2 November 2023 | National Cyber Security Centre NCSC

Semi-annual report 2023/I (January–June)

Information assurance

Situation in Switzerland and internationally

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
National Cyber Security Centre NCSC

1 Overview/contents

1 Overview/contents 2

Management summary 3

Editorial 4

2 Focus: hacktivism 5

2.1 DDoS: disruption to the availability of websites and online services 5

2.1.1 How to deny Denial of Service (Swisscom) 7

2.1.2 Preparation and practice pay off (Swiss Post) 9

2.2 Defacement 10

2.3 Hack and leak 10

2.4 Sabotage 11

3 Reports from businesses and the public 13

3.1 Reports received on cyberincidents – overview 13

3.2 Most frequently reported: fraud 15

3.2.1 Threatening emails allegedly from authorities remain at high levels 15

3.2.2 Other fraud phenomena 16

3.3 Phishing reports 17

3.4 Malware and hacking reports 18

3.4.1 Ransomware incidents: Differing trends for companies and private individuals 18

3.4.2 Hacking reports 19

3.5 Miscellaneous reports 19

3.5.1 Search engine optimisation with abandoned domains and hacked websites 19

4 Situation 20

4.1 Initial access 20

4.1.1 Username/password 20

4.1.2 Malware (Trojans) 21

4.1.3 Exploitation of vulnerabilities 22

4.2 Ransomware 22

4.2.1 Examples of incidents in Switzerland 22

4.2.2 Situation abroad 24

4.2.3 Overview of the most active protagonists and most commonly used infection vectors24

4.3 Industrial control systems (ICS) and operational technology (OT) 25

4.4 Vulnerabilities 26

4.4.1 "MOVEit" (CVE-2023-34362 | CVE-2023-35036 | CVE-2023-35708) 26

4.4.2 Fortinet (CVE-2022-39952 | CVE-2021-42756) 28

4.5 Data leaks and data management 29

4.5.1 From encryption attacks to pure data extortion 29

4.5.2 Data leaks from cyberattacks on and through the supply chain 31

4.6 Website hacking 32

4.7 Update on Ukraine 33

Management summary

Focus: hacktivism

Politically relevant events can lead to illegal activities in cyberspace, also known as hacktivism. This involves hacktivists aiming to attract attention from the media and, in turn, from the public. In June 2023, the Federal Administration twice fell victim to hacktivism. The first DDoS attack followed a decision by the Council of States relating to the War Material Act. The aim was to overload the Parliamentary Services website and make it unavailable to users. The second attack was triggered by the announcement that the Ukrainian president, Volodymyr Zelensky, would be giving an online speech to the Federal Assembly. In addition to several websites of federal offices and Parliament, the websites of major companies in Switzerland, some airports, numerous towns, cities and cantons, as well as the Swiss Bankers Association were also affected by this DDoS attack. The focus of the semi-annual report is therefore on hacktivists' methods and motivations. In addition, two guest articles show how affected large companies reacted to the DDoS attack. At the same time as this semi-annual report, the NCSC publishes a detailed analysis report on these DDoS attacks.

Increase in reports in the first half of 2023

In the first half of 2023, the NCSC received 19,048 reports of cyberincidents. This corresponds to an increase of around 2,000 reports compared to the first half of 2022 (16,951 reports). In the first half of 2023, the most frequent reports to the NCSC again concerned various forms of fraud. Threatening emails, so-called fake extortion, continue to account for the largest share (around 30%). In most cases, the victim of these threatening emails is accused of having allegedly committed a crime. These threats are supposedly sent in the name of domestic and foreign authorities, and over the last six months, the Swiss NCSC's name has also been misused more and more frequently.

Significant increase in phishing reports

The second most frequently reported incident is phishing, the number of reports of which has increased by over 40% and accounted for one fifth of the reports received in the last half year. The main reason for this increase is an extensive phishing campaign against SwissPass holders, which lasted almost the entire first half of 2023. In general, it can be seen that phishing attempts are becoming more elaborate and attackers are trying out new methods of disguising phishing links.

Ransomware incidents: Differing trends for companies and private individuals

In the first half of 2023, the number of ransomware reports (64) remained almost the same as in the previous half-year period (76). While reports from private individuals decreased significantly (from 27 to 8 cases), the number of ransomware reports from businesses increased (from 49 to 56 cases). In addition to short-term operational disruptions as a result of data encryption, the publication of leaked business data causes consequential damage that is hard to quantify.

Editorial

The various distributed denial of service (DDoS) attacks in June on Swiss websites, such as those of Parliamentary Services, various organisations and federal offices, made the headlines. Generally speaking, DDoS attacks are nothing out of the ordinary, as they occur on a daily basis. So why did these attacks in particular cause such a stir?

The political context was crucial. The attackers were pro-Russian hacktivists who wanted to use their attacks to make their political views known, and create the impression that a large-scale Russian attack in cyberspace has to be expected at any time. Media and cyberexperts that embrace this narrative help the hacktivists – who, as far as we know today, are acting on their own initiative – to achieve their objectives.

In Switzerland, too, the hacktivists have succeeded in spreading at least short-term uncertainty, especially among non-specialist organisations, politicians and citizens. Therefore, it is very important to analyse the attacks with a clear head and find answers to the following questions: How great was the damage really? Is greater protection against DDoS attacks economically viable? How can we report on the attacks without providing a platform for the attackers? And how can we best put such attacks into context for ordinary people?

The NCSC has also prepared a detailed analysis report on the DDoS attacks, which is available to interested parties as a supplement to this semi-annual report.

However, in terms of impact, ransomware attacks on companies and authorities remain much more serious than DDoS attacks. The best known is probably the attack on the company Xplain, which supplies both private companies and the Confederation and cantons. As an administrative investigation is currently underway, we will not go into detail about the incident in this report. This will be included in a future report as soon as all investigations have been completed. However, one thing I would like to say at this stage is that from the very beginning we decided to communicate as transparently as possible – without endangering organisations or people whose data was lost. Communicating transparently automatically exposes you to criticism. Equally, legitimate questions are asked and we want to answer these after all investigations have been completed. Such analyses take time, and jumping to conclusions would not be productive.

This report also contains an analysis of the threat situation and an overview of the incidents in cyberspace. Once again, the incidents most reported to the NCSC were various types of fraud. As such, it is still necessary to be vigilant, especially when asked to disclose personal information such as credit card or login details. The report also provides an update on cyberthreats related to the war in Ukraine.

Take the opportunity to give us feedback on this report.

We hope you enjoy reading it.

Florian Schütz, Federal Cybersecurity Delegate

2 Focus: hacktivism

There are many players seeking to attack systems of all kinds using a range of methods. These threat actors cover a broad spectrum depending on their capabilities (i.e. the complexity of their approach) and motives. Since the start of the war in Ukraine, attacks by hacktivist groups have become increasingly common. Two factors characterise such actors: firstly, they are usually not professionals, and secondly, their activities are ideologically motivated (e.g. based on social, political or religious reasons) – as opposed to criminals, who act primarily out of financial interest. Consequently, relatively superficial attacks (such as the temporary unavailability of a website) may be enough to satisfy such hacktivists, provided they are reported in the media, thereby highlighting the attackers' cause. Probably the best-known hacktivist group is Anonymous. For over 15 years, Anonymous hackers around the world have been campaigning for causes such as freedom of speech and the independence of the internet, and against authorities and global corporations.

Against the backdrop of the Ukraine war, countless hacktivist groups have formed and/or expanded since February 2022, siding with one of the two warring parties and regularly launching attacks on facilities or institutions they deem harmful to their camp. Thus, pro-Russian hacktivist groups primarily target institutions of countries that offer support to Ukraine or impose sanctions on Russia.[1] There has been less activity and retaliation from pro-Ukrainian hacktivist groups, not least because they are fewer in number than the pro-Russian groups.[2] In the vast majority of cases, there is no formal affiliation between hacktivists and government agencies, but they can be useful to a government by serving as a proxy with which it can disclaim any ties, and particularly as a propaganda mouthpiece. Such connections have been highlighted in various reports by Western IT security companies.[3] A special case is the IT Army of Ukraine, which, unlike the pro-Russian hacktivist groups, was formed openly and on the initiative of the Ukrainian government. That government is now drafting a law to legitimise the status of the IT Army of Ukraine and officially deploy its members as reservists.[4]

2.1 DDoS: disruption to the availability of websites and online services

In distributed denial of service (DDoS) attacks, a large number of computers in many locations are used to flood an online service with so many requests that it is no longer available to regular users. However, there is no unauthorised extraction of data and no data or systems are destroyed. In the analogue world, a DDoS attack is comparable to a crowd of people attending a press conference, for example, and shouting loudly over each other so as to drown out the journalists' legitimate questions and prevent them from receiving an answer.

Usually, therefore, the only consequence of a successful DDoS attack is that a website – the "information desk" of the affected organisation – is temporarily unavailable. However, if significant parts of its business are carried out via the website, as in the case of online shops

[1] See sections 2.1 and 4.7.

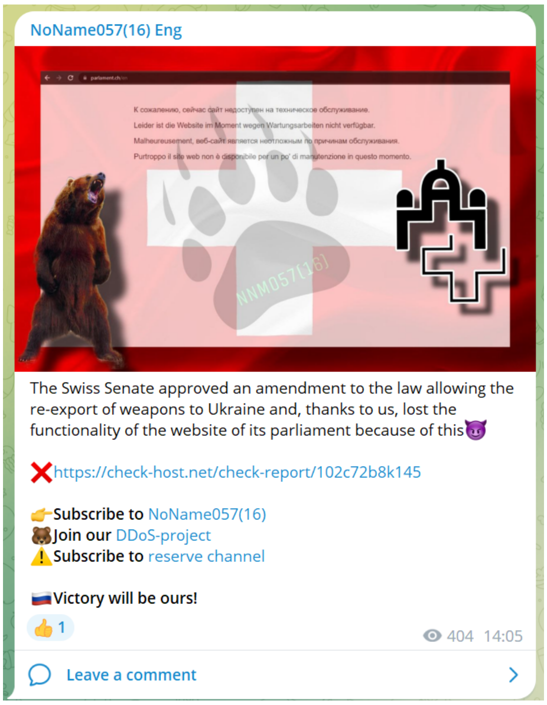
[2] Russia-Ukraine War – Cybertracker May 03 (cyberknow.medium.com)

[3] A year of Russian hybrid warfare in Ukraine (microsoft.com);
GRU: Rise of the (Telegram) MinIOns (mandiant.com)

[4] Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army (newsweek.com)

for example, even a short outage can wreak considerable financial damage. Also, in the case of time-critical communication or information needs, processes can be interrupted as a result.

The aim of hacktivists is to attract attention and, in some cases, to create uncertainty and undermine trust in the organisations operating the websites. Organisations of all kinds are prepared for DDoS attacks and can restore access to their online resources within a very short time. However, activating defensive measures, such as filtering out attack traffic or increasing capacities, takes time and incurs costs. Attackers use this time to prove that a website was down. By posting screenshots, they boast of their exploits on social media and create the impression, even with very brief outages, that they have successfully "hacked" a company or "taken down" or even "killed" a website.



NoName057(16) Eng

К сожалению, сейчас сайт недоступен на техническое обслуживание.
Leider ist die Website im Moment wegen Wartungsarbeiten nicht verfügbar.
Malheureusement, веб-сайт является неотложным по причинам обслуживания.
Purtroppo il site web non è disponibile per un po' di manutenzione in questo momento.

The Swiss Senate approved an amendment to the law allowing the re-export of weapons to Ukraine and, thanks to us, lost the functionality of the website of its parliament because of this😈

❌https://check-host.net/check-report/102c72b8k145

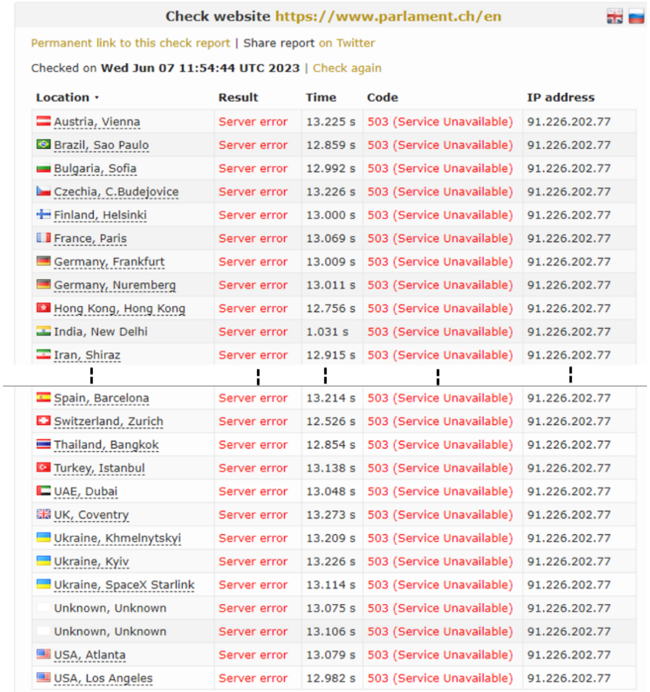
👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!

👍 1 👁 404 14:05

Leave a comment

Fig. 1: Hacktivist message claiming responsibility



Check website https://www.parlament.ch/en

Permanent link to this check report | Share report on Twitter

Checked on **Wed Jun 07 11:54:44 UTC 2023** | Check again

Location ▾	Result	Time	Code	IP address
Austria, Vienna	Server error	13.225 s	503 (Service Unavailable)	91.226.202.77
Brazil, Sao Paulo	Server error	12.859 s	503 (Service Unavailable)	91.226.202.77
Bulgaria, Sofia	Server error	12.992 s	503 (Service Unavailable)	91.226.202.77
Czechia, C.Budejovice	Server error	13.226 s	503 (Service Unavailable)	91.226.202.77
Finland, Helsinki	Server error	13.000 s	503 (Service Unavailable)	91.226.202.77
France, Paris	Server error	13.069 s	503 (Service Unavailable)	91.226.202.77
Germany, Frankfurt	Server error	13.009 s	503 (Service Unavailable)	91.226.202.77
Germany, Nuremberg	Server error	13.011 s	503 (Service Unavailable)	91.226.202.77
Hong Kong, Hong Kong	Server error	12.756 s	503 (Service Unavailable)	91.226.202.77
India, New Delhi	Server error	1.031 s	503 (Service Unavailable)	91.226.202.77
Iran, Shiraz	Server error	12.915 s	503 (Service Unavailable)	91.226.202.77
⋮	⋮	⋮	⋮	⋮
Spain, Barcelona	Server error	13.214 s	503 (Service Unavailable)	91.226.202.77
Switzerland, Zurich	Server error	12.526 s	503 (Service Unavailable)	91.226.202.77
Thailand, Bangkok	Server error	12.854 s	503 (Service Unavailable)	91.226.202.77
Turkey, Istanbul	Server error	13.138 s	503 (Service Unavailable)	91.226.202.77
UAE, Dubai	Server error	13.048 s	503 (Service Unavailable)	91.226.202.77
UK, Coventry	Server error	13.273 s	503 (Service Unavailable)	91.226.202.77
Ukraine, Khmelnytskyi	Server error	13.209 s	503 (Service Unavailable)	91.226.202.77
Ukraine, Kyiv	Server error	13.226 s	503 (Service Unavailable)	91.226.202.77
Ukraine, SpaceX Starlink	Server error	13.114 s	503 (Service Unavailable)	91.226.202.77
Unknown, Unknown	Server error	13.075 s	503 (Service Unavailable)	91.226.202.77
Unknown, Unknown	Server error	13.106 s	503 (Service Unavailable)	91.226.202.77
USA, Atlanta	Server error	13.079 s	503 (Service Unavailable)	91.226.202.77
USA, Los Angeles	Server error	12.982 s	503 (Service Unavailable)	91.226.202.77

Fig. 2: Screenshot of availability check

The pro-Russian group NoName057(16) perpetrated such a DDoS attack on the website of the Swiss Parliament on 7 June 2023. In its message claiming responsibility, posted on the instant messaging service Telegram, it cited as its reason the (interim) decision of the Council of States regarding the revision of the War Materiel Act. Immediately after the attack was launched and before countermeasures were taken, the website was indeed overwhelmed by an extraordinary number of requests, rendering it either unavailable to regular users or extremely slow to respond. At that point, the attackers had a service checking the global availability of websites create a report to prove the success of the attack. However, this was only a snapshot that said nothing about the duration of the impairment. Despite the ongoing attack, the website was usable again after a short time thanks to the countermeasures taken. In the aforementioned scenario, this would be like a short video clip of the press conference showing the uninvited guests shouting crazily but ending before the troublemakers are ejected from the hall by security guards and then prevented from re-entering.

The following week, the pro-Russian group also targeted airports, Swiss Federal Railways (SBB), Swiss Post, the Swiss Bankers Association and numerous cities and cantons, as well as several websites of federal offices, among others.[5] One of the main reasons why Switzerland became a target for hacktivists was the Ukrainian president's appearance before the Federal Assembly. However, the video broadcast of the address was not interrupted. As with other countries hit by NoName057(16), the attacks stopped after a week and the attackers turned to other targets.[6] The NCSC has published a detailed analysis report on these DDoS attacks.

In addition to NoName057(16), KillNet, another pro-Russian hacktivist group,[7] and the group Anonymous Sudan,[8] which appears to be associated with it, made headlines in the period under review with DDoS attacks against targets primarily in Europe and North America.[9] There were also religiously motivated DDoS attacks reflecting the perpetrators' anger at supposedly blasphemous activities. These attacks targeted websites of countries and organisations perceived as enemies of their religion.[10]

Such events are not new: Switzerland already experienced a politically motivated DDoS attack back in December 2010, when the PostFinance website was impaired for hours by presumed WikiLeaks supporters.[11]

Recommendations:

On the NCSC website, you will find various preventive and defence measures against DDoS attacks: Attack on availability (DDoS) (ncsc.admin.ch)

For critical systems, it may make sense to subscribe to a commercial DDoS mitigation or protection service. Many internet service providers offer such services.

2.1.1 How to deny Denial of Service (Swisscom)

By Stefan Kuch, CSIRT Product Owner, Swisscom

On 7 June 2023, the Swiss Parliament fell victim to a DDoS attack. From this point on, Swisscom's cyberdefence team was in close contact with the network operations teams responsible for DDoS protection as well as the NCSC. Preventive protection measures were taken as an initial immediate response.

The following week, pro-Russian hacktivist group NoName057(16) attacked a series of additional targets in Switzerland. These included Swisscom customers as well as Swisscom

[5] Das Gespenst DDoS-Attacke geht um (inside-it.ch)

[6] Following NoName057(16) DDoSia Project's Targets (sekoia.io);
DDoSia Project: How NoName057(16) is trying to improve the efficiency of DDoS attacks (avast.io)

[7] KillNet Showcases New Capabilities While Repeating Older Tactics (mandiant.com)

[8] Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks (microsoft.com)

[9] On its platform Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org), the CyberPeace Institute provides a comprehensive list of cyberattacks carried out as part of the Ukraine conflict. The attacks can be filtered according to various criteria (e.g. "Event Type", "DDoS").

[10] Hacktivists Target Denmark in Ddos Attacks (truesec.com);
Radware Report Ranks Top 15 Most Active Political and Religious Hacktivists (radware.com);
Notable DDoS Attack Tools and Services Supporting Hacktivist Operations in 2023 (cyble.com)

[11] See semi-annual report 2010/2 (ncsc.admin.ch), section 3.2.

itself on 15 June. This report takes a closer look at one such attack on the website of one of our customers. The incident in question was a layer 7 DDoS attack, more specifically an HTTPS flood. This type of DDoS involves inundating web servers with legitimate-looking, constantly changing HTTP GET or HTTP POST requests until resources are exhausted and the web server can no longer service the requests. As a result, the web server denies its service and an outage occurs. In the case of NoName057(16), these requests come primarily from "activists" who voluntarily make their infrastructure available for DDoS attacks. Such a layer 7 DDoS attack is usually very dynamic and therefore virtually impossible to prevent entirely. However, it is important to have the technical infrastructure ready to respond quickly to such attacks.

The volume of the attack described here reached up to 150,000 packets per second (pps) – well beyond the web server's capacity. On normal days, traffic to the website ranges between 400 and 500 pps, with brief peaks of up to 1,200 pps. In the case of intensive attacks, other network components upstream of the attacked web server can also be affected.

As a countermeasure, Swisscom implemented DDoS mitigation, working with the customer to refine and continually adapt the associated rules:

- Blocking of traffic from countries where the bulk of DDoS requests originate. This is the simplest immediate measure to protect a website that is normally accessed mostly from Switzerland.
- Subsequent gradual opening and/or adjustment. If the customer specifically wishes to allow access from certain countries or IP ranges, these will be re-activated.
- Implementation of rate limiting on the upstream load balancer for connections to the attacked domain. This can permanently relieve the load on the web server.
- Permanent blocking of certain layer 7 requests on the upstream reverse proxy. This was done with the help of a blocklist created by the NCSC.

DDoS mitigation reduced the volume back to around 500 pps. This involved blocking requests from around 2,000 IP addresses. The most active IP address alone sent approximately 50 million data packets over the duration of the attack.

The 15 June attack just described was followed by another on the night of 18 to 19 June, but with a much smaller volume of 60k pps. However, because DDoS mitigation had been set up for five days as a precaution, this attack had no negative impact.

After this spate of DDoS attacks in June, anyone who continues to operate their web service without effective DDoS protection and simply hopes for the best would be advised to reconsider. Ultimately, professional precautions help to prevent or minimise possible damage in the event of an attack. Most internet providers offer DDoS protection services and can help customers prepare for and defend against an acute attack.

Thanks to effective cooperation between the various operational areas at Swisscom, such as Network and Major Incident Management, as well as the professional support and information provided by the NCSC, we were able to respond very rapidly to the attacks and protect our customers' services.

2.1.2 Preparation and training pay off (Swiss Post)

By the Swiss Post Computer Emergency Response Team (CERT-Post)

Dealing with DDoS attacks has been one of the predefined scenarios of Swiss Post's IT crisis management for many years. While the intensity of DDoS attacks is generally increasing, we are also improving our defensive capabilities, which are honed by the attacks themselves as well as regular functional checks. In addition to testing technical performance and configuration, we also conduct training to enhance the interaction of the teams involved.

Reaping the benefits during the NoName057(16) attack

After initial attacks on the Swiss Parliament website the previous week, further DDoS attacks were launched on 12 June 2023 against other Swiss organisations and companies, including two Swiss Post web applications (portal and customer login).

The always-on DDoS protection we have from our internet service provider filtered little attack traffic at the start of the attack, but issued an alert reliably at 08:09, before the first customers reported any loss of performance.

The impact of the attack was measurable. Consequently, at 08:11, Swiss Post's Security Operations Centre (SOC) activated initial geofilters for the web applications in question, as the attackers seemingly had an international botnet for carrying out the attacks. Our primary aim was to safeguard customer access from Switzerland as much as possible. Due to its characteristics (HTTPS flood, with relatively modest bandwidth and packet rate), the attack had no further impact on the network connection and other Swiss Post services.

Swiss Post's Computer Emergency Response Team (CERT-Post) took over coordination of the incident at 08:15 in consultation with the SOC and the IT crisis team. Over the subsequent hours and days, the team sent out several situation updates to keep all stakeholders informed of the latest developments. At 08:31, the SOC activated a defence level to better filter the attack traffic in the designated DDoS mitigation centre. Subsequently, the team also conducted log and threat intelligence analyses with its internal and external partners to find out as much as possible about the capabilities of the attackers and their tools. The findings were then incorporated into the defence strategy.

Learning from the first wave of attacks

The following days saw further attacks, with the PostBus Ltd portal targeted on 15 June and a second wave of attacks on the Swiss Post portal on 17 June. In these attacks, we benefited from lessons learnt in the first wave and exchanges within the Swiss CERT communities, meaning that the emergency measures implemented at the start of the first wave were no longer necessary. We continuously incorporated the insights gained into our defence strategy and were thus able to successfully fend off new waves of attacks.

While the average response time of our attacked servers increased measurably and noticeably in the first phase of the attacks on 12 June, no such impact was apparent in the following days.

Our years of regular and systematic preparation for DDoS attacks paid off, although each wave of attacks delivered new insights. In the after-action review, we included various technical and organisational points as learnings in order to further optimise our defences.

2.2 Defacement

Defacement is a change to the visual appearance of a website caused by a cyberattack. In the real world, it is comparable to spraying graffiti on a building or wall. Usually, only the homepage is defaced, with a view to spreading a political or ideological message. For example, the website of a government or organisation may be defaced because the perpetrator does not agree with its activities or goals,[12] the original content being replaced by text, an image or a logo. Defacement attacks temporarily limit the availability of a website and can damage the reputation of the website operator.

In the context of the Ukraine war, a few days after the rebellion by private military company Wagner in Russia in late June 2023, various Russian websites were defaced with the Wagner logo and a statement in support of the group.[13] The political tensions rippling through cyberspace are also affecting countries supportive of Ukraine, especially NATO member states. In May 2023, for instance, a collective named UserSec announced its intention to launch a broad defacement offensive against NATO member states' websites in cooperation with other hacktivist groups. However, the threats were not followed up by successful attacks garnering media coverage.

Recommendations:

Have your website automatically monitored so that you are alerted if it is changed. This will allow you to react quickly and reverse any unauthorised manipulations. Ask your hosting provider about the available options.

2.3 Hack and leak

Hack-and-leak operations are where hacktivists penetrate IT systems in order to obtain and then publish data stored there. In particular, they look for discrediting or incriminating material in order to post it for maximum impact on platforms such as WikiLeaks or DDoSecrets, on social media or on the dark web, in either its original or distorted form. Depending on their ideological motivation and the data hacked, hacktivists may also pass on the information to investigative journalists for detailed analysis, rather than publishing it themselves.

The case of a Swiss hacker created a media stir at the start of 2023. She was able to access a 2019 US no-fly list containing around 1.5 million entries from an airline's poorly secured server.[14] In another case, individuals associated with the hacker collective Anonymous leaked data from Russian internet provider Convex that purported to show illegal state surveillance in Russia.[15] A slightly different model is used by the hacktivists behind the MalasLocker

[12] In Switzerland, for example, various websites belonging to smaller companies were defaced in 2017 after a demonstration in Bern against the Turkish government. A banner reading "Kill Erdogan with his own weapons!" was held up at the demonstration, triggering a diplomatic incident.

[13] The year before, the Wagner Group's website was itself the victim of defacement when pro-Ukrainian cyberactors posted images of war casualties and a political statement in support of Ukraine on the site.

[14] See EXCLUSIVE: Leaked TSA No Fly List: File Found on Airline Server (dailydot.com); Schweizer Hackerin stellt USA bloss: Geheime Flugverbots-Liste erbeutet (watson.ch)

[15] 128GB Of Russian ISP Convex Data Leaked By Anonymous Hacker (informationsecuritybuzz.com)

ransomware. Like traditional ransomware groups (see section 4.2), the hacktivists first obtain a copy of the data from their victims' systems and then launch encryption malware. However, rather than demanding a ransom for themselves, they require the victims to make a donation to charity in order to receive the encryption key and prevent the copied data from being leaked.[16]

2.4 Sabotage

Probably the most dangerous way in which hacktivists seek to gain attention for their causes is by trying to sabotage productive systems. Although in most cases the claimed impacts are greater than what can actually be attributed to hacktivists' cyberactivities, this type of threat certainly merits attention.[17]

A notable group in this regard is GhostSec, an offshoot of the established hacktivist collective Anonymous.[18] In January 2023, the group announced that it had hit Belarusian control systems with the first ransomware specifically geared towards operational technology systems. The attacked system is based on a Linux distribution of a type that has been compromised by ransomware in the past. Although the attack had an operational impact, it did not directly target the controlled physical process.[19]

Hacktivists intending to commit sabotage usually operate in the context of geopolitical conflicts. For example, Team OneFist[20] was formed against the backdrop of Russia's war of aggression in Ukraine. It has claimed responsibility for several incidents with physical effects, primarily in Russia.[21] Groups such as Predatory Sparrow[22] have been active for some time in conflicts in the Middle East, claiming, for example, to have caused physical damage at Iranian steelworks.[23]

The hacktivists' capabilities are mostly still limited to the manipulation of unprotected, internet-accessible control systems or the use of publicly available attack tools such as Metasploit modules,[24] which target industrial systems.

In more complex attacks, there are sometimes suspicions that hacktivist groups have covert state support. For instance, possible links between Russian military intelligence and pro-Russian hacktivist groups have been discussed.[25] Iranian security forces are said to be behind alleged Homeland Justice hacktivists in sabotaging Albanian government systems.[26] And

[16] MalasLocker ransomware targets Zimbra servers, demands charity donation (bleepingcomputer.com); Dark Web Profile: MalasLocker Ransomware (socradar.io)

[17] We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems (mandiant.com)

[18] Ghost Security (wikipedia.org)

[19] Hacker group discloses ability to encrypt an RTU device using ransomware, industry reacts (industrialcyber.co)

[20] About Us | Cyber Security (onefist.org)

[21] Meet the hacker armies on Ukraine's cyber front line (bbc.com)

[22] Predatory Sparrow (Threat Actor) (fraunhofer.de)

[23] Predatory Sparrow massively disrupts steel factories while keeping workers safe (malwarebytes.com)

[24] Metasploit | Penetration Testing Software, Pen Testing Security (metasploit.com) – The Metasploit Framework is a tool allowing security officers to identify and test vulnerabilities in computer systems. Like any tool, it can also be abused for malicious purposes.

[25] GRU: Rise of the (Telegram) MinIOns (mandiant.com)

[26] Microsoft investigates Iranian attacks against the Albanian government (microsoft.com)

recently, security researchers documented Ukrainian activity behind an attack on a Russian satellite operator[27] by alleged hacktivists associated with the Wagner Group.

Given the increased attention resulting from successful sabotage attempts, it is likely that other hacktivist groups will also try to acquire such capabilities in the future. The UK's National Cyber Security Centre has even warned explicitly about destructive attacks planned by pro-Russian hacktivists against Western critical infrastructure.[28] These actors could acquire relevant capabilities through support from state organisations or established cybercriminals.

Conclusion/recommendation:

Developed by the Federal Office for National Economic Supply (FONES) in collaboration with the business community, the ICT minimum standard and ICT minimum standards by sectors serve as recommendations and points of reference for ensuring adequate protection – also against the activities of hacktivists.

[27] Hackers claim to take down Russian satellite communications provider (therecord.media)

[28] NCSC warns of emerging threat to critical national infrastructure (ncsc.gov.uk)

3 Reports from businesses and the public

3.1 Reports received on cyberincidents – overview

Reports to the NCSC in the first half of 2023 (per week)

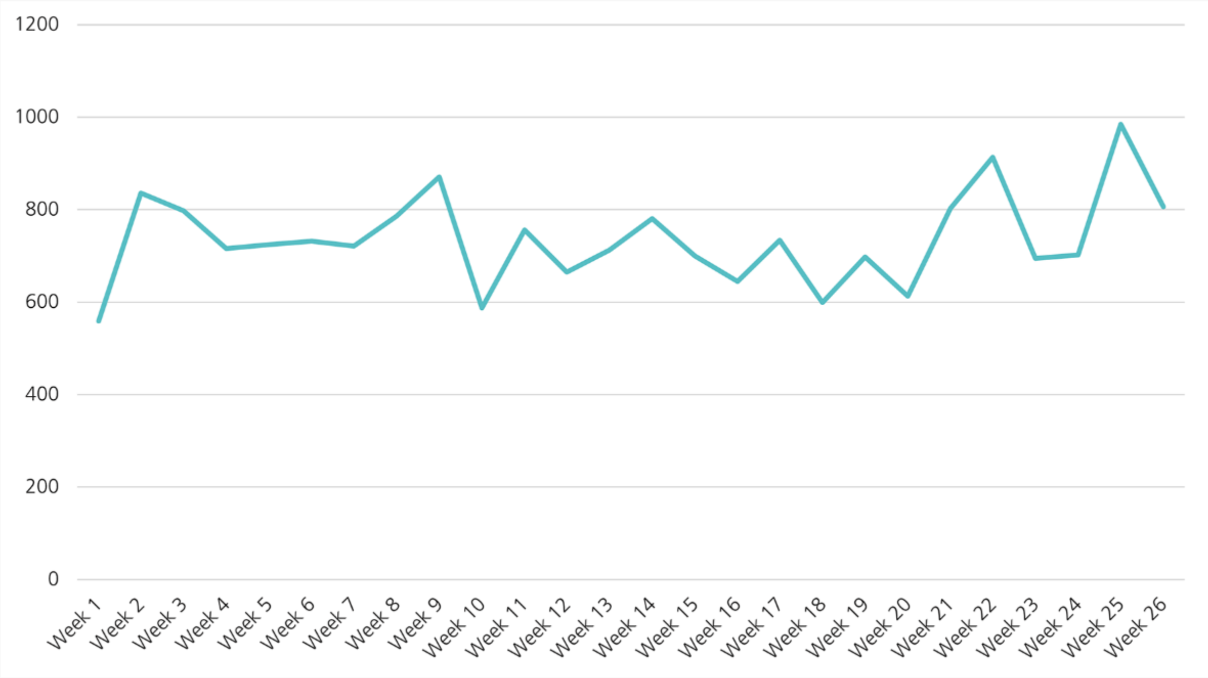


Fig. 3: Number of reports received per week by the NCSC from January to June 2023, see also [Current figures (ncsc.admin.ch)]

Reports to the NCSC in the first half of 2023 (per category)

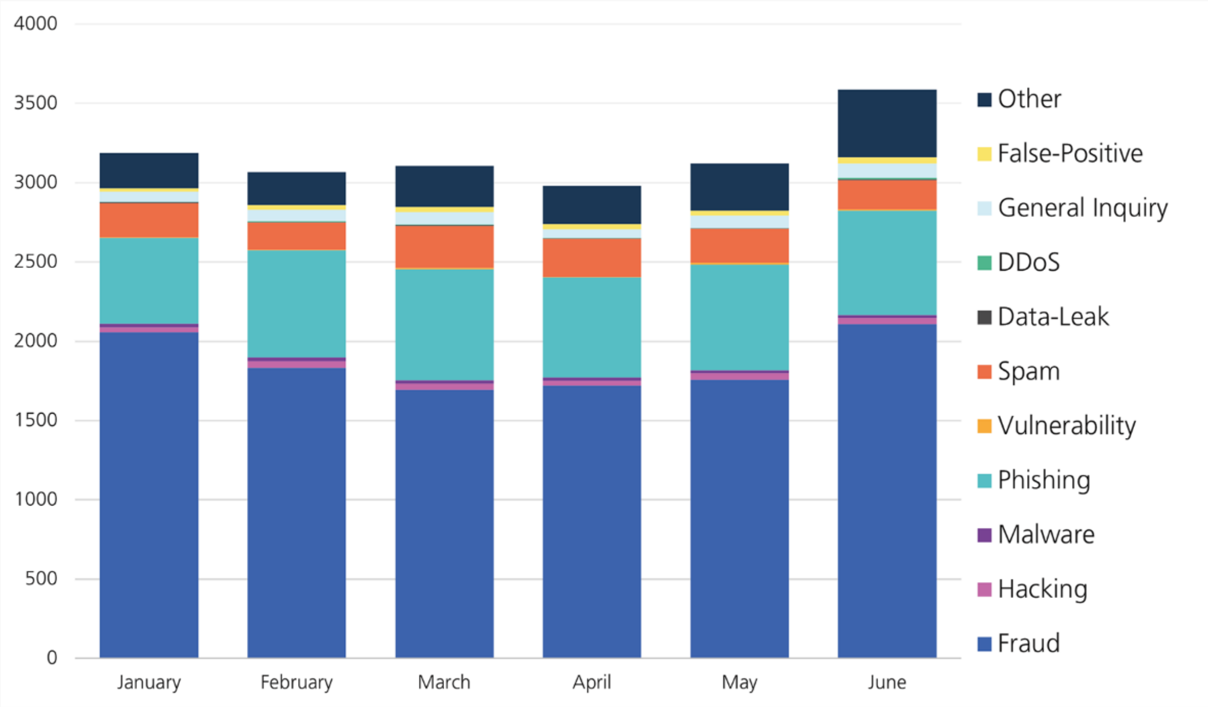
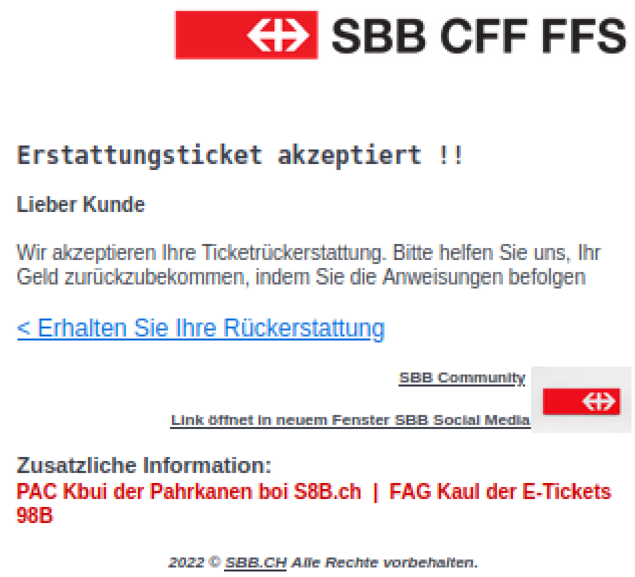


Fig. 4: Reports to the NCSC in the first half of 2023 by category, see also [Current figures (ncsc.admin.ch)]

In the first half of 2023, the NCSC received 19,048 reports on cyberincidents. This is around 2,000 more than in the previous six-month period (16,951) and in the same period the previous year (16,844). The increase is therefore more moderate than a year ago. The proportion of fake threatening emails from authorities (5,511) and reports of telephone spoofing (543) remained virtually unchanged and was still at the same high level as in the previous six months. Fraud reports (11,168) as a proportion of total reports received fell slightly from 62% to 59%. However, there was a marked increase of almost 1,700 in the number of phishing reports compared with the previous half-year. A total of 3,875 reports in the phishing category were submitted during the period under review. The main reason for the rise was a phishing campaign targeting SwissPass customers, which dragged on throughout the first half of the year. The number of reports relating to this phenomenon rose to around 1,000, an almost tenfold increase compared with the previous half-year period.



SBB CFF FFS

Erstattungsticket akzeptiert !!

Lieber Kunde

Wir akzeptieren Ihre Ticketrückerstattung. Bitte helfen Sie uns, Ihr Geld zurückzubekommen, indem Sie die Anweisungen befolgen

< Erhalten Sie Ihre Rückerstattung

SBB Community

Link öffnet in neuem Fenster SBB Social Media

Zusatzliche Information:
PAC Kbui der Pahrkanen boi S8B.ch | FAG Kaul der E-Tickets 98B

2022 © SBB.CH Alle Rechte vorbehalten.

Fig. 5: Example of a phishing attempt involving the alleged refund of an SBB ticket.

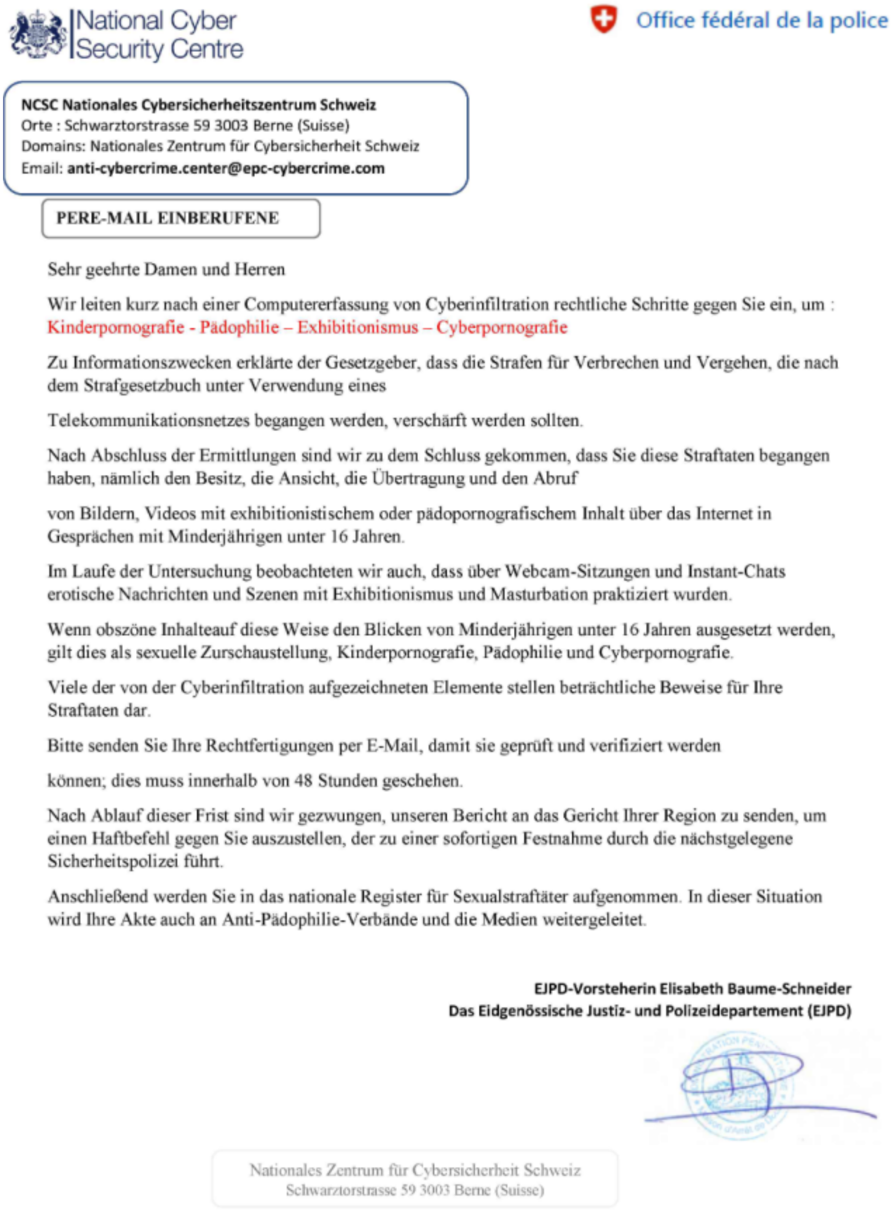
Phishing attempts in connection with classified ads also saw an increase in reports. In such cases, prospective sellers are asked to pay fees or confirm a transaction, the aim being to trick them into providing credit card details. Phishing via text message (known as "smishing") also increased slightly. Phishing attempts linked to fake parcel notifications remained high. Almost 600 such reports were received, accounting for 15% of all phishing reports.

The ratio of reports from the public (86%) to those from businesses, associations and authorities remained stable. Among the types most typically reported by businesses, both CEO fraud (116 reports) and business email compromise (36) fell slightly. However, attacks involving encryption malware (56) and DDoS (24) increased. The most common issue reported by businesses concerns fake threatening emails from authorities, known as fake extortions (346). These include numerous extortion attempts against web administrators, in which the scammers point out a fictitious vulnerability on the website and claim that data has been leaked. Businesses also regularly report phishing attempts. The main aim of these is to access Office 365 login credentials.

3.2 Most frequently reported: fraud

3.2.1 Threatening emails allegedly from authorities remain at high levels

Once again, 30% of all reports received related to fake threatening emails from authorities (fake extortion). Most of these emails accuse the victim of having supposedly committed a crime. Such threats are sent in the name of both Swiss and foreign authorities. In the last half-year period, the name of the Swiss NCSC was increasingly misappropriated in this way, albeit with the logo of its British counterpart. These fake documents usually bore the forged signature of the Head of the Federal Office of Police, Nicoletta della Valle, or a federal councillor. Fraudsters also apparently keep up to date with Swiss politics, given that fake emails featuring the name of newly elect Federal Councillor Elisabeth Baume-Schneider began appearing just six days after she took office.



National Cyber
Security Centre

Office fédéral de la police

NCSC Nationales Cybersicherheitszentrum Schweiz
Orte : Schwarztorstrasse 59 3003 Berne (Suisse)
Domains: Nationales Zentrum für Cybersicherheit Schweiz
Email: **anti-cybercrime.center@epc-cybercrime.com**

PERE-MAIL EINBERUFENE

Sehr geehrte Damen und Herren

Wir leiten kurz nach einer Computererfassung von Cyberinfiltration rechtliche Schritte gegen Sie ein, um : Kinderpornografie - Pädophilie – Exhibitionismus – Cyberpornografie

Zu Informationszwecken erklärte der Gesetzgeber, dass die Strafen für Verbrechen und Vergehen, die nach dem Strafgesetzbuch unter Verwendung eines

Telekommunikationsnetzes begangen werden, verschärft werden sollten.

Nach Abschluss der Ermittlungen sind wir zu dem Schluss gekommen, dass Sie diese Straftaten begangen haben, nämlich den Besitz, die Ansicht, die Übertragung und den Abruf

von Bildern, Videos mit exhibitionistischem oder pädopornografischem Inhalt über das Internet in Gesprächen mit Minderjährigen unter 16 Jahren.

Im Laufe der Untersuchung beobachteten wir auch, dass über Webcam-Sitzungen und Instant-Chats erotische Nachrichten und Szenen mit Exhibitionismus und Masturbation praktiziert wurden.

Wenn obszöne Inhalteauf diese Weise den Blicken von Minderjährigen unter 16 Jahren ausgesetzt werden, gilt dies als sexuelle Zurschaustellung, Kinderpornografie, Pädophilie und Cyberpornografie.

Viele der von der Cyberinfiltration aufgezeichneten Elemente stellen beträchtliche Beweise für Ihre Straftaten dar.

Bitte senden Sie Ihre Rechtfertigungen per E-Mail, damit sie geprüft und verifiziert werden

können; dies muss innerhalb von 48 Stunden geschehen.

Nach Ablauf dieser Frist sind wir gezwungen, unseren Bericht an das Gericht Ihrer Region zu senden, um einen Haftbefehl gegen Sie auszustellen, der zu einer sofortigen Festnahme durch die nächstgelegene Sicherheitspolizei führt.

Anschließend werden Sie in das nationale Register für Sexualstraftäter aufgenommen. In dieser Situation wird Ihre Akte auch an Anti-Pädophilie-Verbände und die Medien weitergeleitet.

EJPD-Vorsteherin Elisabeth Baume-Schneider
Das Eidgenössische Justiz- und Polizeidepartement (EJPD)

Nationales Zentrum für Cybersicherheit Schweiz
Schwarztorstrasse 59 3003 Berne (Suisse)

Fig. 6: Fake extortion email claiming to be from the NCSC with the logo of its British counterpart, purportedly signed by Elisabeth Baume-Schneider. The email was reported to the NCSC on 6 January 2023, shortly after the new federal councillor took office.

3.2.2 Other fraud phenomena

The NCSC continued to receive many reports of advance-fee scams (1,660). Alongside the classics, involving an inheritance or an unclaimed pot of gold, there are some more innovative variants. The recipient receives a username and password in an email and, following the link provided, sees a large sum of cryptocurrency in what is purportedly their account. They are told that the promised sums will be paid out subject to payment of a series of ever-higher fees, but of course this never happens.

Reports of fake sextortion, subscription scams and classified ad scams were at the same level as in the previous half-year period. In the case of classified ads, the scam shifted from fraud to phishing, with the victim being sent a phishing link during the payment process.

The NCSC received 245 reports relating to online investment fraud, slightly up on the previous six months (219). However, the reported losses more than doubled to CHF 9.5 million. The fraudsters appear to have vast human resources at their disposal, given their highly responsive and tailored approach to victims. As well as direct personal contact with prospective victims on various social media channels, where trust is built up over an extended period, websites set up for the online scam offer 24/7 chat-based or telephone hotline support. There are also educational videos explaining the features of the purported investment platform.

Once again, we saw how quickly fraudsters react to the latest news. The launch of the Starship rocket, for example, soon prompted a give-away scam featuring a deepfake of Elon Musk.[29]

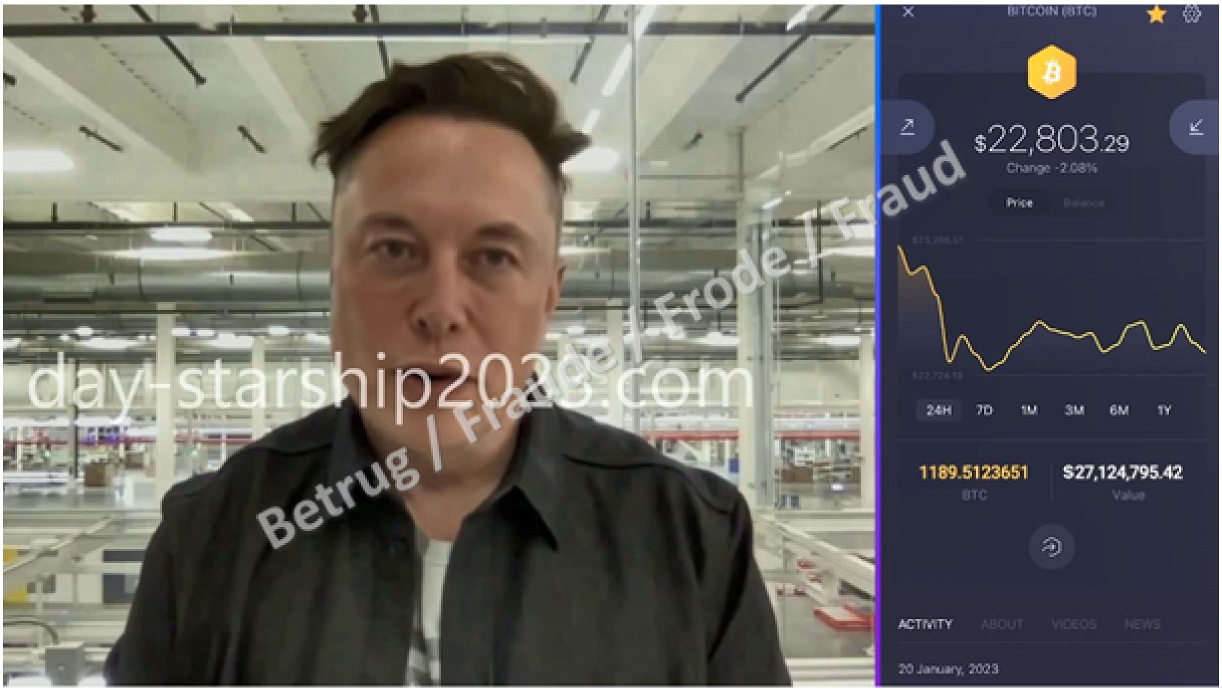


Fig. 7: Deepfake video with Elon Musk. In addition to the visual, the voice was also created using deepfake technology.

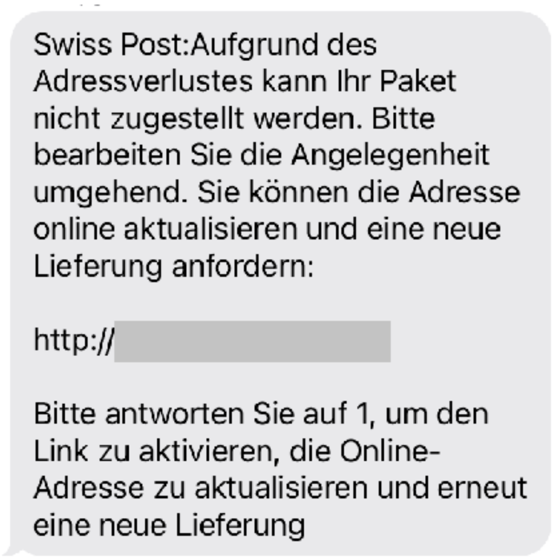
[29] Week 17: Advertisement using a deepfake video for a giveaway scam (ncsc.admin.ch)

3.3 Phishing reports

The second most reported phenomenon is phishing. The number of such incidents was up more than 40% and accounted for one fifth of the reports received in the last six-month period.

One general observation is that phishing attempts are becoming more elaborate, with attackers trying out new methods to disguise the phishing link.

Phishing messages sent by SMS/text message, known as smishings, were also frequently observed, particularly in connection with fake parcel notifications. The recipient receives a message, ostensibly from Swiss Post, DHL, DPD or FedEx, saying that a parcel cannot be delivered due to missing information or outstanding charges. The phishing site is configured so that it is only displayed when accessed via a mobile phone (e.g. the Chrome browser on an Android operating system). On a PC, the user is taken directly to the correct website (e.g. Swiss Post). In this way the attackers try to fool the security authorities into thinking that the message and the link it contains are not fraudulent and so they do not need to take any action. Phishing involving QR codes is still rarely reported.



Swiss Post:Aufgrund des Adressverlustes kann Ihr Paket nicht zugestellt werden. Bitte bearbeiten Sie die Angelegenheit umgehend. Sie können die Adresse online aktualisieren und eine neue Lieferung anfordern:

http://[redacted]

Bitte antworten Sie auf 1, um den Link zu aktivieren, die Online-Adresse zu aktualisieren und erneut eine neue Lieferung

Fig. 8: Typical smishing attempt involving a fake parcel notification claiming to be from Swiss Post. After clicking on the link, the victim is asked to enter credit card details.

A wave of telephone phishing was also observed (known as voice phishing, or vishing). The attackers posed as employees of a telecoms company and used various tricks to try to obtain the second factor sent by text message. Paysafecards were then purchased via the provider webshops.[30]

Office 365 real-time phishing was reported frequently in the first quarter of 2023, mainly by businesses. These scams often involved an HTML document attached to the email. The phishing page, opened locally in the browser, even displayed genuine corporate logos, which were dynamically downloaded in the background from the real company website, using scripts. When a victim entered a username and password on a phishing page, the time-limited second factor also had to be intercepted via the phishing site. To gain more time for subsequent

[30] Week 5: Sophisticated telephone phishing (ncsc.admin.ch)

activities in the background, the attackers – once they had logged in – made the victim believe that there was a temporary network error.[31]

Number of detected phishing URLs per week

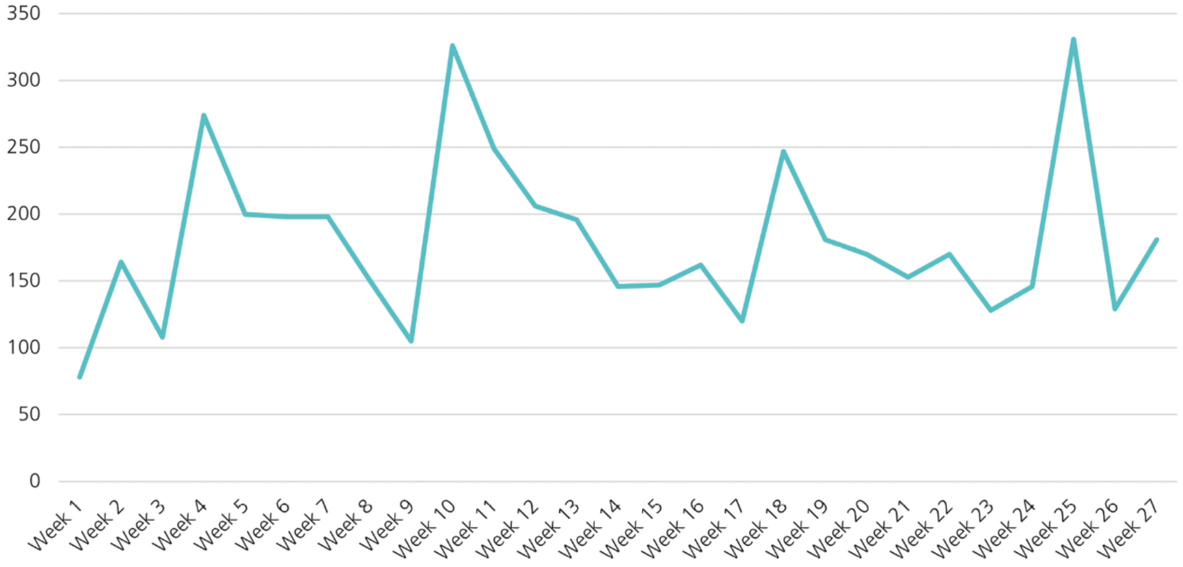


Fig. 9: Number of phishing URLs checked and confirmed by the NCSC per week in the first half of 2023.

3.4 Malware and hacking reports

3.4.1 Ransomware incidents: Differing trends for companies and private individuals

A total of 124 reports in connection with malware were registered in the first half of 2023, representing another decline on the previous half-year period (155). As in the previous six months, there were no major waves of malware sent by email.

While reports of ransomware also fell from 76 to 64, there is absolutely no room for complacency here as the decline in the number of reports was linked not to companies but to private individuals (down from 27 to 8 cases). There were only sporadic attacks on network-attached storage (NAS) systems, which are a particular issue with private individuals.[32] Conversely, there was an increase in reported cases among businesses, administrations and associations, up from 49 to 56. Larger companies are also being targeted, as demonstrated by numerous examples from the first half of 2023 (see section 4.2.1). LockBit ransomware has been particularly active, including in the period under review. Other reported ransomware families include Play, BlackCat, MedusaLocker, Phobos, BlackByte, Black Basta, Babuk, eCh0raix and Akira. In many cases, the family responsible was not yet known at the time of the report, so the NCSC cannot provide meaningful figures on ransomware families. To address this, the NCSC is currently working on a post-incident feedback form that will be sent to companies in order to systematically collect such information.

[31] Week 6: Real-time phishing of secured Office365 accounts (ncsc.admin.ch)

[32] See Week 4: Security vulnerability in QNAP NAS devices and new phishing variant (ncsc.admin.ch)

3.4.2 Hacking reports

Reports of hacking fell from 276 to 225. Almost half of the reports involved hacked social media accounts. The number of reports in this category was virtually unchanged from the previous half-year period, at 101 compared with 108. Hacked social media accounts are also still being used to lend credence to fake sextortion attempts. Another common use of hacked social media accounts is to promote investment scams. Especially with accounts that have many followers, this is a popular way of getting information about dubious investment opportunities to as many potential victims as possible.

3.5 Miscellaneous reports

3.5.1 Search engine optimisation with abandoned domains and hacked websites

When searching for specific topics in standard search engines, people tend to click on results from the first page only. If they are not satisfied with these, they are more likely to tweak the search terms rather than taking the trouble to look for potentially better results on the second or third page.

Operators of dubious websites are aware of this and will try every trick in the book to manipulate the search in their favour so that their sites appear on the first page of results. This increases the chance that potential victims will click on the manipulated search results and thus end up on dubious websites.

The following two practices, among others, were reported to the NCSC in the first half of the year:

The first variant involves the abuse of abandoned domains. Many domain owners are familiar with the problem: they own domains that are actually no longer needed and consider cancelling them because they incur annual fees. However, very few people think about the fact that, after cancellation, the domain becomes available for registration to anyone. New registrants can place whatever content they want on it. In the past, the NCSC repeatedly received reports in which former domain owners complained that dubious webshops or websites with adult content were being displayed under their old website's address. The main targets are domains that have a small following, but one that is nonetheless interesting for attackers. They exploit the ranking acquired by the original websites in search engines. If a relevant search term is entered, the attackers' newly resurrected website is displayed together with its content in the usual place in the search engine ranking, rather than the original site.

In a second variant, attackers use hacked websites to try to manipulate search engine results. At the start of the year, the NCSC discovered that a Google search for websites reported as hacked to the NCSC showed the correct title in the results. However, the extract from the website content below the title had nothing to do with the website. Instead, it contained various links hidden behind combinations of letters and numbers. The list of dubious links was also displayed if the website was opened using Google Cache, i.e. a copy of the website cached by Google. However, if the website was opened directly by entering the URL, the website was correctly displayed. It was assumed that, in this case, different page contents would be displayed – depending on the user agent. The user agent data is sent every time a website is called up and provides the web server with information about the visitor's operating system and the browser. In addition to statistical surveys, such data can also be used to optimise website content for a specific browser type. Google mostly uses the user agent "Googlebot" when crawling the internet. This is how Google search queries can be recognised. However, this function can also be abused to present doctored website content to Google. Since the same links are always displayed on the various hacked websites, Google assumes that the linked websites are of interest and rates them as more relevant than they actually are. They move up in the search results accordingly and then reach more people. For all other visitors to the hacked website and therefore also for its owner, the normal content is displayed. This way, the manipulation is less noticeable and can maintain its effect over a long period of time.

4 Situation

4.1 Initial access

Obtaining access to user accounts or remote access to computer systems is the first step in most types of cyberattack. Such initial access can be gained in various ways,[33] and once obtained can be passed on to other threat actors for them to exploit.

4.1.1 Username/password

Login details are usually obtained through phishing (see also section 3.3). In other words, users are tricked into passing on their details to the attackers. Phishing messages are becoming ever more sophisticated, making phishing increasingly difficult to spot.[34] Cyberattackers are also responding to additional security measures and have developed methods to attack accounts protected by two-factor or multi-factor authentication.[35]

Conclusion/recommendation:

While not offering absolute protection, security measures are worth taking in order not to make life too easy for would-be attackers. It is advisable to choose strong passwords and to protect important accounts with two-factor or multi-factor authentication if possible.[36]

Always check the address behind a link, i.e. the URL.[37] A logo or other image is not proof that an email or website is genuine! Be wary if you are asked to enter passwords or other information.

[33] See also Initial Access, Tactic TA0001 (mitre.org)

[34] Week 25: Spotting phishing is becoming increasingly difficult (ncsc.admin.ch); see also section 3.3

[35] Week 6: Real-time phishing of secured Office365 accounts (ncsc.admin.ch);
Week 8: Text messages supposedly from the Federal Council and other new phishing methods (ncsc.admin.ch);
Week 9: Threatening emails supposedly sent by the NCSC and real-time phishing (ncsc.admin.ch);
Week 19: SIM swapping – how a SIM card can be stolen online (ncsc.admin.ch)

[36] E for Equip (s-u-p-e-r.ch); Protect your accounts (ncsc.admin.ch)

[37] Cybermyth: Link address (ncsc.admin.ch)

4.1.2 Malware (Trojans)

Once installed, Trojans open a backdoor for attackers to the target system. This remains a common method of gaining access to the victim's system. Installation is usually not automatic. The user has to be tricked into performing an action, and attackers use a variety of methods to achieve this. The code that installs the malware is often integrated into another program or otherwise disguised so that the user is unaware that it is being executed.

Malware is very often spread by email. The code for the infection may be contained directly in the attachment or accessed via a link in the email. The context of the email tricks the user into executing the file containing the malicious code. For example, it may refer to everyday transactions such as offers, deliveries and invoices, or promise exclusive information about current events. Some attackers also use genuine, previous email correspondence obtained from past unauthorised access to other organisations to bolster the credibility of the current email containing the malware. This is the case with QakBot malware, for example, where initial infection regularly leads to ransomware infections.[38] Time pressure is often also created, to induce the recipients to take rash action. A specific example involving these various elements (distribution by email, software installation disguised in another program, user urged to respond immediately) was featured by the NCSC in one of its weekly reviews.[39]

Users can also be tricked into installing malware through the purchase of online advertising space or the display of sponsored search results (malvertising). These adverts claim that software the user wants is available via the ad. However, malware is installed at the same time as this (often free) software.[40]

Finally, criminals also use USB sticks as a means of spreading their malware. On the one hand, USB sticks may have been specifically designed for initial infection in a target environment.[41] On the other hand, some malware can copy itself onto USB sticks inserted into an infected computer and then spread to other systems into which the USB stick is inserted afterwards. This technique has been somewhat overlooked of late, but it continues to be used.[42]

Conclusion/recommendation:

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

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

Do not insert unknown or "found" USB devices into a computer.

[38] Week 24: The QakBot malware is still active – and has some new tricks up its sleeve (ncsc.admin.ch)

[39] Week 18: A wolf in sheep's clothing or an incident involving a malicious software update (ncsc.admin.ch)

[40] Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals (trendmicro.com)

[41] Cybertip: manipulated USB flash drives are a gateway for cyberattacks (ncsc.admin.ch)

[42] Beyond the Horizon: Traveling the World on Camaro Dragon's USB Flash Drives (checkpoint.com)

4.1.3 Exploitation of vulnerabilities

As soon as a product vulnerability becomes known, various players begin to scour the internet for vulnerable systems. After a few hours or days, the vulnerability starts to be exploited. Vulnerabilities that have been known for some time and for which a patch is available are also regularly exploited.[43] Sometimes cyberattackers also use "zero-day" vulnerabilities.[44] In early June, the Cl0p ransomware group began exploiting a then-unknown SQL injection vulnerability in the file transfer software MOVEit Transfer. Web applications accessible from the internet were infected with a web shell,[45] which was then used to access underlying MOVEit Transfer databases.[46]

On one side, there are bugs resulting from developer error, which can be remedied with patches or updates. But vulnerabilities can also be caused by the configurations selected when implementing products. Various manufacturers provide configuration instructions for “secure configuration” or “hardening” of their products.

Recommendations:

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

Both private individuals and businesses should always keep software up to date on all devices, preferably by means of an automatic update function.[47] It is strongly recommended to have effective software management with inventory and update processes.[48]

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

4.2 Ransomware

Once again, the first half of the year saw numerous ransomware incidents in a range of sectors, from small local businesses to international corporations. The following examples from Switzerland and abroad illustrate not only the situation in cyberspace, but also the development of groups and patterns of action in the first half of 2023.

4.2.1 Examples of incidents in Switzerland

In Switzerland, LockBit remains the most widespread ransomware. The actors behind it either launch sophisticated phishing campaigns or exploit vulnerabilities in order to penetrate systems. The activities of the Play and Black Basta groups were also very much on the NCSC's radar during this six-month period.

[43] See for example Week 7: Encrypted VMware ESXi systems (ncsc.admin.ch)

[44] A zero-day vulnerability is a vulnerability for which no update or patch is yet available to fix the issue.

[45] A web shell is an interface that enables remote access to a web server via a web browser.

[46] Critical vulnerability in file transfer software "MOVEit" (ncsc.admin.ch);
CL0P Ransomware Gang Exploits MOVEit Vulnerability (cisa.gov); see also sections 4.4.1, 4.5.1 and 4.5.2.

[47] See U for Update (s-u-p-e-r.ch)

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

High-profile attacks by the Play group

The Play group was highly active: its victims included Energie Pool Schweiz in February 2023;[49] two major media players, CH Media and NZZ, in March;[50] the Valais commune of Saxon[51] in April; and the IT service provider Unico[52] and software provider Xplain[53] in May. The disruption caused by the attacks, and the perpetrators' subsequent disclosure of data obtained from the victims, generated a lot of publicity for Play.

Black Basta impacts operations

Another prominent actor in the first half of the year was Black Basta. Its victims included ABB[54] and the industrial machinery and service provider Bobst.[55] In both cases, the incidents disrupted company operations.

Black Basta essentially operates as a ransomware-as-a-service (RaaS) group, but there are no signs that it has attempted to advertise on relevant dark web forums or illegal trading platforms, or to recruit new partners in other ways. Recent evidence suggests that the authors of the software are developing their toolbox themselves. Any cooperation is likely to be confined to a limited number of trusted partners.

Further development of the BianLian group

The NCSC featured an incident involving BianLian in its last semi-annual report.[56] In September 2022, two months after its initial appearance, the group claimed its first Swiss victim. As the NCSC noted at the time, BianLian, like many other malware authors, operates on the principle of double extortion. Before being encrypted, data is exfiltrated, i.e. copied from the victims' systems without authorisation. Since January 2023, however, the group appears to have dispensed with encryption of the victim's data and now simply exfiltrates the data. In fact, a free decryption program for BianLian ransomware was released at exactly that time.

This did not stop the group undertaking further actions. In spring 2023, the Basel Department of Education was hit by a BianLian incident, with data obtained from this attack being posted on the dark web soon afterwards.[57] Other ransomware groups that previously worked with double extortion have also started to dispense with encryption, including BlackCat and Cl0p.[58] Meanwhile, other extortion groups, such as Karakurt, never used encryption at all.

[49] Ransomware-Angriff auf Schweizer Energie-Firma (inside-it.ch)

[50] Daten von CH Media nach Cyberangriff veröffentlicht (chmedia.ch);
Cyberkriminelle veröffentlichen erneut Daten von CH Media (chmedia.ch);
Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet (nzz.ch)

[51] Saxon: Cyberattacke auf die Vormundschaftsbehörde (polizeiwallis.ch)

[52] Ransomware-Attacke auf IT-Dienstleister Unico Data: viele Betroffene (watson.ch)

[53] Federal Administration also impacted by Xplain hack (ncsc.admin.ch)

[54] Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com);
ABB provides details about IT security incident (abb.com)

[55] Cyberattaques ciblées: Bobst résiste à deux piratages informatiques (24heures.ch);
Mutmassliche ABB-Hacker stecken auch hinter Angriff auf Bobst (inside-it.ch)

[56] Semi-annual report 2022/2 (ncsc.admin.ch), section 5.2.2.1.

[57] Grosser Cyberangriff – Kinder betroffen: Daten des Basler Erziehungsdepartements gehackt (srf.ch)

[58] See section 4.5.1.

4.2.2 Situation abroad

When it comes to ransomware, the situation in Switzerland differs little from the international picture. In terms of the number of attacks, LockBit, BlackCat/ALPHV and Royal account for the lion's share, with industrial companies and service providers particularly affected.[59] One of the biggest incidents occurred at Royal Mail in the UK, which had to temporarily suspend international deliveries in January 2023 after being infected with LockBit ransomware.[60]

Aside from continuing attacks by known groups, new ransomware (e.g. Akira) and groups (such as MalasLocker, see section 2.1.1) also emerged, some groups were disbanded (Hive) while others, such as Cl0p, returned to the scene.[61]

4.2.3 Overview of the most active protagonists and most commonly used infection vectors

Riding the trend

LockBit, BlackCat/ALPHV and Cl0p accounted for the most incidents in this six-month period. The infection vectors used come and go as new vulnerabilities are discovered and patches are released to fix them. Cybercriminals can adapt quickly to new technology trends. Examples include using the Go and Rust programming languages,[62] exploiting the vulnerability in VMware ESXi servers[63] and distributing malware via OneNote files.[64] Sometimes there is no need to change the technical approach at all as existing methods based on social engineering are sufficient. Human error remains the most profitable vulnerability for cybercriminals.

Attacks on IT service providers

Ransomware victims also include IT providers. If an IT company is hit by a ransomware attack, this can affect multiple customers at once since IT service providers interface or intersect with numerous customer networks. This multiplier effect makes IT service providers a valuable target for attackers, who see the opportunity for multiple and/or high ransom demands. A business continuity plan (including data backup and the ability to replicate server infrastructure using system images and cloud computing) is key to ensuring that IT service providers can resume their activities quickly after a ransomware attack.

Move away from encryption

For a long time, double extortion was more or less the default technique of ransomware groups and their partners. Some cases even involved triple extortion: in addition to the exfiltration and subsequent encryption of data, third parties and people close to the victim were attacked or blackmailed using the stolen data. The NCSC is now seeing a shift away from encryption among various groups, with data simply being exfiltrated and then used to blackmail victims with the threat of publication (see section 4.5.1).

[59] March 2023 broke ransomware attack records with 459 incidents (bleepingcomputer.com); Ransomware Trends 2023, Q2 Report (cyberint.com)

[60] LockBit leaks more Royal Mail data after ransomware attack (techmonitor.ai)

[61] See sections 4.1.1 and 4.5.2.

[62] See semi-annual report 2022/2 (ncsc.admin.ch), section 5.2.2.

[63] Week 7: Encrypted VMware ESXi systems (ncsc.admin.ch)

[64] Qakbot evolves to OneNote Malware Distribution (trellix.com)

Conclusions, outlook and recommendations:

Ransomware groups and their practices are evolving and changing at an ever faster pace. It is therefore important to take preventive measures at a technical and human level wherever possible.[65]

Important aspects of incident management are described on the NCSC website:

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

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

Opportunistic attacks against networks of organisations that also operate industrial control systems and operational technology remained the greatest threat to the secure operation of these systems in the first half of 2023. In Switzerland, Black Basta ransomware attacks at the industrial group ABB[66] and the machinery manufacturer Bobst[67] had at least a temporary impact on the operation of their own facilities. In the energy supply sector, Energie Pool Schweiz[68] fell victim to Play ransomware (see section 4.2.1).

Internationally, from the start of the year, increased activity involving data-destroying malware (known as "wipers") caused operational disruptions for organisations in Ukraine.[69] For example, NikoWiper[70] was used against a company in the energy sector. A new actor, known as Cadet Blizzard[71] or Frozen Vista,[72] also contributed to the increased use of wipers. It was responsible, among other things, for attacks with the WhisperGate wiper in the early days of the war. Outside the conflict arena, a cyberincident on a Canadian pipeline caused disruptions to energy transmission.[73] According to information gleaned from the Pentagon leaks, the pro-Russian hacktivist group Zarya claimed responsibility for this incident. Further potentially destructive activities by hacktivists are discussed in the Focus section (see section 2.4).

At the end of May, security service provider Mandiant published findings on the ICS-specific malware CosmicEnergy.[74] This attacks devices operated according to the IEC-104 power supply standard. Both Mandiant and other ICS security specialists[75] assume that CosmicEnergy is a tool used for training exercises. It does not have the destructive potential of malware like Industroyer 2.0 or Pipedream, which came to prominence in the first half of 2022.[76]

[65] See methods and measures in section 4.1.

[66] Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com); ABB provides details about IT security incident (abb.com)

[67] Mutmassliche ABB-Hacker stecken auch hinter Angriff auf Bobst (inside-it.ch)

[68] Ransomware-Angriff auf Schweizer Energie-Firma (inside-it.ch)

[69] Ukraine Suffered More Wiper Malware in 2022 Than Anywhere, Ever (wired.com)

[70] New Report Reveals NikoWiper Malware That Targeted Ukraine Energy Sector (thehackernews.com)

[71] Cadet Blizzard emerges as a novel and distinct Russian threat actor (microsoft.com)

[72] Fog of war: how the Ukraine conflict transformed the cyber threat landscape (blog.google)

[73] Russian hacktivist threat on Canada's pipelines is 'call to action,' top cyber official says (therecord.media)

[74] CosmicEnergy: New OT Malware Possibly Related To Russian Emergency Response Exercises (mandiant.com)

[75] CosmicEnergy: Malware Is Not an Immediate Threat to Industrial Control Systems (dragos.com)

[76] See semi-annual report 2022/1 (ncsc.admin.ch), section 5.4.1

The risk of targeted attacks against processes controlled by operational technology (OT) continues to be greatest in the context of existing conflicts such as the war in Ukraine and tensions in the Middle East. The US cybersecurity agency CISA[77] warns of activities by the state actor Volt Typhoon, which according to Microsoft[78] is also building disruptive capabilities that could be used, for example, in an escalation around Taiwan.[79]

Efforts are being made worldwide to secure the systems that control critical infrastructure processes. In this connection, the EU has adopted the NIS 2 Directive, which requires operators to take appropriate security measures.[80] In the United States, CISA has published a white paper on enhancing the resilience of cyber-physical critical infrastructure.[81] Industry has also been active, establishing the ETHOS project as a private-sector initiative to promote the sharing of OT-specific early warnings and threat information.[82]

Conclusion/recommendations:

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

Suitable measures can be found in the ICT minimum standards of the Federal Office for National Economic Supply (FONES), updated in 2023, and in the respective sector standards: ICT minimum standards (ncsc.admin.ch).

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

4.4 Vulnerabilities

4.4.1 "MOVEit" (CVE-2023-34362 | CVE-2023-35036 | CVE-2023-35708)

In late May 2023, a critical zero-day vulnerability (CVE-2023-34362) was discovered in Progress's data transfer software MOVEit Transfer and MOVEit Cloud, affecting all versions of the application. Many companies worldwide use the application for sharing and exchanging files.

The vendor published an advisory[83] on 31 May 2023, detailing the vulnerability and explaining the action needed to fix it. At this point, the vulnerability was already being actively exploited by criminal actors.

[77] People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection (cisa.gov)

[78] Volt Typhoon targets US critical infrastructure with living-off-the-land techniques (microsoft.com)

[79] Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target? (nytimes.com)

[80] Directive […] for a high common level of cybersecurity across the Union (NIS2 Directive) (ec.europa.eu)

[81] Research, Development, and Innovation for Enhancing Resilience of Cyber-Physical Critical Infrastructure: Needs and Strategic Actions (cisa.gov)

[82] ETHOS | Emerging Threat Open Sharing (ethos-org.io)

[83] MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362) (progress.com)

The issue affects Windows servers running a vulnerable version of the MOVEit software. An attacker can detect such systems relatively easily using public internet indexing services or port scanning and so identify potential targets.

The MOVEit web application, which allows users to manage and share files in a simple and convenient way, is susceptible to an attack vector known as SQL injection. By exploiting this vulnerability, an attacker is able to access the target system (in this case, primarily the MOVEit Transfer database), execute system commands and gain unauthorised access to information from the company concerned. The main aim of such an attack is to steal data in order to then extort a ransom from those affected. However, this also gives third parties the opportunity to change existing data in the system or to introduce new files, including malware, into the target system.

Shortly after the zero-day vulnerability was disclosed, the ransomware group Cl0p claimed responsibility for hundreds of attacks on organisations worldwide. Swiss companies in various industries were among those successfully targeted by the criminal actors using the above attack scenario, before they had a chance to install the vendor's patches on their systems.

With the release of its advisory on the CVE-2023-34362 vulnerability on 31 May 2023, the vendor Progress provided detailed instructions as well as patches, which enabled the vulnerability to be fixed immediately. At the same time, Progress also commissioned another company to review the software code for the MOVEit application as part of its investigation into CVE-2023-34362. The outcome of this code review resulted in the identification of two further critical vulnerabilities a few days later, for which additional patches for installation were released on 9 June 2023 (CVE-2023-35036) and 15 June 2023 (CVE-2023-35708).

These two subsequently disclosed vulnerabilities – CVE-2023-35036 and CVE-2023-35708 – are in the same vulnerability category as CVE-2023-34362. All three patches provided by the vendor are designed to address SQL injections.

Conclusion/recommendations:

If a vulnerability has already been demonstrably exploited by the time it is made public, it is important to follow the vendor's emergency measures immediately and to have an efficient patch management process in place within the company. In addition, it is vital to perform an active and thorough search for signs of previous attacks on potentially affected systems. The rapid detection of such indicators of compromise may help to contain an attack at an early stage of the attack cycle, thereby mitigating adverse impacts on a company's business activities and processes.

4.4.2 Fortinet (CVE-2022-39952 | CVE-2021-42756)

On 16 February 2023, Fortinet disclosed two critical vulnerabilities that had been identified by its own Product Security Incident Response Team (PSIRT).

While CVE-2021-42756[84] affects FortiWeb, CVE-2022-39952[85] is a security vulnerability in FortiNAC. FortiNAC uses a range of functions to detect and protect devices connected to an enterprise network by controlling access to network resources and automatically responding to security events. FortiWeb, on the other hand, focuses on protecting web applications and APIs against DDoS attacks, OWASP Top 10 threats[86] and malicious bot activity.

In both cases, it is possible, under certain circumstances, for an attacker to execute code or system commands on the vulnerable target system and so bring about remote code execution (RCE).

At the time the vulnerabilities were made public, neither was being actively exploited – or at least exploitation was not publicly known. However, IT security researchers published exploit code for CVE-2022-39952 on 21 February 2023, just days after Fortinet informed the public about the vulnerabilities. This greatly increased the likelihood of exploitation by criminal actors. Within hours of this exploit code appearing, there were various reports of active attempts at exploitation.

The two critical vulnerabilities are of particular interest to threat actors because Fortinet's products have an extremely large and widespread global user base. The company has a very extensive cybersecurity portfolio with over 10 million devices shipped. This makes Fortinet products with known vulnerabilities very attractive to attackers. With a large number of products in use worldwide, there is a high probability of identifying non-updated devices that are ripe for an attack.

At the same time that it issued its two advisories for CVE-2021-42756 and CVE-2022-39952 on 21 February 2023, Fortinet also published the actions required to fix the critical vulnerabilities. In both cases, an upgrade of the products used, FortiWeb and FortiNAC, is required to ensure lasting protection against the threat.

Conclusion/recommendations:

Vulnerabilities are often exploited very soon after being disclosed – and sometimes even before this. It is therefore extremely important to update products and services as quickly as possible and to install patches according to the manufacturer's recommendations and instructions. You should also make a regular and proactive effort to find out about any new product vulnerabilities. Many manufacturers provide their customers with various channels to access the relevant information. These include information published on their website and subscribing to RSS feeds or email newsletters. In this way, details of new vulnerabilities can be incorporated into a company's vulnerability management process without delay and security loopholes can be closed.

[84] PSIRT Advisories FG-IR-21-186 (fortiguard.com)

[85] PSIRT Advisories FG-IR-22-300 (fortiguard.com)

[86] OWASP Top Ten (owasp.org)

4.5 Data leaks and data management

Data security remains a challenge for businesses and individuals in 2023. This applies to data controllers (who hold data and store it or have it stored), to all providers involved in storing data in any form, and to those individuals to whom the data relates. Although the issue is gaining attention, and awareness is therefore growing, data leaks are still a regular occurrence in the context of cyberattacks. Criminal actors are increasingly eschewing the classic technique of data encryption and extortion in favour of extorting money from victims simply by obtaining data and threatening to publish it (see section 4.2). Attacks on third-party vendors can also result in critical data leaks. In such cases, it may be difficult for the vendor's customers to obtain detailed information about the incident and the exact impact of the data leak.

4.5.1 From encryption attacks to pure data extortion

In late January 2023, the Canton of Basel-Stadt's Department of Education was the target of a cyberattack by the BianLian ransomware group.[87] Around 1.2 terabytes of illegally obtained data were published on the dark web in May due to non-payment of the ransom. Contrary to BianLian's usual practice, the department's systems remained unencrypted.

This case illustrates a change in strategy among some ransomware groups, which are increasingly relying on data extortion alone, rather than double extortion,[88] which has been the dominant tactic in recent years. After exfiltrating the data, they then refrain from encrypting the systems, on the assumption that just publishing the data would be damaging enough to force the victims to pay up. It became clear in the first half of 2023 that victims of ransomware attacks only involving encryption are becoming increasingly unwilling to pay ransoms.[89] Improved security awareness and corresponding measures (e.g. offline backups),[90] as well as efforts by IT security service providers to supply decryption software, are among the factors contributing to this.[91]

Ransomware groups are financially oriented actors. Cyberattacks with encryption entail significant effort and expense, not least because of the victim follow-up involved: the criminals have to establish contact with the victims, conduct negotiations and potentially assist them with decryption after payment. By simplifying the business model, cybercriminals can reduce their own costs and invest time in additional attacks. Cl0p's exploitation of a vulnerability in the document transfer software MOVEit[92] for a mass compromise (see section 4.4.1) exemplifies the change in approach: by the end of June 2023, the names of around 500 affected organisations had been published on the Cl0p leak site. The stolen data includes information from around 30 million individuals worldwide. Handling such a wide-ranging attack with

[87] Grosser Cyberangriff – Kinder betroffen: Daten des Basler Erziehungsdepartements gehackt (srf.ch)

[88] In a double-extortion cyberattack, the data theft is coupled with encryption of the data in order to blackmail the data owners and/or sell the data. A ransom is demanded on the one hand for decrypting the data and/or backups, and on the other hand for deleting or not publishing the stolen data.

[89] Big Game Hunting is back despite decreasing Ransom Payment Amounts (coveware.com)

[90] Improved Security and Backups Result in Record Low Number of Ransomware Payments (coveware.com)

[91] BianLian, for example, switched to a "data theft only" approach after an IT security company published a free decryption program for the BianLian encryption software in early 2023.

[92] Critical vulnerability in file transfer software "MOVEit": apply patch quickly (ncsc.admin.ch)

encryption would involve a lot of effort and expense for the cybercriminals. Even if only a few victims pay the ransom demanded, the approach is still financially attractive for the group.

Where data is obtained without encryption, the victim is still technically able to operate. However, a leak of sensitive corporate and personal data can mean reputational damage and a violation of data protection rules. Furthermore, such data can be used subsequently for other criminal purposes. Even after the ransom is paid, there is no guarantee that the data will actually be deleted and not published or resold. However, some victims try to cover up the incident by paying the ransom.

Conclusion/recommendation:

Increasingly, some actors are shifting their focus away from data encryption to pure data theft with extortion. Precautionary measures can reduce the damage caused. Users should therefore be made aware of the issue and given training in accordance with internal guidelines. With a positive error culture, internal processes can be optimised in cooperation with employees before data leakage occurs.

Clean data management

General rule: Categorise data according to its required level of protection and protect it appropriately based on these categories. Data requiring protection should be stored in encrypted form wherever possible.

Retention rules (5 Ws): Determine **who** stores and processes **which** data in **what form, where,** and with **whom** it is shared. Only data that is necessary for business operations should be retained. The deletion of obsolete data or data that is no longer actively required should be checked periodically. Digital offline archiving of data may also be considered.

Statistical measures

Data sets: Statistical data sets, e.g. from surveys, or data used for testing purposes should be anonymised or pseudonymised. It is also a good idea to store the identifiers separately and in encrypted form. The raw data should ideally be stored separately in an offline backup.

Technical measures/cyberhygiene

Password management: Implement a password policy and multi-factor authentication.

Observe the principle of least privilege.

Implement network segmentation.

Patch management: When vulnerabilities are identified, implement the necessary patches as quickly as possible, taking into account product life cycles.

Organisational measures

Develop and test an emergency incident response plan with clear responsibilities.

In the event of a data leak, technical emergency measures must be implemented as quickly as possible and, if necessary, external specialists called in. Coherent and transparent communication, both internally and externally, is recommended. Ideally, a communication strategy should be prepared in advance.

You should also ascertain which individuals and organisations need to be informed about the data leak promptly, taking into account the new Data Protection Act (in force from 1 September 2023). If data security has been breached, the Federal Data Protection and Information Commissioner (FDPIC) must be notified quickly.

4.5.2 Data leaks from cyberattacks *on* and *through* the supply chain

Organisations and companies often procure services and capital goods from third-party vendors or suppliers. In this context, cyberattacks can take place *on*[93] or *through*[94] the supply chain. Given the increasingly interconnected nature of business processes and the continuous growth of digitalisation, such attacks can result in operational disruptions or interruptions. Aside from the disruption to core business, consequences such as data leaks can also be devastating. Cyberattacks on suppliers often result in the leaking of access details and data relating to their customers. Moreover, compromised supplier systems or software can be used to extract data directly from customers.

The first half of 2023 saw several incidents in Switzerland and internationally in which third-party data was leaked or data was leaked via third parties. In several cases[95] in Switzerland, cybercriminals exfiltrated data from third-party vendors, which they later used either for sale on the dark web and/or as leverage for extortion on leak sites (see section 4.2.1). In addition to the vendors' own information, data from their customers was also leaked because, as IT service providers, they supplied at least parts of these customers' infrastructure. In other countries too, financially motivated actors used data extortion to exert pressure on both suppliers and their customers.[96] The number of affected customers was very high, particularly in connection with vulnerabilities in document transfer software.[97]

[93] In cyberattacks *on* the supply chain, the threat actor focuses primarily on the third-party vendor. However, the supplier's customers may suffer collateral damage.

[94] A cyberattack *through* the supply chain, or supply chain attack, is a combination of two attacks, but the main target of the threat actor is the supplier's customers. While the first attack is directed against a supplier, the second attack uses the supplier's compromised infrastructure to compromise the main victim, namely the customer.

[95] National incidents included:

- CH Media/NZZ: Cyberkriminelle veröffentlichen erneut Daten von CH Media (chmedia.ch); Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet (nzz.ch)
- "Schweizer Revue" printing house: Data leak affects 425,000 Swiss Abroad (swissinfo.ch)
- Xplain AG: Federal Administration also impacted by Xplain hack (admin.ch)

[96] International incidents included:

- Capita: UK pension funds warned to check on clients' data after Capita breach (therecord.media)
- Alliance Healthcare: Cyberattack cripples Spanish drug giant Alliance Healthcare (cybernews.com); Un ciberataque impide […] medicamentos […] a las farmacias (elpais.com)
- Managed Care of North America: Nearly 9 million people affected by data breach from cyberattack on dental insurer (therecord.media)

[97] See Progress Software and MOVEit vulnerability (section 4.4.1) and Fortra and GoAnywhere vulnerability: Summary of the Investigation Related to CVE-2023-0669 (fortra.com)

Conclusion/recommendation:

Supply chains pose a major challenge for cybersecurity and require active risk management. In the event of a data leak, assessing the impacts is highly resource-intensive. In addition to secure data management measures and good cyberhygiene (see recommendations in section 4.5.1), organisations and businesses should generally share data with third parties on a need-to-know basis only. They should also identify their specific threat landscape and critical risks, and synthesise them in a risk reduction plan which they update regularly, reviewing all business areas according to their criticality with regard to supplier and service dependencies. Based on this risk profile, a right to audit third-party vendors and an obligation to report incidents should be contractually stipulated, especially in cases of high criticality. Smaller organisations or businesses can contact associations or specialist consultants for assistance with an independent review.

Technical measures to monitor your own systems are also important so that logins and other activities can be analysed and countermeasures taken in the event of irregularities. This means ensuring that connection and communication channels between suppliers and your own organisation are optimally protected. Organisations should also develop, continually update and test an emergency plan. The exercise scenarios should, among other things, take into account supplier relationships and indirect effects of data leaks.

4.6 Website hacking

Hacked websites can be exploited for a variety of purposes. As well as the placement of political messages (see section 2.2), content for search engine optimisation (see section 3.5.1) or phishing pages, they can also be used to spread malware. If such unauthorised changes are detected by security researchers or other individuals, they usually try to inform the website operator so that the website can be cleaned up. Often, however, the relevant contacts are not easy to find on websites, or are not even listed. To address this issue, the Internet Engineering Task Force (IETF) has developed a standard according to which website operators should store key contact details in a text file called "security.txt" in the predefined directory "/.well-known" on the website.[98]

Recommendations:

Include your security contact on your website.[99]

Protect your website in line with NCSC recommendations.

[98] RFC 9116 – A File Format to Aid in Security Vulnerability Disclosure (ietf.org)

[99] Include your security contact on your website (ncsc.admin.ch)

Notifications to website operators per week

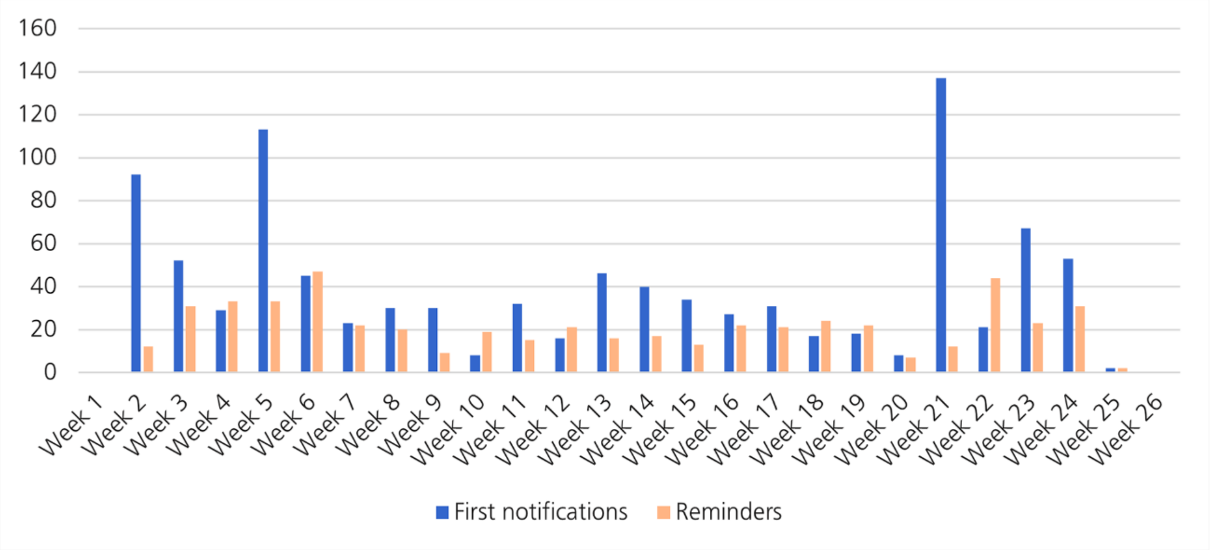


Fig. 10: NCSC notifications to website operators concerning websites that have been hacked or modified without authorisation.

4.7 Update on Ukraine

The first half of 2023 saw the first anniversary of Russia's invasion of Ukraine on 24 February 2022. The last two semi-annual reports dealt with activities observed in cyberspace in the context of this war up to the end of 2022.[100]

Key developments since the start of 2023

Actors linked to the Russian state are particularly active in espionage as well as sabotage. These activities primarily involve the distribution of malware via email in order to gain initial system access. Phishing campaigns are also used to obtain login details for certain systems from victims. These activities were mainly observed in Ukraine, but other countries – mostly Ukraine's allies and NATO members – also reported espionage campaigns.

For the most part, hacktivist groups carry out attacks designed to disrupt the availability of websites (DDoS attacks). Pro-Russian hacktivist groups choose target countries primarily on the basis of whether they offer support to Ukraine or impose sanctions on Russia. These activities have been repeatedly observed outside Ukraine, mainly in EU countries and/or NATO member states. Switzerland was itself targeted by pro-Russian hacktivist group NoName057(16) for over a week in early June, in the run-up to the Ukrainian president's address to the Federal Assembly via video link on 15 June 2023.[101] While the attacks by these groups caused only marginal damage, they are exploited for propaganda purposes.

[100] See semi-annual report 2022/1 (ncsc.admin.ch), section 3;
semi-annual report 2022/2 (ncsc.admin.ch), section 5.6.

[101] See section 2.1.

Future developments

There is nothing to suggest a decline in malicious cyberactivity linked to the Ukraine war. As long as the war continues, Russia will most likely continue to engage in cyberattacks and exploit all opportunities to achieve its goals, whether combined with activities at other operational levels or not. The actions of hacktivist groups represent an important risk factor for the future. A number of groups have said that they intend to launch even more destructive attacks than the DDoS attacks seen to date. So far, no group has demonstrated the necessary competencies to achieve these new goals, but if this were to happen, the extent of collateral damage could increase.