18 November 2025 | National Cyber Security Centre NCSC

Semi-Annual Report 2025/I (January – June)

Cybersecurity

Situation in Switzerland and internationally

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Defence,
Civil Protection and Sport DDPS
National Cyber Security Centre NCSC

Management summary

In this semi-annual report, the National Cyber Security Centre (NCSC) presents the relevant incidents and developments in the context of cyberthreats against Switzerland and internationally. In the first half of 2025, the NCSC received 35,727 cyberincident reports, confirming that the volume of reports has stabilised at a high level. Of these reports, 58 % were related to fraud. The main cyberthreats facing Switzerland remained the same, although attackers continued to innovate in their methods.

The challenge of ransomware and data extortion

Ransomware and associated data extortion continue to pose a significant threat to organisations of all types in Switzerland.[1] In the first half of 2025, the NCSC received 57 reports of ransomware incidents, mostly from companies and organisations. This represents a slight increase compared with the 44 incidents reported during the same period the previous year. Where the ransomware strain was identified, the majority of reports cited ‘Akira’, with ‘LockBit’ the next most common. One of the key challenges facing organisations is cyberattacks within the supply chain, as an attack on an IT company can also have a negative impact on its business customers.

Fraudulent advertising as an attack vector

A key issue in the distribution of real-time phishing,[2] malware,[3] and fraudulent investment products is the growing exploitation of paid advertising on search engines and social media. Online investment fraud in particular involves victims being tempted to make ill-considered investments by such adverts.[4] Recovery fraud – where victims of online investment scams are approached again with false promises of getting their money back – has now also taken hold in Switzerland.

Phishing: Bank customers targeted

In the first half of 2025, several real-time phishing campaigns and two-stage phishing attacks specifically targeted Swiss bank customers. Victims were lured to fake e-banking pages via paid advertisements that appeared in search engine results ahead of the genuine login sites. Criminals also spread phishing pages via online classified ads to steal credit card details, Twint account and e-banking logins. Two-stage phishing attacks were increasingly reported. In this type of attack, customers are first asked to provide less sensitive details, such as their phone number, on a phishing page. In a second step, the scammers then use this information to call their victims, pretending to warn them about fraudulent transactions. This is how they obtain access to their victims' e-banking credentials.

[1] Ransomware (ncsc.admin.ch)

[2] Phishing, vishing, smishing (ncsc.admin.ch)

[3] Malware (ncsc.admin.ch)

[4] Investment fraud (ncsc.admin.ch)

Hacktivism: DDoS attacks as an established tool

Switzerland was affected by distributed denial-of-service (DDoS) attacks again in this reporting period.[5] In addition to pro-Palestinian groups, pro-Russian hacktivist groups also relied on DDoS attacks, temporarily disrupting publicly accessible services such as websites.[6] Notably, targeted prevention and defence measures successfully averted significant impact during the Annual Meeting of the World Economic Forum (WEF) and the Eurovision Song Contest (ESC). DDoS attacks do not involve breaking into systems, but rather overwhelming services with traffic, which leads to temporary outages. For hacktivists, DDoS attacks remain attractive during high-profile events with international attention, as they generate media coverage for their cause and unsettle the public.

Other developments

Due to its strong international ties and reliance on widely used software products, vulnerabilities that are relevant globally also affect Switzerland's IT landscape. Attackers exploit these vulnerabilities to gain access to companies' IT systems, which can result in data leaks. State actors may also exploit vulnerabilities for espionage or sabotage purposes. Despite the increasingly challenging nature of navigating an international environment marked by geopolitical tension and conflict, Switzerland's cyberthreat situation has so far remained relatively stable.

[5] DDoS attack – what next? (ncsc.admin.ch)

[6] See Semi-Annual Report 2023/1, ch. 2.

Contents

Editorial

In the first half of 2025, Switzerland hosted two major international events: the Annual Meeting of the World Economic Forum (WEF) in Davos in January, and the Eurovision Song Contest (ESC) in Basel in May. Such events are often targeted by hacktivists, who exploit the global media spotlight by disrupting or altering websites and leveraging the resulting publicity to spread their political message. Targeted prevention, technical protection and close cooperation with organisers and security authorities meant that DDoS attacks around both events in Switzerland were successfully repelled. This coordinated, forward-looking approach was key and shows that Switzerland is on the right track in terms of cyber resilience, as envisaged in the National Cyber Strategy (NCS).

At the same time, another facet of the threat landscape is emerging: Cybercriminals are exploiting not only events but also well-known public figures. The National Cyber Security Centre (NCSC) regularly receives reports from the public about fake adverts featuring, for example, the Swiss President of the Federal Council Karin Keller-Sutter endorsing an investment platform. Deepfake technology is used to mimic their faces and voices, making the scam appear trustworthy. These deceptively realistic manipulations are designed to cloud victims' judgement. The combination of a familiar face, an authentic-sounding voice and the promise of high returns makes the fraud appear highly credible, and is particularly devious. The NCSC provides ongoing information on how to spot such deepfakes, what precautions to take and consistently calls on people to stay alert.

Overall, the threat level remains high. In the first half of 2025, the NCSC received around 36,000 reports – a steady but elevated figure. More than half (58 %) were related to attempted fraud. Criminals are continually refining their methods. One recent example is a two-step phishing approach in which victims are first lured to phishing websites and then contacted by phone. The aim here is to obtain sensitive data such as e-banking credentials through psychological manipulation.

In the business sphere, attacks on IT service providers are attracting growing attention. Such incidents affect not only the providers themselves but also their customers, for example when confidential information ends up on the darknet. Cybersecurity in the supply chain is therefore becoming a central issue. The NCSC provides companies with tools and recommendations to help them protect themselves against these types of indirect attacks.

Another important step towards strengthening cyber resilience was the introduction of mandatory reporting for cyberincidents involving critical infrastructure. Since 1 April 2025, operators of such infrastructure have been legally required to report serious incidents to the NCSC. This ensures that relevant information flows quickly, risks are identified at an early stage and coordinated measures can be initiated.

Cybersecurity is omnipresent, whether on the political stage, at major events or in everyday life. All the more important, then, that responsibility for cybersecurity is shared by everyone – the government, businesses, and the general public. Resilience is built where cooperation, vigilance and technology go hand in hand.

Florian Schütz, Director of the National Cyber Security Centre

1 Cyberthreats in Switzerland: An overview

In cyberspace, the threat landscape for businesses, organisations and individuals is shaped by various players with different motives and capabilities. While geopolitical tensions and international escalations have led to significant changes in the risk analysis for critical infrastructure in other Western countries, Switzerland must also assert itself in a more tense threat landscape. Unlike these threats, the Swiss situation related to the reported incidents has so far remained relatively stable. Although security experts have noticed challenging developments due to innovations in the methods of attack, the core phenomena identified and the conclusions drawn from them have remained fairly constant over time.

In order to obtain a broader assessment of the cyberthreat situation in future and to warn the operators of critical infrastructures at an early stage, Parliament adopted a reporting obligation for cyberattacks on critical infrastructures.[7] Since 1 April, the NCSC has been receiving such reports through the Cyber Security Hub (CSH). As the obligation to report cyberattacks came into force halfway through this six-month period, there is not yet enough data from these mandatory reports to provide a complete analysis for this semi-annual report. Thus, incidents subject to mandatory reporting will only be systematically analysed in this year's second semi-annual report. As in previous years, this current report therefore relies mainly on voluntary reports from individuals and companies.

A total of 35,727 reports were received in the first half of 2025, which is a slight increase of 938 compared to the same period the previous year (see fig. 1).[8] Once again, fraud was the most frequently reported category of attack (see fig. 2). Two developments stand out in particular: Reports of threatening scam calls in the name of authorities dropped sharply from 13,730 in the previous year to 10,578, while reports of investment fraud advertising increased.[9] March was especially notable here. The NCSC received 851 reports, almost eight times more than in March of the year before (112). The NCSC also recorded an increase in ransomware incidents, from 44 in spring 2024 to 57 in the first half of 2025, with several reports in April in particular. This may be linked to the heightened media attention and debate surrounding the introduction of mandatory reporting of cyberincidents. From May onwards, the number of reports settled back down to between zero and two incidents per week.

The ratio of reports from the general public (90 %) to reports from businesses, associations, and authorities (10 %) has remained unchanged. Just like private individuals, companies are affected by threatening fake calls in the name of authorities and phishing attempts. However, two attack types are typical for organisations, namely invoice manipulation fraud[10] and CEO fraud[11] (see ch. 5). There was a particularly sharp increase in CEO fraud, continuing the trend from 2024.[12] The 605 attempted CEO fraud cases reported in this period are nearly equal

[7] Information on the reporting obligation (ncsc.admin.ch)

[8] The NCSC's statistics include all reports received. These also cover general enquiries, information and reports that cannot be categorised. In the first half of 2025, this equated to 1,430 reports that could not be assigned to a specific incident or category.

[9] To provide more information on threatening scam calls purporting to be from the authorities, the NCSC published a supplementary report alongside the Semi-Annual Report 2024/1.

[10] Business Email Compromise (BEC) (ncsc.admin.ch)

[11] CEO fraud (ncsc.admin.ch)

[12] See also the Semi-Annual Report 2024/2, ch. 5.3.

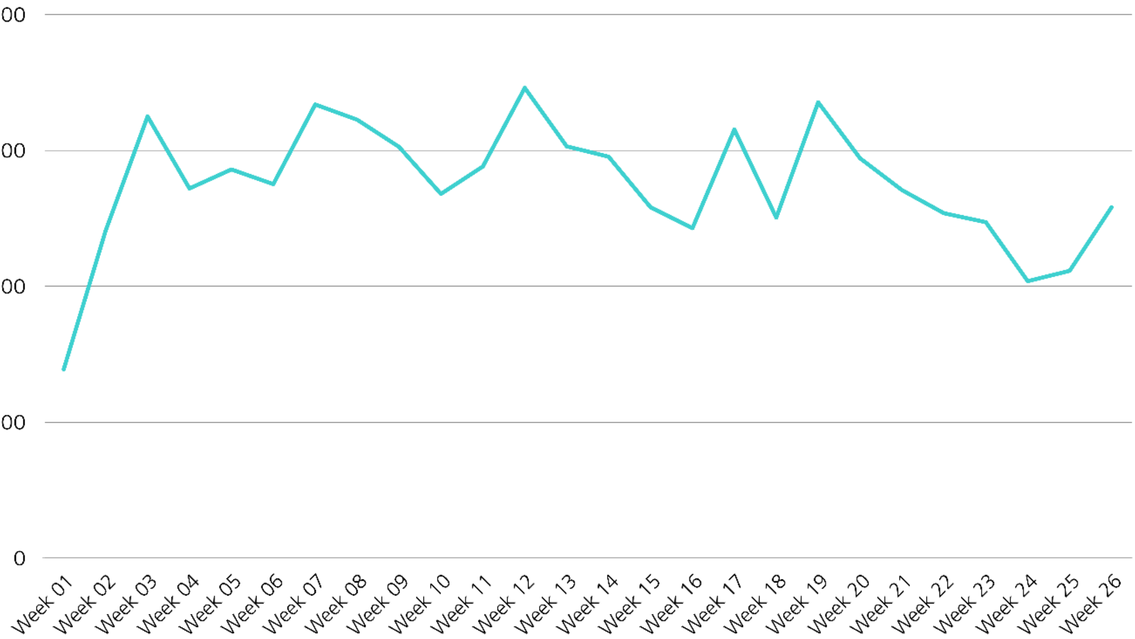

Fig. 1: Number of reports to the NCSC in the first half of 2025, see [Current figures (ncsc.admin.ch)]

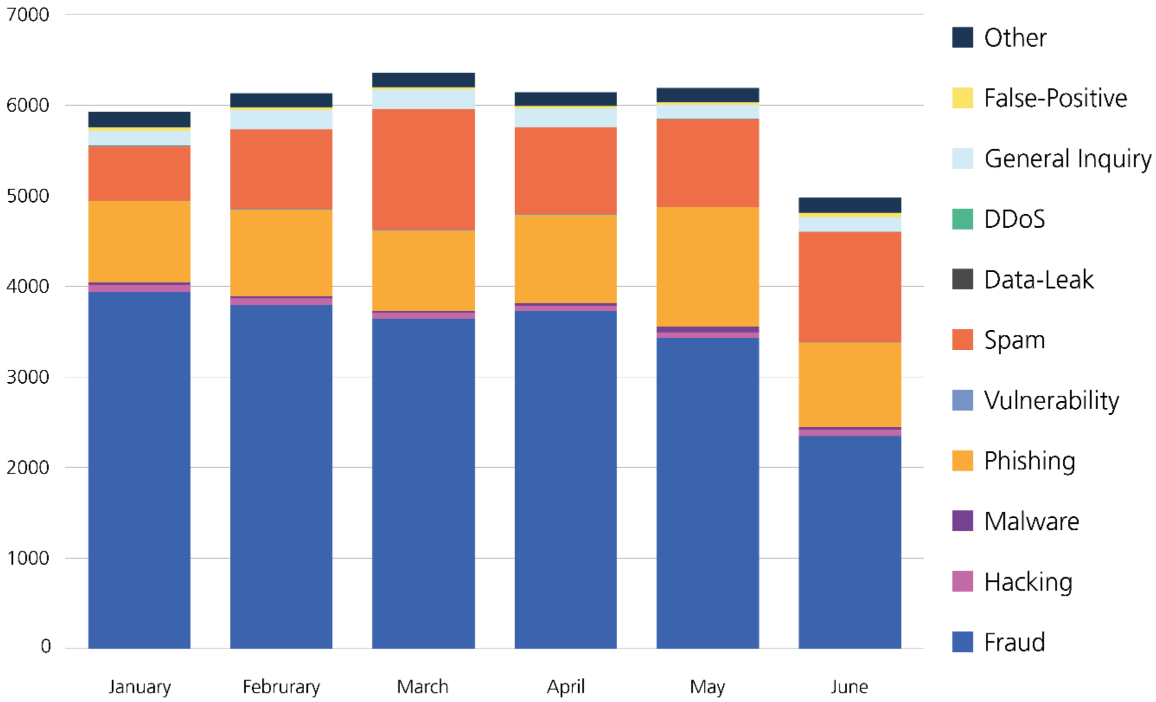

Fig. 2: Number of reports to the NCSC in the first half of 2025 by category, see [Current figures (ncsc.admin.ch)]

to the total number for the whole of 2024. Communes, schools and churches remain especially affected.

The statistics show that cybersecurity and protecting Switzerland from cyber risks is an ongoing challenge for business, government and society. This semi-annual report therefore sets out the main areas that define Switzerland's cyberthreat landscape: phishing, malware, vulnerabilities, fraud, social engineering, distributed denial-of-service (DDoS) attacks on websites and other online services, data leaks, and cyberespionage and cybersabotage.[13] The report focuses primarily on incidents and developments in Switzerland, but it also refers to international trends where these help to illustrate the situation in Switzerland (see ch. 8). The various sections of the report give readers an overview of how these key threats are currently playing out, along with notable incidents and developments. In line with the principle of shared responsibility for a safer digital Switzerland, the report provides the public with recommendations on how to respond to these challenges.

2 Phishing

Phishing enables attackers to collect login credentials, financial details, and other confidential information without the user's knowledge. Typically, social engineering plays a central role in influencing recipients while no malware is distributed.[14] The classic approach involves sending a message containing a link to a large number of recipients. The link leads to a phishing website that is designed to resemble a legitimate site. If recipients believe the phishing website is genuine, they enter sensitive information – such as e.g. login or credit card details – which then goes straight to the phishers. Although email remains the most common method of phishing, other approaches use phone calls (voice phishing, or 'vishing'), text messages (SMS phishing, or 'smishing'), or other types of mobile messaging to obtain information. When phishing is directed at a specific person or selected group of people, it is referred to as 'spear-phishing'. Unlike the mass-distributed form, spear phishing is much harder for victims to detect since it is tailored to them.

In the first half of 2025, the NCSC received 5,981 reports of phishing attempts via its reporting form. This was 662 reports fewer than in the same period of the previous year. The phishing statistics for reports received via the NCSC-operated website ‘antiphishing.ch’ were similar.[15] After several periods of steady increase, a decline was also recorded in this regard. While 11,505 unique phishing URLs were reported in the first half of 2024, this figure fell to 7,412 in the same period of 2025. To make phishing sites appear as convincing as possible, phishers often impersonate well-known brands and companies to lure victims. The most frequently targeted in this reporting period were postal services (23 %), the financial sector (22 %), public

[13] Social engineering (ncsc.admin.ch)

[14] There is no single international definition of phishing, so other definitions often include the distribution of malware (see Phishing (attack.mitre.org)). The NCSC explicitly excludes this aspect in the definition it applies.

[15] The NCSC receives phishing reports in the form of incident notifications, as well as via the antiphishing.ch website, which draws on additional sources. As a result, the figures presented here may differ from the number of direct phishing reports.

transport (19 %), IT (9 %) and telecommunications (7 %). Since the beginning of the year, there has been a continuous rise – averaging 6 % – in unique phishing sites that impersonated insurance companies, such as health insurers. Conversely, the number of reported phishing sites linked to the IT sector declined during this reporting period. There was a sharp drop in reported phishing sites in March and April, primarily because public transport was much less frequently exploited for phishing during this time (see fig. 3).

A large proportion of the reports involved classic credit card phishing. However, phishers also sought to improve their chances of success by restricting access to their phishing sites to mobile users, which made early detection by the authorities, who primarily use PCs, less likely. There was also a continued high number of Microsoft 365 phishing attacks linked to 'chain phishing'.[16] In some cases, methods to bypass multi-factor authentication (MFA) were also used. The NCSC also observed more sophisticated phishing attempts targeting Twint and e-banking. For these, criminals used channels such as classified ad platforms or a two-step approach combined with vishing. Although these methods are more labour-intensive than classic mass phishing emails, they create a stronger sense of trust, thereby increasing the phishers' chances of success. These attempts appear credible, especially through personal contact, which is sometimes maintained over several days. Thus. the criminals can react with an individual response whenever victims begin to show signs of doubt.

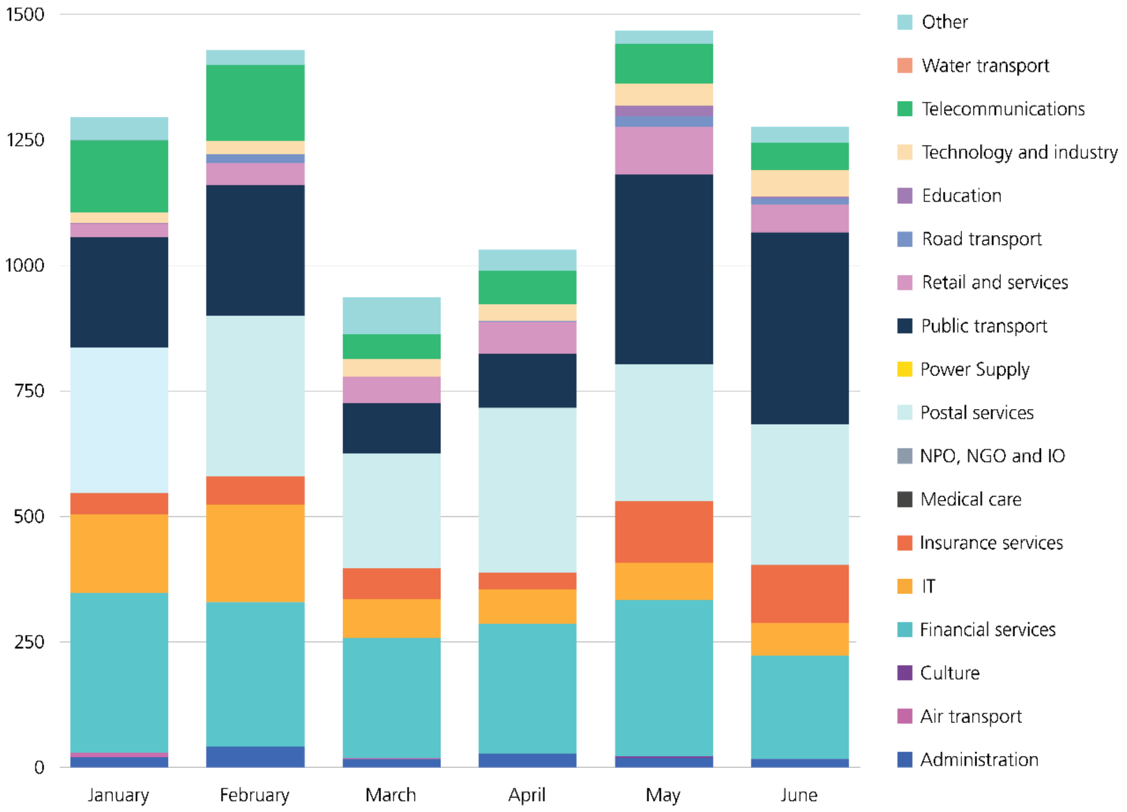

Fig. 3: Number of phishing URLs confirmed by the NCSC by sector of impersonated brands in the first half of 2025

[16] Chain phishing involves a chain reaction of spam or phishing emails. Once an email account has been compromised, phishing emails are immediately sent to all the address book contacts.

Recommendations

Report suspicious phishing attempts to the NCSC via reports@antiphishing.ch or directly via the website antiphishing.ch. If you would like feedback, you can also report the phishing incident using the report form or by contacting the NCSC's specialists at incidents@ncsc.ch. By doing so, you help the NCSC to issue targeted warnings and take action to ensure that fraudulent websites can be blocked.

Real-time phishing: Focusing on banking applications

Swiss banks generally use MFA for greater protection when accessing e-banking and authorising payments, typically requiring a code sent by text message, or a push confirmation. This prevents stolen access data from being used to access banking applications. A decade ago, cybercriminals often relied on malware, such as 'Retefe' in 'Operation Emmental', to bypass security mechanisms in banking apps.[17] Today, however, e-banking malware has all but disappeared in Switzerland. Most attacks on e-banking accounts now use a mix of social engineering and real-time phishing, and these reached a peak towards the end of June. Unlike classic phishing, real-time phishing – as the name suggests – involves attackers stealing login credentials in real time and using them straight away before their expiration.

Victims were lured to fake e-banking webpages via paid advertisements that appeared in search engine results ahead of the genuine login sites. These phishing campaigns, which mainly imitated cantonal banks, often included domains[18] with the endings .app, .digital or .help.[19] As soon as someone entered their login details on the fake site, the scammers accessed the genuine e-banking site from their computer and logged in to the victim's account. During this time, the scammers kept the victim waiting by simulating a delay in the login process – for example by displaying an hourglass. When the genuine e-banking site requested the second factor, the attackers forwarded the request to the victim's screen. Once the victim had entered the second factor, the scammers gained access to their e-banking account. To avoid raising suspicion, scammers often then displayed an error message claiming the victim needed to log in again.

From classified ads to Twint account takeovers

Real-time phishing is also common in classified ad scams, and the number of such attempts has increased fivefold since August 2024 (see fig. 4). These attacks often start innocuously: A supposed buyer gets in touch shortly after an ad is posted, offering to arrange delivery and advance payment via Swiss Post, for example. The victim then receives a link to supposedly collect the money that has already been transferred. However, the website behind the link is malicious and requests credit card details, Twint access or e-banking logins. These sites are especially convincing because they are customised to the specific item being sold, including the correct price and product photo.

[17] See *Retefe: Angriff auf Schweizer Bankkunden - Präzisierung durch MELANI* (de, fr, it; ncsc.admin.ch)

[18] See Glossary (ncsc.admin.ch), 'domains'.

[19] See Warning: Real-time phishing on behalf of cantonal banks (ncsc.admin.ch)

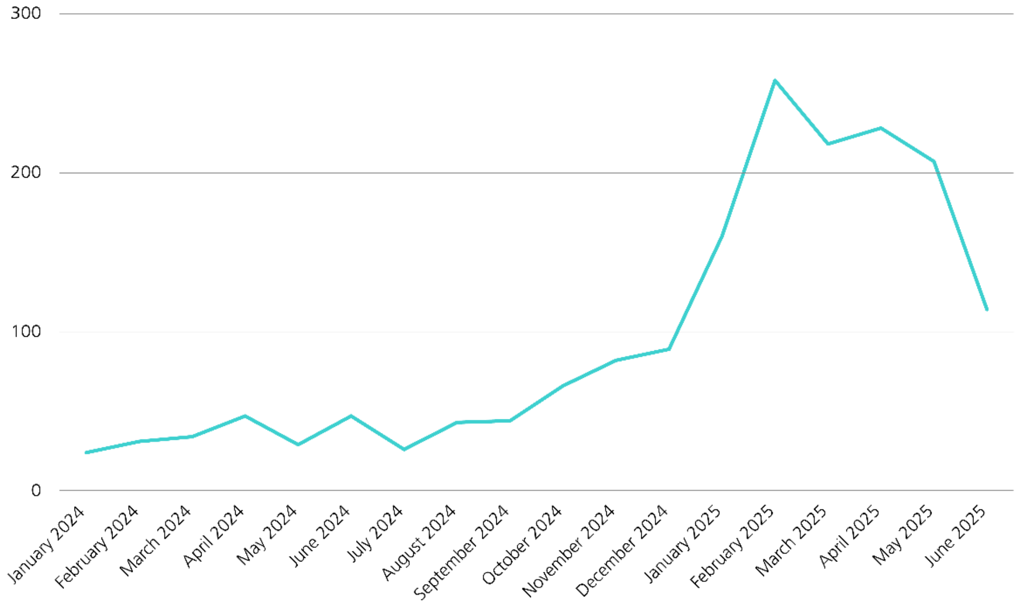

Fig. 4: Increase in phishing through classified ads since January 2024

Once the victim has entered their details, the attackers delay them while logging in to their e-banking account in the background. It appears that the attackers are primarily after the Twint accounts that are linked to the bank accounts, rather than the bank accounts directly. Rather than initiating a fraudulent e-banking payment, they link one of their own devices to the victim's Twint account. This allows them to make transactions straight away that cannot be reversed. The fraud often goes unnoticed by the banks for some time, enabling the criminals to transfer even more money. They then cover their tracks by transferring the stolen funds through several accounts – some of them hacked – to obscure the money trail.

Two-step phishing attacks and vishing

Vishing (voice phishing) is a form of real-time phishing. A recent development is the growing use of a two-step procedure. In a first step, criminals use phishing pages to obtain less sensitive information from victims. This typically does not include e-banking credentials, but details such as the victim's phone number and the bank they use.

In a second step, the process follows the usual pattern of voice phishing: the criminals call the victim, often pretending to be 'Mr. Fischer' from the security department of the indicated bank by the victim in the first step. The caller ID is usually spoofed to display an official number from this bank, a technique that can also be used to forge email addresses.[20] Victims are told they need to stop a fraudulent transaction, usually said to be for CHF 800. To prevent the supposed fraud, victims are instructed to install remote access software on their computer and give the criminals access both to their device and to their bank account. This gives the criminals the ability to move money from the victim's e-banking unnoticed. These cases demonstrate the importance of thorough training for bank staff in customer-facing roles. It is up to them to issue early warnings about potential fraud attempts in the bank's name when dealing with respective questions from customers.

[20] Spoofing (ncsc.admin.ch)

Recommendations

Wherever possible, enable multi factor authentication (MFA) as an additional security measure for your accounts. Although MFA reduces the risk of your account being compromised, it can still be bypassed using social engineering.[21] So be wary of fake requests, especially via email and text message when you are asked to confirm access or forward your security token to someone else. Remember that email addresses and phone numbers can easily be spoofed to make messages appear more credible. Never enter credit card details or other sensitive data on a website that you have accessed via a link in an email or text message.

3 Malware

Malware is a primary tool that attackers use to gain access to devices or networks. As a rule, such programs execute unwanted and usually harmful functions on IT systems without the user's knowledge.[22] This can include stealing, altering and/or destroying data. Malware infections can occur in various ways via different channels, and any type of device or infrastructure can be affected.

3.1 Initial access with malware

Initial access describes all actions an attacker must take to compromise another system. This can be achieved by obtaining login credentials, such as usernames and passwords, through social engineering and phishing (see ch. 2), by exploiting vulnerabilities (see ch. 4), or by using malware, such as trojans. The latter usually requires the user to execute an action and relies on various deception mechanisms (social engineering) to trick victims into installing the malware. For instance, the malware may be concealed within another program, email attachment, or link that seems harmless at first glance.

The NCSC also observed malware distribution campaigns targeting systems in the first half of 2025. In addition to using images (.svg files) for malicious purposes, attackers also sent fake invoices to install malware on target devices. There were no indications that these campaigns were specific to Switzerland; they followed international patterns.
According to the NCSC's information, distribution of malware by email ('malspam') plays a relatively minor role in infections of corporate networks. Conversely, compromised websites[23]

[21] Social Engineering (ncsc.admin.ch)

[22] Malware (ncsc.admin.ch)

[23] ClearFake's New Widespread Variant: Increased Web3 Exploitation for Malware Delivery (sekoia.io)

and malicious advertising ('malvertising') in search engines[24] are increasingly common techniques among cybercriminals (see ch. 3.3).

A method that was observed more frequently in connection with these approaches is known as ‘ClickFix’.[25] ClickFix was observed particularly on websites imitating well-known hotel-booking portals. With this method, a script is copied to the victim's clipboard via a malicious site or compromised website. The user is then prompted to press keyboard shortcuts such as ‘Windows + R’, ‘Windows + X’, or ‘Ctrl + V’, for what is presented as a necessary step. Under the pretext of completing a CAPTCHA[26] or accepting cookies,[27] attackers get victims to perform the required action. In reality, this triggers the execution of the malicious script from the clipboard, which can install malware, for example via PowerShell.[28]

‘Lumma Stealer’ is a type of malware often associated with ClickFix that has become increasingly popular among cybercriminals.[29] In May, IT companies and law enforcement authorities conducted a joint operation to seize the Lumma Stealer infrastructure, temporarily disrupting the spread of the malware.[30] That same month, security forces furthered international cooperation by dismantling the infrastructure of seven malware types in ‘Operation Endgame’.[31] Such measures disrupt the activities of criminal service providers who supply initial access, thereby affecting the criminal economy. However, these providers are likely to attempt to rebuild their infrastructure immediately. Other criminals who were not directly affected by the operations may also exploit the resulting market gap and supply their own products to meet demand. One example is the ‘Rhadamanthys’ malware, which has been observed in connection with ClickFix and has been seen in email distribution campaigns in Switzerland and across Europe. In these emails, the criminals impersonated law firms and threatened the recipients with legal action for alleged copyright infringement. The details of the alleged infringement were said to be contained in a PDF which the recipient had to download. However, the PDF turned out to be an executable malicious file that ultimately led to a Rhadamanthys infection.[32]

Recommendations

Never click on links, open attached files, or scan QR codes in suspicious messages. If in doubt, contact the purported sender via a trusted channel to verify that the message is really from them. Always be suspicious when a download window pops up.

When searching for software, download it only from the product's official website or from a reputable download site. Pay attention to whether a search result is marked as paid advertising

[24] University site cloned to evade ad detection distributes fake Cisco installer (malwarebytes.com)

[25] See Semi-Annual Report 2024/2, ch. 3.1.

[26] Week 9: Hotels and guests targeted by cybercriminals (ncsc.admin.ch)

[27] Abuse.ch: Booking themed ClickFix campaign using a fake cookie banner (linkedin.com)

[28] See Semi-Annual Report 2024/2, ch. 3.1.

[29] See Semi-Annual Report 2024/2 ch. 3.1.

[30] Disrupting Lumma Stealer: Microsoft leads global action against favored cybercrime tool (microsoft.com)

[31] Operation ENDGAME strikes again: the ransomware kill chain broken at its source (europol.europa.eu)

[32] Copyright Phishing Lures Leading to Rhadamanthys Stealer Now Targeting Europe (cybereason.com)

and treat these results with caution, as attackers often use them to appear at the top of search listings.

Regularly patch your systems and restrict access rights as much as possible. If you suspect an infection, have your computer examined immediately by a specialist and cleaned if necessary. The safest option is to completely reinstall the operating system of your computer. However, do not forget to back up all personal data beforehand.

3.2 Ransomware

Ransomware is an attack type in which criminals deploy malware to encrypt data on a victim's IT systems, rendering it unusable.[33] Typically, they take a copy of the data before encryption and demand a ransom afterwards. The criminals promise to provide a decryptor if the victim pays. If the victims do not react to the demands, they threaten to publish the stolen data if it refuses to pay the ransom. Ransomware groups often increase the pressure – for example by contacting the victim's customers and suppliers and threatening to publish the stolen data – to push the victim to a payment.

In the first half of 2025, the National Contact Point Cyber for Cyber-Risks operated by NCSC received 57 ransomware reports, most of which were from companies (see fig. 5). This represents a slight increase compared to the first half of 2024, when 44 incidents were reported. The actual number of ransomware incidents in Switzerland is likely to be higher, as not all affected organisations file reports. The most active ransomware groups in Switzerland in early 2025 were the same as in the previous year: Eight incidents were attributed to Akira, and seven to LockBit.[34] Since March 2023, Akira has also been one of the most active groups internationally, targeting organisations of all sizes and in all sectors. LockBit, by contrast, was one of the most disruptive and influential ransomware groups worldwide until February 2024. However, its activity fell sharply in early 2025 due to various international law enforcement operations and internal data leaks, despite the release of a new ransomware version, 'LockBit 4.0'.[35] In a relatively large number of ransomware reports (21), the type of ransomware was not specified; these are shown as 'unknown' in the chart.

The statistics show that the threat of ransomware remains high. The situation continues to be shaped by the emergence of new groups and the disappearance or transformation of existing ones. Contributing factors include internal restructuring,[36] data leaks[37] and law enforcement operations.[38] Although none of the known groups specifically target Swiss organisations, op-

[33] Ransomware (ncsc.admin.ch)

[34] See Semi-Annual Report 2024/1 and 2024/2, ch. 3.2 on ransomware.

[35] What the LockBit 4.0 Leak Reveals About RaaS Groups (darkreadings.com)

[36] Lynx Ransomware: A Rebranding of INC Ransomware (paloaltonetworks.com)

[37] LockBit Ransomware Gang Hacked, Operations Data Leaked (darkreading.com)

[38] Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown (europol.europa.eu)

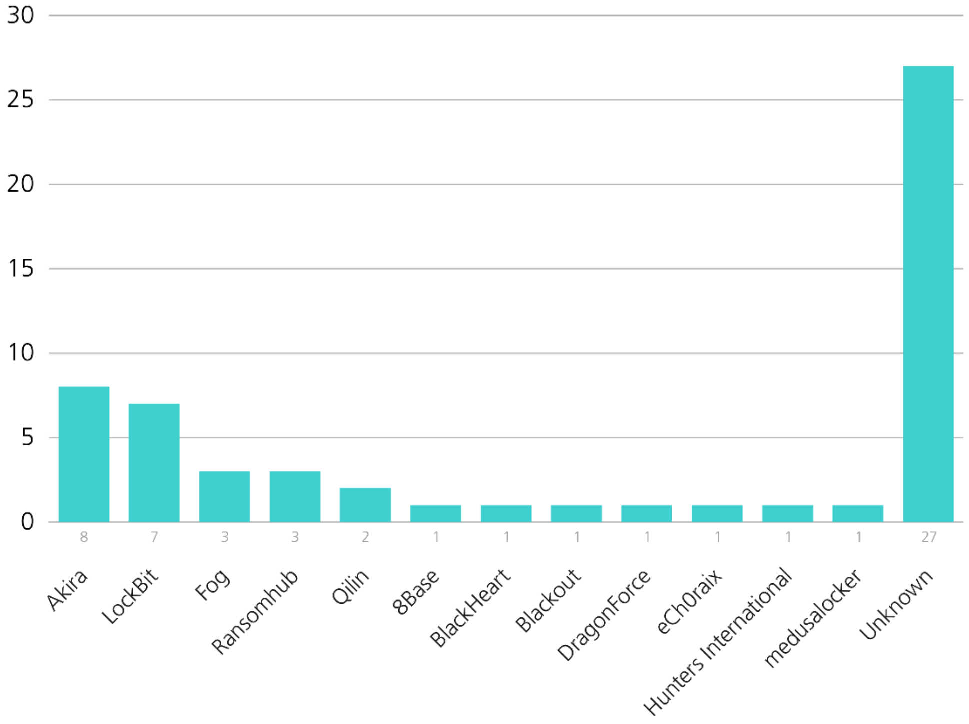

Fig. 5: Number of ransomware incidents reported to the NCSC in the first half of 2025

portunistic attacks are commonplace and therefore affect Switzerland too. These attacks are mainly based on initial access gained through malware, exploited vulnerabilities, or stolen login details obtained via phishing campaigns and infostealers.[39] This development takes place within a criminal economy marked by division of labour and specialisation: some players focus on gaining access, while others develop new ransomware. Business models such as 'Ransomware-as-a-Service' (RaaS) are thriving as a result, enabling individuals with limited technical knowledge to launch attacks. On turnkey platforms, developers provide and maintain the necessary tools for the various stages of a ransomware attack (e.g. data exfiltration, encryption, communication and payment). The 'DragonForce' group, which also operates in Switzerland, is an example of this trend. First observed in 2023, the group has since evolved to offer partners a comprehensive platform that they can operate under their own name.[40] In return, the ransomware developers retain a share of the ransom.[41]

Alongside developing their infrastructure, the most capable groups are constantly refining their techniques to evade ever-evolving defensive measures. Some now use EDR killers, which can be either malicious software or legitimate tools deployed for this purpose.[42] These allow ransomware groups to prevent early detection by modifying or completely disabling security software at the start of an attack. This gives them time to identify sensitive data before exfiltrating

[39] An infostealer is malware that collects sensitive information (e.g. access data) and passes it on to the hacker.

[40] See Semi-Annual Report 2023/2, ch. 3.4.2.

[41] DragonForce expands ransomware model with white-label branding scheme (bleepingcomputer.com)

[42] Ransomware crews add EDR killers to their arsenal – and some aren't even malware (theregister.com)

and encrypting it. To maximise their impact, ransomware groups typically strike outside normal working hours (e.g. at night, at weekends or during public holidays).

Several incidents in Switzerland in spring 2025 highlighted the danger that ransomware attacks pose to third parties. Once a supplier has been compromised, any access obtained can potentially serve as an attack vector. One example is the ransomware attack on Cistec, a Swiss software company that specialises in hospital information systems. Cistec's remote access to hospital systems for software maintenance could have been used to carry out further attacks on the hospitals themselves.[43] Other cases involving IT service providers demonstrated the direct impact on their customers. In an attack on a subsidiary of Ilem, around 15 % of its customers temporarily lost access to the company's cloud services.[44] At 2sic, an attempted attack was thwarted by taking systems offline, resulting in a two- to three-day outage during which customers could not access the systems.[45] Some incidents have also highlighted the risk of data leaks when the victim is directly involved with business clients or other third parties (see ch. 7). Following the attack on the health promotion foundation Radix, stolen data was published. Radix's customers include various offices of the Federal Administration. Although Radix did not have direct access to federal systems, information relating to the Federal Administration may still have been among the compromised data.[46]

Recommendations

On the NCSC website, you find a list of preventive measures to protect against ransomware as well as guidance on what to do in the event of an incident. It is essential to provide staff with training and exercises on how to handle IT outages, in order to ensure a fast and effective response in an emergency. In general, the NCSC and its international partners advise ransomware victims not to pay.[47] There is no guarantee that cybercriminals will keep their word. Paying the ransom only serves to fund their operations and enable further attacks.

3.3 Malvertising: Abuse of search engine ads

In 2025, the NCSC observed several cases in which search engine ads were used for phishing purposes (see ch. 2) and to distribute malicious software, called malvertising. Cybercriminals specifically use paid advertising that imitates legitimate websites or well-known brands. Because these ads appear above the regular, unpaid search results, users are more likely to click on them and are then redirected to a fraudulent website. The scam site may either download malware directly or prompt the person to install infected files.[48] Such campaigns often target popular search terms such as 'download', 'update', or 'support', as well as well-known software

[43] *Ransomware-Angriff auf KIS-Anbieter Cistec* (inside-it.ch); *'An einer Katastrophe vorbeigeschlittert'* (inside-it.ch)

[44] *Ransomware-Angriff auf Genfer IT-Gruppe Ilem* (inside-it.ch)

[45] *Ransomware Angriff auf 2sic Hosting abgewehrt* (2sic.com)

[46] Cyberattack on Radix: Federal Administration data also affected (ncsc.admin.ch)

[47] Guidance for organisations considering payment in ransomware incidents (ncsc.gov.uk)

[48] What Is a Drive by Download Attack? (kaspersky.com)

such as Chrome. Attackers may, for example, place an ad that appears to offer official software but contains a trojan or ransomware in reality. What makes this especially dangerous is that it works even on major search engines such as Google or Bing. As the ads appear in real time, criminals are able to adapt their campaigns swiftly and sidestep countermeasures.

Recommendations

You should only download software from official vendor websites or trusted portals, even if search engines display what looks like a legitimate ad. When reviewing search results, check carefully whether an entry is marked as an ad (e.g. there is a 'sponsored' declaration) or appears as a regular indexed website. In addition, using ad blockers, keeping security patches up to date, and implementing endpoint protection solutions can significantly reduce your risk of infection. In companies, it is advisable for staff to check with their IT services before downloading software to avoid inadvertently installing malware.

4 Vulnerabilities

A vulnerability is a security weakness in an IT system. These may be flaws in the software or design, but they can also result from weak configurations, such as the use of default passwords.[49] Zero-day vulnerabilities – discovered flaws for which no vendor patch is yet available – are especially difficult to manage as attackers can exploit them before mitigation measures are in place. With growing digitalisation and the networking of devices, even the exploitation of a single vulnerability – or a chain of them – can result in data and systems being compromised.

Due to the international interconnectedness of Switzerland's IT landscape, the country is directly exposed to global vulnerabilities. Businesses, administrations and critical infrastructures largely rely on products from leading international vendors. Consequently, Switzerland was affected by critical security flaws in products from well-known global providers such as Fortinet, Microsoft and Ivanti in the first half of 2025. Cyberspace and the associated threats are independent of political borders, meaning that global problems can also have negative consequences for Switzerland.

A familiar pattern continues to emerge: The categories of systems with the greatest number of vulnerabilities, and the most critical ones, remain largely unchanged. Attackers and security researchers focus on two main areas: The first is about end-user devices, such as laptops, workstations, and mobile phones; the second is internet-exposed infrastructure. Components such as firewalls and VPN gateways form the first line of defence, yet they are also the most common entry points for compromise. If attackers exploit a vulnerability in this exposed part of

[49] Vulnerability (ncsc.admin.ch)

the infrastructure, they gain initial access to the network, allowing them to establish a foothold and carry out further actions.

This dynamic means that Swiss businesses and government agencies must continually manage a high volume of security updates for these essential components. Timely and comprehensive patch management is essential for safeguarding digital assets and ensuring resilience against cyberattacks.

Recommendations

If possible, always let programs update themselves automatically. Otherwise, always use the integrated update function or download the latest version directly from the manufacturer.

It is particularly important for companies to implement robust patch management processes to address vulnerabilities promptly. This requires an up-to-date inventory of your infrastructure and deployed products. Prioritise vulnerabilities in the parts of your infrastructure that are exposed to the internet. Carry out regular penetration tests and vulnerability scans to proactively identify potential weaknesses. Decommission software or systems that have reached their end-of-life (EOL) and are no longer supported by the vendor. If this is not possible, move them to a separate, isolated network zone. Use monitoring and threat intelligence services to respond quickly to developments. Real-time monitoring combined with automation can help you to detect attempted intrusions and anomalies promptly. Consider complementary measures, such as red-teaming exercises, regular security audits, and operating a bug bounty programme, to continuously assess and strengthen the effectiveness of your security processes.[50]

5 Fraud and social engineering

Fraud is the deliberate deception of a person with the aim of unlawfully enriching oneself or another, causing the victim to suffer material loss.[51] In the online context, a particular challenge is that criminals can operate from afar – often from countries where law enforcement is difficult. Rather than relying on technically sophisticated attacks, cybercriminals typically manipulate potential victims through social engineering, prompting them to carry out steps of the fraud themselves.[52]

As in previous years, fraud was the most frequently reported phenomenon to the NCSC in the first half of 2025, accounting for 58 % of reports (20,878). Compared with the same period last year, this represents a decrease of around 2,000 reports. This decline was particularly driven by a fall in reports of threatening phone calls impersonating authorities (see fig. 6). The record

[50] A red team is an independent group that tests an organisation's infrastructure and processes under real conditions by taking on the role of a potential attacker. The aim is to uncover and fix any existing security gaps before a real-life cyberattack can be carried out (cf. red team (wikipedia.org)).

[51] See Art. 146 Swiss Criminal Code for a legal definition.

[52] Social engineering (ncsc.admin.ch)

weekly volumes of over 1,000 reports seen in the comparison period last year did not recur in the second quarter of this reporting period. With the data available, the NCSC cannot say whether the decline will last, nor to what extent measures by telecom providers contributed to it.

The same trend was observed with fake extortion emails purporting to be from the authorities, in which the recipients were accused of a crime. These emails were less prevalent in Switzerland than the previous year, with 1,487 reports compared to 2,252 before. Bogus prize draws, which typically lead to subscription traps or phishing pages, were also reported less often. Following a peak of 2,398 reports in the second half of 2024, this figure has dropped to 1,916. In these cases, criminals exploited the names of well-known Swiss food and retail companies, electronics retailers and public transport providers. In contrast, reports of fake sextortion remained almost unchanged at 1,136.[53]

Following the trend seen in the second half of 2024, the NCSC recorded a renewed increase in CEO fraud.[54] While a total of 719 cases were reported in 2024, by the end of the first half of 2025 there were already 605. As before, organisations that were transparent about their structure and contact details, such as communes, schools and churches, were particularly affected. For the related but more technically complex invoice manipulation fraud[55] (business email compromise, BEC), there was a slight decrease compared with the year before, from 65 to 59 reports. Investment fraud also frequently results in substantial financial losses. There was a marked increase in misleading advertising directing users to such sites: There were 729 reports in the same period last year; by the first half of 2025 this had already risen to 3,485. Also linked to online investment fraud, recovery scams have become established in Switzerland, with 145 reports. In this type of scam, cybercriminals contact victims of investment fraud, claiming they can recover the stolen funds – but only if the victim first pays for the supposed service. The sections below take a closer look at fraudulent advertising for online investment fraud, recovery scams, and BEC and CEO fraud.

Fraudulent advertising linked to investment fraud

Dubious websites are regularly promoted through adverts and links on social media, streaming platforms or paid ads. According to reports to the NCSC, fraudulent ads increased by around five times in spring 2025. Mimicking news portals, they use fake celebrity interviews to promote supposed investment opportunities, promising high returns with minimal risk and starting capital (e.g. CHF/EUR 250; see fig. 7). These fake news portals imitate well-known Swiss media outlets such as Blick, 20 Minuten, SRF or RTS. For their fabricated interviews, scammers use public figures from sport, the media or politics.[56] They also increasingly use deepfake videos,

[53] See Semi-Annual Report 2024/2, ch. 5.2.

[54] See Semi-Annual Report 2024/2, ch. 5.3.

[55] Internationally, the term business email compromise (BEC) is not used uniformly. In other definitions, CEO fraud is for example understood as a subform of BEC (see Business Email Compromise (fbi.gov)). However, the NCSC explicitly distinguishes between the two phenomena and follows the definition of the Federal Office of Police (fedpol).

[56] Week 35: Scams involving public figures – the dark side of artificial intelligence (ncsc.admin.ch)

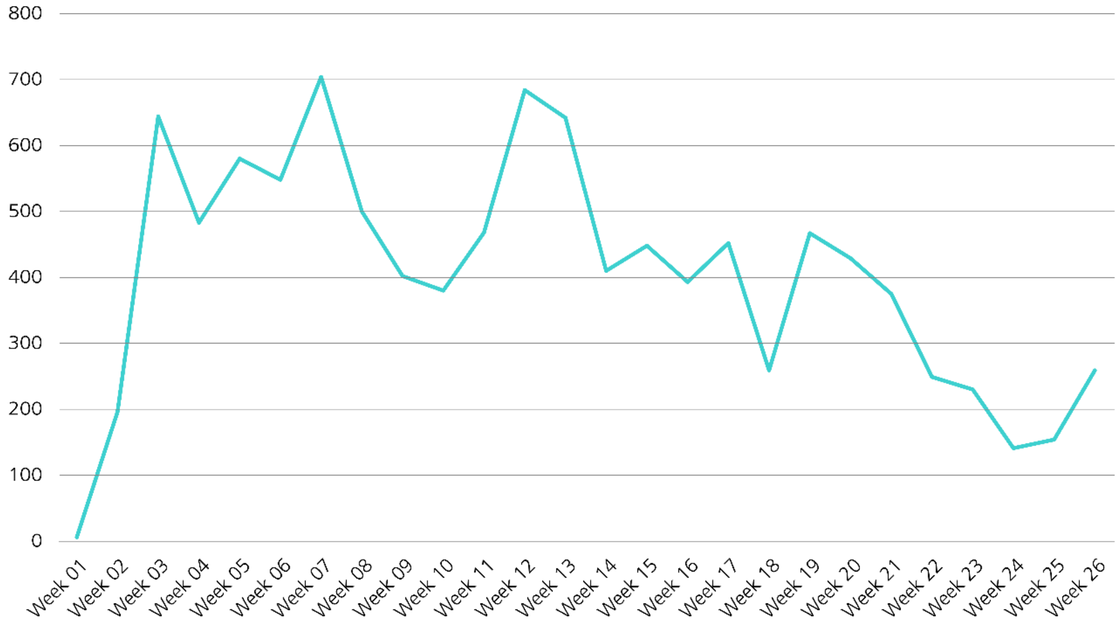

Fig. 6: Decline in reports of threatening calls impersonating authorities in the second quarter of 2025

for example, imitations of ‘Tagesschau’ broadcasts.[57] Once a victim has been lured into making a first investment, they are shown a specially prepared online portal suggesting that their investment is growing rapidly. The aim is to tempt victims into transferring more money to the fraudsters. The problem with this is that criminals can automatically publish large volumes of fraudulent content on websites within a short period of time without the content having to undergo even minimal checks by the platform providers before it is uploaded. Detecting, reporting and taking down such content is a much more protracted process, leaving authorities in a constant race to catch up.

Recovery scams following online investment fraud

Reports of recovery scams in Switzerland have risen from 31 in the first half of 2024 to 145 in 2025. After falling victim to investment fraud, people often still hope to recover their lost money somehow. Scammers exploit this, posing as authorities or reputable companies and claiming to have located the missing funds. In order to retrieve these supposedly recovered sums, victims are told that they must first pay taxes, fees, or other costs. Scammers try to boost credibility by backing up their demands with forged documents that look official, often in the names of British or Cypriot authorities.

Business Email Compromise (BEC) and CEO fraud

During the reporting period, attempts at CEO fraud increased sharply, while reports of related – and often more technically complex – invoice manipulation schemes (business email compromise, BEC) decreased slightly. In both scenarios, typical tactics include sending forged emails to the accounts payable department with urgent transfer requests, creating fake supplier invoices, or spoofing letters from lawyers regarding supposed confidential acquisitions. In CEO fraud cases, attackers exploit publicly available information. In contrast, in business email

[57] Deepfake (wikipedia.org)

compromise cases – especially when hijacking existing email threads – criminals first compromise business email accounts and then use the internal context they find to tailor their scam to the victim and make their demands more credible. Rather than sending generic requests, they include details such as bank account numbers or invoice references and adapt their writing style to that of the impersonated company. This requires more effort on the part of the criminals, since targeted attacks involve technical skill and greater preparation – for example, by spying on communication patterns or internal processes. The extra effort often pays off, and the financial damage to victims is usually higher.

Access to a business mailbox is fundamental for a successful BEC attack. This is evident from the numerous phishing attacks on Microsoft 365 accounts in Switzerland (see ch. 2). Criminals exploit such compromises in two ways: first, by contacting all the victim's contacts to spread additional phishing attacks – for example, through chain phishing – thereby potentially gaining access to further accounts; and second, by combing through the compromised mailbox for information of financial value. If, for instance, the attackers find correspondence about an outstanding invoice, they may insert themselves into the conversation. Although BEC can be carried out directly from a compromised email account, attackers often also register a domain similar to that of the victim company. They then create email addresses using this domain to make it easier to deceive customers. For example, they may instruct customers with outstanding invoices to transfer funds to a different account – one belonging to the criminals. Because the style and invoice details match the earlier correspondence, the customers believe they are still communicating with the right person. This type of email fraud can result in not only financial losses but also reputational damage. Since attackers may also steal sensitive information such as customer data, partners may lose trust in the organisation (see ch. 7).

Recommendations

Be sceptical of emails, text messages or phone calls threatening you with consequences and creating time pressure (e.g. loss of money, criminal charges, account or card blocking). Remember that criminals can easily falsify their identity through spoofing.[58] Always be cautious of unusual payment requests or prize offers. All processes relating to payment transactions should be clearly regulated internally in companies. No bank or credit card company in Switzerland will ever send you an email requesting that you change your password or verify your credit card details. Bank employees will also never use security tokens or other personal e-banking or Twint credentials as a way of verifying your identity over the phone.

[58] Spoofing (ncsc.admin.ch)

6 Attacks on the availability of websites and webservices

Attacks on the availability of websites and web services, most often in the form of distributed denial of service (DDoS), involve attackers trying to disrupt an internet-facing service by flooding it with a large volume of requests. These attacks do not, in themselves, result in unauthorised access to data, data exfiltration, or lasting damage to systems. This type of attack is particularly used for activism in cyberspace (hacktivism), to conceal other activities or for extortion.

At the start of the year 2025, there was a notable increase in DDoS attacks. On 10 January, a DDoS attack disrupted telephony, Outlook, and various federal websites and specialist applications for around 45 minutes. Thanks to the countermeasures that were implemented, the situation was quickly stabilised.[59] Just a few days earlier, several Swiss banks had already experienced disruption to some of their online services.[60] The pro-Palestinian hacktivist group 'RooTDoS' claimed responsibility for these attacks, citing the introduction of the ban on face coverings as their motivation.[61]

As expected, various Swiss websites were targeted by DDoS attacks towards the end of January in connection with the Annual Meeting of the World Economic Forum (WEF). These attacks had no impact on the event itself.[62] The pro-Russian hacktivist group 'NoName057(16)' claimed responsibility; it has previously sought to draw attention to its cause by carrying out similar actions around major Swiss and international events.[63] The main aim here is to create a sense of threat among the public that is not based on an actual danger.

On 19 March, various IT services of the Federal Administration were temporarily impaired by intensive DDoS attacks.[64] Neither the origin of nor the motivation behind these attacks could be determined. As at the WEF Annual Meeting, DDoS attacks also occurred in mid-May in connection with the Eurovision Song Contest (ESC) in Basel.[65] However, due in part to preventive measures by the organisers, the attacks had no impact on the event itself.[66]

In addition to hacktivist activity, there were isolated DDoS attacks linked to extortion. In these cases, the extortionists carried out a brief initial demonstration attack and then threatened a major forthcoming assault in the name of the well-known hacker group NoName057(16). However, no such large-scale attack was ever confirmed. [67] Because NoName057(16) do not usually engage in DDoS extortion, the incident was most likely carried out by imitators using their name.

The perpetrators and motives behind most DDoS attacks usually remain unknown. This is because attack infrastructures can be rented by different actors and directed at any target.

[59] Disruption to federal IT systems due to DDoS attack (ncsc.admin.ch)

[60] *Massive technische Störung bei der Migros Bank* (watson.ch)

[61] CyberKnow: Pro-Palestine hacktivists, RootDos are targeting Migros bank in Europe (x.com)

[62] Expected DDoS attacks have begun (ncsc.admin.ch)

[63] *Plusieurs sites web suisses touchés par une cyberattaque* (swissinfo.ch)

[64] Disruption to federal IT systems due to DDoS attack (ncsc.admin.ch)

[65] Expected DDoS attacks have begun (ncsc.admin.ch)

[66] Cyber resilience during major events and international conferences (ncsc.admin.ch)

[67] See Semi-Annual Report 2024/1, ch. 6, for a similar campaign.

They are also becoming increasingly powerful.[68] According to a sector-specific analysis of the financial sector, threats to internet-facing services pose an increasing strategic challenge.[69] The steadily growing capabilities of cyberactors demand conscious risk management to protect critical functions.

Recommendations

The NCSC website provides information and measures under the heading Attack on availability (DDoS) on how to prevent and defend against such attacks. You should work with your service provider or host to prepare for a potential attack in order to minimise the impact. For critical systems, it may be advisable to seek support from a commercial DDoS protection provider.

In the case of extortionate DDoS attacks, the NCSC recommends that you do not respond to the demands. The perpetrators may ask for more money after an initial payment and then continue with the attacks. Instead, you should report the case to the NCSC and contact the police to make a criminal complaint. In the event of an attack, see DDoS attack – What next? on the NCSC's website.

7 Data management, leaks and extortion

Data leaks and unintended data exposure are recurring topics in Switzerland and abroad. In cases where there is a downstream risk for other organisations or private individuals, data leaks can cause additional harm beyond the loss of confidentiality. For example, if a supplier experiences a breach, companies may need to monitor access to their IT infrastructure, and they also face an elevated risk of fraud attempts (see ch. 5). Similarly, leaked personal information can be exploited for account takeovers, phishing (see ch. 2), identity theft, or financial fraud. Data leaks play a particularly significant role in ransomware and other extortion-related attacks. Criminals will typically publish the data if no ransom is paid, or they will monetise it by selling it, for example (see ch. 3.2). Poor data management within an organisation's own infrastructure, vulnerabilities (see ch. 4) and technical misconfigurations can also lead to data exposure.

A security incident at a cloud service provider presented challenges for its business customers, both internationally and in Switzerland: On 20 March, a hacker using the alias 'rose87168' posted on the hacker forum ‘BreachForums’[70], claiming to have hacked Oracle servers and stolen data from approximately six million accounts.[71] In the same post, the hacker offered

[68] Defending the Internet: How Cloudflare blocked a monumental 7.3 Tbps DDoS attack (cloudflare.com)

[69] From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector (fsisac.com)

[70] See Semi-Annual Report 2024/1, ch. 7.2 for more information on BreachForums and data trading.

[71] Oracle denies breach after hacker claims theft of 6 million data records (bleepingcomputer.com)

Oracle's business customers the option of paying a ransom to have their data deleted. For these business customers, the situation was particularly challenging because Oracle communicated only slowly and cautiously. This made it difficult for both affected organisations and public authorities to gauge the scale of the leak.[72] It was not until 16 April that the US cybersecurity agency CISA clarified that the outdated Oracle Classic cloud system had been accessed without authorisation.[73] Customers who had not changed their passwords and logins after migrating to Oracle Cloud were particularly at risk, as the attackers had obtained their credentials.

In contrast to the Oracle incident, the Swiss procurement service provider Chain IQ was directly targeted by data extortion from the 'World Leaks' group. On 12 June, the group published around 900 GB of Chain IQ data, including customer data from other Swiss finance, retail, and construction companies.[74] This included internal telephone numbers of business contacts, and information on procurement projects.[75] Chain IQ stated that an unknown type of malware had been used in the attack that enabled the intruders to move undetected through Chain IQ's systems.[76] Around a month elapsed between the initial intrusion and the ransom demand, presumably to make technical clean-up efforts more difficult once the breach was detected.
World Leaks is a new group that grew out of the ransomware group 'Hunters International'.[77] It presents itself as an extortion operation that steals data but does not encrypt systems – even though its processor Hunters International carried out classic ransomware attacks, including against Swiss victims.[78] In practice, that claim does not always hold; in several internationally reported cases linked to World Leaks, files were encrypted with malware.[79]

Not only companies but also private individuals are affected by data leaks, when their information ends up on dark- or deep web[80] sites.[81] This data can then circulate in criminal networks, for example after a cyberincident or data exposure, as the two cases from the first half of 2025 illustrate.

Recommendations

Once data is on the internet, it is almost impossible to delete it entirely. Best practice is to define who may store and process which data, in what form, where it is kept, and with whom

[72] Oracle attempt to hide serious cybersecurity incident from customers in Oracle SaaS service (doublepulsar.com)

[73] CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise (cisa.gov)

[74] *Plus de 100 000 employés d'UBS touchés par un vol massif de données sensibles, affectant aussi Pictet* (letemps.ch)

[75] Cyber-Attack Chain IQ Group AG (chainiq.com)

[76] Cyberattacks pose security risks for all companies (chain iq.com)

[77] The beginning of the end: the story of Hunters International (group-ib.com)

[78] See *Cyberangriff auf die Ausgleichskasse Swissmem – Vorfall bewältigt, Konsequenzen gezogen, für die Zukunft gerüstet* (ak-swissmem.ch)

[79] World Leaks: An Extortion Platform (blog.lexfo.blog.fr)

[80] Deep web (wikipedia.org), Dark web (wikipedia.org)

[81] Leaked: Politicians' emails and passwords on the dark web (proton.me); see *Datenleck: Parlamentarier-Daten landen im Darknet* (srf.ch)

it is shared. Store only what is necessary, review data regularly, and delete anything that is longer needed. Encrypt particularly sensitive data. Move data that must be retained but is no longer used to offline storage. Implement clear, practical processes for handling and protecting data, and ensure they are followed.

Data from previous breaches can be reused in subsequent attacks. Regularly check whether your credentials have been part of a data leak, for example using Have I Been Pwned[82] or the Identity Leak Checker from the Hasso Plattner Institute.[83]

8 Cyberespionage and cybersabotage

State and state-affiliated actors represent a distinct type of threat in cyberspace. These groups – often referred to as 'advanced persistent threats' (APTs) – conduct espionage operations, and more rarely sabotage, when it serves the interests of their state.[84] Cyberespionage is a constant challenge for Swiss counterintelligence, whereas targeted cybersabotage is usually observed only in the context of conflicts and periods of heightened geopolitical tension.[85] Unlike financially motivated cybercriminals, APTs select their targets deliberately and invest enormous resources to obtain the information they seek or to achieve the intended effect. Organisations that may be targeted need to structure their defences comprehensively against this kind of threat. Because APT groups have extensive human, technical and financial resources, they can prepare for years before carrying out an active exploitation.

8.1 Cyberespionage

In the second half of 2024, attacks on US and European telecommunications providers allegedly by the Chinese APT group 'Salt Typhoon' were already a major topic.[86] In February 2025, a security company reported new activity by the same group targeting vulnerable Cisco network devices.[87] Just a month later, the activities of another cyberespionage group, believed to be operating on behalf of China, were detected. This group, known as 'Silk Typhoon', has been linked to a number of international attacks across different sectors, using sophisticated methods such as zero-day exploits. Notably, it has carried out supply chain attacks by compromising IT service providers to gain access to customer environments of interest.[88]

[82] See Have I Been Pwned (haveibeenpwned.com)

[83] See Identity Leak Checker (sec.hpi.de)

[84] APT – Glossary (csrc.nist.gov)

[85] See also press release on the situation report Switzerland's Security 2025: Global confrontation has direct effects on Switzerland (vbs.admin.ch)

[86] See Semi-Annual Report 2024/2, section 8.1.

[87] RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers (recordedfuture.com)

[88] Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457) (cloud.google.com)

Like many other APTs, Silk Typhoon also operates attack networks made up of devices under its control, known as ORB networks ('operational relay box').[89] A key factor here is the compromise of poorly secured network devices. These edge devices serve also as access points to company networks. Recent examples include the infection of firewalls,[90] VPN solutions for remote access,[91] and routers.[92]

A new espionage group suspected to be linked to Russia has emerged under the name 'Laundry Bear'. The Dutch authorities hold this APT responsible for attacks on various organisations in the country, including the Netherlands Police.[93] According to Microsoft, this same group (referred to 'Void Blizzard' by Microsoft), has been active since at least April 2024, primarily targeting NATO and Ukraine-related entities. Other established groups in the Russian espionage sphere were also active in spring 2025. In May, for example, US authorities accused 'APT28' of targeting Western logistics and technology firms, particularly those providing support to Ukraine.[94] French authorities also reported attacks by this APT and attributed officially.[95] This reflects a trend in which Western countries are becoming less hesitant to publicly and politically attribute cyberattacks that serve state interests. For example, at the end of May 2025, the Czech Republic officially attributed a cyberattack on its foreign ministry to China.[96]

While state and state-affiliated threat actors typically engage in espionage, those associated with the North Korean regime are also believed to carry out financially motivated activities, such as stealing cryptocurrency.[97] In the context of the 'Contagious Interview' campaign, suspected North Korean threat actors once again posed as recruiters on LinkedIn. People applying for software development positions were asked to complete tasks on their own computers in unsecured environments. The code the applicants were given contained malicious packages that installed malware.[98] In another approach, linked to ClickFix (see ch. 3.1), applicants were tricked into downloading software during the hiring process that was supposedly needed because another programme was not working.[99] Another typical example is the deployment of covert North Korean IT specialists working remotely. On behalf of the regime, they earn a salary through their overseas IT work – and also extract data for espionage and subsequent

[89] See Semi-Annual Report 2024/1, section 8.1.2.

[90] Console Chaos: A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls (arcticwolf.com)

[91] Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation (cloud.google.com), Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457) (cloud.google.com)

[92] Tracking AyySSHush: a Newly Discovered ASUS Router Botnet Campaign (censys.com)

[93] Dutch intelligence unmasks previously unknown Russian hacking group 'Laundry Bear' (therecord.media)

[94] Russian GRU Targeting Western Logistics Entities and Technology Companies (cisa.gov)

[95] Russia – Attribution of cyber attacks on France to the Russian military intelligence service (APT28) (April 29th 2025) (diplomatie.gouv.fr)

[96] Czech Republic says China behind cyberattack on ministry, embassy rejects accusations (reuters.com)

[97] Bybit loses nearly $1.5 billion in crypto hack – What we know so far (economictimes.indiatimes.com)

[98] Another Wave: North Korean Contagious Interview Campaign Drops 35 New Malicious npm Packages (socket.dev)

[99] Lazarus ClickFake Interview Campaign: From Contagious to ClickFix Malware Tactics (blog.sekoia.io)

extortion against their employers.[100] Such activities have increasingly been observed in Europe, including Switzerland.[101] In order to operate successfully and unnoticed abroad, North Korean threat actors often require a degree of local support. To this end, they try to recruit individuals in target countries who are usually unaware of the full extent of their role. One possible explanation for the shift from targeting US firms to European ones is that US authorities have increased their vigilance and countermeasures against such campaigns.

Recommendations

Countering this type of threat requires a defence-in-depth strategy that incorporates multiple layers.[102] As these attackers are willing to invest considerable time and resources in developing their tools, they can identify and exploit new vulnerabilities in each target. Therefore, a successful defensive strategy must take into account different parts of the IT infrastructure. This includes the perimeter, the network, endpoints, and the human factor, as well as the organisation itself. Given the immense resources and capabilities of an APT, it is important to understand that an intrusion can never be ruled out entirely – even if an organisation has a well-established, multi-layered security plan. Network segmentation, where critical systems or sensitive data are isolated, can help prevent a compromise from spreading to all systems. For more recommendations, see the ICT minimum standards.

8.2 Threats to industrial control systems and operational technology

Digitalisation is driving the growing use of IT in data and information management, and is increasingly affecting – and controlling – physical processes. Operational technology (OT), such as industrial control systems (ICS), which were previously often isolated, are now being networked with wider system environments and exposed to the risks that come with them. Outside the industrial sphere, this trend is most visible in building automation and smart home projects.

Attacks on industrial control systems aimed at sabotage occur mainly in the context of geopolitical escalation, such as the war in Ukraine or the conflict between Israel and Iran in mid-June. In addition to directly manipulating the systems themselves, wiper malware can be used to disable them, bringing supply and production to a halt. A striking example was the deployment of ‘PathWiper’ malware against critical infrastructure in Ukraine in June 2025.[103] In Switzerland,

[100] See Semi-Annual Report 2024/2, ch. 8.1.

[101] DPRK IT Workers Expanding in Scope and Scale (cloud.gloogle.com)

[102] See Minimum standard for improving ICT resilience (ncsc.admin.ch), section 1.6 'The defence-in-depth concept'.

[103] Newly identified wiper malware 'PathWiper' targets critical infrastructure in Ukraine (blog.talosintelligence.com)

sabotage of this kind by state-sponsored cyber actors has not been observed and is considered highly unlikely. However, collateral damage from attacks abroad cannot be ruled out.[104]

Such targeted attacks are less common than opportunistic manipulation attempts against inadequately protected industrial controllers that are exposed to the internet. Hacktivist groups use these attacks to generate publicity, and some are even commissioned by state authorities. The attackers generally demonstrate no advanced capabilities; they simply toggle the first switches they can access. The targets are usually non-critical systems, such as dams that regulate the flow of water for fish farms[105] or small hydroelectric plants at mills.[106]
In addition to these different types of attack, the overall system landscape is expanding due to the large number of new operators, most of whom are private. As solar power grows, for example through grid-connected photovoltaic installations, the number of controllable systems increases. Many inverters, which are a key component for connection to the power grid, contain vulnerabilities that could allow unauthorised access.[107] Reducing the vulnerability of such grid-connected systems requires giving cybersecurity the necessary priority.

Recommendations

Secure your industrial control systems to prevent the types of attacks described in this chapter. The NCSC suggests a number of measures to protect ICSs on its website. For more comprehensive guidance, see the minimum standards by sector, developed by the Federal Office for National Economic Supply (FONES) in partnership with the relevant industry bodies. Further guidance is provided by the recommendations on OT[108] from the Information Security Society Switzerland (ISSS).

[104] 'Switzerland's Security 2025': Global confrontation has direct effects on Switzerland (vbs.admin.ch)

[105] Cyberattack on Norwegian Dam Highlights Password Exposure Risks (claroty.com)

[106] Hacktivists Target France Over Diplomatic Moves (cyble.com)

[107] SUNDOWN A Dark Side to Solar Energy Grids (forescout.com)

[108] ISSS Operational Technology (OT) Empfehlungen (cybernavi.ch)