2 November 2021 | National Cyber Security Centre NCSC

Semi-annual report 2021/1 (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/content

Management summary

The National Cyber Security Centre's (NCSC) second semi-annual report deals with the most important cyberincidents of the first half of 2021 in Switzerland and internationally. The main topic is dedicated to vulnerabilities in IT systems that can be exploited to carry out cyberattacks.

Vulnerabilities in hardware and software make welcome attack targets if the vulnerable components are not updated promptly with patches. The MS Exchange Server vulnerabilities as well as Sonic Wall, PrintNightmare and QNAP NAS are just a few examples that are highlighted in the current focus topic.

Expanding vulnerability management

The NCSC is expanding vulnerability management so that security vulnerabilities can be disclosed in a coordinated manner on a single platform (coordinated vulnerability disclosure), but also to give those who discover security vulnerabilities the opportunity to report their findings anonymously to a public authority. In addition, the public is informed about critical security vulnerabilities that are in circulation and receives support in the form of appropriate security measures. In order to detect security vulnerabilities, the NCSC provided close support in the first half of 2021 for the test phase of the infrastructure for the Covid certificate and the first bug bounty pilot programme in the Federal Administration.

Most common reports of fraud

In the first half of 2021, the majority of reports to the NCSC again concerned various forms of fraud. In particular, CEO fraud, fake support calls and classified ad fraud were reported very frequently. Investment fraudsters are currently luring people with promises of enormous profits when investing in cryptocurrencies. The NCSC's contact point received a total of 10,234 reports of various cyberincidents during the reporting period. This is almost twice as many as in the first half of 2020. The reasons for this sharp increase are twofold: firstly, the introduction of the NCSC's new reporting form and its prominent placement on the homepage and, secondly, several large waves of attacks involving fake sextortion and phishing.

Increase in reports of ransomware and phishing

The high number of reported incidents involving encryption Trojans, i.e. ransomware, is also striking. The number has tripled from 32 cases in the first half of 2020 to 94 cases in the current reporting period. Qlocker ransomware, which mainly targeted private individuals and QNAP network storage devices, was behind the majority of these cases.

The NCSC also recorded a significant increase in phishing reports. While in the first half of 2020, 497 reports of phishing were submitted via the reporting form, in 2021 there were 2,439 reports in the same period. This represents an almost fivefold increase. This was mainly due to the higher number of reports of emails and text messages with bogus parcel notifications, which have increased significantly in recent months.

2 Editorial

Participative security – working together successfully for cybersecurity

Dear reader,

Cybersecurity has evolved. Years ago, it was a specialised discipline in the field of IT that mainly dealt with the protection of data and systems. Businesses were happy to have employees who took care of these aspects. They usually only stood out when a firewall hindered the functioning of a system. Occasionally, the entire firewall was deactivated when such incidents occurred, since it only seemed to get in the way and nothing had ever really happened.

Fig. 1: Marcel Zumbühl, CISO of Swiss Post Group and Co-President of ISSS

Those days are over! Cybersecurity has become a mainstream risk for all businesses and institutions, and beside management, even boards of directors are now forced to address it. It has become an economic factor in a networked digital world. Customers now critically ask whether they can trust a given digital service and whether the respective business takes the issue seriously. What's more, cybersecurity is not a discipline in which only large corporations need to be fit. In Switzerland, it is precisely the smaller and medium-sized businesses that have become the target of criminals, because they see a chance to make a quick buck and believe that they will meet little resistance. The fraudsters count on the fact that businesses are afraid of negative press and also of being exposed publicly.

Fortunately, the tide is turning in this respect as well. We have learnt that successful cyberattacks are first and foremost criminal acts. What matters is not whether we should have protected ourselves better, but that the culprits are found and prosecuted. We have learnt that we must not blame the victims but rather the perpetrators. We have also learnt that we should not make ransom payments to the perpetrators of extortion attacks in hope of protecting our reputation. Not least because businesses that pay extortion money are asked to pay again in 80% of cases, as a recent study by Cybereason shows.

When it comes to cybersecurity, we have to learn to network. The buzzword of the hour is "participative security". Businesses are learning that cybersecurity is not a matter for a niche department, but is a natural part of application and system developments. In agile DevSecOps development models, for example, developers play a decisive role. At Swiss Post, a team of dedicated “Security Champions” promotes the topic of security in all crucial projects.

And it is not only the communities inside a business that help to advance security; those outside also play their part. Circles of trust and exchange platforms between security experts from different organisations have always existed, and it often happens that experts are networked in more than one exchange group. Together, ideas and best practices emerge, experts learn from each other and are thus always one step ahead of the attackers.

Collaboration with ethical hackers is a relatively new phenomenon and brings the participative security approach to a higher level. Businesses invite hackers to put their online services through their paces and attack them. Those who find a loophole are rewarded. Swiss Post has been using this participative security approach since 2019 and the programme is accessible worldwide. It is not only online services, such as the "Webstamp" digital stamp and the Swiss Post app, that are kept at a high level of security in this way. Now, digital health systems and electronic voting services also benefit from this new technique of error detection and elimination. It is clear that we can detect and eliminate errors at an early stage in collaboration with internal and external experts. All software has bugs, but we do our utmost to find them in good time.

Switzerland's National Cyber Security Centre (NCSC) provides invaluable services in this participative security network. The Confederation's experts help businesses such as Swiss Post to identify and avert threats in good time and to learn from other organisations. The NCSC's reports are essential reading for all security experts and I would like to take this opportunity to thank the NCSC for their great commitment to Switzerland's participative security.

Marcel Zumbühl, CISO of Swiss Post Group and Co-President of ISSS

3 Focus: Vulnerabilities

3.1 Prominent vulnerabilities in the first half of 2021

3.1.1 Microsoft Exchange: ProxyLogon

The security firm Volexity detected attacks exploiting several vulnerabilities in Microsoft's Exchange Server software earlier this year.[1] This prompted Microsoft to release an out-of-band security update on 2 March 2021.[2] The following day, US security authorities warned of ongoing attacks via these vulnerabilities by Chinese state actors.[3]

The attack chain in question consists of four previously unknown vulnerabilities. Both the critical vulnerability, which is at the start of the attack chain, and the attack chain as a whole are titled "ProxyLogon".[4]

The attack chain affected Microsoft Exchange Servers 2013, 2016 and 2019 and required a connection to the Exchange Servers port 443, which is responsible for secure HTTPS connections. The attack chain begins with the exploitation of a vulnerability that enables server-side request forgery (SSRF): this allows attackers to send arbitrary HTTP requests and authenticate themselves as Exchange Servers. The vulnerability was classified as critical, as it enables the other vulnerabilities to be exploited downstream.[5] The severity of the three other vulnerabilities was rated as high because they allow code execution on the victim's infrastructure, as well as file reading and writing.[6]

Exploiting this attack chain allows attackers to bypass authentication and impersonate an administrator. It is thus possible to take complete control of the Exchange Server and read and manipulate email traffic, calendar data, contact details and tasks. Exchange Servers frequently also function as domain controllers for authenticating computers and users in the network. Therefore, they represent a high-value target for attackers.

After it was revealed in March, the attack chain was not only exploited by other state actors, but also increasingly misused by criminals to spread ransomware, among other things.[7] In some cases, actors simply placed a web shell, and thus a backdoor, on vulnerable systems in order to still have access after any updates that fix the vulnerabilities, and to be able to carry out attacks at a later stage. This made it necessary for system operators to analyse logs and conduct forensic investigations, in addition to updates, in order to find and remove such web shells. The US Department of Justice even authorised official interventions on victims to

---

1 See Operation Exchange Marauder (volexity.com) and ProxyLogon (proxylogon.com)

2 On-Premises Exchange Server Vulnerabilities Resource Center (microsoft.com)

3 Mitigate Microsoft Exchange Server Vulnerabilities (cisa.gov); see also section 4.6.2 below.

4 ProxyLogon (proxylogon.com)

5 NVD – CVE-2021-26855 (nist.gov)

6 For more information on the two post-authentication file write vulnerabilities and the deserialization vulnerability, see NVD - CVE-2021-26857 (nist.gov), NVD - CVE-2021-26858 (nist.gov) and NVD - CVE-2021-27065 (nist.gov)

7 For example DearCry (fraunhofer.de), also known as DoejoCrypt, and BlackKingdom (fraunhofer.de)

combat these attacks.[8] In Switzerland, hundreds of unpatched servers were found to be vulnerable to such attacks in early March. The NCSC informed the affected companies and strongly recommended that they update their systems and check if they had been compromised.[9]

Recommendations:

In order to better protect Exchange Server infrastructures, the NCSC generally recommends implementing the following security precautions:

- Exchange Servers must not be directly accessible from the internet. Either place a WAF (web application firewall) upstream or place an SMTP filtering proxy in front of the Exchange Server.
- Create a process for the emergency installation of security updates and ensure that updates can be installed within a few hours. This applies primarily to all systems that are directly accessible from the internet.
- Use life cycle management to ensure that you only use versions for which the manufacturer (in this case Microsoft) provides security updates.
- Monitor all Exchange Server log files closely, collect them in a SIEM (security information and event management) system and search them for unusual patterns.
- Set up two-factor authentication for all users on all systems.
- Use a dedicated management framework for high privilege access to Exchange Servers.
- Record all Active Directory logs centrally and analyse them regularly.
- Increase the visibility of your endpoints by using an endpoint detection and response (EDR) tool.

For more information and recommendations, please visit our websites:

Exchange vulnerability 2021 (govcert.admin.ch)

Vulnerability in Exchange servers (ncsc.admin.ch)

Microsoft closes further Exchange Server vulnerabilities (ncsc.admin.ch)

3.1.2 PulseSecure and SonicWall

On 20 April 2021, critical vulnerabilities were discovered in two remote access products that affected the manufacturers PulseSecure and SonicWall. The NCSC provided the public with information about the threats and issued recommendations.[10]

---

8 Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities (justice.gov)

9 Exchange vulnerability 2021 (govcert.admin.ch); Vulnerability in Exchange servers (ncsc.admin.ch); Microsoft closes further Exchange Server vulnerabilities (ncsc.admin.ch).

10 Critical zero-day vulnerability in PulseSecure and SonicWall products (ncsc.admin.ch)

PulseSecure: The security service provider FireEye reported advanced attacks in which a previously unknown vulnerability in a PulseSecure product was exploited, and indicated that twelve different types of malware were spread via this route.[11] The vulnerability in question allows unauthenticated persons to remotely execute arbitrary code via the SSL VPN product PulseSecure Connect. While initially only a workaround existed to address this problem, PulseSecure then published a patch for the vulnerability in question as well as for three other security vulnerabilities on 3 May.[12] However, researchers found that the patch did not completely close the gaps.[13] PulseSecure made a tool available on 16 June to check the integrity of software installations.[14]

SonicWall: A number of vulnerabilities were also found in SonicWall Email Security which, when used together, allowed administrative access and code execution on the target system.[15] FireEye reported that the vulnerabilities were being exploited to compromise corporate networks.[16] SonicWall released patches on 20 April 2021.[17]

Conclusion/recommendations:

Due to their functionality, vulnerabilities in products that allow remote access offer very high potential for misuse.

Two-factor authentication should be set up for all login credentials. Single-factor credentials (username/password combination) offer insufficient protection and should be prevented by technical means.

Remote access products must be configured in such a way that both successful and failed access attempts are logged. Remote access services must also be monitored so that unusual activities can be detected and appropriate countermeasures can be taken within a reasonable time frame in the event of misuse.

3.1.3 Accellion

The Accellion File Transfer Appliance (FTA) file sharing software was close to the end of its life when it was attacked by players associated with Clop ransomware in December 2020.[18] The attackers used various vulnerabilities to gain access to the data of up to 320 Accellion customers[19] and threatened to publish it on the dark web if no ransom was paid. The victims across several countries included large institutions such as the Reserve Bank of New Zealand

11 Check Your Pulse (mandiant.com) and Re-Checking Your Pulse (mandiant.com)
12 Pulse Security Advisory: SA44784 - 2021-04 (pulsesecure.net)
13 Technical Advisory: Pulse Connect Secure (nccgroup.com)
14 Pulse Secure Article: KB44755 - Pulse Connect Secure (PCS) Integrity Assurance (pulsesecure.net)
15 Critical zero-day vulnerability in Pulse Secure and SonicWall products (ncsc.admin.ch)
16 Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise (mandiant.com)
17 Security Notice: SonicWall Email Security Zero-Day Vulnerabilities (sonicwall.com)
18 Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion (mandiant.com)
19 Accellion FTA Attack Customer FAQs (accellion.com)

and the Office of the Washington State Auditor. Even six months after the incident, victims are still being reported regularly; an unsavoury end to a product's career.[20] Accellion's announcement of the vulnerabilities and the corresponding patches apparently reached its customers too late.[21]

Conclusion/recommendation:

Software in use must be kept up to date at all times. This applies to both suppliers and users. If it is foreseeable that the manufacturer will no longer support a product, the process to replace it should be initiated immediately. This ensures that the new solution will neither be delayed nor have to be organised and implemented under time pressure. The use of software after its end of life or end of support dates poses a high security risk for companies and private individuals.

3.1.4 PrintNightmare

On 8 June 2021, Microsoft released a security update to close the PrintNightmare vulnerability in the printer queue (known as print spooler).[22] Shortly afterwards, further vulnerabilities that likewise affected the print spooler were discovered.[23] In particular, the vulnerabilities found could also be used by attackers for lateral movements in networks. Ransomware actors took advantage of this opportunity too.[24] Until Microsoft was able to publish special security updates, it was recommended to deactivate the print spooler on systems that were not used for printing. This typically includes domain controllers and many server systems.[25]

The NCSC informed the general public about the threat and issued recommendations.[26]

Conclusion/recommendation:

In order to reduce the attack surface, standard services should generally be deactivated on systems that do not need them. This should be included as part of processes for hardening systems when they are installed.

---

20 Accellion Announces End of Life (EOL) for its Legacy FTA Product (accellion.com)

21 Accellion FTA vulnerability: the notifications in question (lemagit.fr)

22 CVE-2021-1675 – Security vulnerability in Windows print spooler (microsoft.com)

23 CVE-2021-34527 – Security vulnerability in Windows print spooler (microsoft.com)

24 Ransomware: Now attackers are exploiting Windows PrintNightmare vulnerabilities (zdnet.com)

25 CVE-2021-1675: Incomplete Patch and Leaked RCE Exploit (sans.edu)

26 Critical vulnerability affecting the Windows Print Spooler service of Microsoft systems (ncsc.admin.ch); Patches available – Critical vulnerability affecting the Windows Print Spooler service of Microsoft systems (ncsc.admin.ch).

3.1.5 QNAP NAS

Users of network attached storage (NAS) systems from the Taiwanese company QNAP were the target of attacks with the Qlocker ransomware from April 2021 onwards.[27] The attackers exploited a critical vulnerability[28] for which QNAP provided an update on 16 April 2021. However, numerous users installed this update late or not at all. Several Swiss victims, mainly private individuals and SMEs, reported such incidents to the NCSC.

The NCSC informed the general public about the threat and issued recommendations.[29]

Conclusion/recommendations:

Network storage devices are often connected directly to the router in home networks and may therefore be exposed, depending on the configuration.[30]

NAS systems should never be directly accessible from the internet. In both business and home environments, it is important to avoid this and instead access these resources via a VPN with two-factor authentication.

Under no circumstances should the management interface be exposed to the internet.

Data and backups stored on NAS systems must also be backed up (additionally offline).

3.1.6 Dell BIOSConnect vulnerabilities

On 24 June 2021, researchers from the security firm Eclypsium published several vulnerabilities in Dell's SupportAssist program.[31] This software is pre-installed on most of Dell's Windows devices and enables, among other things, firmware updates and the recovery of important functions in the event of a hard disk failure or damage. The problem is said to affect 129 models and thus over 30 million devices. The vulnerabilities would allow attackers to control the device's boot process and thus bypass the operating system and higher-level security controls. However, the attackers would first have to compromise the network in which the computer is located and also obtain a trusted certificate. Finally, they would additionally have to rely on a local user to actively initiate the update or recovery.[32]

---

27 Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices (bleepingcomputer.com); QNAP late to secure NAS against Qlocker attacks (heise.de).

28 NVD – CVE-2020-36195 (nist.gov); SQL Injection Vulnerability – Security Advisory (qnap.com)

29 Week 16 in review (ncsc.admin.ch); Week 17 in review (ncsc.admin.ch)

30 The reason why you shouldn't connect QNAP NAS directly to the Internet without any protection (qnap.com)

31 Eclypsium Discovers Multiple Vulnerabilities in Dell BIOSConnect (eclypsium.com)

32 DSA-2021-106: Dell Client Platform Security Update for Multiple Vulnerabilities in the BIOSConnect and HTTPS Boot features as part of the Dell Client BIOS (dell.com)

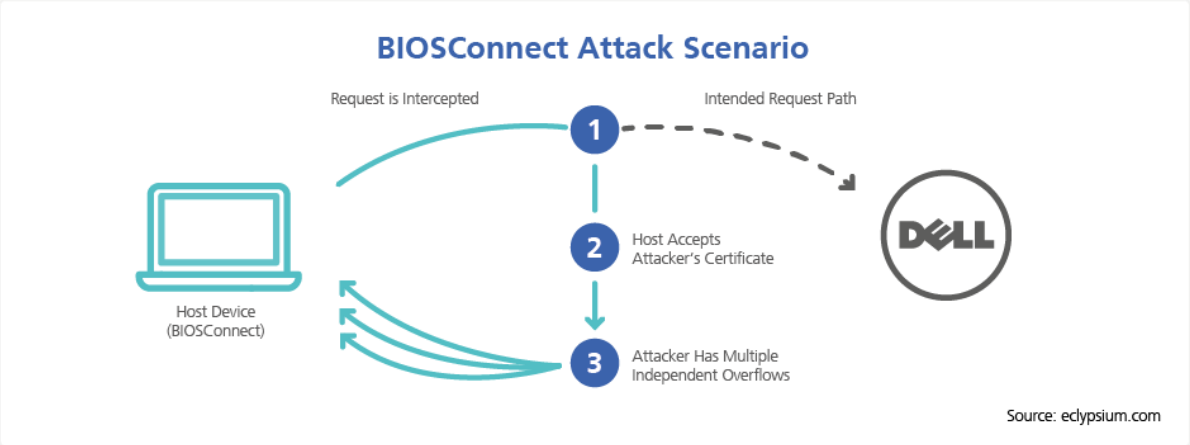


Fig. 2: The connection to Dell's server is intercepted.

Conclusion:

These vulnerabilities were probably not widely exploited because the attack depends on many conditions. It is worth noting that vulnerabilities at this level allow any security measures on the endpoint device to be evaded, as they are not activated until after start-up. However, in compromised corporate networks, such vulnerabilities can lead to a large number of end devices being infected.

3.1.7 BadAlloc

Security researchers from Microsoft's Section 52 team discovered several vulnerabilities related to memory allocations.[33] Since each of these involves bad allocation of memory, this series of vulnerabilities has been dubbed BadAlloc. By provoking buffer overflows, attackers could execute malicious code on the target device or force it to crash. A lack of input validation was identified as the cause.

Microsoft, in cooperation with the US Department of Homeland Security (DHS), informed the various manufacturers of vulnerable devices so that they could fix the vulnerabilities and provide updates.[34] However, since the affected systems include real-time operating systems in industrial facilities and (certified) medical devices, securing them is not a trivial matter. If these systems are cleanly separated from surrounding systems in line with recommended practice, attackers should be prevented from exploiting the vulnerabilities.

33 "BadAlloc" – Memory allocation vulnerabilities could affect wide range of IoT and OT devices in industrial, medical, and enterprise networks (microsoft.com)

34 ICS Advisory (ICSA-21-119-04) – Multiple RTOS (cisa.gov)

Conclusion:

Already during the programming phase, attention must be paid to the implementation of security measures (security by design). Otherwise, an enormous amount of time and effort will be required for remediation of vulnerabilities, assuming this is even possible.

3.2 Software management: inventory and update processes

Cyberattacks can take place not only via vulnerabilities but also through software supply chains. In these attack scenarios, the perpetrator intervenes in the software production or update process, which then causes compromised software to be distributed via regular channels. Most of the time, the compromised software is easy to detect once such an attack is known, but this is not always the case. During the global response to the SolarWinds compromise[35], companies had to check which version they were using and whether they were affected. However, the software was installed by original equipment manufacturers (OEMs) in some cases and end users were not aware that the software was part of the product they were using.

This complexity is also evident in the case concerning Codecov. On 15 April 2021, the manufacturer of a software audit tool informed its customers about a security breach concerning its Bash Uploader product.[36] The corresponding script is used by thousands of customers and is also integrated in various programs, which is why it is difficult to identify who is actually affected by this incident.

In order to respond appropriately to an incident, system and network operators need to keep an up-to-date inventory. This applies not only to hardware, but also to the software and dependencies present in their environments. Maintaining such an inventory is demanding, must be done on an ongoing basis and requires appropriate resources.

In view of the increasing complexities of hardware and software, as well as the advancing digitalisation of society, it is not least software dependencies that pose a major challenge to the security of companies. In recent years, the US National Telecommunications and Information Administration (NTIA) has been working with partners to develop a Software Bill of Materials (SBOM).[37] Similar to food, where the ingredients used to make the final product must be declared, the SBOM would require digital products to state which components were used to make the final product. On 12 May 2021, the US government published the Executive Order on Improving the Nation's Cybersecurity,[38] which specifically mentions the SBOM in the chapter on improving the security of the software supply chain.

Increasing the transparency of digital products is a means of keeping track of the products used and their dependencies. However, the increasing complexity and wealth of information

---

35 See NCSC semi-annual report 2020/2, section 4.7.2

36 Bash Uploader Security Update (codecov.io)

37 SOFTWARE BILL OF MATERIALS | National Telecommunications and Information Administration (ntia.gov)

38 Executive Order on Improving the Nation's Cybersecurity (whitehouse.gov)

in this area also require a certain degree of automation in the maintenance of the software inventory and the processing of security advisories that relate to the elements of the inventory.

Currently, security advisories are published in different ways and in different formats: some manufacturers publish them on their websites, for others you have to log into their portal, others send them as PDF files. How the advisories are structured depends on the individual preferences of each organisation.

OASIS Open, a non-profit body for open source standards, launched a discussion on a new format for automation, the Common Security Advisory Framework (CSAF 2.0). This should make it possible to create the necessary security advisories in a standardised and machine-readable way. The aim is to establish a standard for the automated processing of security advisories.[39]

Conclusion:

Keeping and continuously updating an inventory of all hardware and software components is an essential aspect of securing any IT infrastructure. Ideally, an overview of all software dependencies should also be maintained. The introduction of the SBOM would provide this overview, but would additionally increase the complexity of the databases to be maintained. Not least for this reason, a means of automatically recording and processing security advisories for the elements present in the network would be beneficial. CSAF 2.0 developed by OASIS Open could be a possible way of achieving this.

3.3 Vulnerability management from the NCSC's standpoint

IT security vulnerabilities are increasingly in the public eye. The recent attacks on SolarWinds products[40], the vulnerabilities in Microsoft Exchange[41] and those in the printing process of Microsoft Windows[42] show how such gaps are now being exploited by state and non-state actors. Until a few years ago, such attacks were almost exclusively carried out by states with significant offensive cyber capabilities, but today security vulnerabilities are increasingly being exploited by criminals. With the advent of easily accessible and usable criminal services (crimeware-as-a-service) and the vast amount of software in circulation, security vulnerabilities have become a nightmare for IT security managers worldwide in just a few years. The NCSC set up a department to deal with security vulnerabilities. The aims are manifold: to inform, raise awareness and support the public (private individuals, companies, public authorities) about the critical security vulnerabilities in circulation and the corresponding security measures; to provide a bug bounty platform for public authorities to identify possible security vulnerabilities in public IT networks; to open a platform for coordinated vulnerability disclosure to give those

39 Common Security Advisory Framework (CSAF) Website (csaf.io, oasis-open.github.io, oasis-open.org); BSI - Common Security Advisory Framework (CSAF) (bsi.bund.de)

40 See NCSC semi-annual report 2020/2, section 4.7.2 and below section 4.6.1.

41 See section 3.1.1 above and section 4.6.2 below.

42 See section 3.1.4 above

who discover security vulnerabilities the opportunity to report their findings anonymously to a public authority.[43] These are just some of the aims that the NCSC has set itself with the new department, some of which have already been achieved. As security issues related to software and hardware vulnerabilities are expected to increase in the near future, the NCSC's work in preventing, detecting and remedying problems in this area will become increasingly important.

3.4 Federal Administration bug bounty programme

An important pillar of vulnerability management are so-called bug bounty programmes. Ethical hackers are called upon to find vulnerabilities in an organisation's IT systems. For every confirmed bug they find, the successful hacker receives a reward (bounty), based on the severity of the vulnerability (bug).

From 10 to 21 May 2021, the National Cyber Security Centre (NCSC) conducted a bug bounty pilot project in collaboration with Bug Bounty Switzerland GmbH, the Federal Department of Foreign Affairs (FDFA) and Parliamentary Services (PS). A total of 15 ethical hackers commissioned by the Confederation took part in this pilot project. They found ten security vulnerabilities. The project was very successful and the lessons learned are to be incorporated into the implementation of further bug bounty programmes in the Federal Administration.[44]

The pilot project demonstrated that vulnerabilities in IT systems and applications can be efficiently identified and remedied by means of bug bounty programmes. The return on investment was found to be high. A Federal Administration bug bounty programme, operated by the NCSC, makes an important contribution to reducing the Confederation's cyber-risk exposure.

4 Events/situation

4.1 Reports of cyber incidents received – overview

In the first half of 2021, the NCSC contact point received a total of 10,234 reports. This is almost twice the number received in the first half of 2020. Reasons for this sharp increase include the introduction of the new reporting form[45] and its prominent placement on the launch page. But the high number is also due to several major fake sextortion[46] and phishing waves. This is seen primarily in the high reporting numbers around weeks 5 and 16.

---

43 Coordinated vulnerability disclosure (CVD) (ncsc.admin.ch)

44 Successful bug bounty pilot project in Federal Administration (ncsc.admin.ch)

45 NCSC reporting form (ncsc.admin.ch)

46 Information on fake sextortion (ncsc.admin.ch); Stop sextortion (stop-sextortion.ch).

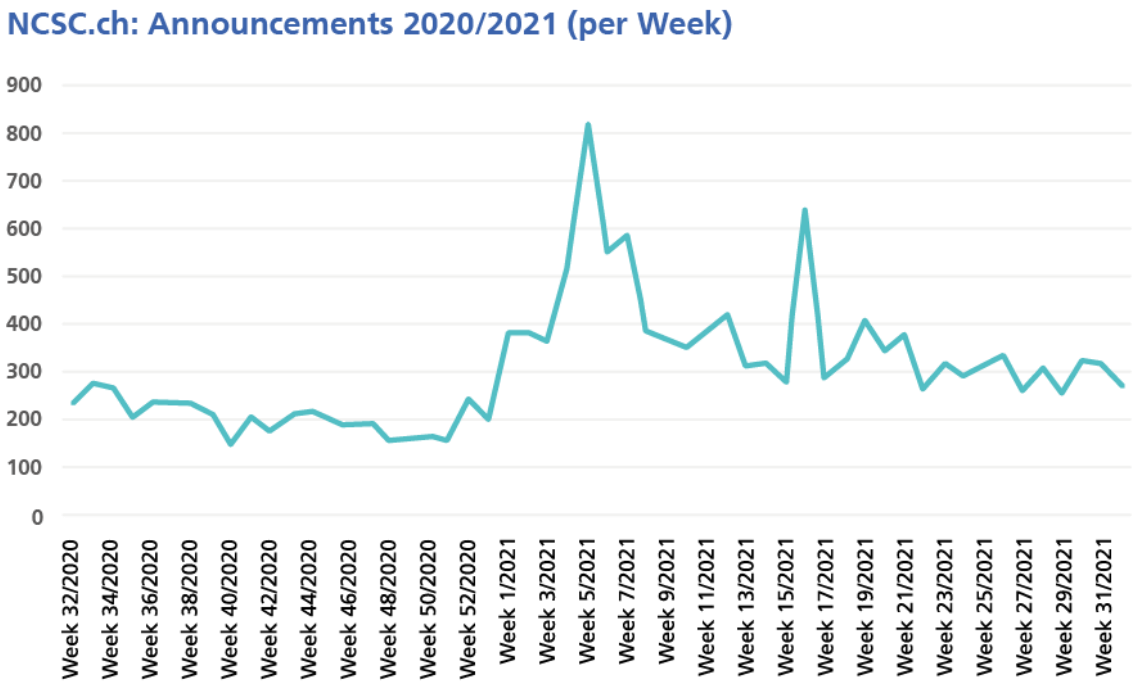


Fig. 3: Number of reports to the NCSC per week from August 2020 to July 2021, see also Current figures (ncsc.admin.ch).

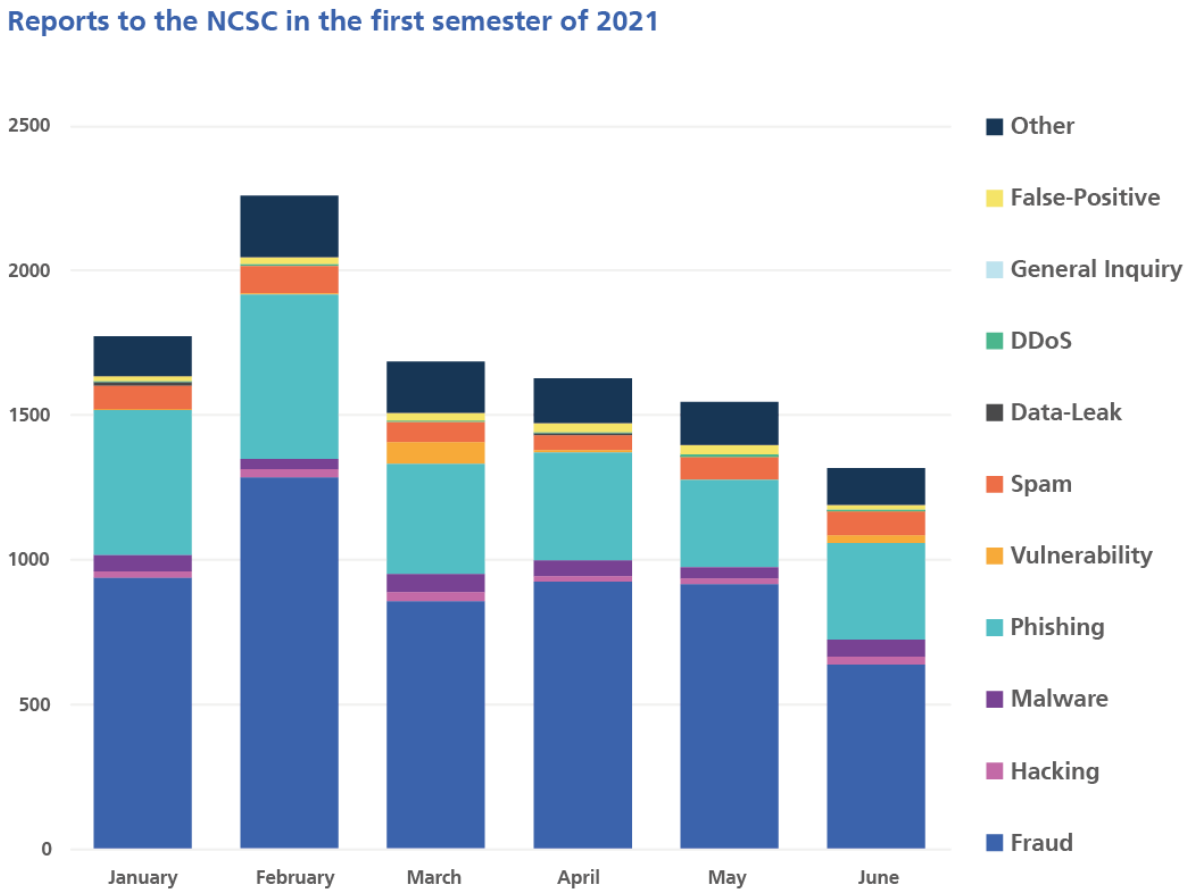


Fig. 4: Reports to the NCSC in the first half of 2021 by category, see also Current figures (ncsc.admin.ch).

4.1.1 Reports of fraud

The main category "fraud" counted 5,526 reports, making up more than half of all reports. Fake sextortion was the most frequently reported scam in the first half of 2021, with 1,351 reports, bumping reports of advance fee scams to second place with 1,284 reports. Advance fee scams[47] had been the most frequently reported phenomenon in the two preceding half-years.

Other frequently reported scams are CEO fraud[48] (239), fake support calls[49] (370), and classified ad scams[50] (307). Alongside the classic variant of classified ad scams involving sales of non-existent goods or failure to deliver goods after payment, the most frequently observed variant involved a bogus request to transfer funds to the buyer or a third party after the sale, such as for arranging transport. There is also a variant where the payment is to be processed via PayPal. A fraudulent email is then sent with a bogus PayPal sender claiming that fees have to be paid before the transaction can be performed.

Investment fraud[51] is an offence typically involving high damage amounts. A total of 252 cases were reported to the NCSC, of which 38 cases resulted in a financial loss. Examples of current approaches can be found below in section 4.8.

4.1.2 Phishing reports

The NCSC also recorded a sharp increase in the number of phishing reports to the contact point.[52] While 497 phishing reports were filed using the reporting form in the first half of 2020, the number in the same period of 2021 rose to 2,439.[53] The figure thus nearly quintupled. The increase is mainly due to the surge in reporting of emails and text messages with fake parcel notifications in recent months.[54] In these cases, a parcel purportedly could not be delivered, so that a small fee would have to be paid for another delivery attempt. The victim is asked to click on a link and then provide credit card details. In most cases, a large amount is deducted directly from the credit card shortly afterwards. In a similar variant, which was reported 479 times, it is not the credit card data that is requested, but rather customs fees to be paid with Paysafe cards. The purported sender of these emails is usually the Federal Customs Administration (FCA). The numbers of the Paysafe cards enabling the perpetrators to withdraw the money are then to be sent to an email address. What is perfidious about this variant is that the fraudulent email address is hidden behind the official address of the FCA and becomes visible only when clicked. Since these emails and text messages often coincide with online orders, the suspicion sometimes arises that there must be some data leak at the FCA or post office. To date, however, no data breaches have been detected either at Swiss Post or at the

47 Information on advance-fee scam (ncsc.admin.ch)

48 Information on CEO fraud (ncsc.admin.ch)

49 Information on fake support (ncsc.admin.ch)

50 Information on classified ad scams (ncsc.admin.ch); Classified ad fraud – pay despite sale (ncsc.admin.ch).

51 Information on investment fraud (ncsc.admin.ch); see also section 4.8.

52 Information on phishing (ncsc.admin.ch)

53 This figure covers reports on phishing emails received via the NCSC reporting form. These reports are analysed, and the fraudulent links are then forwarded to the antiphishing.ch portal operated by the NCSC. The antiphishing.ch figures (see section 4.7.1 below) therefore encompass the figures from the NCSC reporting form.

54 See Week 11 in review (ncsc.admin.ch), Week 23 in review (ncsc.admin.ch) and section 4.7.2.

Federal Customs Administration. The reason why such messages are received while waiting for a parcel has more to do with statistical factors. There has been a real boom in online orders, particularly in COVID-19 times. Since the outbreak of the pandemic, criminals have also caught on to this and have stepped up the sending of bogus parcel notification emails and text messages. It is therefore not at all unlikely that an actual order and a fraudulent notification coincide in time.

4.1.3 Malware reports

The high number of reported incidents involving encryption Trojans – also referred to as ransomware – in the first half of 2021 is also striking. The number tripled from 32 cases in the first half of 2020 to 94 cases in the current reporting period. This is primarily due to the Qlocker ransomware, which mainly targeted private individuals using network attached storage devices of the QNAP brand (see section 3.1.5 above). With its 39 cases, Qlocker was by far the most reported ransomware. Many people also detected and reported emails with malicious attachments or suspicious links (see also the following chapter).

4.2 Malware

4.2.1 Spread of malware

The most common way to spread malware is still by email. Malware can be attached directly to email messages, or it may be downloaded and installed by opening an attached file, or the email may link to a website where a malicious file is downloaded or a drive-by infection[55] occurs. Using social engineering[56], recipients are tricked into performing actions that result in the installation of malware.

A computer or network is typically infected in several phases. First, the attackers aim to achieve an initial infection. The initial malware is often widely distributed via large-scale malspam campaigns, such as AgentTesla, Lokibot, and FormBook in Switzerland over the past half year. Such malware typically serves as a door opener, often collecting information about the infected system and reloading its own function modules or other software/malware as needed. Access to infected devices is then traded in the underground market by cybercriminals.

The following figure shows malware families that were analysed and identified by the NCSC over the past half year. The analysed files and codes originate from various sources such as sensors, reports from security officers of critical infrastructures, citizens, and SMEs. The reported files and codes are analysed and assigned to a malware family. The NCSC shares the identified indicators of compromise (IOCs) with critical infrastructure operators so that they can protect themselves.

[55] See section 4.3.2

[56] See section 4.7

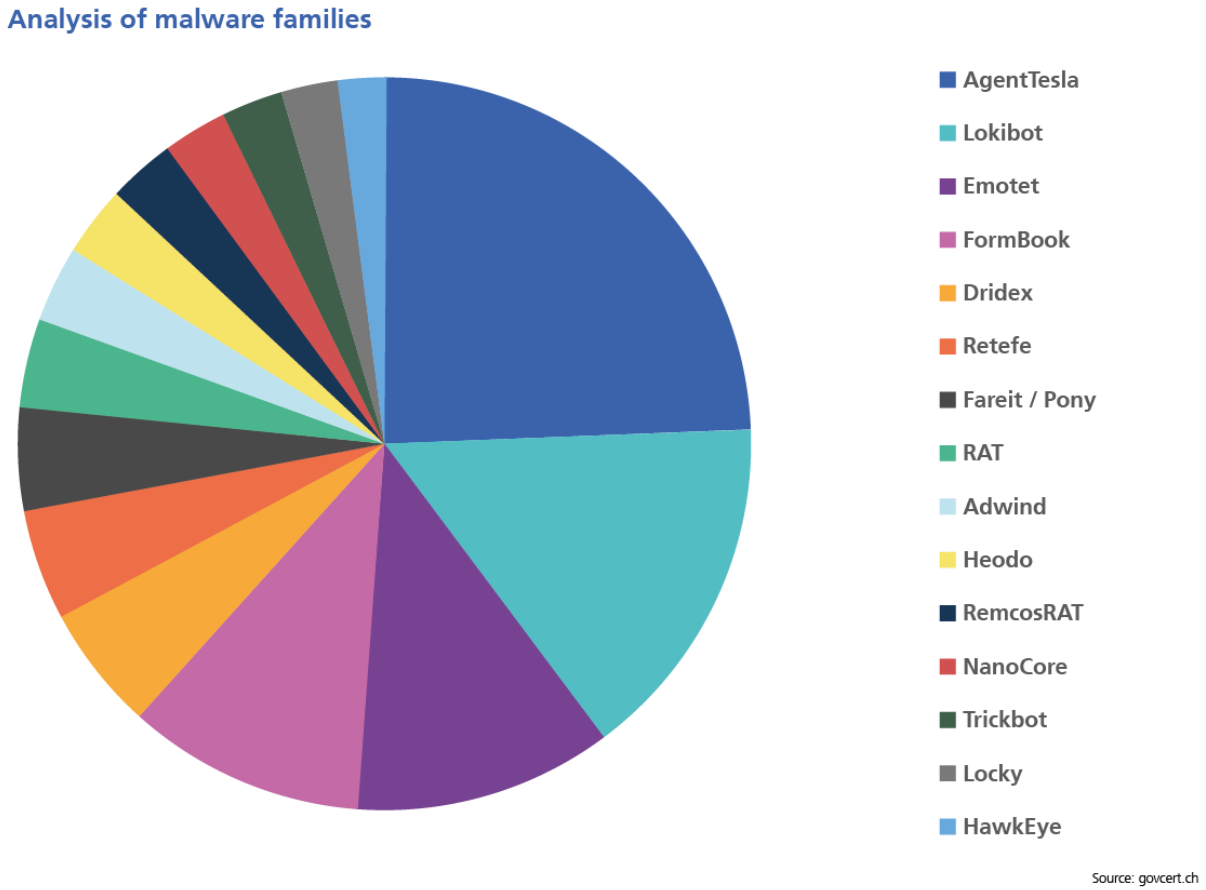


Fig. 5: Analysis by the NCSC of malware families in Switzerland in the first half of 2021.

After law enforcement authorities dismantled and shut down the Emotet infrastructure at the beginning of 2021,[57] other malware families are (again) increasingly coming into play. Alongside well-known names such as TrickBot, Retefe, Dridex, and Qbot, some of the currently observed malware families, such as IcedID, were previously less common.

In February 2021, a major malspam campaign was observed in which the DocuSign brand was misused and TrickBot was spread via malicious Excel files. This was the first major TrickBot wave since October 2020. The emails and documents used for the widespread campaign were written in English and very generic.

The malware QBot (also known as QakBot and QuakBot) is installed via SilentBuilder, a malicious macro in Excel documents. The NCSC received reports of several cases in which maliciously prepared Excel documents passed through several security layers unnoticed and were then opened by the end users. The perpetrators employed a variety of social engineering techniques to convince recipients to open the attached Excel file and to activate the macro. As soon as the computer is infected, a Cobalt Strike Beacon[58] is installed which grants the

[57] See World's most dangerous malware EMOTET disrupted through global action (europol.europa.eu) and NCSC semi-annual report 2020/2, section 4.3.2.

[58] See section 4.2.2

attackers interactive access to the system and consequently allows them to perform reconnaissance and lateral movements and to extend permissions.

A sharp increase in the dissemination of IcedID has been observed since March – also in emails written in German.[59] IcedID has since been observed especially in ransomware infection chains, in which IcedID is spread using web contact forms to send messages to the target company, referencing Google links or Google Sites respectively and from there infect companies with Cobalt Strike.[60] In this way, the attackers gained control of the network and were then able to encrypt data using ransomware.

Retefe is spread in a different way: Usually, publicly available telephone numbers (e.g. on company websites) are called, and the recipient of the phone call is tricked into opening a Google link, which then triggers the installation of Retefe.[61]

Recommendations:

- Check how your security products support the detection and/or blocking of documents that contain macros. Make sure that this is done in archive files as well.
- Where possible, block the file types enumerated in this NCSC list.
- In your network, allow only digitally signed macros to be executed and verify which applications can be executed from which path (e.g. using AppLocker).
- Make sure that your internal network is sufficiently patched. Make sure that, for instance, no domain controllers are still susceptible to the Zerologon vulnerability (CVE-2020-1472).[62]
- Increase visibility at endpoints using an EDR (endpoint detection and response) tool and/or Sysmon (system monitoring).
- Raise the awareness of your employees so that they recognise suspicious messages and phone calls and know how to react.
- Establish internal processes for reporting to security officers.

The figure below shows data from DNS sinkholes. DNS sinkholes are used to render malware harmless by removing the associated domain names from the access of criminals and reregistering them to a security organisation. In this way, infected devices can be identified, since they no longer connect to the servers of the malware operators but instead to the servers of the security organisation. The NCSC collects and analyses this data for the entire Swiss IP address space and informs the users of these devices of the infection via ISPs.

59 Aufstieg von IcedID (computerworld.ch)

60 Investigating a unique "form" of email delivery for IcedID malware (microsoft.com)

61 See Malware after call (ncsc.admin.ch); Aktuelle Ransomware-Angriffe mit Pakettrick (infoguard.ch).

62 CVE-2020-1472 (mitre.org); NVD - CVE-2020-1472 (nist.gov); What is Zerologon? (trendmicro.com).

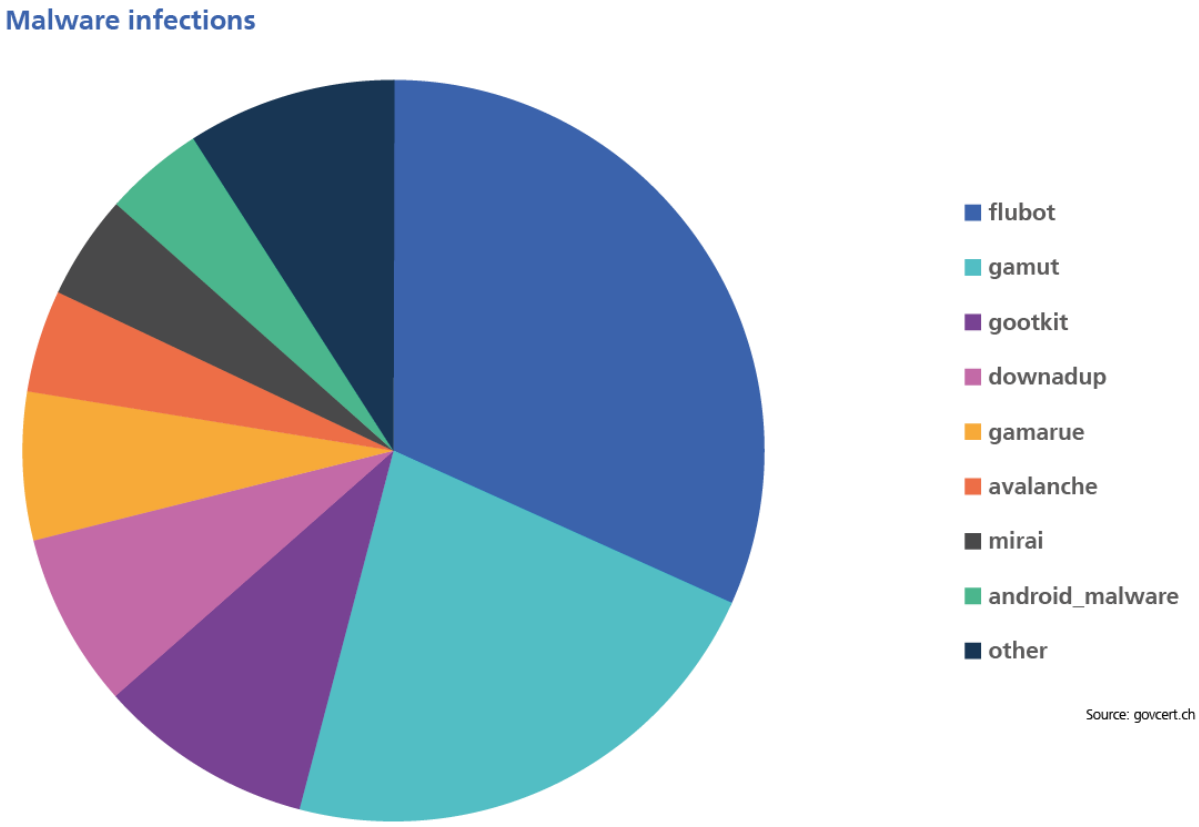


Fig. 6: Partition of malware infections in Switzerland detected by the NCSC in the first half of 2021.

In the first half of the year, the Flubot malware spread throughout Europe by way of major text message dissemination campaigns. After an initial focus on Android smartphone users in Nordic countries and the UK, the threat reached Switzerland and Austria in June.

There are several scenarios for dissemination of text messages containing a Flubot-infected link. In Switzerland, a text message written in German notifies the user of a supposed voicemail message. Users clicking on the link are asked to initiate a download which then installs the malware on the device.[63]

Fig. 7: Example of a text message with a Flubot link.

63 Das SMS "Neue Voicemail" ist die gefährliche Schadsoftware FluBot (cybercrimepolice.ch)

Flubot can layer itself over other apps ("overlay attack") and in that way spy on the e-banking activities of the victim, for instance. It can also spread as a worm via the victim's contact list, automatically sending the same text message to all contacts. This explains the rapid dissemination of the threat in the countries affected.

The NCSC informed companies and the public about Flubot.[64]

Recommendations when receiving suspicious SMSs and other text messages

- Do not click on links sent by unknown senders.
- Delete SMS or other message.
- If an app was installed:
  - restore factory settings on the phone,
  - inform mobile service provider,
  - block credit cards,
  - reset access to bank, crypto and email accounts.

4.2.2 Dual-use software Cobalt Strike

The commercial security testing tool Cobalt Strike was developed to simulate an advanced persistent threat (APT) in the network, to perform corresponding activities, and to test the detection and defence capabilities of network administrators. Of course, such a tool can also be used by real attackers. Pirated copies of Cobalt Strike are popularly used by criminals and state actors to move and spread in systems after a successful infection. Cobalt Strike is also used by criminals to extract data and then deploy ransomware. Using Cobalt Strike, state actors can make it harder to detect or attribute targeted espionage attacks.

4.2.3 Ransomware

Ransomware – also known as encryption Trojans – disrupts business processes and restricts the ability of companies to operate. This can have far-reaching consequences, from production outages and delivery stops to bankruptcy. Customers who depend on the services of the attacked company can also be adversely affected.

Criminals often use a double or even triple extortion tactic.[65] Once the criminals have access to the victim's systems, they first copy the data. If the victim refuses to pay the ransom for decryption, the attackers threaten to publish the data. If the victim does not respond to the first two demands, individuals and organisations that have a direct connection to the data, such as contractual partners or customers, are contacted. Sometimes, the criminals additionally launch DDoS-attacks on the affected company to increase the pressure.[66]

---

64 Week 24 in review (ncsc.admin.ch)

65 See NCSC semi-annual report 2020/2, section 4.3.1

66 Extortion Payments Hit New Records as Ransomware Crisis Intensifies (paloaltonetworks.com)

During the reporting period, attacks were perpetrated in Switzerland against private individuals and SMEs in a variety of economic sectors using a wide range of ransomware.[67]

Internationally, several spectacular incidents occurred. In the southeast of the United States, for instance, motorists had to queue up for hours at petrol stations to fill up their tanks for fear of supply shortages:[68] On 7 May 2021, the Colonial Pipeline Company had suspended operations of its oil and gas pipelines after their administrative IT systems had been infected by the DarkSide[69] ransomware.[70] While the control systems used for physical operations of the pipeline were not directly affected by the encryption Trojan, these systems were also shut down as a precautionary measure. Mutual dependencies between the IT and OT environments for the optimisation of higher-level business processes pose major challenges to the self-sufficient operation of industrial control systems. Until now, attacks by specific ransomware families known to target industrial processes, such as EKANS[71] and Mega Cortex[72], had been perceived as the primary threats to industrial control systems. Attention by the media and the authorities caused the DarkSide group to retreat from a large part of its activities.[73] Later, it became known that Colonial paid a ransom, despite the availability of backups.[74] Law Enforcement was able to seize part of the ransom paid during their investigations.[75] This incident, the attack against the major meat processor JBS at the end of May,[76] and other incidents in which cybercriminals interfered with the operation of critical infrastructures have accelerated the US government's efforts to enhance cybersecurity regulations and other efforts.[77]

The Conti ransomware also caused a stir after attacking the Irish Department of Health and the Irish Health Service Executive (HSE).[78] On 13 May 2021, the Irish National Cyber Security Centre (NCSC) gained knowledge of suspicious activities in the network of the Irish Department of Health, involving an attempt at remote access using the Cobalt Strike software.[79] On 14 May 2021, the encryption attempt at the Department of Health was foiled in time, but the HSE fell victim to Conti on the very same day. Large parts of the HSE network were temporarily taken offline as a precaution. Services were accordingly available only to a

---

67 Successful ransomware attacks on Swiss companies (ncsc.admin.ch);
Ransomware-Angreifer erpressen Schweizer Industriefirma Griesser (netzwoche.ch);
Ransomware Angriffe in der Schweiz – was steckt dahinter? (entec.ch).

68 Colonial Pipeline systems resumes operations but Southeast still reeling from panic buying and gas price spikes (washingtonpost.com); Ransomware: Last Week Tonight with John Oliver (HBO) (youtube.com).

69 DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks (cisa.gov)

70 The Colonial Pipeline Hack Is a New Extreme for Ransomware (wired.com)

71 This is how EKANS ransomware is targeting industrial control systems (zdnet.com)

72 See MELANI semi-annual report 2020/1, section 4.3.1

73 DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized (krebsonsecurity.com)

74 Colonial Pipeline CEO: Paying DarkSide ransom was the 'right thing to do for the country' (zdnet.com)

75 DoJ Seizes USD 2.3 million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (justice.gov)

76 JBS: FBI says Russia-linked group hacked meat supplier (bbc.com);
Ransomware: Meat firm JBS says it paid out USD 11 million after attack (zdnet.com).

77 Executive Order on Improving the Nation's Cybersecurity (whitehouse.gov)

78 Department of Health hit by cyberattack similar to that on HSE (irishtimes.com)

79 See section 4.2.2 above on Cobalt Strike.

limited extent; numerous treatments and diagnostic procedures had to be postponed. According to HSE, critical functions in intensive care and emergency treatments were ensured, however. While the perpetrators eventually provided an encryption programme for free, they had stolen patient data from the HSE network and threated to publish it if they did not receive a ransom. Sample data was published as proof.

Successes were also reported in the fight against ransomware, however: law enforcement authorities in Ukraine were able to arrest several members of the Clop ransomware gang and shut down the infrastructure that the group had used for its attacks. Clop has caused financial damage totalling around USD 500 million worldwide.[80]

Conclusions/recommendations:

Ransomware can cause considerable damage, especially if data backups are also affected. In the event of such an incident, remain calm and act with caution. Important aspects of incident management are finding the infection path and preventing a reinfection. Reboot the affected systems and restore data with existing backups.

If the necessary expertise is not available in your organisation, seek support from a specialised company.

The NCSC recommends that victims never pay a ransom. By making a payment, victims confirm the criminals' business model, support them financially, and encourage them to continue and develop their activities. In the worst case, victims will lose both the data and the money. The NCSC advises victims to file a complaint with the competent police authority.

Coverage for cyber incidents through cyber insurance has become increasingly popular in recent years. Such insurance products do have their justification, given that they cover risks including those related to cybercrime and offer good support for issues such as internet commerce, damage to reputation, virus attacks, and data or identity theft. However, if ransom payments are covered by insurance, this can cause blackmailers to focus on insured companies, giving the criminals a greater chance of being paid. The decision for or against cyber insurance is the sole responsibility of the companies. The pros and cons should be well considered. Under no circumstances should the conclusion of cyber insurance lead to a reduction of the IT budget or neglect of the secure IT operations.

Further information is available on the NCSC website: Ransomware (ncsc.admin.ch).

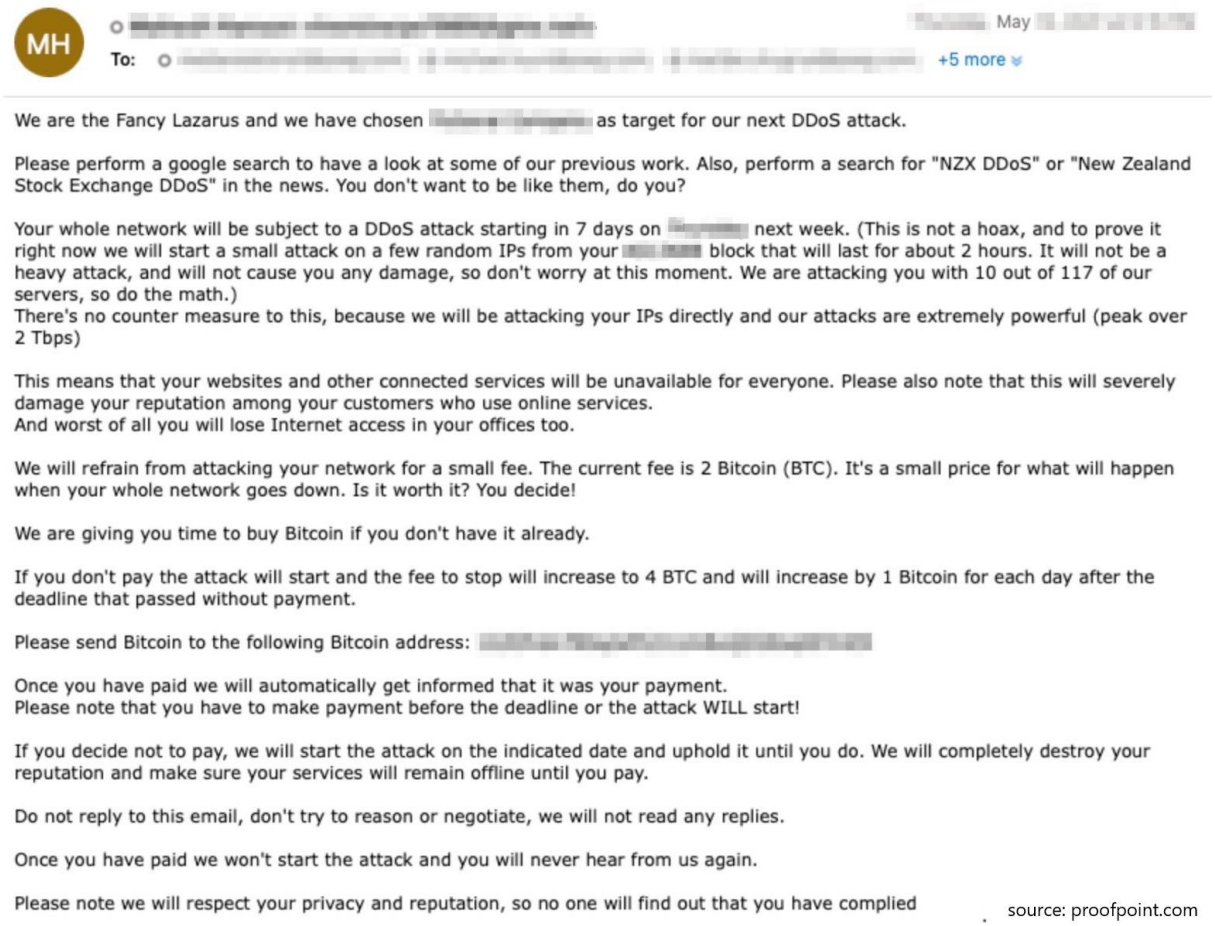
4.3 Attacks on websites and web services

4.3.1 DDoS

As was the case in 2020, distributed denial of service (DDoS) attacks took place in Switzerland and internationally in the first half of 2021. 26 DDoS incidents were reported to the NCSC. The majority of the reports described the following approach by the perpetrators: a considerable

[80] Ukraine arrests Clop ransomware gang members, seizes servers (bleepingcomputer.com)

but basically defensible demonstration attack was launched first (usually between 40 and 120 gigabits per second), followed or preceded by an extortion email demanding a ransom which, if not paid, would be followed by a more massive attack of over 2 terabits per second. This represented a bluff to intimidate the targeted organisations. In the cases observed, the threatened massive attacks were not carried out, even when the ransom was not paid. The attacks targeted organisations in various sectors such as finance, healthcare, and aviation. Several internet service providers were also attacked. However, thanks to the providers' defensive measures, the attacks hardly had any impact on their customers – except in the case of one web hosting provider: In this attack, the websites of the canton, the city, and the police of St Gallen were disabled for several hours.[81] In the past, the blackmailers had appropriated the names of two very well-known state cyber actors (Lazarus and Fancy Bear).[82] During the last wave of attacks, the perpetrators now referred to themselves as Fancy Lazarus.


MH

May

To: +5 more

We are the Fancy Lazarus and we have chosen as target for our next DDoS attack.

Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days on next week. (This is not a hoax, and to prove it right now we will start a small attack on a few random IPs from your block that will last for about 2 hours. It will not be a heavy attack, and will not cause you any damage, so don't worry at this moment. We are attacking you with 10 out of 117 of our servers, so do the math.)
There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.
And worst of all you will lose Internet access in your offices too.

We will refrain from attacking your network for a small fee. The current fee is 2 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to 4 BTC and will increase by 1 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address:

Once you have paid we will automatically get informed that it was your payment.
Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again.

Please note we will respect your privacy and reputation, so no one will find out that you have complied

source: proofpoint.com

Fig. 8: Sample extortion email from Fancy Lazarus.

[81] Hackergruppe greift St. Galler Hoster nicht mehr an (netzwoche.ch)

[82] See NCSC semi-annual report 2020/2, section 4.4.1

In Belgium, a massive simultaneous attack targeted Belnet and other telecom providers in May, resulting in the disruption of internet connections for several hours and – as a domino effect – the interruption of numerous services such as the debates of the Belgian Parliament (held by video conference), online university courses, and the websites of numerous public services.[83]

Conclusion/recommendations:

DDoS extortion is a large-scale business. Attackers try their luck with as many companies as possible in a relatively undifferentiated manner. If they are unsuccessful, they try elsewhere. If they succeed in disrupting a company's systems with a (demonstration) DDoS attack, however, they focus on that company as a potential victim. In the hope that a ransom will be paid, the perpetrators intensify their efforts. It is accordingly advisable to be well prepared for potential DDoS attacks.

The NCSC recommends subscribing to commercial DDoS protection for critical systems. Many internet service providers offer such DDoS mitigation services.

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

4.3.2 Compromising of websites

Attackers can access the website administration with stolen access data or via unpatched security vulnerabilities and place arbitrary code there. One use case is the placement of drive-by infections attempting to infect the devices of website visitors with malware. Other phenomena include redirecting visitors to questionable advertisements, fraudulent websites, or dubious offers. Website access can also be used for Black Hat SEO,[84] i.e. content is inserted on the website to influence search engine results.

When the NCSC detects compromised websites, it informs their operators or webmasters and hosting providers so that they can take countermeasures. In the first half of 2021, 803 initial notifications to that effect and 445 reminder emails were sent to websites in the Swiss domain space (websites ending in .ch or .swiss).

---

83 Belgium's government network goes down after massive DDoS attack (therecord.media)

84 Black hat SEO and You Won (ncsc.nl); SEO stands for "search engine optimisation". This refers to measures to ensure that a website is displayed as close to the top as possible in the results of internet search engines. See Search engine optimization (wikipedia.org).

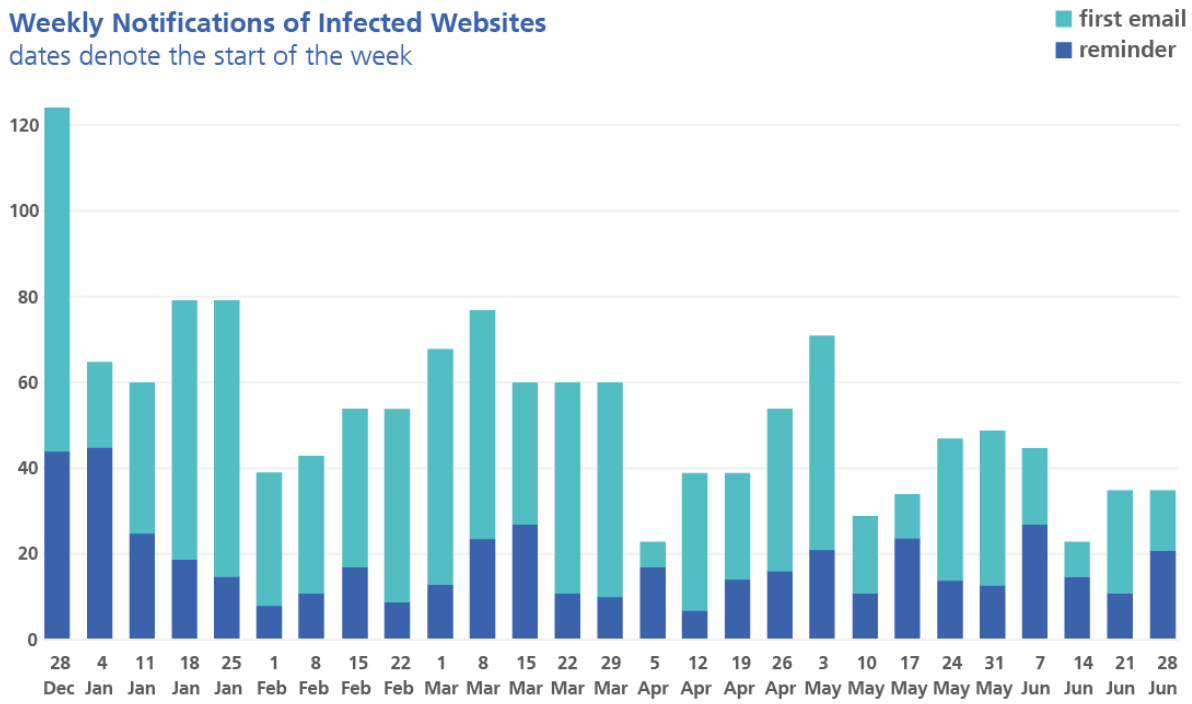


Fig. 9: Notifications sent by the NCSC to website operators and webmasters or hosting providers.

Recommendations:

If a website has been hacked, a systematic clean-up is required by locating and removing the malicious code or external content on the website. Furthermore, the latest versions of the content management system (CMS) and the plug-ins must be installed. All computers used for website administration must be scanned for malware and cleaned if necessary. Finally, all access passwords must be changed. Information is available on the NCSC website:

Hacked website – what next? (ncsc.admin.ch)

After cleaning up the website, additional measures are recommended to prevent cybercriminals from gaining access again in the future. The NCSC website also contains

Measures to secure content management systems (ncsc.admin.ch).

4.4 Industrial control systems and OT

The pandemic and extreme weather conditions have increased the focus on the importance of critical infrastructures in recent months. Many critical infrastructure processes are supported or made possible in the first place by operational technology (OT) and controlled by industrial control systems (ICSs). In addition to environmental impacts and faulty operation, malicious attacks against these systems or connected devices pose a risk to the availability and integrity of critical infrastructures.

4.4.1 RedEcho infiltrates Indian power supply

At the end of February, security researchers at RecordedFuture reported that the actor referred to in the report as RedEcho[85] successfully penetrated systems of several critical infrastructure operators in India. In addition to two ports, power supply organisations – specifically regional load dispatch centres – were among the targets of the series of attacks, which relied on malware including Shadowpad.[86]

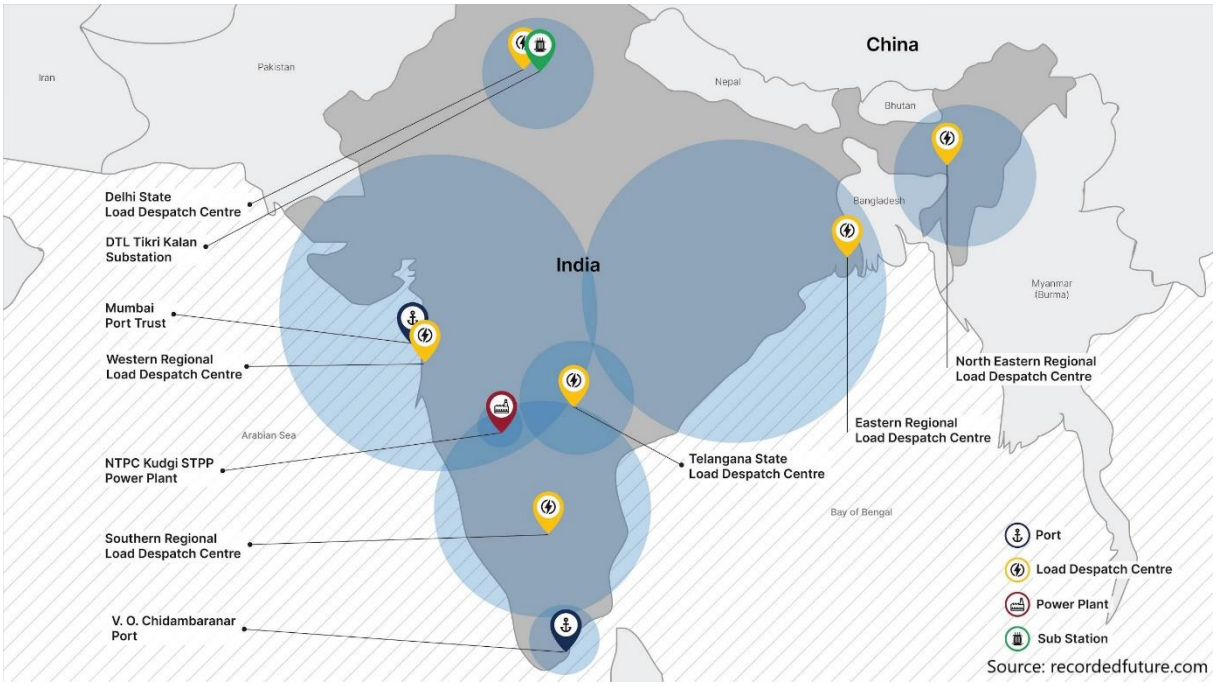


Fig. 10: Targets of RedEcho

In its analysis, RecordedFuture finds no evidence of attempted sabotage, but it does point to the ongoing tensions on the India-China border which were correlated in time. Accompanying coverage in the New York Times[87] raises the hypothesis that the abusive infiltration of these networks might have been intended as a threat. The power blackout in Mumbai in autumn 2020[88] is also mentioned as an example, but a connection with the activities of RedEcho cannot be proven, according to RecordedFuture.

4.4.2 Attempted manipulation of Florida water supply

In February 2021, the mouse cursor of a control computer at the drinking water treatment plant in Oldsmar, Florida, started moving on its own.[89] The technician on duty just managed to intervene as the intruder tried to remotely raise the sodium hydroxide content in the water

85 Chinese Group RedEcho Targets the Indian Power Sector (recordedfuture.com)

86 ShadowPad (Malware Family) (fraunhofer.de)

87 China Appears to Warn India: Push Too Hard and the Lights Could Go Out (nytimes.com)

88 See NCSC semi-annual report 2020/2, section 4.5.1

89 A Hacker Tried to Poison a Florida City's Water Supply, Officials Say (wired.com)

supply to a dangerous level. The city's infrastructure almost met with disaster due to inadequately secured remote access software,[90] which the saboteur used to gain access to the device that operated the drinking water treatment control system.

Information / Recommendations:

To prepare for threats against the process control of industrial control systems, industry associations from the power, water, waste water, gas, and food industries as well as public transport, together with the Federal Office for National Economic Supply (FONES), have drawn up industry standards to provide assistance:

Minimum standards by sector (bwl.admin.ch)

4.5 Data leaks

Data leaks continue to be a concerning phenomenon in the first half of 2021, occurring in a variety of contexts. Besides ransomware groups whose modus operandi now includes threats to release data (see section 4.2.3), data leaks may also occur in the context of espionage operations. In this case, government data or intellectual property data is often affected.

The monetary value of certain types of data – such as medical data, customer or identity data and bank data – makes them preferred targets. But even supposedly less valuable data can be used by cybercriminals for a variety of purposes, e.g. to create scenarios that can then be used to commit fraud via social networks, but also simply to collect email addresses to which targeted or bulk phishing, malware, or scam emails can then be sent.

4.5.1 SITA: Theft of passenger data

Société Internationale de Télécommunications Aéronautiques (SITA), the worldwide leading provider of passenger processing systems for the aviation industry, was the victim of a cyberattack[91] in which the passenger data of several airlines was stolen.

The incident affected the Passenger Service System (PSS), i.e. the servers on which the passenger data of many airlines is stored. In particular, millions of datasets from the frequent flyer programmes of Star Alliance and OneWorld were compromised, including the customer data of 1.35 million participants in Miles-and-More.[92] Swiss is one of the customers of this IT service provider. Although at the time when SITA reported the attack, it appeared that no personal data critical to security had been stolen, Air India was one of the airlines to report five weeks later that the incident had affected 4.5 million of its passengers and that the stolen information also included passport and credit card data.[93]

90 Compromise of U.S. Water Treatment Facility (cisa.gov)

91 SITA statement about security incident (sita.aero)

92 Hacker erbeuten 1,3 Millionen Datensätze von Swiss- und Star-Alliance-Kunden (inside-it.ch)

93 Data Breach Notification.pdf (airindia.in)

4.5.2 Attacks on social networks and data scraping

At the beginning of April, the data of about 533 million Facebook profiles was published on a hacker forum. Users from more than a hundred countries were affected. The data – which included phone numbers, email addresses, full names, dates of birth, and locations of users – had apparently been known since January and was being offered for sale on the underground market. However, the actual data leak probably dates back to an earlier time. Facebook reported that the data leak was likely due to a vulnerability that was remedied in August 2019.[94]

At the end of June, a database containing 700 million LinkedIn profiles was offered for sale on the darknet. The information covering more than 90% of the social network's users apparently does not include credit card or password information. Although users were asked to change their passwords as a precaution, LinkedIn denies that its servers were hacked and claims that this is a case of data scraping.[95]

Large amounts of data can in fact be obtained through data scraping: Content such as telephone numbers and email addresses can be systematically extracted from websites that are publicly accessible using a wide variety of techniques. Such activities are also carried out by companies in various fields, e.g. for marketing optimisation or business intelligence. This includes the Chinese company SocialArks, a data management platform for targeted advertising that collects data from social networking platforms such as Facebook, Instagram, and LinkedIn. This was revealed by a misconfigured server that contained more than 400 GB of public and private profile data of 214 million social media users and a total of 318 million unprotected datasets. In this case, for unexplained reasons, the database also contained data that was not publicly accessible.[96]

Finally, data from various data leaks can be combined into a large information package that is particularly attractive due to its size. This is the case with the Compilation of Many Breaches (COMB), the largest dataset found so far, which contains 3.2 billion email/password combinations from old data leaks of a variety of companies, including Netflix and LinkedIn.[97]

Conclusion/recommendations:

The careful and responsible handling of data is an important topic for companies. In addition to appropriate security measures, every company should also prepare for a data breach scenario and draw up a corresponding response plan in advance. This will enable rapid and coordinated action in the event of an incident.

Internet services that make data collections publicly available should protect their platforms against automated (bulk) queries by taking appropriate precautions.

---

94 Bot Lets Hackers Easily Look Up Facebook Users' Phone Numbers (vice.com);
533 million Facebook users' personal data leaked online (cyberscoop.com).

95 LinkedIn denies exposure of 700 million user records is a data breach (computerweekly.com)

96 The SocialArk Data Breach Uncovered the Open Source Paradox (cybersecurity-magazine.com);
Millions of Social Profiles Leaked by Chinese Data-Scrapers (threatpost.com).

97 COMB: over 3.2 Billion Email/Password Combinations Leaked (cybernews.com)

To protect yourself from scraping as a private individual, you should limit public access to your social profiles and generally think twice about the content you post online.

It is also advisable to pay attention to the settings of the applications you use and not give them more permissions than they need.

Further information is available on the NCSC website: Dataleak (ncsc.admin.ch).

4.6 Espionage

4.6.1 Nobelium: new campaign after SolarWinds

On 27 May, Microsoft published an article about the advanced persistent threat (APT) they call Nobelium, and warning about a new email campaign spreading malware. One of the attacks for which Nobelium is responsible was against SolarWinds.[98] The campaign followed a trial period lasting from the beginning of 2021 until the end of May. During that period, Microsoft observed a series of technical developments in the transmission method of phishing messages and in the profiling of recipients. This ability to constantly innovate and adopt target-specific tools and infrastructures makes Nobelium a highly sophisticated threat and difficult to detect. On 25 May, the campaign used the legitimate mass mailing service Constant Contact, purporting to be a US development organisation and targeting more than 3,000 accounts of 150 organisations, mostly in the United States – in particular NGOs, research institutions, government agencies, and international agencies. The emails referenced foreign threats to the 2020 US elections and included a URL that first directed victims to the legitimate Constant Contact service, which then redirected them to the infrastructure controlled by the group.[99]

4.6.2 Hafnium exploits MS Exchange

In March 2021, Microsoft announced[100] that a group they call Hafnium had exploited several previously unknown vulnerabilities in Microsoft Exchange Servers.[101] Hafnium had already been suspected of using stolen passwords to gain access to Microsoft Exchange Servers and of maintaining access to the networks of the companies and authorities concerned for an extended period of time. The targets included university and research institutions in the field of infectious diseases, law firms, defence companies, think tanks, and NGOs.[102] Hafnium generally exfiltrates data to file sharing websites such as MEGA.[103]

---

98 See NCSC semi-annual report 2020/2, section 4.7.2

99 New sophisticated email-based attack from NOBELIUM (microsoft.com)

100 HAFNIUM targeting Exchange Servers with 0-day exploits (microsoft.com)

101 See section 3.1.1

102 HAFNIUM, Operation Exchange Marauder, Group G0125 (mitre.org)

103 HAFNIUM (Threat Actor) (fraunhofer.de)

4.7 Phishing and social engineering

4.7.1 Phishing

In the first half of 2021, 4,682 phishing websites which had been reported via the antiphishing.ch portal operated by the NCSC were verified. Compared to 4,498 detected phishing websites in the second half of 2020, the level stayed practically the same, with a slight increase.

The NCSC has observed a shift of phishing attempts from major international markets to companies operating on the Swiss market. The current target groups continue to include the financial sector,[104] but also logistics companies,[105] internet providers,[106] and others.

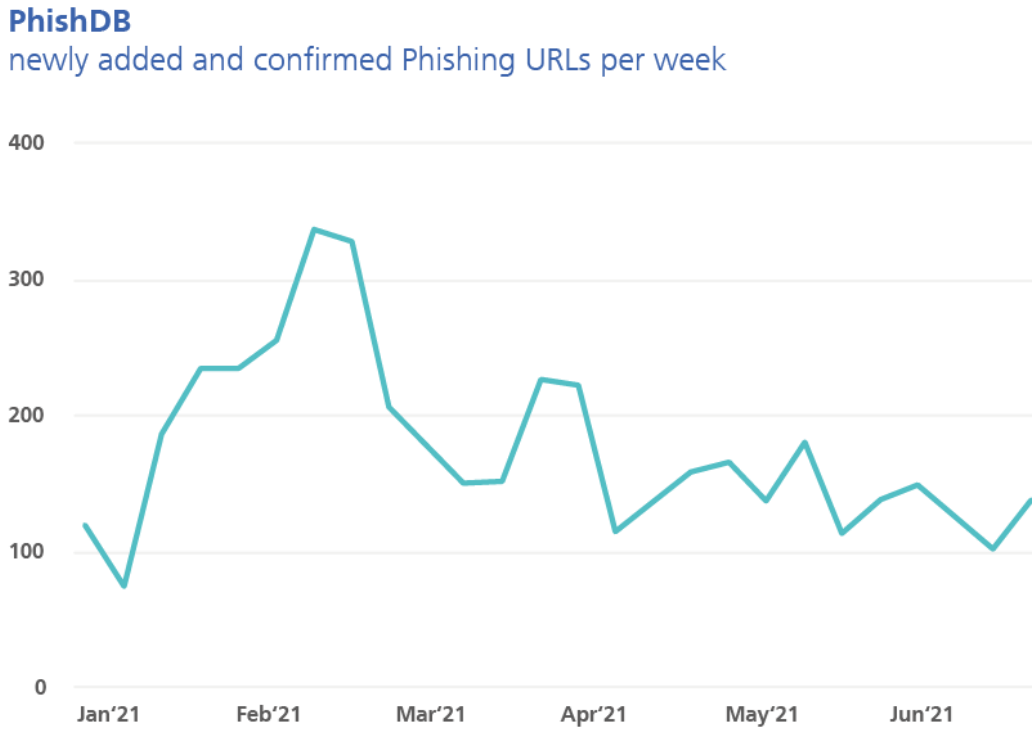


Fig. 11: Number of phishing URLs checked and confirmed by the NCSC per week in the first half of 2021. Current data can be found at: https://www.govcert.admin.ch/statistics/phishing/

Multi-faceted content tactics are used in phishing and other social engineering attacks. As a rule, the topics involve alleged incidents with an everyday reference that are often taken to be real. At first glance, the messages often appear to be from trustworthy and well-known companies, complete with logo, which are misused for these purposes.

---

104 Viseca Phishing Mails - nicht autorisierte Transaktion - Zugriff eingeschränkt (cybercrimepolice.ch)

105 Phishing Mail im Namen der Post - Paket konnte nicht geliefert werden, da kein Zoll bezahlt wurde (cybercrimepolice.ch)

106 E-Mail angeblich von der Swisscom (Schweiz) AG betr. Rückerstattung (cybercrimepolice.ch); attacks against website owners have also continued: Phishing attackers targeting webmasters (govcert.admin.ch).

4.7.2 Smishing

SMSs and other text message services are increasingly also used for phishing – or "smishing".[107] Such messages also appear on mobile phones with everyday content and a link. The link in the message leads to a website specially designed by criminals, on which the user is asked to enter personal data or credit card details.

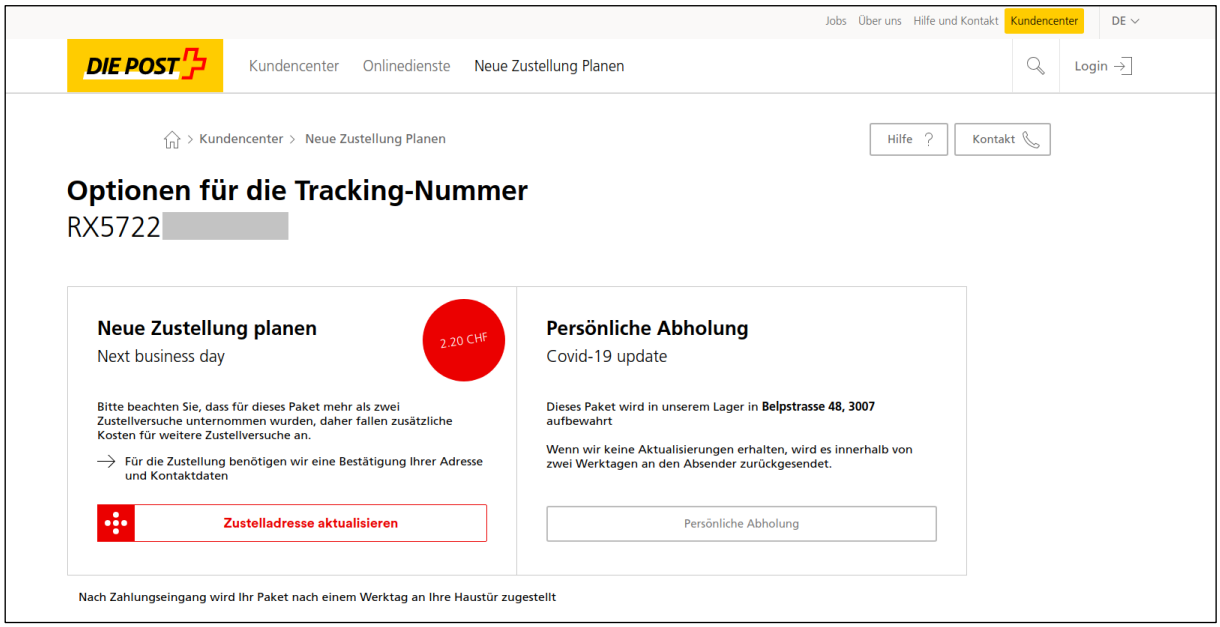


Fig. 12: Example of a spoofed website for the purpose of stealing access data.

4.7.3 Social engineering

There are now a wide variety of malware families that intercept email conversations on infected systems. Criminals may of course also gain access to email conversations through phished access data. As a consequence, more and more emails are being sent to people who were involved in such email conversations. Often, the purported sender is another person from this conversation. The sender's address is either spoofed or the email is sent from a compromised account and, accordingly, from the real address but not from the real person. The email then looks as if it has been resent (now with a prepared attachment) or as if it is a continuation of the conversation. If additional text is inserted, it is (so far) mostly in English and very generic (e.g. "Good day. Please check the attached documents" or "Hello, the attached document contains interesting information"), and any file attachments also have either nondescript names (e.g. "Documentation (60243).xls", "docs_(20210412).xls" or "Application (756.466).xls") or names intended to arouse curiosity (e.g. "CompensationClaim.xls" or "Payroll.xls"). Clicking on such an attachment is the first step towards infection of the device.

107 SMS - Sie haben eine DIE POST-Sendung (cybercrimepolice.ch)

Recommendations:

- Caution is called for with regard to emails and text messages not only from unknown persons, but also from (supposedly) known senders.
- Be suspicious if you unexpectedly receive documents without further comment or if the text of the email message is very generic.
- If you are asked to enable macros when opening a file, report this to your security officers.
- Be sceptical if you receive emails or text messages that are designed to arouse your curiosity or require action on your part (follow a link or open a document). Often, you will be given a deadline to perform this action so as to increase the pressure.
- Do not click on any attachments in suspicious messages and do not follow any links, not even out of curiosity – otherwise, you run the risk of your device being infected with malware or you could end up on dubious websites. In case of any doubt, contact the supposed sender using an already known contact option or one of the ones listed on their website, for example, and ask about the exact nature of the matter and whether they actually sent the email.

4.8 Fraud: Current variants of investment fraud

Most of the reports received by the NCSC concern various types of attempted fraud. One variant is the investment scam or investment fraud. It is very easy to spread such bait advertising via email, websites, and social media. Currently, the hype surrounding cryptocurrencies is being heavily exploited, and scammers promise that high profits can be made in a very short time with small investments in such currencies. In some cases, a deposit is even followed by a (minor) pay-out. However, this is only done to build trust and convince victims to make larger investments.[108]

[108] Krypto Anlagebetrüger ködern Nutzer mit SMS (cybercrimepolice.ch)

Von: Zahlungsüberprüfung
Gesendet: Freitag, 6. August 2021
An: [redacted]
Betreff: Zahlung akzeptiert

Geschätzter Gewinn für August: €6.461,01 BitTraders

Mögliche Gewinne für August:
%-Rücklaufquote:
Startdatum:
End-Datum:

€6.461,01
2431%
03/08/2021
20/08/2021

Wenn Sie heute investieren, können Sie einen Gewinn von 6.461,01 Euro erwarten, wenn Ihre Investition am 03/08/2021 abgeschlossen ist.

Befolgen Sie die folgenden Anweisungen, um zu beginnen.

Profil erstellen
Anweisungen:
Profil erstellen --> Investitionen einleiten --> Sehen Sie, wie Ihr Geld wächst --> Ziehen Sie Ihren Investitionsgewinn auf Ihr Bankkonto ab

Mit freundlichen Grüßen,
BitTraders

Fig. 13: Example of an advertising email with the promise of enormously high profits.

Already in previous years, there were reports regarding bogus online trading platforms and advertising portals, which often used the names of celebrities such as Roger Federer and DJ Bobo. In fictitious interviews, it was claimed that they owed their wealth to cryptocurrencies.[109]

Von: Kronen Zeitung
Gesendet: Dienstag, 6. Juli 2021
An: [redacted]
Betreff: Dietrich Mateschitzs neueste Investition sorgt für Begeisterung bei Fachleuten und Angst bei den Großbanken

Dietrich Mateschitz neueste Investment-Überraschungsexperten und Großbanken.

ÖsterreicherInnen verdienen von zu Hause aus bereits Millionen Euro mit diesem "Vermögensschlupfloch" – aber ist es legitim?

Der österreichische Geschäftsmann Dietrich Mateschitz gibt ehrlich zu, wie er sein Geld verdient und teilt es jetzt mit allen.

aktuelles Interview mit Dietrich Mateschitzs

Lesen Sie die ganzen Nachrichten

Siehe auch
Was ist die deutsche BTC-Ära und wie funktioniert sie?

privacy policy | unsubscribe

Fig. 14: Example of a scam email using the wealthiest Austrian as bait.

[109] See MELANI semi-annual report 2019/2, section 4.4.5

The current variants of investment fraud are described in the NCSC weekly reviews.[110] So that they stand out in the glut of advertising, the scammers currently appear to be outbidding each other with unrealistic returns. In one case, earnings of EUR 12,000 were promised for an investment of just EUR 250, all in 72 hours.[111] The criminals may then even try to defraud the victims a second time by having purported lawyers, notaries, or even law enforcement agencies and regulators contact them after a while and promise to get the money back. In the first stage, a relationship of trust is established and relatively sensitive data such as a copy of an identification document, an IBAN or similar must be provided. In the second stage, "fees" are demanded for the supposed help. In some cases, improvised websites of the purported support organisations are set up to secure the victims' trust.[112]

The danger is of losing large sums of money. One case reported to the NCSC resulted in a loss of over CHF 1 million.[113]

Conclusion/recommendation:

Promises of extraordinary returns in a short time period (and without work) are dubious.

If you have suffered a loss, report it in person to your local police station and file a criminal complaint.

Be careful if you are suddenly offered help by a third party after a case of fraud. In particular, do not make any further payments, including any purported fees, to recover the money you lost.

Further information can be found on the NCSC website: Investment Fraud (ncsc.admin.ch).

The website of the Swiss Financial Market Supervisory Authority FINMA contains Information on authorised financial service providers in Switzerland (finma.ch). Particular caution is required if the financial service provider is not on this list. Check out the financial service provider using online experience reports. FINMA also maintains a non-exhaustive Warning list of companies and individuals who may be carrying out activities that require authorisation without such authorisation and that are supervised by FINMA (finma.ch).

110 Hot topics (ncsc.admin.ch)
111 Week 14 in review (ncsc.admin.ch)
112 Week 21 in review (ncsc.admin.ch)
113 Week 11 in review (ncsc.admin.ch)