ProxyNotShell) despite NCSC warning (ncsc.admin.ch)

8 See semi-annual report 2021/1 (ncsc.admin.ch), section 3.2

5.2 Malware

5.2.1 Malware spread

The chart below shows malware families analysed and identified by the NCSC over the last six months. The analysed files and codes come from various sources such as sensors, reports from security officers for critical infrastructures, members of the public and SMEs. The reported files and codes are analysed and allocated to a malware family. The NCSC informs the operators of critical infrastructures of any indicators of compromise (IOCs) it finds, so as to allow them to take protective measures.

Analysis of malware families by the NCSC

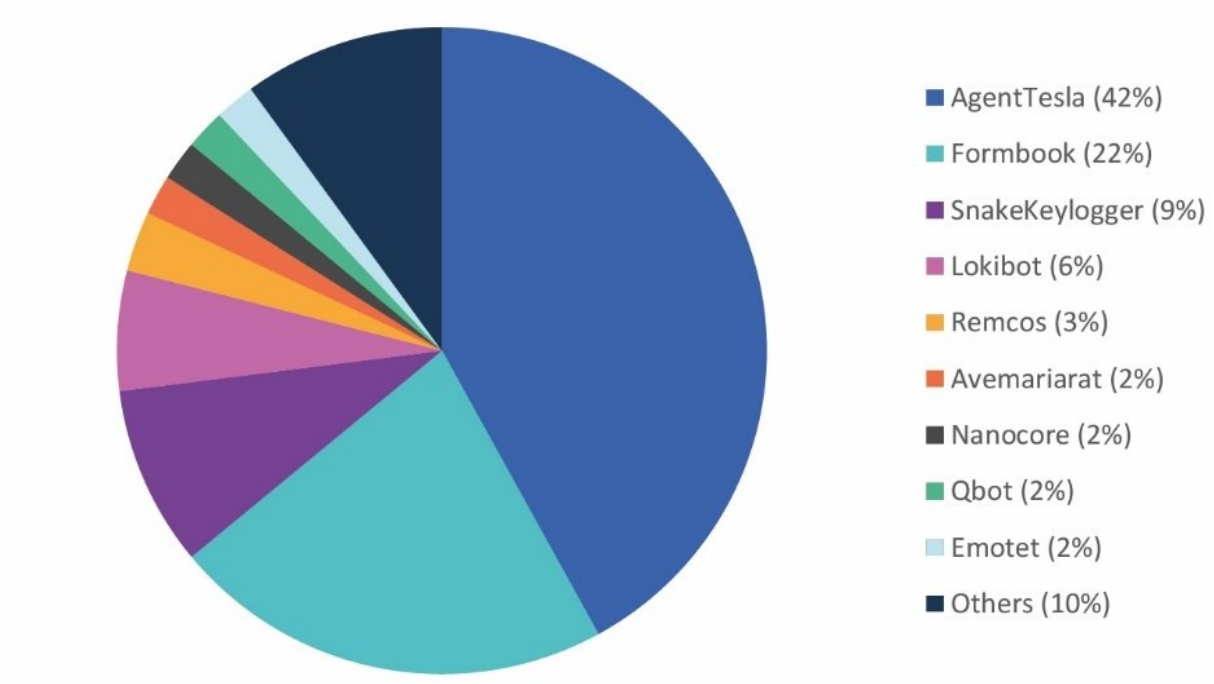

Fig. 9: NCSC analyses of malware families spread in Switzerland in the second half of 2022

5.2.2 Ransomware

Ransomware attacks remain a common cyberthreat faced by organisations in Switzerland, and are probably the most serious in terms of consequences. In the second half of the year, primarily small and medium-sized industrial companies and IT service providers were affected. Ransomware developers are adopting new strategies and methods to infiltrate systems and blackmail their victims. These include new versions of the ransomware, code in the Rust programming language used for Windows and Linux, and publication of data on regular websites (not just the dark web). They often rely on double extortion to maximise profits: data is exfiltrated from the compromised network before being encrypted, so that the victims can also be blackmailed with the threat of publication. Given the rising number of ransomware cases, the availability of ransomware as a service (RaaS) and the proliferation of ransomware strains and families, cybersecurity firms and government agencies are working more closely together to find decryption keys and develop decryption programs.

5.2.2.1 Examples of incidents in Switzerland

Play: when an incident affects third parties

In late November, a Bern-based provider of cloud computing services had to shut down its data centres due to a ransomware attack, probably launched by the Play group. Some of the data was saved thanks to backups carried out four days earlier. This incident had consequences for all the provider's customers, with some no longer able to access their cloud service. This meant, for example, that they were unable to continue issuing invoices or calculating and paying salaries. However, no data was exfiltrated during the attack. Similar incidents bearing Play's signature were also reported in other cantons over the course of the year.

Double extortion – attack combining encryption and data loss

On 5 September 2022, a chocolate factory was hit by a ransomware attack that affected its production, logistics and administration. Two weeks after the attack, these departments were fully operational again. However, the company confirmed that the cyberattack had probably resulted in a data leak. A month later, ransomware group BianLian published files about the firm's operations on the dark web.

BianLian uses custom malware written in the Go programming language.[9] The group started its online activities in December 2021, ramped them up in July 2022 and massively bolstered its command-and-control (C2) infrastructure in August 2022.

5.2.2.2 Incidents abroad: attacks on the energy sector

In the semi-annual report 2022/1, the NCSC presented some examples of sectors affected by ransomware, and noted that criminals appeared to be particularly targeting governments, authorities and energy infrastructures. This trend was confirmed in the second half of the year, and much was written about the energy sector. The heightened interest in this industry may be due in part to the fact that the energy sector, as critical infrastructure, has to be permanently operational and is under particular pressure in the current geopolitical context. Several European energy providers were hit by ransomware attacks.[10] Not surprisingly, the perpetrators who claimed responsibility for these incidents, such as BlackCat and Everest, are pro-Russian groups. Energy suppliers in Switzerland have so far been spared such attacks, and it is currently fairly unlikely that Switzerland will be specifically targeted. However, opportunistic attacks on vulnerable systems or collateral damage from attacks on European suppliers cannot be ruled out.

5.2.2.3 Most active protagonists and most commonly used infection vectors

The most commonly deployed ransomware in Switzerland in 2022 was LockBit (version 2.0 or 3.0, the latter also known as Black), followed by DeadBolt and Play (see section 4.4.1). Globally, the LockBit group continued to lead the field, followed by Black Basta and BlackCat.

---

9 MalwareHunterTeam on Twitter: A BianLian x64 ransomware sample (twitter.com)

10 2022 saw ransomware attacks on major gas companies in Italy, such as GSE SpA and Amalfitana Gas Srl, the oil company Eni, the Luxembourg electricity and natural gas network operator Creos Luxembourg SA, and Greece's National Natural Gas System Operator (DESFA).

In some months, other groups unexpectedly topped the rankings, although not for long. Examples include Hive, Sparta, Cuba, Royal and BianLian.

LockBit Black: version update keeps LockBit in top spot

In July 2022, the LockBit group announced the development of version 3.0 of its ransomware. This upgrade made its presence felt in Switzerland from November 2022 onwards, with the police recording a rise in cases linked to this malware.

However, some sectors were spared, as LockBit's code of ethics (or its terms of service as a RaaS group) does not allow the encryption of data at schools and hospitals. Nevertheless, a Canadian children's hospital did fall victim to such an attack. It turned out that the perpetrators were affiliates of the LockBit group. The group apologised on social media and said it had kicked out the affiliate in question. It also provided the hospital with a free decryptor to unlock its data.

As part of investigations into LockBit, French and Canadian authorities, together with the FBI, were able to identify around 1,800 actual or suspected LockBit victims.[11] The attacked systems had a security vulnerability in their FortiGate or SonicWall firewalls. Affected organisations in Switzerland were notified by the police.

Agenda and Hive: old ransomware given new lease of life by Rust

Many ransomware players have developed upgraded versions of their software in the cross-platform language Rust, meaning that the malware can be deployed on both Windows and Linux operating systems. One example is Agenda (also known as Qilin), originally written in the Go programming language. Currently, the authors of Agenda seem to be in the process of migrating their ransomware's code to Rust, as the latest editions of the software are missing some features that were in the original code. Agenda, like the ransomware Royal, uses partial encryption (also called intermittent encryption), where the percentage of file content to be encrypted is determined by set parameters. This allows for faster encryption while avoiding detections that rely heavily on read/write file operations. Attackers are increasingly using Rust, as it is harder to analyse and many antivirus programs are currently not very good at detecting malware written in Rust. In Switzerland, a communal administration in the canton of Zurich was hit by Agenda ransomware. It was able to recover the encrypted data thanks to backups.

BlackCat and IceFire: publication of leaked data on the internet

A new extortion technique developed by ransomware group ALPHV/BlackCat involves creating a copy of the victim's website and publishing the stolen data on it in order to increase pressure on the victims. On the copied website, BlackCat replaces the original headings and subheadings to organise the leaked data. The cloned website is put online so that the stolen files are more readily available than they would be on the dark web. The extortion website is often hosted on a typo domain.[12] This is more problematic for the affected company than releasing the data on a Tor-network website on the dark web, as data posted on regular websites can be easily accessed and viewed by anyone. This puts added pressure on victims to pay the ransom, as they want to avoid their customers or other people seeing the data.

---

11 Police arrest suspected LockBit operator as the ransomware gang spills new data (techcrunch.com)

12 Also known as a typosquatted domain, e.g. adimn.ch, adnim.ch or adrnin.ch instead of admin.ch

This idea has been taken up by the ransomware group IceFire, which attacked a Swiss company in mid-August 2022. IceFire appeared on the scene in March 2022, using the same technique as BlackCat to pressurise its victims.

Play aka PlayCrypt: governmental focus

From its first appearance in summer 2022, the Play group focused its attention on government agencies. This is rather unusual given the law enforcement reaction that has to be expected after such attacks. Most of Play's attacks take place in Latin America. However, there have also been victims on other continents and in other sectors besides public administration.

Play is known for its strategy of big game hunting, i.e. attacks on large, financially powerful organisations, using Cobalt Strike for the post-breach phase and SystemBC RAT for persistence, for example. Just recently Play hackers have started exploiting the ProxyNotShell vulnerabilities in Microsoft Exchange. Analyses have revealed parallels between the ransomware variants Play, Hive and Nokoyawa.

BianLian and MegaCortex: decryption using decryptors...

In January 2023, a free decryptor (program for decrypting ransomware-encrypted files) was released for the BianLian ransomware strain, just six months after its peak impact in summer 2022.[13] In addition, a developer of the MegaCortex ransomware was arrested in a joint action by Europol and the Zurich cantonal police, enabling decryption software to be developed for this strain. There are now many free decryption programs available online.[14] Cybersecurity companies are scrambling to develop these in order to tackle the ever-growing number and variety of ransomware strains.

… and using decryption keys (DeadBolt)

In October 2022, Dutch police managed to obtain 150 decryption keys from ransomware group DeadBolt by means of trick Bitcoin payments.[15] DeadBolt, which mainly encrypts NAS devices manufactured by QNAP, has also claimed a number of devices in Switzerland among its victims. Getting hold of these keys was a major victory, as it enabled multiple victims to decrypt their data carriers. It is now possible to check online whether a key is available for a DeadBolt-infected device.[16]

Conclusions, outlook and recommendations:

Ransomware attacks increasingly involve both encryption and exfiltration of (sometimes sensitive) data, a technique known as double extortion. Some attackers no longer even bother to encrypt the systems and just threaten their victims with publishing their data.

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

Ransomware – What next? and A data leak – what next? (ncsc.admin.ch).

---

13 Decrypted: BianLian Ransomware (avast.io)

14 See, for example, the No More Ransom project (nomoreransom.org)

15 Police tricked a ransomware gang into handing over its decryption keys. Here's how they did it (zdnet.com)

16 Deadbolt Decryption (responders.nu)

5.3 Industrial control systems (ICS) and operational technology (OT)

Destructive cybersabotage attacks are sporadically observed in the context of geopolitical conflicts,[17] as recently demonstrated by the war in Ukraine. In order to have an impact on physical processes, it is almost inevitable that the operational technology and/or its control systems will have to be manipulated. Only in very rare cases are the controlled physical processes directly affected. It is much more common for the server and network infrastructure to be attacked in order to disrupt operations.[18]

5.3.1 Sabotage attempts in conflict situations

At the start of the war,[19] attempted sabotage attacks using malware specifically targeting electricity supply systems[20] were foiled, attack infrastructure[21] used by the same players was exposed, and a panoply of attack tools[22] were published prior to their deployment. In the second half of the year, attempts at sabotage were limited to the use of destructive wipers[23] and destructive attacks masquerading as ransomware.[24] Specific abilities to manipulate industrial systems were no longer observed, but the attacks were directed against IT systems of transport organisations[25] in Ukraine and Poland, for example.

Claims by hacktivist groups like OneFist[26] and GhostSec[27] that they were involved in incidents at industrial plants have not been confirmed or independently verified. The clips posted by the groups point to simple attempts at manipulation of internet-accessible and poorly protected displays or user interfaces for industrial controls.

5.3.2 Strained energy supply sector targeted

A side effect of the war in Ukraine has been to impair the security of energy supply in Europe and thus also in Switzerland. In Switzerland, this has particularly affected gas and electricity. To reduce the likelihood of shortages, an energy-saving campaign was launched, among other initiatives.[28]

In such a tight situation, a successful cyberattack on supply system control mechanisms could have more serious implications than if sufficient substitution options were available. Barring an escalation of the war to other parts of Europe, a targeted attempt at state cybersabotage[29] against Swiss energy supply systems remains unlikely. A far greater danger is posed by

---

17 See in particular Stuxnet in the semi-annual report 2010/2 (ncsc.admin.ch), sections 4.1 and 5.1) and Triton/Trisis in the semi-annual report 2017/2 (ncsc.admin.ch), section 5.3.2

18 How Many ICS-OT Directed Attacks In 2022? (linkedin.com)

19 NCSC semi-annual report 2022/1, sections 3 and 5.4

20 Industroyer2: Industroyer reloaded (welivesecurity.com)

21 New Sandworm malware Cyclops Blink replaces VPNFilter (ncsc.gov.uk)

22 APT Cyber Tools Targeting ICS/SCADA Devices (cisa.gov)

23 Russian APT groups continue their attacks against Ukraine with wipers and ransomware (eset.com)

24 RansomBoggs: New ransomware targeting Ukraine (welivesecurity.com)

25 New "Prestige" ransomware impacts organizations in Ukraine and Poland (microsoft.com)

26 The Increasing Threat Posed by Hacktivist Attacks (forescout.com)

27 Country-Specific ICS Targeting: Shining a Light on GhostSec (otorio.com)

28 Energie: Bundesrat startet Sparkampagne (admin.ch)

29 Switzerland's Security 2022: The Federal Intelligence Service publishes its latest situation report (admin.ch)

ransomware attacks.[30] If the resulting encryptions paralyse systems involved in energy supply operations, this could lead to restrictions and interruptions in productive operation.[31]

Another factor in this context is the systems' physical security. The example of the mechanical severing of Deutsche Bahn control cables[32] shows, on the one hand, the real threat posed by sabotage attacks on the ground.[33] On the other hand, it highlights the importance of planning measures to restore operational readiness in order to strengthen the resilience of the overall system.

Conclusion/recommendations:

Thinking about the resilience of systems and organisations is key to keeping industrial plants operational, even in difficult situations. This also includes continuous training for staff.

Suitable measures can be found in the ICT minimum standard of the Federal Office for National Economic Supply (FONES) and the respective sector standards:

ICT minimum standard (ncsc.admin.ch)

On its website, the NCSC recommends measures to protect industrial control systems (ncsc.admin.ch).

5.4 Vulnerabilities

5.4.1 Systems with publicly viewable configuration files

Security researchers regularly report vulnerabilities to the NCSC via the coordinated vulnerability disclosure process.[34] A number of vulnerabilities reported in this half-year period can be traced back to a software misconfiguration, where the configuration files are in a directory on a web server and can be accessed without restrictions.

A common example concerns the files created by the versioning software Git. This software creates a folder called ".git " in which all the source code is stored. If this folder is visible and accessible via a web server, an attacker with technical know-how can access potentially sensitive data such as login credentials or passwords.

The NCSC identified 1,300 affected systems in Switzerland and notified their operators.

Git is not the only software that creates such configuration files and hidden folders. Another example is PHP profiler pages, a component of the Symfony framework.[35] Text files such as .env are also often used to store access keys and passwords used by a system. If they do not have the correct access rights, they too can be read and misused by an attacker.

30 Dragos Industrial Ransomware Analysis: Q4 2022 (dragos.com)
31 Cybersecurity Research Report January 2023 (nozominetworks.com)
32 Sabotage bei der Bahn: Viele vertrauliche Infos sind offen zugänglich (heise.de)
33 BfV-Sicherheitshinweis für die Wirtschaft 04/2022 (wirtschaftsschutz.info)
34 Coordinated Vulnerability Disclosure (CVD) (ncsc.admin.ch)
35 Covid-Center & andere Webseiten: Bedienen Sie sich! (dnip.ch)

The NCSC works actively with security researchers to inform affected operators and raise awareness of the risks and dangers of such configuration errors.[36]

Conclusion/recommendations:

Configuration files like the .git folder should never be publicly accessible on the internet. If it is not possible to remove the folder at short notice, access to the folder should at least be restricted and protected accordingly (e.g. using .htaccess rules or similar technical access restrictions, depending on the technology used).

Preventive measures such as reviewing and adapting the development process are even more effective. This should ensure that only the desired and intended data (build files) is stored at all. Sensitive or secret data such as passwords, API keys, etc. should never be stored in the source code or in the application itself (hardcoded), or at least it should be ensured that it is not stored in the .git folder but instead is ignored (gitignore file). These basic security measures and best practices should be observed in all instances.

5.4.2 ProxyNotShell

In late September 2022, a Vietnamese cybersecurity company[37] reported attacks that had taken place on critical infrastructures worldwide in August 2022. Its investigation identified two zero-day vulnerabilities in Microsoft Exchange servers that were leveraged for the attack. The first vulnerability (CVE-2022-41040) was a server-side request forgery (SSRF) that enabled an authenticated attacker to trigger the second vulnerability (CVE-2022-41082), known as a remote code execution (RCE) vulnerability. This allows malicious code to be executed remotely via the internet. The two vulnerabilities in combination could be used to gain access to vulnerable systems, for example.

Shortly afterwards, Microsoft confirmed the vulnerabilities in Microsoft Exchange Server 2013, Microsoft Exchange Server 2016 and Microsoft Exchange Server 2019, and recommended that immediate measures be taken. The vulnerability was named ProxyNotShell because it was related to an Exchange vulnerability named ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) which emerged in 2021 and bore certain similarities to the new vulnerability.

On 10 November 2022, Microsoft released software updates that patched the vulnerabilities. On 18 November 2022, the NCSC identified 2,800 servers in Switzerland that had still not installed the latest security updates and were vulnerable at that time.[38] It notified those affected by registered letter in early December 2022.

Conclusion/recommendations:

The ProxyNotShell vulnerability was already actively exploited before an official patch was available. In these cases, it is important to react quickly and follow recommendations – which

[36] Unprotected .git folders on the internet pose a security risk (ncsc.admin.ch)
[37] Two Microsoft Exchange zero-days exploited by attackers (helpnetsecurity.com)
[38] Over 2,800 vulnerable Microsoft Exchange servers in Switzerland once again (ProxyNotShell) (ncsc.admin.ch)

can go as far as shutting down the vulnerable system – until an official patch is available. A clear strategy for direct internet access to administrative interfaces and internal applications can help reduce an organisation's attack surface. If sensitive applications need to be accessible via the internet, access to them should be specially protected (e.g. using a VPN with multi-factor authentication, access list of authorised IPs for maintenance, etc.). If no patch is available yet for an actively exploited vulnerability, good management of external access can provide additional reaction time for defensive measures, if required. However, this is no substitute for the installation of system updates and patches as soon as they become available.

5.4.3 Retbleed

On 12 July 2022, ETH Zurich[39] disclosed a vulnerability in Intel and AMD microprocessors. Known as Retbleed, it potentially allows an attacker to access any memory area. The name Retbleed was coined by analogy with previous vulnerability names such as Heartbleed, which also allowed data to be read from memory. RET is short for RETURN, a program instruction in processors. Particular caution is required with shared infrastructure and when running untrusted software.

The NCSC assisted the ETH Zurich researchers with coordinating the disclosure and assigning the CVE numbers. The CVE numbers assigned to Retbleed were CVE-2022-29900 (for AMD processors) and CVE-2022-29901 (for Intel processors).

Conclusion/recommendations:

Retbleed is a very complex vulnerability that has not been actively exploited to date, or at least no exploitation is known.

However, the vulnerability requires certain conditions in order to be successfully exploited, so the risk to users is very limited.

Both Intel and AMD are working on patches to minimise and resolve the vulnerability. As ever, it is important to run only trusted software on a system and to be sceptical about third-party software. It is also essential that manufacturers' updates and patches be installed promptly and their recommendations followed.

5.5 Data leaks

Data security is one of the key challenges of digitalisation, both for data owners and for individuals and businesses whose information is included in data sets. Despite steadily increasing awareness of data security and data protection in the digital space, data leaks, for a variety of reasons, remained an issue in the second half of 2022. Insufficiently protected or maintained systems, as well as human error and cyberattacks, resulted in the publication of sensitive data. In the case of cyberattacks, data theft – often coupled with encryption (see

[39] Speculative calculations open a backdoor to information theft (ethz.ch)

section 5.2.2 on ransomware) – may be used to blackmail the data owners and/or sell the data to the highest bidder.

Although ransomware attacks grab the headlines, it is important to emphasise that a considerable proportion of cases involving the publication of sensitive data could be avoided by greater awareness concerning data management. The following sections highlight two cases where information was published unwittingly or data entrusted to third parties was passed on without authorisation.

5.5.1 Metadata in published files

Websites are key platforms enabling companies and institutions to communicate and provide information to the outside world. In the process, internal information in the files' metadata[40] may also unintentionally be made public. For example, the names of employees, usernames, email addresses, folder structures, the software used and its version numbers may become visible to outsiders. With regard to cyberattacks, information about version status and the application used is particularly valuable to attackers, as it can suggest possible attack vectors.

This issue relating to metadata has also been recognised in the Federal Administration, which has introduced appropriate measures to raise employee awareness.

Conclusion/recommendation:

As a first step, organisations should take stock of the situation and check all published files to see what metadata they contain. The files can then be cleaned up if necessary and republished. Furthermore, it is recommended that files be cleaned according to a prescribed process before being shared or published. There should be appropriate employee awareness and training in this regard.

5.5.2 Disposal of IT resources and data carriers

In December 2022, it was reported in the media that the Department of Justice of the Canton of Zurich had failed to properly dispose of storage devices for a number of years. As a result, between at least 2006 and 2012, sensitive, unencrypted data ended up in the hands of criminals. The data carriers contained, among other things, telephone numbers and private addresses of prosecutors and judges, criminal files, psychological reports and building plans.[41]

An external investigation report on the incidents also found that employees had created shadow files on local drives in order to process cases more efficiently due to an unreliable legal information system. However, these drives were not adequately protected, as the data on them was not systematically encrypted.[42]

---

40 Metadata (file information and properties) is contained in all types of files. While documents such as Word or PDF files may contain author details, for example, photo files include, among other things, location information (GPS) as data fields in the metadata.

41 Schweiz aktuell – Datenleck bei Justizdirektion Kanton Zürich: GPK stellt Antrag auf PUK (srf.ch)

42 Datenskandal Justizdirektion: Zürich setzt die Prioritäten falsch (nzz.ch)

Conclusion/recommendation:

This incident perfectly illustrates the need to pay special attention to data security against the backdrop of increasing digitalisation. The processes involved in secure data storage should be user-friendly to ensure that all employees comply with the requirements.

There are various ways to properly dispose of data carriers: overwriting the data or demagnetising or physically shredding the data carrier. If you outsource data erasure, choose the service provider carefully, opt for an appropriate method and ensure that the process for destroying the data (or data carrier) is logged.

The NCSC provides guidance on data leaks for companies.

5.6 Update on Ukraine

5.6.1 Cyberspace activities continuing, but without any notable success

The war in Ukraine remained a major geopolitical event in the second half of 2022. The most important cyberspace incidents in the context of the Ukraine war and the run-up to it were highlighted in the previous semi-annual report.[43] Since then, there have been no significant changes in the types of cyberincidents, but such incidents have seemingly increased in intensity.[44] Thus, the Security Service of Ukraine reported that 4,500 cyberattacks were neutralised in 2022, triple the number from the previous year.[45] Russia therefore continues to exert pressure on Ukraine via cyberspace, but without any obvious success so far. In the last semi-annual report, three hypotheses were proposed to explain the apparent absence of destructive Russian cyberattacks:

1. Russia is successfully conducting destructive cyberattacks against Ukraine, but these are not publicised, principally because the war is ongoing;
2. Russia is carrying out destructive cyberattacks against Ukraine, but Ukraine is successfully defending itself, not least thanks to the support of other countries and private partners;
3. Russia is not carrying out destructive cyberattacks against Ukraine, in particular because the use of conventional military means is better suited to achieve certain goals.

The information that has since become available about cyberspace activities related to the war in Ukraine suggests that the second hypothesis is closest to the reality. Russia appears to be highly active and since October 2022 has been targeting Ukraine's energy infrastructure particularly intensively, but it has been prevented from scoring any successes in cyberspace by Ukraine's effective self-defence.[46] These cyberattacks are apparently not seen as an alternative to conventional military means, but are often deployed simultaneously, including in

---

43 Semi-annual report 2022/1 (ncsc.admin.ch), section 3

44 The number of cyberattacks on Ukraine keeps increasing (cip.gov.ua)

45 SSU neutralized over 4,500 cyberattacks on Ukraine in 2022 (ssu.gov.ua)

46 SSU neutralized hundreds of cyberattacks on Ukrainian cogeneration plants and energy companies in 2022 (ssu.gov.ua)

conjunction with influence operations. An example of this operational multidimensionality was the campaign against Ukrainian power plants in October and November 2022, which featured rocket attacks accompanied by cyberattacks and propaganda. The cyberattacks were intended to increase the pressure on a sector already having to get by with limited resources, some of which had been destroyed by conventional military means. The propaganda aimed to shift responsibility for the consequences of the attacks (including power outages) onto Ukrainian state authorities, local governments or large Ukrainian businesses.[47] However, because Ukraine had anticipated this tactic, the cyberoperations failed to achieve the intended success. This underscores a factor that could explain Russia's lack of success in cyberspace: the absence of new types of attack. The cyberattacks observed were carried out according to familiar patterns which could be thwarted using tried-and-tested defence strategies.[48]

5.6.2 Different cyberattacks with different consequences

Numerous cyberattacks were reported on in connection with the war in Ukraine, including in the non-specialist press. Unfortunately, some of these articles do not detail the nature or impact of these attacks, which prevents a differentiated analysis of the events. The description of selected cyberattacks in the following sections is intended to serve as an example of the different impacts and to underline the need for caution when reading articles that use non-specific terminology.

5.6.2.1 Distributed denial of service (DDoS) attacks

DDoS attacks were one of the most visible types of cyberattack during the period under review.[49] These attacks aim to make websites or other online services inaccessible, mainly by overloading them with a large number of requests. These attacks were mainly carried out by hacktivist groups backing one or other of the warring parties. Pro-Russian hacktivist groups like KillNet target assets and countries based on the support they provide to Ukraine or the sanctions they impose on Russia. In the context of the war in Ukraine, the damage from these attacks has so far been marginal and consisted mainly of reputational damage.

For instance, the DDoS attacks by KillNet on US airport websites in October 2022[50] led to temporary outages of such websites, meaning that passengers were unable to get flight status updates, for example. However, the attacks had no impact on the operational activities of the affected airports.

5.6.2.2 Spreading malware

During the period under review, numerous malware distribution campaigns were reported, mostly targeting Ukrainian institutions.[51] These campaigns aim to gain access to systems by infecting them with malware. In a war context, this access is used primarily for espionage (theft of information) or sabotage (disruption of system functions). The malware is often sent via

47 Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression (cip.gov.ua); Preparing for a Russian cyber offensive against Ukraine this winter (microsoft.com)

48 Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression (cip.gov.ua)

49 Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

50 Coverage of Killnet DDoS attacks plays into attackers' hands, experts say (therecord.media)

51 Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

emails claiming to be from official bodies. This, combined with topical subject matter, is intended to trick recipients into performing an action that is necessary to infect the target system. Another observed tactic is the creation of fake websites, purporting to belong to official bodies, in which the malware is hidden in a program to be installed by the user. Finally, malware can also be spread by exploiting vulnerabilities in a system. In this case, the interaction of a user of the target system is not usually required. The impacts of such campaigns vary considerably depending on the type of malware and the infected system. To take a simple example, malware that steals information from a school pupil's computer is very likely to have less severe consequences than malware on a hospital system that disrupts the hospital's operation.

For example, in July 2022, Ukrainian authorities were targeted by GammaLoad malware. In a campaign attributed to the Russian advanced persistent threat (APT) group Gamaredon,[52] GammaLoad was distributed in the form of an information sheet attached to emails that spoofed the identity of the National Academy of the Security Service of Ukraine. Once the target system was infected with GammaLoad, the Gamaredon group could extract information or load additional malware with more functionality, e.g. for sabotage purposes, onto the system.

In another case, in October 2022, three transport and logistics companies in Ukraine and Poland were infected with the Prestige ransomware, all within a few hours.[53] This ransomware has been attributed to the Russian APT group Sandworm. A ransomware incident can affect the operations of the companies concerned. In this case, for example, the transport of goods could have been impacted. However, the success of this attack was limited thanks to a rapid response.

5.6.3 Future developments

There are currently no signs of a slowdown in cyberspace activity linked to the war in Ukraine. As long as the war lasts, Russia will most likely continue to conduct these kinds of attacks, taking every opportunity to achieve desired effects, whether or not in combination with activities in other spheres of operation.

---

52 Кібератаки групи UAC-0010 (Armageddon) з використанням шкідливої програми GammaLoad.PS1_v2 (CERT-UA#5003,5013,5069,5071) (cert.gov.ua)

53 New "Prestige" ransomware impacts organizations in Ukraine and Poland (microsoft.com)