3 November 2022 | National Cybersecurity Centre NCSC

Semi-annual report 2022/I (January – June)

Information assurance

Situation in Switzerland and internationally

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
National Cybersecurity Centre NCSC

1 Overview/content

Management summary

Cyberspace and armed conflicts.

Armed conflicts are increasingly being conducted with the help of cyberattacks. Such attacks can be perpetrated not only by state players, but also by non-state attackers such as hacktivists or criminal groups. The Ukraine conflict in particular shows where cyberattacks can be used as a tool. This multi-faceted issue is the focus topic of this report, which explores it from a variety of angles.

Huge increase in threatening emails

In the first half of 2022, the NCSC saw a huge increase in reports from the general public. By the end of June, the NCSC had received 17,186 reports, which was around 70% more than in the previous half-year period, when 10,234 reports were received. This considerable increase was driven primarily by reports on threatening emails supposedly from the police, so-called fake extortion emails.

Fraud still leading the pack nationally

During the period under review, most of the reports to the NCSC concerned various forms of fraud (10,447 reports). About half of these were reports concerning fake extortion emails (5,872 reports). Other types of fraud included advance-fee fraud (1,834), fake sextortion (615) and classified ad fraud (419). Reports on phishing and malware remained at the same level as in the previous half-year period.

Heavy losses in investment fraud and business email compromise

Aside from ransomware, the NCSC saw the greatest potential for damage for companies in the phenomenon of business email compromise. In the first half of 2022, the NCSC received 47 reports in this regard, with total losses amounting to CHF 2.3 million. Investment fraud is one of the crimes with the highest losses, especially among private individuals. In the first half of 2022, cases with total losses exceeding CHF 3 million were reported to the NCSC.

Slight decrease in ransomware reports

Although ransomware reports edged down from 91 to 83 relative to the previous half-year period, this form of attack is still the most acute cyberthreat facing organisations in Switzerland. Since the start of the year, various organisations in Switzerland from different sectors have been the target of ransomware attacks.

Spoofing on the rise

The NCSC also saw a dramatic increase in reports concerning falsified (spoofed) telephone numbers. In this case, dubious call centres spoof the caller ID and display the telephone numbers of private individuals, thereby luring the person being contacted into taking the call. The NCSC received 319 reports in the first half of 2022, whereas there were only 17 reports in the 2021 reporting period.

Editorial

Looking at the last six months, one cannot avoid talking about the Ukraine conflict when discussing cyber. The conflict had little direct impact on Switzerland's cyber space - apart from the fact that the threat from ransomware has eased somewhat. This is primarily due to two reasons. Groups that had Russian and Ukrainian members fell out, and various groups began to engage in the conflict and were busy with that.

The Ukraine conflict also shows where cyber can be used as a tool and where the limits are. In the conflict, cyber is mainly used for information operations or tactical attacks, primarily on communications assets that serve military purposes. Wide-scale cyberattacks on infrastructure have little effect in conflict. Bombs are often a more efficient and less expensive means. Also, the collateral damage of these attacks are not easy to control and there is a risk of so-called "spillover" effects, which could lead to uncontrolled expansion.

The situation was different in the run-up to the conflict, where attempts were made to cripple strategically important infrastructures in Ukraine by means of cyberattacks. However, these attacks were only successful to a very limited extent. This is primarily because Ukraine's cyber defenses are well prepared. The key here is civilian authorities and companies. Because the conflict shows: The army must also fight in cyberspace, but is absorbed with warfare. Before and also during the conflict, it is therefore existentially important that digital infrastructures can be secured by civilian means and that cooperation between civilian and military agencies is ensured in the event of a crisis. Much like in the physical space, where if a bomb hits, the fire department has to extinguish it because the army is busy with combat operations. In his guest article, Stéphane Duguin of the CyberPeace Institute addresses the issue of cyberattacks on civilian infrastructure. This is followed by a discussion of implications of cyber operations in Ukraine for both the region and globally.

For Switzerland, reports of online fraud continue to dominate, increasing by 70 percent. Here, fake extortion, advance fee fraud, fake sextortion, and classified ad fraud are the primary means used by fraudsters. In this report, we discuss the current scams and their impact.

In the Situation Overview section of this report, we focus on how initial access to systems is gained. Of course, there are also recommendations on how to make such attacks more difficult. Unfortunately, it is still the case that many basic cyber hygiene measures, such as keeping systems up to date, are often not taken. This makes it easier for attackers than it has to be. Of course, there is again an overview of the most important malware families and on the topic of ransomware. The report is rounded off with the presentation of some concrete cases.

I hope you enjoy reading this report. As in the past, we ask you, dear reader, to give us your feedback. This is the only way we can continuously adapt the semi-annual report to your needs.

Florian Schütz, Federal Cybersecurity Delegate

2 Guest article from the CyberPeace Institute

Stéphane Duguin is Chief Executive Officer of the CyberPeace Institute, a neutral and independent non-governmental organisation (NGO) working for cyberpeace. The Institute tracks and analyses cyberattacks against civilian objects through its Cyber Attacks in Times of Conflict Platform #Ukraine.

How an armed conflict is destabilising cyberspace for us all

Stéphane Duguin,
CEO CyberPeace Institute

Beyond land, sea and air, armed conflicts are increasingly being waged in outer space, the information space and cyberspace. The borderless nature of these domains has changed how an armed conflict between countries may have an impact beyond the military objectives of those parties. The military invasion of Ukraine in February 2022, preceded by a series of cyberattacks affecting Ukrainian public institutions and organisations, set the scene for what is today a war fought both online and on the ground. Attacks and operations, deployed in cyberspace in the context of the war between the Russian Federation and Ukraine, have destabilised cyberspace and threatened the safe, secure and trusted use of technology.

When critical infrastructure comes under fire

Critical infrastructure is no stranger to cyberattacks – an oil pipeline (United States, 2021), water pumping stations (Israel, 2020), healthcare services (United Kingdom, 2017) and the armed conflict in Ukraine have starkly illustrated this. In the lead-up to and during the early days of the conflict, six different strands of data-wiping malware were deployed against Ukrainian organisations in critical sectors. Malware can cause significant harm as it disrupts critical services for the civilian population. The attack on ViaSat's KA-SAT satellite network, reportedly intended to hit aspects of military command and control in Ukraine, resulted in the major loss of internet communication for users across Europe and impacted a German energy company, which lost remote monitoring access to over 5,800 wind turbines. Both this attack and other data-wiping malware deployed during the conflict have been attributed to highly sophisticated nation-state players.

Unconventional players disrupting cyberspace

In addition to the traditional parties to the armed conflict, this armed conflict has seen others playing a significant role and the boundaries between them are increasingly blurred. Created by the Ukrainian government, the IT Army of Ukraine is a less conventional player whose Distributed Denial of Service (DDoS) attacks are heavily impacting Russian online resources. Meanwhile, so-called hacktivist collectives have flooded the networks of government institutions, state-owned enterprises and other organisations with DDoS attacks. They have played an active role in disrupting the public-facing online infrastructure of their targets. This has resulted in downtime for websites and portals, many of which are used by the general population to conduct routine activities such as booking transport tickets or submitting tax declarations.

A significant number of NATO member countries, not parties to the conflict, have been particularly impacted by cyberattacks in recent months. These were carried out by hacktivist collectives, seemingly in response to those countries' public positions on geopolitical, ideological or economic subjects.

The publication of large volumes of sensitive data has become part and parcel of the cyberthreat landscape during the conflict. Acting in the name of anti-war activism, collectives have conducted a significant number of hack-and-leak attacks which lead to sensitive customer and corporate data, including personal data, being made publicly available. These attacks raise significant questions relating to the protection of individuals, data protection, and the potential for malicious use of this data in the future.

A number of questions arise from less traditional players participating in the armed conflict, not least with regard to attempts to attribute attacks, i.e. to determine who developed, launched or authorised a particular cyberattack.

Protecting "our" cyberspace

Cyberattacks and operations conducted in the context of war or in peacetime, by countries and non-state players, have contributed to the destabilisation of cyberspace and in turn of society, which so heavily depends on technology. Such destabilisation has long-lasting impacts, many of which are yet to be uncovered. Advancing responsible behaviour in cyberspace is essential to ensuring an open, free, stable and secure digital environment, and will require commitment and engagement from all:

- Whether in war or peacetime, cyberattacks should not be directed against critical infrastructure essential for the survival of civilian populations, respecting international law and norms.
- The potential harm and impact on people, and the humanitarian consequences of the use of cyber, must be a primary consideration before its use.
- Countries must ensure accountability for cyberattacks that breach international laws and norms.
- Public institutions such as Computer Emergency Response Teams (CERTs) are essential for the protection of systems and the investigation of attacks through effective collaboration and information sharing.
- Private companies can play a role in developing and providing secure products and services to the most vulnerable in society, and proactively protecting governments and their citizens.
- And last but not least, civil society organisations can contribute to documenting and analysing cyberattacks and the impact they have on people to facilitate investigations and support the policy debate.

3 Focus: Cyberspace and armed conflicts

This section highlights the main events that have taken place in cyberspace during the current war between Russia and Ukraine. Influence operations make up a significant part of what goes on in cyberspace. The aim of those is to influence the ideas, opinions and motivations of specific target groups and to intervene in their decision-making processes. However, this report does not address these types of influence operations, but rather considers actions in cyberspace that have a direct impact on the confidentiality, integrity and availability of data, or even a physical impact.[1]

3.1 Cyberactivities before the invasion

Ukraine has been a target of cybersabotage for several years now. Here are three prominent examples:

- In 2015, the BlackEnergy3 malware, attributed to the Russian cyberactor Sandworm, caused power outages of up to six hours and affected several hundred thousand consumers.[2]
- In 2016, Sandworm was active again, this time with Industroyer, a specially developed malware designed to infect industrial control systems used in power supply, which led to power outages lasting around an hour in parts of Kyiv.[3]
- In contrast to the targeted attacks on the power supply in 2015 and 2016, the NotPetya malware was distributed en masse in 2017. This malware first encrypts the data of the infected system and then causes a message to appear demanding a modest ransom. The NotPetya attack started with a manipulated update of a Ukrainian accounting program, which resulted in numerous systems in Ukraine being infected. However, the malware also spread beyond Ukraine's borders and affected systems in more than 65 countries. Its modus operandi, Ukraine as its target and the lack of a decryption option, which is unusual for ransomware, indicate that it was not a case of extortion but of sabotage.[4]

The Security Service of Ukraine (SSU) claims to have repelled more than two thousand cyberattacks against government systems and critical infrastructure in Ukraine in 2021 alone, with the SSU linking some of these attacks to Russian intelligence services.[5] Then, in early 2022, there were several high-profile cyberincidents in Ukraine. For example, on 15 January 2022, Microsoft announced that it had discovered a form of malware called WhisperGate, which had been attacking the systems of government institutions, IT companies and non-profit organisations in Ukraine since 13 January 2022.[6] WhisperGate was made to look like ransomware, but the lack of a data recovery mechanism suggests that it was in fact a wiper –

---

1 For examples of influence operations in the context of the Ukraine war, see section 4 of the Microsoft report of 22 June 2022 on the war in Ukraine (microsoft.com); see also EU vs DISINFORMATION (euvsdisinfo.eu)

2 See semi-annual report 2015/2 (ncsc.admin.ch), section 5.3.1

3 See semi-annual reports 2016/2 (ncsc.admin.ch), section 5.3.1 and 2017/1 (ncsc.admin.ch), section 5.3.1

4 See semi-annual report 2017/1 (ncsc.admin.ch), section 3

5 SSU neutralizes over 2,000 cyber attacks on government resources in 2021 (ssu.gov.ua)

6 Destructive malware targeting Ukrainian organizations (microsoft.com)

malware that overwrites and thus irrevocably deletes data on infected target systems. After the malware had been analysed, the Ukrainian government spoke of a false-flag Russian operation that aimed to pin the responsibility for WhisperGate on Ukrainian cybercriminals.[7] At the same time as WhisperGate emerged, countless Ukrainian government websites were defaced by defacement attacks.[8] Then, in mid-February, numerous DDoS attacks took place, affecting the availability of several websites and online services in Ukraine, including those of financial institutions and state authorities.[9]

3.2 Prominent cyberincidents in the current war in Ukraine

3.2.1 Disruption of satellite links

On 24 February 2022, about an hour before the start of the Russian offensive against Ukraine, various European connections to the KA-SAT satellite operated by the US company ViaSat failed. Numerous European companies, public authorities and private individuals use this telecommunications satellite for internet access, especially in remote regions. The incident led to disruptions both in Ukraine and beyond its borders. For example, in Germany, access to monitoring and remote control systems of wind power plants was no longer possible. On 30 March 2022, ViaSat published an analysis of the incident.[10] It concludes that this was a targeted attack that focused only on the part of the satellite network responsible for covering Ukraine, but that its effects were not limited to this. The attackers exploited the faulty configuration of a VPN connection to gain access to the administrator interface. This allowed them to initiate a manipulated firmware update for numerous client devices. As a result, the affected systems could no longer establish a connection and had to be restored manually on site. At the beginning of May 2022, the European Union and its member states as well as the United States, the United Kingdom and other countries condemned the attack, for which they officially held Russia responsible.[11]

Comment:

Cyberattacks on infrastructures used for both military and civilian purposes, sometimes even by stakeholders of and in multiple countries, raise several questions regarding the norms of state behaviour in cyberspace. The aspects of proportionality, collateral damage and duty of consideration on the part of state aggressors are likely to be widely discussed in the coming years.

---

7 Information on the possible provocation (cip.gov.ua)

8 Ukraine hit by 'massive' cyber-attack on government websites (theguardian.com)

9 Ukraine Ministry of Defense confirms DDoS attack; state banks lose connectivity (zdnet.com); DDoS attacks hit Ukrainian government websites (therecord.media)

10 KA-SAT Network cyber attack overview (viasat.com)

11 Russian cyber operations against Ukraine: Declaration by […] the European Union (europa.eu); Attribution of Russia's Malicious Cyber Activity Against Ukraine (state.gov); Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion (www.gov.uk)

3.2.2 Attempt to sabotage power supply: Industroyer2

On 12 April 2022, the Computer Emergency Response Team of Ukraine (CERT-UA), together with Microsoft and the Slovakian IT security company ESET, announced that they had detected and disabled Industroyer2, the first malware in this war of aggression to target industrial control systems.[12] It is said to have been a new version of the Industroyer malware used in 2016, which caused power outages in Kyiv at the time (see section 3.1), with the new version also having been developed by Sandworm.[13] The attack targeted an electricity provider in Ukraine whose IT network had already been infiltrated by the attackers in February 2022. The attackers managed to penetrate the control and management network of the operational technology via the IT network and place the Industroyer2 malware there. The attack was supposed to unleash its destructive power on 8 April 2022, when electrical substations were to be taken offline and parts of the company's infrastructure paralysed. In addition to Industroyer2, the wiper CaddyWiper is said to have been active at the same time. This was probably with the aim of making it more difficult to restore the systems and removing evidence of the attack. A few days after the CERT-UA announcement, the Ukrainian government reported that more than 50 similar attacks had been thwarted since the beginning of the war. Contradicting this announcement, a leaked confidential report said that nine substations had been brought down in a cyberattack that had taken place shortly beforehand.[14]

Comment:

Industroyer2 is the first malware discovered since the beginning of the invasion of Ukraine which, on account of its functionality, was intended not only to disrupt IT systems but also to affect physical processes through direct interaction with industrial control systems.

3.2.3 Wipers

Numerous different wipers have emerged since the beginning of the war in Ukraine.[15] The aim of such malware is to destroy data or make it unreadable by encrypting or overwriting it and thus to delete it irrevocably. Organisations from different sectors such as government services, energy and the financial sector were targeted. However, no information is available from official sources on the precise extent and success of the attacks. According to analyses, the malware is always programmed so that it does not spread in an uncontrolled manner, as was the case with NotPetya in 2017. Nevertheless, on 23 February 2022, HermeticWiper was discovered in Lithuania and Latvia at companies that also provide services to the Ukrainian government.[16]

---

12 Heavy cyberattack on Ukraine's energy sector prevented (cip.gov.ua);
Industroyer2: Industroyer reloaded (welivesecurity.com)

13 Ukraine Power Grid Cyberattacks (securityboulevard.com);
INDUSTROYER.V2: Old Malware Learns New Tricks (mandiant.com)

14 Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine (wired.com);
Russian hackers tried to bring down Ukraine's power grid to help the invasion (technologyreview.com)

15 An Overview of the Increasing Wiper Malware Threat (fortinet.com)

16 Russia unleashed data-wiper malware on Ukraine (theguardian.com)

Comment:

Russian state actors seem very keen to limit the impact of their cybersabotage attacks to Ukraine. No country, much less NATO, should be given a pretext to actively intervene in the conflict.

3.3 Non-state aggressors on both sides

Following the Russian offensive of 24 February 2022, numerous non-state actors (hacktivist organisations and criminal groups) announced their intention to participate in the war in cyberspace. They either claim attacks as their own or threaten those who attack "their" warring party with reprisals. In total, more than 80 such non-state groups have been identified.

One of the most significant groups on the Russian side is Killnet. In response to the support given to Ukraine and the sanctions against Russia, the group has carried out numerous DDoS attacks.In particular, websites of airports, state institutions and financial institutions of numerous European countries were affected. The resulting damage depends heavily on how dependent the respective victims are on their internet presence and how well prepared they are for such attacks. In most cases, DDoS attacks can be blocked or rendered harmless relatively quickly.

On the Ukrainian side, the Anonymous collective claimed numerous attacks on Russian organisations, as well as on Western companies that continued to operate in Russia. For example, on 20 March 2022, Anonymous called on Western companies operating in Russia to withdraw from the Russian market within 48 hours. If they failed to do so, they risked becoming a target of the group. Since then, Anonymous has carried out numerous hack-and-leak attacks: confidential corporate and government data, mainly from Russia, has been stolen and published.

On 26 February 2022, Ukraine announced the creation of an IT Army of Ukraine and called for volunteers from all over the world to join it and carry out attacks in cyberspace in favour of Ukraine. One of the main pillars of this group is its Telegram channel, which it uses to communicate the targets of its DDoS attacks.

Despite the high frequency of attacks by non-state groups, the impact of these attacks on the course of the war appears marginal so far.

Comment:

Criminal acts, such as damage to property, are repeatedly committed in the context of politically motivated demonstrations on the streets. On the internet, hacktivists carry out comparable virtual campaigns (defacement, DDoS). However, when hacktivists engage in armed conflicts between countries, they could possibly qualify as participants in war (combatants) and thus become legitimate targets for counterattacks. Questions also arise regarding the responsibilities of countries from whose territory hacktivists launch their attacks.

3.4 Other aspects of the conflict in cyberspace

3.4.1 Support by countries and companies

At the beginning of 2022, various support measures for Ukraine in the field of cybersecurity were announced. On 14 January 2022, the NATO Secretary General held out the prospect of signing an agreement with Ukraine to increase cyberdefence support. The statement also said that NATO had been working with Ukraine for years to improve the country's cyberdefences, including onsite support. For its part, the European Union announced on 22 February 2022 the formation of a team of experts of around ten representatives from various European countries to help Ukraine deal with increasing cyberthreats, both on the ground and remotely.

More specific data on how other countries are assisting Ukraine became available on 10 May 2022. In a statement, the European Union and its member states, as well as the United States, the United Kingdom and other countries, condemned the attacks on ViaSat (see section 3.2.1) and announced that they would continue to support Ukraine to strengthen its cyber-resilience. At the same time, the US provided more details on how the country will support Ukraine in ensuring internet access and cybersecurity.[17]

On 1 June 2022, the commander of the US Cyber Command announced that the United States had implemented a number of offensive and defensive operations, and information measures, in cyberspace in support of Ukraine.[18] Since the majority of these measures have not been made public, it is difficult to assess their impact. The analysis published in April 2022 of a malware that had been designed for attacks on industrial control systems (see section 5.4.1), but had not been deployed by then, is likely to be related to these measures taken by the US Cyber Command. The malware could have been used for future attacks against Ukraine, but also against other countries. Another operation that potentially helped Ukraine and that has been made public is the partial shutdown of the CyclopsBlink botnet infrastructure used by Sandworm (see section 5.2.4).

Numerous IT security companies give special importance to the war in Ukraine and devote analyses and reports to this topic. For example, ESET and Microsoft, together with the Ukrainian CERT, publicised the discovery of Industroyer2. On 22 June 2022, Microsoft published a report on the company's observations concerning cyberthreats in the war in Ukraine.[19] The report stated, among other things, that Microsoft and other technology companies had helped Ukraine move most of the Ukrainian government's data and digital activities to clouds outside its borders within ten weeks. Thus, when Ukrainian data centres were destroyed in missile attacks at the beginning of the Russian offensive, Ukraine was able to continue to function digitally. The report also notes the IT company's close cooperation with the Ukrainian government. In its report, Microsoft stated that it had supported Ukraine with free services worth an estimated total of USD 239 million. Assistance from private companies is undoubtedly essential for Ukraine, as they also provide system protection under normal circumstances and typically have insight into many more systems and operations than any of the authorities.

---

17 U.S. Support for Connectivity and Cybersecurity in Ukraine (state.gov)

18 US military hackers conducting offensive operations in support of Ukraine (sky.com)

19 Defending Ukraine: Early Lessons from the Cyber War (microsoft.com)

3.4.2 Use of cybertools in the context of armed conflict

The cyberattacks in Ukraine that have become public so far do not paint a complete picture, nor do they allow for a conclusive assessment of how cyberspace might be used in the context of armed conflict in the future.

As this is an ongoing war, many incidents, and their implications, are not made public. When the protagonists lay claim to successful or averted attacks, the corresponding announcements often serve to influence the public opinion and mood positively or negatively. Independent verification is often not possible. Also, no cyberattacks against military systems have been made public so far. An example for this kind of attack would be the one suspected in Syria in 2007, when Israeli forces allegedly used their cyberexpertise to disable air defence systems so that they could launch an air strike against targets in Syria.[20]

After the annexation of Crimea in 2014, the conflict between Ukraine and Russia, specifically the separatist areas in eastern Ukraine, simmered, with periods of reduced and then increased activity. During this time, cyberoperations were also carried out (see section 3.1 above) which the purported perpetrator was able to deny more or less credibly. However, since the beginning of the Russian offensive, the use of conventional military means may also have eclipsed the use of cyberinstruments. Indeed, many military objectives can be achieved faster, more precisely, more easily and with greater lasting effect by conventional military means than through cyberattacks.

There are various hypotheses for the lack of any reports of successful destructive cyberattacks by Russia (i.e. attacks resulting in physical destruction) against Ukraine:

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.

Ultimately, the apparent absence of such attacks is probably due to a combination of the various hypotheses, and very likely more cyberincidents are happening than is publicly known.

[20] Operation Orchard/Outside the Box (2007) - International cyber law: interactive toolkit (ccdcoe.org); Cyberattacken auf syrische Luftabwehr (cyber-peace.org)

4 Reports from the public

4.1 Reports received on cyberincidents – overview

In the first half of 2022, the NCSC registered a total of 17,186 reports, which was around 70% more than in the previous half-year period, when 10,234 reports were received. This considerable increase was driven primarily by reports on fake extortion emails, which now account for around a third of all reports and half of the fraud reports. Reports in the "Fraud" main category were by far the most frequent, with 10,447 reports. Aside from the already mentioned fake extortion, other relevant types of fraud are advance-fee fraud (1,834), fake sextortion (615) and classified ad fraud (419). Reports on phishing and malware remained at the same level as in the previous half-year period.

Reports to the NCSC in the first semester of 2022 (per week)

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

Reports to the NCSC in the first semester of 2022 (by category)

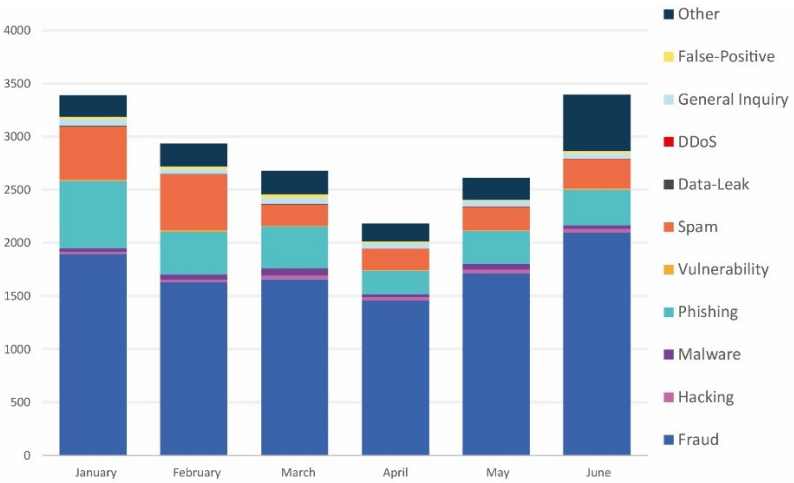
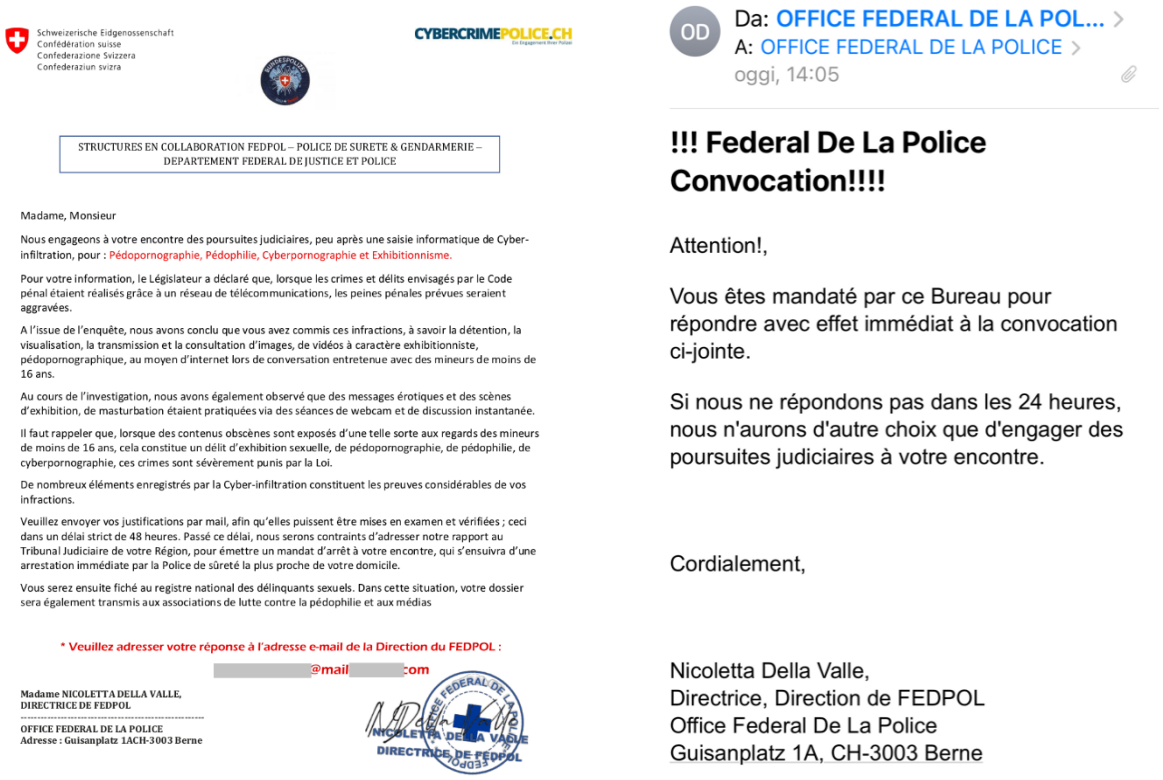


Fig. 2: Reports to the NCSC in the first half of 2022 by category, see also Current figures (ncsc.admin.ch)

4.2 Most frequently reported: fraud

4.2.1 Persistent trend towards more fake extortion

The upward trend concerning threatening emails supposedly sent by the police, which had already become apparent at the end of last year, continued in the first half of 2022. Such so-called fake extortion emails now account for around a third (5,872) of all reports received and around half of the fraud reports. Fake extortion is a type of fraud in which the fraudsters claim that the people contacted have been found guilty of significant misconduct (typically in connection with child sexual abuse images) and that the charges against them can be dropped only if they pay money. The scam was first observed in France several years ago, and it then hit Switzerland. Initially, the fraudulent emails were found solely in French, but then also in German, and in mid-May 2022, the first such messages written in Italian were reported to the NCSC. The most common variant claims to be from the Federal Office of Police or, more precisely, from the fedpol Director, Nicoletta Della Valle.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

CYBERCRIMEPOLICE.CH

STRUCTURES EN COLLABORATION FEDPOL – POLICE DE SURETE & GENDARMERIE – DEPARTEMENT FEDERAL DE JUSTICE ET POLICE

Madame, Monsieur

Nous engageons à votre encontre des poursuites judiciaires, peu après une saisie informatique de Cyber-infiltration, pour : Pédopornographie, Pédophilie, Cyberpornographie et Exhibitionnisme.

Pour votre information, le Législateur a déclaré que, lorsque les crimes et délits envisagés par le Code pénal étaient réalisés grâce à un réseau de télécommunications, les peines pénales prévues seraient aggravées.

A l'issue de l'enquête, nous avons conclu que vous avez commis ces infractions, à savoir la détention, la visualisation, la transmission et la consultation d'images, de vidéos à caractère exhibitionniste, pédopornographique, au moyen d'internet lors de conversation entretenue avec des mineurs de moins de 16 ans.

Au cours de l'investigation, nous avons également observé que des messages érotiques et des scènes d'exhibition, de masturbation étaient pratiquées via des séances de webcam et de discussion instantanée.

Il faut rappeler que, lorsque des contenus obscènes sont exposés d'une telle sorte aux regards des mineurs de moins de 16 ans, cela constitue un délit d'exhibition sexuelle, de pédopornographie, de pédophilie, de cyberpornographie, ces crimes sont sévèrement punis par la Loi.

De nombreux éléments enregistrés par la Cyber-infiltration constituent les preuves considérables de vos infractions.

Veuillez envoyer vos justifications par mail, afin qu'elles puissent être mises en examen et vérifiées ; ceci dans un délai strict de 48 heures. Passé ce délai, nous serons contraints d'adresser notre rapport au Tribunal Judiciaire de votre Région, pour émettre un mandat d'arrêt à votre encontre, qui s'ensuivra d'une arrestation immédiate par la Police de sûreté la plus proche de votre domicile.

Vous serez ensuite fiché au registre national des délinquants sexuels. Dans cette situation, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux médias

* Veuillez adresser votre réponse à l'adresse e-mail de la Direction du FEDPOL :

[redacted]@mail[redacted].com

Madame NICOLETTA DELLA VALLE,
DIRECTRICE DE FEDPOL

OFFICE FEDERAL DE LA POLICE
Adresse : Guisanplatz 1ACH-3003 Berne

NICOLETTA DELLA VALLE
DIRECTRICE DE FEDPOL

OD Da: OFFICE FEDERAL DE LA POL...
A: OFFICE FEDERAL DE LA POLICE
oggi, 14:05

!!! Federal De La Police Convocation!!!!

Attention!,

Vous êtes mandaté par ce Bureau pour répondre avec effet immédiat à la convocation ci-jointe.

Si nous ne répondons pas dans les 24 heures, nous n'aurons d'autre choix que d'engager des poursuites judiciaires à votre encontre.

Cordialement,

Nicoletta Della Valle,
Directrice, Direction de FEDPOL
Office Federal De La Police
Guisanplatz 1A, CH-3003 Berne

Fig. 3: Threatening emails supposedly from the fedpol Director, Nicoletta Della Valle.

However, the senders used in the threatening emails supposedly from the authorities change frequently and are also strung together in a completely incoherent manner. Other variants were supposedly from various cantonal police forces and the police portal Cybercrimepolice. The name of the NCSC was also misused to make the fraudulent emails look official. The perpetrators often use hacked email accounts of students from various universities in Europe and Brazil to communicate with the victims. In this context, the NCSC already reported hundreds of fake and hacked email accounts to the corresponding providers in order for them to take measures to counter the abuse.

4.2.2 Heavy losses in investment fraud and business email compromise

Investment fraud continues to be one of the crimes with the highest losses. In the first half of 2022, cases with total losses exceeding CHF 3 million were reported to the NCSC. Six-figure sums per case are not uncommon. In times of rising inflation and low interest rates, such investment offers seem to be booming. Blinded by the (suspiciously) high returns promised, the victims ignore all signs and indications of fraud. In most cases, for example, the dubious investment websites are only a few months old.

Aside from ransomware, the NCSC saw the greatest potential for damage for companies in the phenomenon of business email compromise. It received 47 reports in this regard during the period under review. In this type of fraud, reference is made to existing email communication between the contracting parties that contains a payment instruction or invoice. The fraudsters change the IBAN to which the amount is to be paid. In order to access the email communication, attackers must have access to either the sender's or the recipient's email account. Supplier companies in particular are targeted. Firstly, the invoice amounts are often high and secondly, various invoices are usually sent at the same time, which increases the fraudsters' chances of success. Losses totalling CHF 2.3 million were reported to the NCSC in this category.

4.2.3 Spoofing on the rise

Reports of falsified (spoofed) telephone numbers have virtually exploded, with the number of reports rising from 17 to 319 relative to the previous half-year period. The background involves calls from dubious call centres with spoofed telephone numbers that are actually assigned to private individuals. In the case of fraudulent calls or calls from dubious call centres, it is common practice to spoof the caller ID and display an innocuous Swiss number in order to thereby lure the person being contacted into taking the call. When the same numbers are repeatedly used for spoofing, the actual owners of these numbers are literally flooded with return calls. Some of those who submitted a report received up to 50 calls per day. Normally, the call centres change the spoofed numbers regularly, with the result that the callbacks stop at some point. In some cases, however, the same telephone numbers were used for weeks if not months. This is more than annoying for the actual owners of the numbers, especially since little can be done about it.[21]

4.3 Phishing reports

Phishing reports remained at about the same level as in the previous half-year period. The number of reports submitted via the reporting form was down by 100, to 2,308 cases, but a total of 4,535 pages were processed directly via the specialised portal antiphishing.ch. The predominant ones remained emails with fake parcel notifications supposedly sent by various parcel service providers. This variant alone accounted for 464 reports. Another perennial favourite in the phishing category involves bills from internet service providers such as

[21] See BBl 2017 6559 – Dispatch on the revision of the Telecommunications Act (admin.ch), 6581 and 6596

Swisscom or Sunrise that have purportedly been paid twice. The fraudsters promise that money will be transferred to the victim's credit card if the credit card number is provided.

With a total of 145 reports in the first half of 2022, phishing attempts in connection with classified ads likewise increased. This phishing variant involves the perpetrators feigning interest in a product. Once a sales price has been agreed upon, the buyers state that they will arrange transport and that money to cover the transport costs incurred will be transferred together with the purchase price. The sellers are then supposed to pay the transport company by credit card by entering their card details on the websites of alleged parcel service providers that then contact them. These websites are sometimes highly customised and, aside from the seller's name and address, often also contain a picture of the item for sale, which the phishers previously copied from the classified ads platform. The attackers therefore make quite an effort, but it seems to be worth their while.

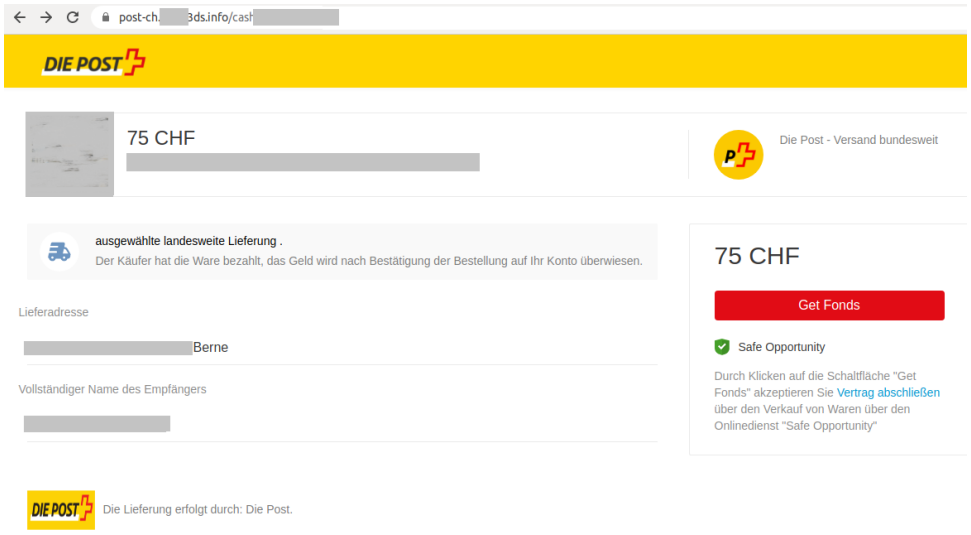


Fig. 4: Customised website with the seller's address and a picture of the product

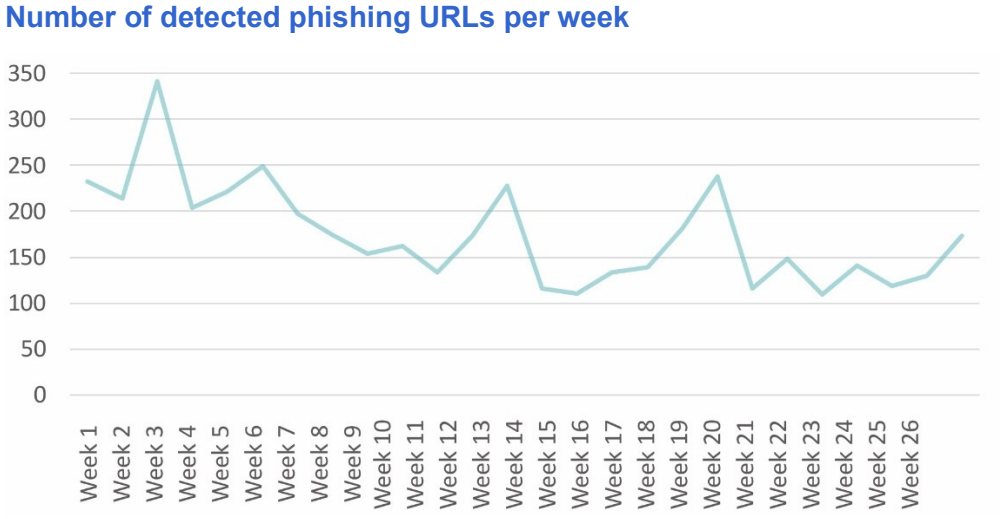


Fig. 5: Number of phishing URLs checked and confirmed by the NCSC per week in the first half of 2022; current data can be found at: https://www.govcert.admin.ch/statistics/phishing/

4.4 Malware and hacking reports

A total of 255 malware reports were registered in the first half of 2022, representing a decline of 20% on the previous half-year period. There were no major waves. However, two smaller FluBot waves stood out in March and May, and gave rise to a total of 56 reports. In these cases, the victims were sent text messages containing notifications of supposed parcel deliveries using various wordings. The link under the text led to a website which prompted the victims to download and install an app of the alleged parcel service provider on an Android smartphone. International investigators succeeded in bringing down the network behind the FluBot Trojan in June 2022 (see section 5.2.3).

Another wave that gave rise to 30 reports concerned the malware QakBot (also known as QuackBot or QBot). This malware is spread via emails. The cybercriminals often use companies' existing email exchanges (e.g. with suppliers or clients), which have fallen into their hands through previous attacks, to get the recipients to open malicious attachments. This is how the malware is installed, and it is subsequently exploited as a gateway to penetrate corporate networks (see section 5.1.2) and then install encryption Trojans, i.e. ransomware.

Ransomware reports decreased slightly relative to the previous half-year period, going from 91 to 83 reports. Primarily the ransomware families QLocker and DeadBolt, which target NAS devices, as well as LockBit 2.0, Sodinokibi and Conti were reported. In contrast, hacking incidents were up, going from 139 to 184 reports. The focus here was mainly on social media accounts. As many as 91 reports concerned social networks such as Facebook, Instagram and Twitter.

5 Events/situation

5.1 Initial access

Obtaining access to user accounts or remote access to computer systems is the first step in most types of cyberattack. This is because it is the only way for the attackers to achieve their actual goal, be it to abuse the system or account for fraud, to obtain unauthorised access to data or to plant encryption malware (ransomware). Such initial access can be gained in various ways.

5.1.1 Username/password

Access is most easily gained when an account or system is secured with only a username (often the email address) and password. Then, the password can be obtained by simply phishing the email address and thus accessing the account or system. Attackers thereby have full access and can do anything they want with it, just like the legitimate users, regardless of whether they are currently online or not.

In the case of access that is secured solely with a username and password, there is also the risk of multiple accounts being attacked if the same password is reused across several sites. Cybercriminals often use credential stuffing for this purpose, i.e. they try out the stolen credentials for all the usual services (email provider, Twitter, Facebook, Instagram, Amazon, etc.). Afterwards, the credentials verified in this way are sold on.

Conclusion/recommendation:

Two-factor or multi-factor authentication, for example, offers protection against this threat

The Federal Data Protection and Information Commissioner (FDPIC) contributed to a recent Global Privacy Assembly report[22] and guidelines[23].

5.1.2 Malware (Trojans)

Another method of gaining unauthorised access is to use malware to create a backdoor to the system. Along the lines of the Greek legend about the Trojan horse, the malware is smuggled into a system unnoticed and then opens a path for the attackers to install further malware. Various social engineering methods are used to persuade users to make the decisive click on a link or to open a Trojanised file. Typical elements of these manipulation attempts are arousing people's curiosity or fears that they have missed something, and citing urgency.

Most Trojans these days contain functionalities for downloading and installing further malware (e.g. Emotet[24], Qakbot[25], FormBook/XLoader[26]). However, Trojans that primarily take screenshots and record keystrokes (so-called keyloggers) still exist. At regular intervals, the Trojan independently sends usernames and passwords obtained in this way (as well as credit card details and other information) to its operators or the attackers, or stores them online in so-called drop zones, where they can be picked up by the criminals. One such Trojan that was highly active during the period under review is Snake Keylogger[27].

Conclusion/recommendation:

The most popular vector for spreading 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 pandemic, the war in Ukraine, natural disasters or sporting events is provided in the hope of arousing curiosity. In many cases, urgency is also feigned in order to trick recipients into acting rashly.

Do not open any attachments or click on links in suspicious emails.

---

22 22-06-27-Credential-Stuffing-General-Public-Awareness.pdf (globalprivacyassembly.org)

23 22-06-27-Credential-stuffing-guidelines.pdf (globalprivacyassembly.org)

24 Emotet (fraunhofer.de); Emotet Botnet C&Cs (abuse.ch); URLhaus | emotet (abuse.ch)

25 QakBot (fraunhofer.de); Qakbot Botnet C&Cs (abuse.ch); URLhaus | Qakbot (abuse.ch); see semi-annual report 2021/2 (ncsc.admin.ch), section 4.2.3

26 FormBook (fraunhofer.de); XLoader (fraunhofer.de); URLhaus | FormBook (abuse.ch)

27 404 Keylogger (fraunhofer.de); URLhaus | SnakeKeylogger (abuse.ch)

5.1.3 Exploitation of vulnerabilities

Software vulnerabilities and incorrect configurations lead to vulnerabilities that can be exploited either for direct access or for the purpose of gaining subsequent access. Systems that can be accessed directly from the internet are particularly vulnerable, as these are not (or cannot be) protected by another layer of security in all cases.

One software package whose vulnerabilities have regularly caused a stir since the beginning of 2021 is Microsoft Exchange.[28] Various other vulnerabilities in Microsoft Exchange have emerged since the first big fuss in March 2021. Given that so many companies use this email server software, attackers have a huge range of potential victims, especially since not all system administrators apply updates as soon as they are available. Remote access products and firewalls that are not kept up to date are likewise popular gateways for cybercriminals to penetrate networks.[29]

Platforms that are operated in the cloud are also exposed and can be attacked in the event of inadequate protection or faulty configuration, or via software vulnerabilities. The situation is similar for user interfaces (web interfaces) of systems that are monitored and controlled remotely.

Conclusion/recommendation:

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.

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

The NCSC regularly informs organisations that are vulnerable because of outdated systems.[30] 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 until they receive a message from the NCSC. It is strongly recommended to have your own effective software management with inventory and update processes.[31] However, prompt action is required at the latest when an organisation receives a registered letter from the NCSC.

5.2 Malware

5.2.1 General situation

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

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

[29] See semi-annual report 2021/1 (ncsc.admin.ch), section 3.1.2

[30] High time to fix the security vulnerabilities in Microsoft Exchange Servers (ncsc.admin.ch); MS Exchange vulnerabilities still not patched (ncsc.admin.ch)

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

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

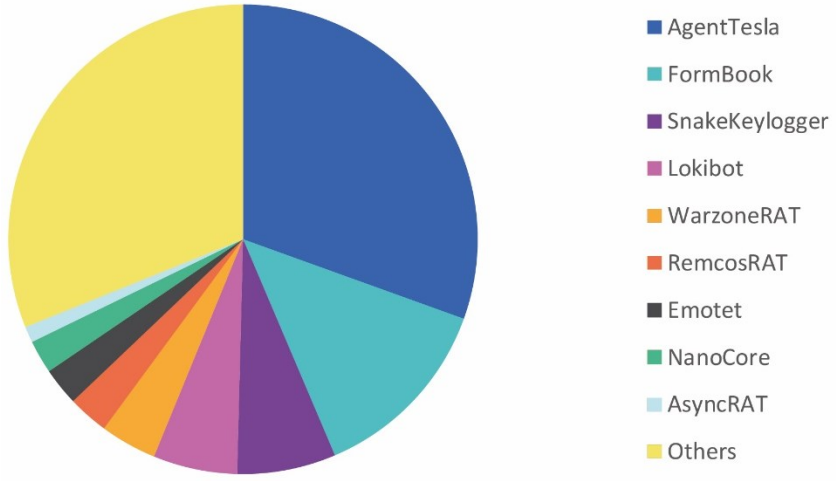


Fig. 6: NCSC analyses of malware families in Switzerland in the second half of 2022

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

Malware infections

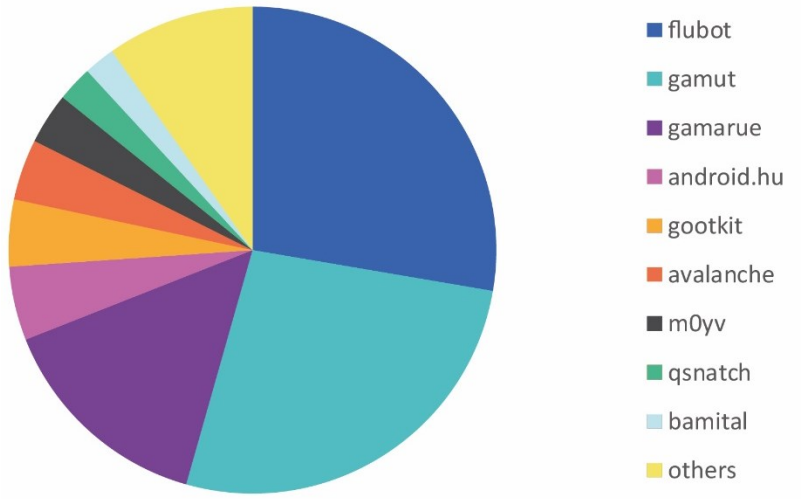


Fig. 7: Distribution of malware infections detected by the NCSC in Switzerland in the second half of 2022

5.2.2 Ransomware

This year too, cybercriminals have engaged in ransomware campaigns. All industries are now affected by this kind of attack[32] and ransomware[33] continues to be the greatest cyberthreat facing organisations in Switzerland.

5.2.2.1 Incidents in Switzerland

Since the start of the year, various organisations in Switzerland from different sectors have been the target of attacks.[34]

In the incidents concerning the healthcare sector, the attackers often used a double extortion technique involving LockBit 2.0 ransomware[35]; here, the victim's sensitive data is first copied and then encrypted on the victim's systems. A number of Swiss healthcare institutions found themselves having to deal with encrypted servers and data leaks. Often, the information ended up on the darknet. So these attacks affect not just the institutions themselves, but also indirectly the patients, because the leaked information frequently contains their personal details and sensitive data such as medical records.[36]

In sectors such as transport and logistics, on whose smooth functioning many other industries rely, the perpetrators try to cause as much disruption to operations as possible, in order to put pressure on their victims and coerce them into paying a ransom.[37] In the case of Swissport, the company's business continuity management and backups helped to limit the impact on other companies.[38]

In the education sector, the University of Neuchâtel was the target of a ransomware attack. This did at least result in the early implementation of new security measures which were already planned by the canton in light of previous cyberattacks on the communes of Rolle and Montreux.[39] These measures comprise, in particular, repeated penetration tests and improved early detection.[40]

The examples above provide only a snapshot of the ransomware attacks that have taken place in Switzerland so far this year. Various media sources provide a more comprehensive list of ransomware attacks in Switzerland and abroad in 2022.[41]

---

32 2021 Trends Show Increased Globalized Threat of Ransomware (cisa.gov)

33 Ransomware (ncsc.admin.ch); What Is Ransomware? (trellix.com)

34 Hackerangriff auf Schweizer Spitalverband (inside-it.ch); Hackerangriff auf Swissport sorgt für Verspätungen im Flugbetrieb (computerworld.ch); Cyberangriff auf Luzerner ÖV bleibt ohne grössere Folgen (inside-it.ch); Cyberattaque contre Emil Frey: des données publiées sur le darkweb (ictjournal.ch); Ransomware-Attacke: «BlackByte» hackt Schweizer Logistikkonzern (watson.ch); Le pire est survenu: les données volées à l'Université de Neuchâtel ont été publiées (letemps.ch)

35 Hacker veröffentlichen erneut sensible Schweizer Gesundheitsdaten (inside-it.ch)

36 Des hackers diffusent les données médicales de Neuchâtelois (watson.ch)

37 The future of cyber security: Ransomware groups aim for maximum disruption (darktrace.com)

38 BlackCat ransomware gang claims responsibility for Swissport attack (computerweekly.com)

39 Neuchâtel a amélioré sa cybersécurité (rtn.ch)

40 Cyberattaque: le canton a pris des mesures (swissinfo.ch)

41 The terrifying list of cyber attacks worldwide (konbriefing.com);
Hacker schlagen in der Schweiz zu: Die unfassbar lange Opfer-Liste (watson.ch)

5.2.2.2 Incidents abroad

Attacks against governments and authorities

Since April 2022, a number of government authorities in Latin America have been victims of ransomware attacks which probably involved Russian-speaking perpetrators.[42] Countries such as Costa Rica, Peru, Mexico, Ecuador, Brazil and Argentina were among the states condemning Russia's invasion of Ukraine at the United Nations General Assembly. The attacks even caused Costa Rica to declare a national state of emergency. These attacks on South American governments involved ransomware groups such as Conti, ALPHV/BlackCat, LockBit and BlackByte. On 24 May, the IT systems of the Austrian region of Kärnten were subject to a ransomware attack by the BlackCat group; it led to some disruption of public services.[43]

Attacks on energy infrastructures

In Europe at the end of January 2022, several oil terminals in Belgium (Antwerp), the Netherlands (Amsterdam, Rotterdam) and Germany (Oiltanking GmbH) were hit by IT problems.[44] Cyberspecialists in those countries stated that they had no reason to assume that these attacks were connected.[45] Across the world, a total of roughly ten oil terminals reported their operations being disrupted.[46] The Russian ransomware groups BlackCat and Conti were associated with these incidents.[47]

5.2.2.3 The most active protagonists in brief

Conti and its successors

The successful Russian group Conti[48] ended its activities in May 2022.[49] Having proclaimed its support for Russia shortly after the invasion of Ukraine, the group hit the headlines in the spring,[50] especially when an insider leaked internal chats between members that revealed the group's modus operandi.[51] The "Conti Leaks"[52] incident and political differences probably led to the group splitting up. Various former members then organised their own smaller groups concentrating on the individual stages of a ransomware attack, such as network access or data theft.[53] There are, for example, certain similarities between Conti's tactics, techniques and

---

42 Latin American Governments Targeted By Ransomware (recordedfuture.com)
43 Hackerangriff auf Land Kärnten: "Black Cat" will fünf Millionen Dollar in Bitcoin (derstandard.at)
44 Des cyberattaques signalées contre des sites portuaires en Allemagne, en Belgique et aux Pays-Bas (lemonde.fr)
45 String of cyberattacks on European oil and chemical sectors likely not coordinated, officials say (therecord.media)
46 Oil terminals in Europe's biggest ports hit by a cyberattack (securityaffairs.co)
47 BlackCat ransomware implicated in attack on German oil companies (zdnet.com)
48 The Conti Enterprise: ransomware gang that published data belonging to 850 companies (group-ib.com); The hateful eight: Kaspersky's guide to modern ransomware groups' TTPs (securelist.com)
49 Conti ransomware finally shuts down data leak, negotiation sites (bleepingcomputer.com); Ransomware-Gang Conti schließt Leak- und Verhandlungsplattform (heise.de)
50 Conti ransomware gang backs Russia, threatens US (techtarget.com)
51 Inside Conti leaks: The Panama Papers of ransomware (therecord.media)
52 Conti-nuation: methods and techniques observed in operations post the leaks (nccgroup.com)
53 Conti ransomware shuts down operation, rebrands into smaller units (bleepingcomputer.com); Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members (spiceworks.com)

procedures and those of the new groups Black Basta[54] and BlackByte[55]. Black Basta came under the spotlight back in April when, within a matter of weeks, it infected at least a dozen companies across the world.[56] It shares characteristics with Conti in terms of data leak blogs, payment pages, recovery portals, communication with victims and negotiation methods.[57] BlackByte's ransomware has functionalities and features very similar to those of Conti.[58]

A new arrival: BlackCat

BlackCat, also known as ALPHV, whose operator group of the same name is made up of former members of the notorious BlackMatter/DarkSide organisation[59], first made an appearance in November 2021. This ransomware is extremely adaptable and offers various encryption methods and options, allowing attacks on a large number of companies (especially big ones).[60] A particular feature of the business model used is the fact that, in the first stage of the extortion, the victim's name is not immediately published; instead, only a description of the affected organisation is posted on the data leak site. Alternatively, the perpetrators set up a hidden website, whose address is sent only to the victim as verification. In this way, the perpetrators give their victims the opportunity to negotiate the ransom discreetly while keeping up the pressure with the threat to publish the data.[61] If the group ultimately decides to publish the data, it uses a regular website rather than one on the darknet. This enables it to reach a wide audience. This means that even less technically well-versed users (such as employees or customers) can check whether their data has been compromised, and can even download all the data and documents that were stolen from the company.[62]

Comeback by REvil and Cl0p

Early 2022 saw the emergence of new ransomware groups, and the return of others.

At the end of April, the notorious ransomware organisation REvil returned with a new infrastructure and refined ransomware.[63] The REvil ransomware group had shut down their activities in October 2021. In January 2022, a coordinated police operation between the United States and Russia led to the arrest of REvil members in Russia.[64] According to Russian reports, communication between the two countries ceased following the Russian military action against Ukraine, and the US government had not passed on sufficient information to enable charges to be brought.[65]

---

54 Shining the Light on Black Basta (nccgroup.com)
55 Threat Spotlight: The BlackByte ransomware group is striking users all over the globe (talosintelligence.com)
56 New Black Basta ransomware springs into action with a dozen breaches (bleepingcomputer.com)
57 New Black Basta Ransomware Possibly Linked to Conti Group (securityweek.com)
58 Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members (spiceworks.com)
59 Aggressive BlackCat Ransomware on the Rise (darkreading.com)
60 Threat Assessment: BlackCat Ransomware (paloaltonetworks.com)
61 Ransomware gangs now give victims time to save their reputation (bleepingcomputer.com)
62 Ransomware gang publishes stolen victim data on the public Internet (helpnetsecurity.com)
63 REvil ransomware returns: New malware sample confirms gang is back (bleepingcomputer.com)
64 Russia takes down REvil hacking group at U.S. request - FSB (reuters.com)
65 REvil prosecutions reach a 'dead end,' Russian media reports (cyberscoop.com)

Likewise, after a few months of apparent inactivity, the Cl0p group resurfaced in April. Researchers discovered the ransomware group's return after it added 21 new victims to its data leaks site in a single month.[66]

LockBit

The LockBit ransomware as a service (RaaS)[67] group has already been behind many incidents this year.[68] Its data leaks site names the victims and a countdown shows when the stolen data will be published. It turns out, however, that LockBit's announcements have to be taken with a pinch of salt. For example, it is not the French Justice Ministry that has been hacked, but a firm of lawyers in Caen.[69] Likewise, the claim to have obtained data from the US security service provider Mandiant turned out to be untrue.[70] It seems that sometimes the group's main objective is to attract attention. However, the potential impact of this ransomware group should not be underestimated, given that there were around 100 victims in Europe within six months.[71]

The ransomware used is regularly updated, in the same way as normal software. Following the appearance of version 2.0 in June 2021,[72] we are now already on version 3.0.[73]

Conclusions, outlook and recommendations:

Ransomware attacks are likely to grow further this year and to focus increasingly on critical infrastructures. Already in 2021, the US Cybersecurity and Infrastructure Security Agency (CISA) had noted an increase in sophisticated attacks on critical infrastructures with serious consequences.[74] Ransomware strategies and techniques were indeed refined in 2021, which, in addition to technological advances, is reflected in the growth of ransomware threats for all types of organisations worldwide.[75]

Although the outbreak of war in Ukraine has led to a reorganisation of the cybercrime ecosystem, ransomware perpetrators are proving resilient. Groups split up, reform, change names or replace operatives as needed, for example if the pressure from prosecution authorities gets too high or if, in the context of the war in Ukraine, differences of opinion hamper cooperation within the group.

---

66 Clop ransomware gang is back, hits 21 victims in a single month (bleepingcomputer.com)

67 Ransomware as a service (RaaS) is a business model between operators of ransomware and their partners, in which the partners pay for attacks to be launched using the ransomware developed by the operators. This can be regarded as a variation of the software as a service (SaaS) business model; Ransomware as a Service (RaaS) Explained (crowdstrike.com)

68 LockBit overtakes Conti as most active ransomware group so far in 2022 (scmagazine.com)

69 Ministère de la Justice : Le groupe Lockbit publie des données, mais pas les bonnes (zdnet.fr)

70 Mandiant: "No evidence" we were hacked by LockBit ransomware (bleepingcomputer.com)

71 Ransomware LockBit : une centaine de victimes par mois au premier semestre (lemagit.fr)

72 LockBit 2.0: How This RaaS Operates and How to Protect Against It (paloaltonetworks.com)

73 LockBit 3.0: Significantly Improved Ransomware Helps the Gang Stay on Top (darkreading.com)

74 2021 Trends Show Increased Globalized Threat of Ransomware (cisa.gov)

75 Ransomware: Over half of attacks are targeting these three industries (zdnet.com)

In addition to cybersecurity measures that protect systems from malware infections generally, and hence also from ransomware, there are also measures that could be used behind the first line of defence. Researchers have discovered "vulnerabilities" in some ransomware which could be exploited in order to at least prevent the final encryption of data.[76]

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?.

Furthermore, the US Cybersecurity and Infrastructure Security Agency (CISA) has published a document which is designed to show companies how to prevent data leaks from ransomware attacks and respond to them.[77]

5.2.3 Mobile malware

After the last big wave in autumn 2021, FluBot malware began circulating in Switzerland again on 18 March 2022. Text messages were used to trick the victims into installing malware on their smartphones. This latest wave was on an international scale[78] and targeted Android devices. In Switzerland, the text messages mainly contained fake parcel delivery notifications, while at international level there were also text messages asking "Is that you in the video?" or fake demands to update browsers or operating systems. The NCSC reported on this in weekly review 12.[79]

FluBot specialised, among other things, in stealing text messages from mobile phones. The aim here was to find one-time passwords among the stolen text messages. In addition, once infected, a smartphone's entire address book was sent to the attackers' control server. The smartphone then received a list of phone numbers from other hacked smartphones to which it was supposed to send the malicious text message. In the first half of 2022, the NCSC registered a total of 56 reports on FluBot.

At the beginning of May, the Dutch police succeeded in destroying FluBot's infrastructure, at which point this malware strain became inactive. The police operation followed a complex investigation involving the prosecution authorities from Australia, Belgium, Finland, Hungary, Ireland, Spain, Sweden, Switzerland, the Netherlands and the United States. International operations were coordinated by Europol's European Cybercrime Centre (EC3).[80] No FluBot activity has been detected in Switzerland since then.

---

76 Conti, REvil, LockBit ransomware bugs exploited to block encryption (bleepingcomputer.com)

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

78 New FluBot and TeaBot campaigns target Android devices worldwide (bleepingcomputer.com)

79 Week 12: FluBot malware is active again in Switzerland and various web administrators receive a threatening email from purported Ukrainian hackers (ncsc.admin.ch)

80 Takedown of SMS-based FluBot spyware infecting Android phones (europol.europa.eu)

Recommendations:

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

5.2.4 Cyclops Blink botnet – disruption of VPNFilter's successor

In May 2018, the security firm Cisco Talos published the latest findings on the VPNFilter malware[81], which typically tried to infect the routers of small and home office (SOHO) users and network-attached storage (NAS). Following a largely successful takedown of the VPNFilter infrastructure by the US Justice Department[82], the activities ascribed to the Sandworm group[83] died down.

On the eve of the Russian attack on Ukraine, British[84] and US security services published details on the probable successor botnet, Cyclops Blink, which mainly infects WatchGuard devices and Asus routers[85].

Operators of infected devices, including some in Switzerland, were informed via their internet service provider or national CERTs.[86] In the case of some of the botnet's command-and-control devices that the operators had not cleaned up, the US Justice Department obtained a court order allowing it to step in and remotely remove the malware.[87]

Thus, the western cybersecurity community was able to effectively disrupt Sandworm's attack infrastructure and prevent, or at least hamper, further potential attacks, such as those described in the focus topic (sections 3.1 and 3.2) or the section on industrial control systems (section 5.4.1).

Recommendations

The NCSC website contains recommendations on the secure use of devices for end users and operators in the Internet of Things (IoT).

81 New VPNFilter malware targets at least 500K networking devices worldwide (thalosintelligence.com)

82 Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices (justice.gov)

83 Sandworm (Threat Actor) (fraunhofer.de); see also sections 3.1 and 3.2.2

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

85 Cyclops Blink Sets Sights on Asus Routers (trendmicro.com)

86 Shadowserver Special Reports – Cyclops Blink (shadowserver.org)

87 Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) (justice.gov)

5.3 Attacks on websites and web services

As in the past, DDoS attacks affecting the availability of websites remain a persistent phenomenon in Switzerland and abroad. In the first half of 2022, ten such incidents were reported to the NCSC by various Swiss SMEs from different sectors. Such attacks can be carried out for extortion, to damage competitor companies, or out of political motivation.

According to reports from globally active security companies, although there are increasingly intense (record 1.4 Tbit/s) and complex (combination of different attack methods) attacks,[88] the vast majority of DDoS attacks continue to be carried out at relatively low speeds (below 10 Gbit/s).[89] In addition to the data transfer rate, factors such as packets per second (pps) and requests per second (rps) must also be taken into account. For example, Cloudflare registered an attack involving 26 million requests per second, which originated from a small but powerful botnet with only 5,067 devices.[90]

In the war of aggression against Ukraine, a pro-Russian and anti-NATO hacktivist group called Killnet has carried out a series of DDoS attacks since April 2022 against countries that have supported Ukraine with arms deliveries, money or sanctions. Websites of the UN, the OSCE, NATO and organisations in Ukraine, the Czech Republic, Estonia, Latvia, Lithuania, Germany, Norway, Poland, Romania, the United Kingdom, Italy and the United States were attacked, among others. These included many airports[91], numerous government agencies, banks, railway companies, energy companies and internet service providers (see also section 3.3).

Conclusion/recommendations:

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

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

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

In the context of geopolitical conflicts, destructive cybersabotage attacks are sporadically observed.[92] 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. Such attacks are time- and resource-intensive, and their effect tends to be easier to achieve using kinetic means in a conflict that has already escalated into armed violence (see focus topic section 3.2.2 on Industroyer2).

88 DDoS attacks becoming larger and more complex, finance most targeted sector (helpnetsecurity.com)

89 DDoS threats growing in sophistication, size, and frequency (helpnetsecurity.com)

90 Cloudflare mitigates 26 million request per second DDoS attack (cloudflare.com)

91 Russia-Ukraine: malicious cyber activity targeting aviation entities (ospreyflightsolutions.com)

92 For more information on Stuxnet, see semi-annual report 2010/2 (ncsc.admin.ch), sections 4.1 and 5.1 and on Triton/Trisis in semi-annual report 2017/2 (ncsc.admin.ch), section 5.3.2

5.4.1 Pipedream/Incontroller: OT attack tools

On the day following the announcement of the Industroyer2 attacks (see section 3.2.2), several US authorities published a joint warning detailing another collection of modular attack tools[93] that could be used for cybersabotage purposes against devices in the energy supply and related sectors. This was a pre-emptive measure taken before any operational use of one of the malware variants mentioned had been observed.

The publication of the cybersabotage tools discovered by the US government was prepared in cooperation with two American cybersecurity companies that specialise in industrial systems, which named the malware collection "Pipedream"[94] or "Incontroller"[95], respectively. The pre-emptive disclosure was the latest in a series of announcements concerning predominantly Russian attack infrastructure. In addition to compromising the deployment potential of the means of attack that was uncovered, the Biden Administration also used the exposure of potential attackers' capabilities to emphasise to domestic critical infrastructure operators the urgency of implementing recommended protective measures in a timely manner under the slogan "Shields Up".[96]

5.4.2 ICEFALL: 56 OT vulnerabilities

The call for multi-layered defences stems not only from new insights into the capabilities of attackers[97] of industrial control systems, but also from the way the technology used is designed, which is sometimes insufficiently secure. As a result, the cybersecurity company Forescout published a collection of 56 vulnerabilities in known OT products under the name ICEFALL.[98] The CISA ICS-CERT also continuously publishes new security recommendations[99] from the various manufacturers. To keep track of these, the Common Security Advisory Framework (CSAF) can be used, which was co-developed by the armasuisse Cyber Defense Campus together with the experts from the German BSI.[100]

Conclusion/recommendations:

The newly uncovered attack tools and vulnerabilities demonstrate the need to invest in secure access to industrial control systems and to monitor operations and manipulations so that timely responses can be made if improper changes are suspected.

On its website, the NCSC recommends Measures to protect industrial control systems (ICSs)

93 APT Cyber Tools Targeting ICS/SCADA Devices (cisa.gov)
94 CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS) (dragos.com)
95 INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple ICS (mandiant.com)
96 Shields Up (cisa.gov)
97 Three new ICS threat groups discovered, one primed to disrupt energy targets (scmagazine.com)
98 OT:ICEFALL: 56 Vulnerabilities Caused by Insecure-by-Design Practices in OT (forescout.com)
99 ICS-CERT Advisories (cisa.gov)
100 Successful cooperation between the Cyber-Defence Campus and the German Federal Office for Information Security (BSI) (admin.ch)

5.5 Vulnerabilities

5.5.1 Log4Shell

The Log4Shell vulnerability, which was already mentioned in the NCSC semi-annual report 2021/2, is still current. In the first half of 2022, this vulnerability was used in particular to attack and compromise VMware servers on which the patches had not been installed.[101]

Due to the nature of this vulnerability, it can be embedded in an application or system that does not fall under the direct responsibility of an organisation's security team, thus making it difficult to detect and remedy.

In a recent report, the US Department of Homeland Security's Cyber Safety Review Board stated that: "Log4j is an 'endemic vulnerability' and that vulnerable instances of Log4j will remain in systems for many years to come, perhaps a decade or longer. Significant risk remains." [102]

Conclusion/recommendations:

Considering this type of vulnerability can enter an organisation's infrastructure through software provided by third parties, it is recommended that organisations develop the capacity to maintain an accurate inventory of IT assets and applications, prioritise the implementation of software updates, and invest in the ability to detect vulnerable systems. The Cyber Safety Review Board report also provides more detailed recommendations on Log4Shell.

5.5.2 Follina

On 31 May 2022, Microsoft assigned vulnerability identifier CVE-2022-30190 to a vulnerability called Follina. This vulnerability allows remote code execution via msdt (a Microsoft support tool) when a document is opened or previewed in Office suite applications, even when macros are disabled. Microsoft was notified of this vulnerability in March 2021. However, the CVE identifier was not assigned until the vulnerability had already been exploited.

Security researchers published several defence and detection techniques online, but the vulnerability was only remedied during Patch Tuesday in June 2022.

A chronology detailing the sequence of events documents the exploitation of this vulnerability before it became public knowledge, from detection to implementation of defensive measures.[103]

---

101 Log4Shell Vulnerability Targeted in VMware Servers to Exfiltrate Data (threatpost.com)

102 CSRB Report on Log4j - Public Report - July 11 2022_508 Compliant (cisa.gov)

103 Follina — a Microsoft Office code execution vulnerability (doublepulsar.com)

Conclusion/recommendations:

In the case of Follina, the details required for an exploit were published before an official patch was available and the vulnerability had already been exploited by various actors. In such cases, it is important for companies and organisations to constantly keep up to date, analyse the latest recommendations and, if necessary, implement risk-mitigating measures until an official patch is available and can be installed.

It is still recommended to follow best practice with regard to computer security. Training employees to recognise malicious emails and not to download or open attachments can help thwart these types of attacks.[104]

5.5.3 Confluence

On 2 June 2022, Atlassian published a security bulletin on a critical vulnerability in their Confluence wiki software (CVE-2022-26134).[105] A successful exploit allowed remote execution of arbitrary code on Confluence servers. At the time of the bulletin's release, no patch was yet available, even though the details enabling an exploit were publicly available and the vulnerability was being actively exploited. It was therefore strongly recommended to restrict access to Confluence instances from the internet or disable them until the patch was released.

The patch was released the following day. In Switzerland, the vulnerability was exploited in at least one ransomware case.

Conclusion/recommendations:

As with Follina, the CVE-2022-26134 vulnerability was actively exploited before an official patch was available. It is therefore important to react quickly and follow recommendations – which 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, 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 does not replace the installation of patches as soon as they become available.

104 Handling emails securely (ncsc.admin.ch)

105 Confluence Security Advisory 2022-06-02 | Confluence Data Center and Server 7.18 (atlassian.com)

5.6 Data leaks

5.6.1 Data protection requires data security

A data leak is an unpleasant situation for all concerned. No one wants to disclose personal or protectable content without being asked, or to have to tell someone that this has happened to their data. However, poorly protected or poorly maintained systems, human error and criminal attacks mean that data leaks happen time and again. It is also possible that in the case of a ransomware attack, the perpetrator may extract data from a system as an additional means of extortion. In such cases, the victims can also be threatened directly by the criminals. This is then called triple extortion: if the hacked company is unwilling to pay anything either for decryption or to prevent publication of the data, the extortionists may contact the individuals concerned directly, either with the threat of publication or in the form of an individual and very personal social engineering attack. This poses a risk, especially in the case of particularly sensitive personal data such as patient records. On its website, the NCSC provides a Guide to data leaks for companies.

Comment:

In Switzerland, there is no legal obligation to report data security breaches or data leaks yet. However, in the future, the operators of critical infrastructures will have to report cyberattacks to the authorities, and the new Data Protection Act also includes a duty to report or provide information.

5.6.2 Lapsus$

The cybercriminal group Lapsus$ attracted attention in late 2021 with numerous attacks in South America and Portugal. In one of these attacks, more than 50TB of data from the Brazilian Ministry of Health was stolen and then deleted from the authority's systems.[106] Another attack hit Impresa, Portugal's largest media conglomerate, leaving its websites defaced with a ransom note revealing that the criminal group had gained access to the company's cloud.[107] In both cases, Lapsus$ blackmailed its victims and demanded money in exchange for the return of the data or its non-disclosure. In the first months of 2022, the group gained notoriety after successfully carrying out attacks on large international technology companies such as NVIDIA[108], Samsung[109], Vodafone[110], Ubisoft[111], Microsoft[112] and Okta[113]. These attacks led to confidential data of the affected companies being disclosed. As a result, Lapsus$ reportedly suffered a counter-attack from NVIDIA and then complained that data belonging to the group

106 Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes (zdnet.com)
107 Lapsus$ ransomware gang hits SIC, Portugal's largest TV channel (therecord.media)
108 NVIDIA confirms data was stolen in recent cyberattack (bleepingcomputer.com)
109 Hackers leak 190GB of alleged Samsung data, source code (bleepingcomputer.com)
110 Vodafone Investigating Source Code Theft Claims (securityweek.com)
111 Ubisoft Cyber Security Incident Update (ubisoft.com)
112 DEV-0537 criminal actor targeting organizations for data exfiltration and destruction (microsoft.com)
113 Updated Okta Statement on LAPSUS$ (okta.com)

had been encrypted.[114] In late March 2022, seven people aged between 16 and 21, potential members of the group, were arrested in the UK. Two of them were charged in early April 2022. The group's activities subsequently subsided and no further reports were received up to the end of the first half of 2022. When it first began its activities, Lapsus$ was believed to be a group that operated with ransomware. However, the group only exfiltrated data, sometimes deleting it, and then blackmailed its victims by threatening to publish it. To gain access to their victims' systems, Lapsus$ often used social engineering techniques to obtain login credentials.[115] Some of their attacks may also have been facilitated by employees of the target companies who collaborated with them (insiders, internal threat). The group had posted an announcement to this effect on their Telegram channel, offering to pay large sums to employees at companies in sectors of interest to them in exchange for remote VPN access.[116] This Telegram channel was also the group's only public platform on which its members reported on their activities, partly in real time; it had more than 60,000 followers. In sum, although Lapsus$ did not exist for very long, it managed to successfully attack numerous renowned companies and exfiltrate data in a short period of time using modest means and unsophisticated techniques.

114 vx-underground on Twitter (twitter.com)

115 LAPSUS$: Recent techniques, tactics and procedures (nccgroup.com)

116 Lapsus$ Ransomware Group Announced Recruitment of Insiders (securityaffairs.co)