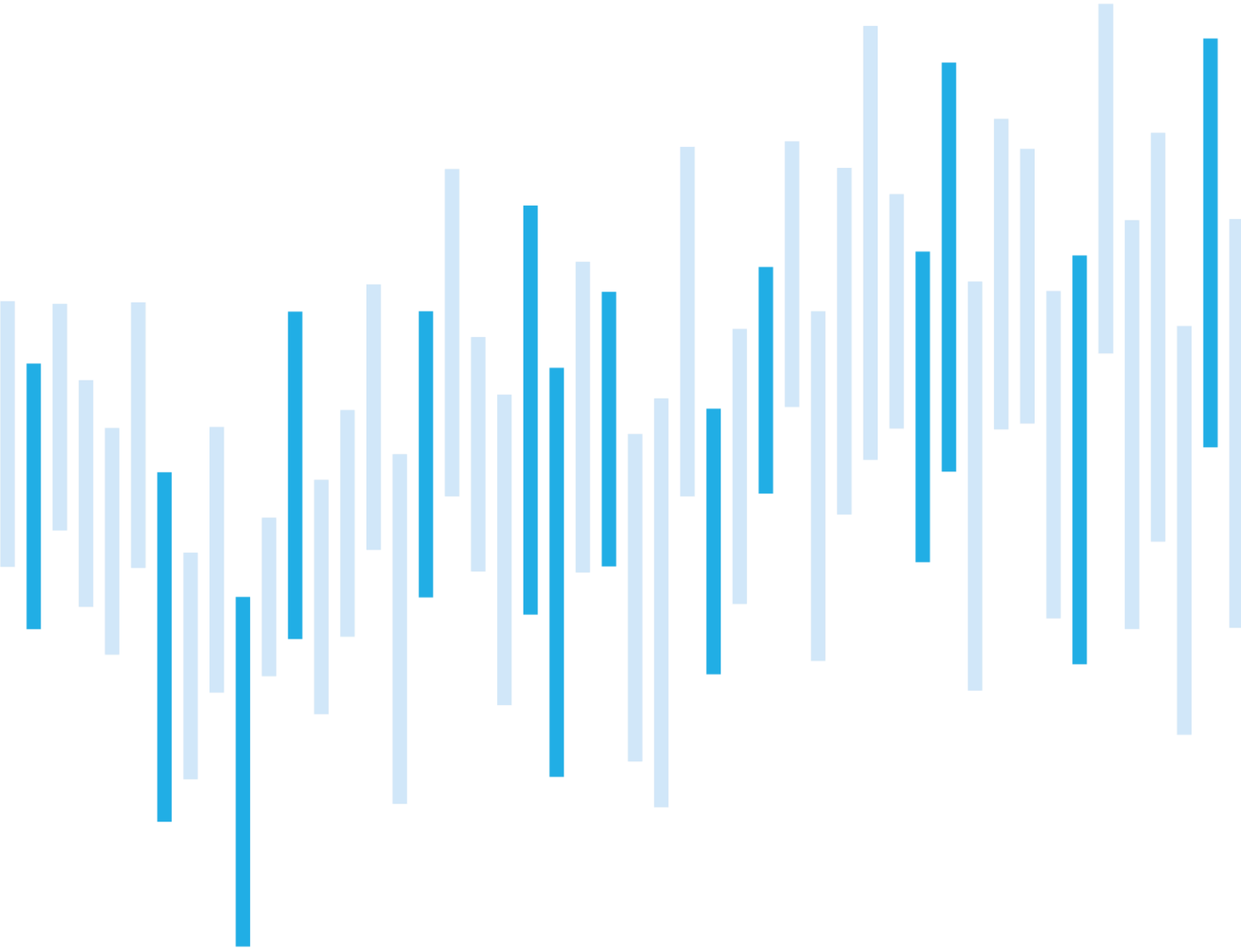
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

MARCH 2022



National
Cyber and Information
Security Agency

Summary of the month

So far, NÚKIB has not registered any Czech cyber security incident provably related to the Russia-Ukraine war. We have been continuously monitoring the situation and evaluating potential cyber threats to the Czech Republic. In line with it, NÚKIB issued a warning in March, associated with the economic sanctions imposed on the Russian Federation.

As in previous months, phishing campaigns and ransomware occurred in the March incidents. Each of these categories amounted to one-fifth of incidents.

The cases of phishing registered by NÚKIB were not exceptional. However, a new Browser-in-the-Browser technique has emerged on the cyber scene, making phishing difficult to detect. It is described in chapter "Technique of the month."

One of the March ransomware attacks differed from the others. In that case, the attacker did not encrypt stations and servers with a malicious code but with a legitimate Bitlocker tool. The last chapter discusses in detail the behaviour of attackers.

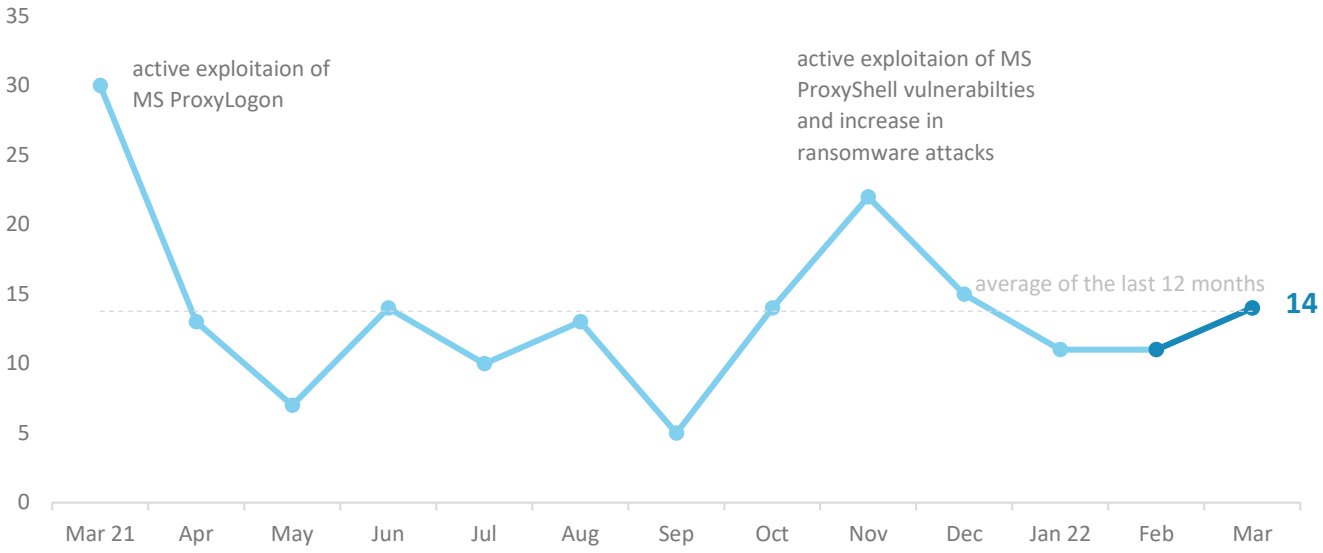
Table of Contents

The following report summarises the events of the month. The data, information and conclusions contained herein are primarily based on cyber incidents reported to NÚKIB. If the report contains information from open sources in some sections, the origin of this information is always stated.

You can send comments and suggestions for improving the report to the address komunikace@nukib.cz.

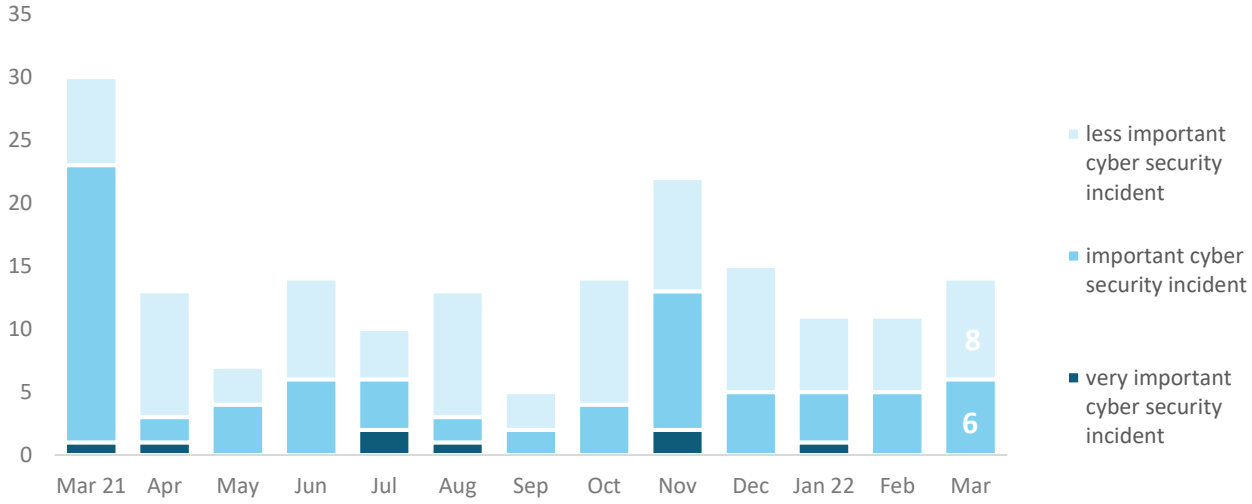
Number of cyber security incidents reported to NÚKIB

Considering the number of incidents, March, with its 14 incidents, was an average month.[1]



Severity of the handled cyber incidents [2]

In terms of the severity of incidents, March was not very different from rest of the months of the past year. None of the incidents had such serious consequences that NÚKIB would assign it the highest possible seriousness; most incidents were of a less serious nature. The ones with more significant impacts mainly included ransomware attacks, which limited functioning of the attacked entities.

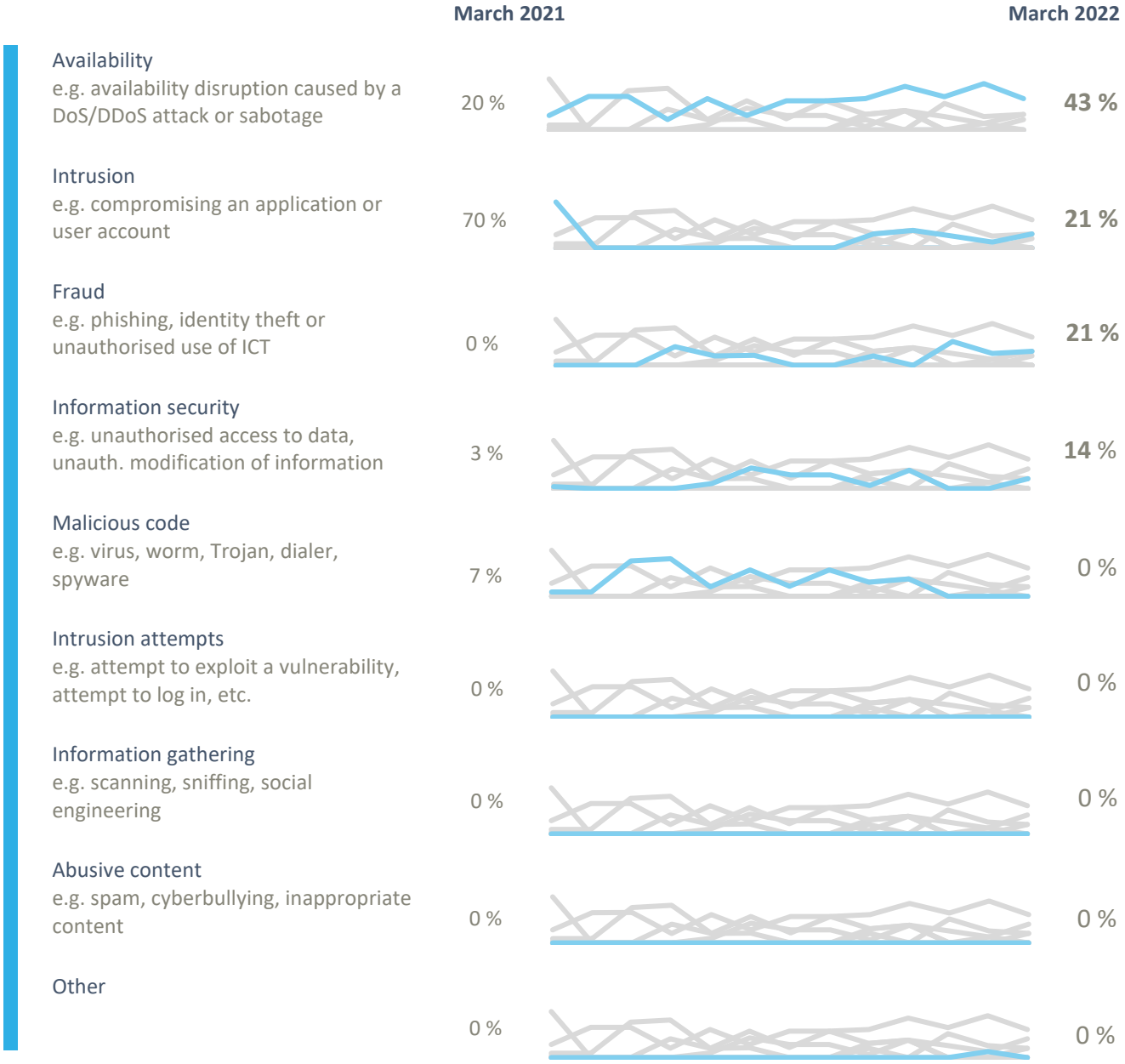


[1] A half of the incidents were reported to NÚKIB by obligated persons according to the Cyber Security Act. The remaining seven incidents were reported by entities that do not fall under this law.
[2] The severity of cyber incidents is defined in Decree No. 82/2018 Coll. and in NÚKIB's internal methodology.

Classification of the incidents reported to NÚKIB[3]

The March incidents were divided into four categories:

- Six incidents resulted in unavailability of services. Half of them were not caused by a targeted attack but a technical error. In two cases, functioning of the organizations was affected by ransomware, which temporarily shut down the infected systems. The last unavailability of the attacked organization's systems was due to a DDoS attack;
- The second and third most common categories were penetrations and frauds. The frauds involved incidents in which unknown attackers compromised mailboxes and sent phishing and spam to other institutions from them;
- The fourth and last category in March was information security. This category also included the last of the three March ransomware attacks, in which the attackers managed to exfiltrate victim's data. The attacker used the so-called double-extortion, threatening the victims not only with the loss of data, but also with their publication.



[3] The cyber incident classification is based on the ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA (europa.eu)

March trends in cyber security from the NÚKIB's perspective[4]

Phishing, spear-phishing, and social engineering

In March, NÚKIB dealt with three cases in which attackers phised mailbox login details and subsequently sent spam and phishing from them. There is a steady trend of last months of phishing accounting for about one-fifth of the incidents handled by NÚKIB (see the "Fraud" chart on p. 3).
In one of the attacked companies, the attacker followed up a historic conversation between the company's employee and client. Then, the attacker contacted the client from a fake e-mail address that resembled the employee's legitimate address and tried to arrange for a change in the bank account to

Malware

Apart from the ransomwares mentioned below, no other malicious code appeared in the March incidents.

Vulnerabilities

In March, NÚKIB began monitoring newly published vulnerabilities in industrial control systems. More than 500 alerts issued in 2021 were examined, and 111 devices located in the Czech Republic accessible from the Internet and potentially vulnerable were discovered. None of these devices was in a regulated system under the Cyber Security Act. Nevertheless, NÚKIB contacted the providers who have these devices in their network and alerted them about the possible vulnerabilities.

Ransomware

As last month, ransomware caused one-fifth of March's incidents. These were carried out by both large organised-crime groups (LockBit) and smaller players targeting small and medium-sized enterprises.
In one of the March cases, the attacker did not use any malicious code to encrypt the data, but the legitimate Bitlocker tool. More information on this attack is available on page 7.

Attacks on availability

The March incidents included one successful DDoS attack, which the attacked entity managed to handle with its own resources. Interestingly, the attack was accompanied by a ransom email, in which the attackers demanded $ 4,000 to stop the attack. They also threatened to publish data. However, no data was exfiltrated from the victim's network; the attackers did not compromise the victim's network at all. The attackers signed the email DarkSide. However, since the DarkSide group has already disappeared, it cannot be ruled out that someone on feeding on its name.

[4] The development illustrated by the arrow is evaluated in relation to the previous month.

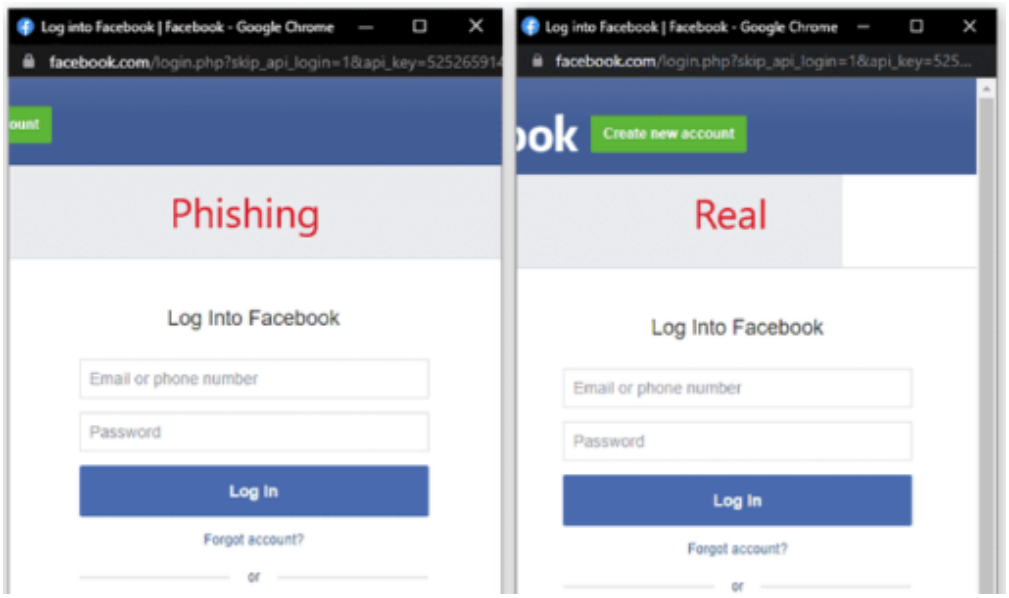
Technique of the month: Browser-in-the-Browser

As in previous months, phishing-related techniques predominated in the March incidents. In March, a new Browser-in-the-Browser technique appeared on the cyber scene in connection, which is difficult for the average user to recognize. In the MITRE ATT&CK framework, the technique fall under T1204.001: User Execution: Malicious Link. So far, it has not appeared in the incidents handled by NÚKIB, but since the attackers have used it in attacks on Ukrainian targets last month, it cannot be ruled out that, given the Czech active support of Ukraine, it will eventually appear in the incidents registered by NÚKIB.

The **Browser-in-the-Browser (BITB)** technique is a phishing method, by which the attackers try to steal victims' login details. Many online services use third-party Single Sign-On for logging in, most commonly Google, Apple, Microsoft, or Facebook, i.e. accounts to which an attacker tries to gain access. Normally, after clicking on a login, a new browser window opens with a field for login details. In the case of Browser-in-the-Browser, however, clicking opens a fake login window that mimics the appearance and behaviour of the browser. It is only an interactive object created using HTML, CSS and Javascript. An attacker can also exploit the code from two-factor authentication in this was, supposing the user has it turned on.

Carefully prepared phishing using this technique can be visually indistinguishable from the authentic login box, including the URL in the address bar of the "window" and the indication of the HTTPS connection, which adds to the plausibility even more (Fig. 1). One cannot even rely on the display of the destination URL when hovering the cursor over the link button as this information can also be forged using Javascript.

Figure 1



Source: Browser In The Browser (BITB) Attack | mr.d0x (mrd0x.com)

Mitigation: BITB can be recognized as follows:

- If you pull the login box out of the currently open browser, a new window will open (Fig. 2). However, in case of BITB, a fake window cannot be moved or enlarged outside the area of the current page (Fig. 3);

Figure 2

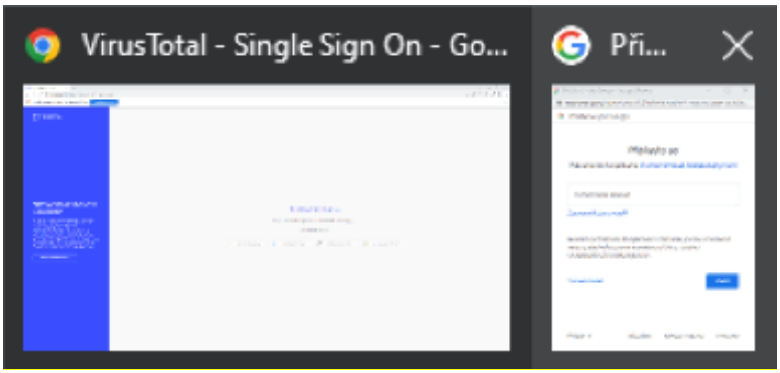
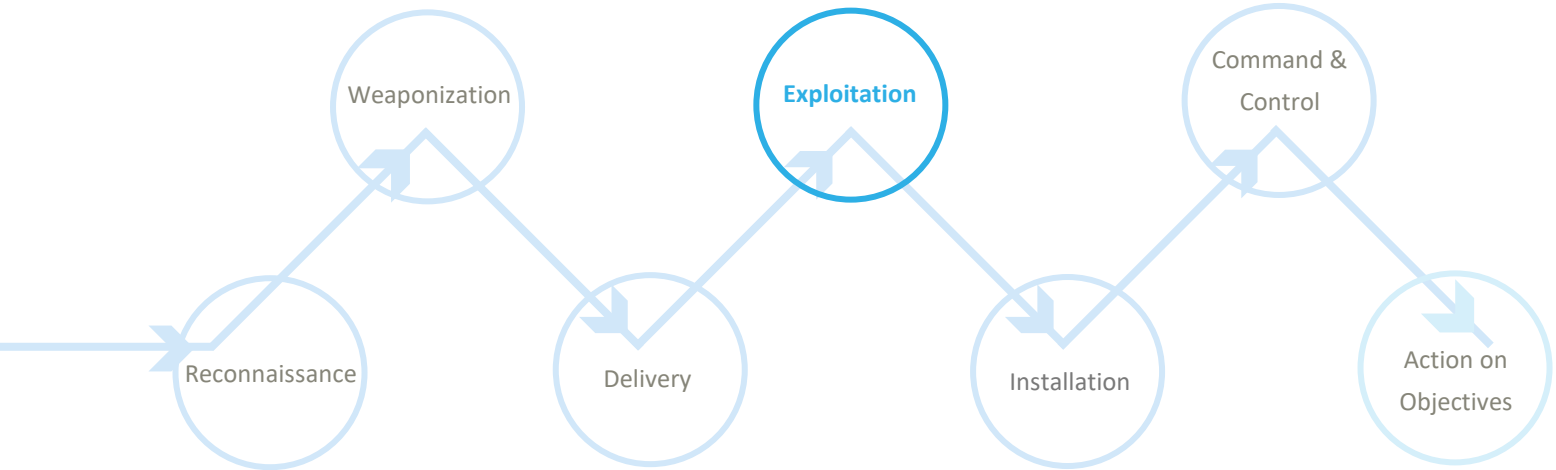


Figure 3

- The authentic login dialogue opens a new browser window, which can be verified in the panel of running applications. If only one instance of the browser is running, it is likely to be a scam;
- Check that the appearance of the login window matches your operating system and the browser's visual scheme, and that the dialogue is in your language;
- The icon indicating HTTPS is only a visual element in the fake window; in an authentic window, it is possible to display the page certificate by clicking on it.

A representation of the BITB in kill chain showing at which point attackers use the technique:



Focus on an incident: Ransomware in public administration

One of the March ransomware attacks differed from most of the cases handled by NÚKIB. This time, the attacker did not encrypt stations and servers using malicious code, but a legitimate Bitlocker tool, which protects data stored on users' disks against unauthorized access.

The victim of this attack was a public administration organisation. The attacker managed to encrypt approximately 10% of its user stations and several servers. In a message he left printed at the printer, the attacker threatened to disclose the organisation's data if he did not get paid. NÚKIB has not determined yet whether the data were actually exfiltrated, as the analysis of the data from gradually restored logs of older backups is still in progress. The attacked organisation detected the attacker at the very moment he began encrypting the organisation's disks and servers.

As the analysis of the incident is still ongoing, NÚKIB does not have all the necessary information yet on the basis of which it could draw precise conclusions about the attacker's goals and motivation. For this reason, too, the incident cannot be attributed to a specific actor at the moment.[5]

To get a better idea of the attacker's behaviour, the current findings on the incident have been put into a cyber kill chain:

Recoinnassance

Due to the lack of data, NÚKIB cannot determine whether the attacker actively scanned the organisation's external environment before attacking it. Nor can it rule out that the attacker initially sought information about the victim in open sources and then used it for a phishing campaign. The victim organisation is a public institution, which has a number of potentially useful information such as names and contacts of key employees publicly available by its nature.

Weaponization

Since the original attack vector is not known, NÚKIB does not have the necessary information for this phase of the kill chain.

Delivery

Based on the currently available data, it is not possible to confirm with certainty how the attacker gained initial access to the organisation's network. So far, the most likely option is that the attacker exploited the ProxyShell vulnerability on a Microsoft Exchange server. The server was already demonstrably compromised using this vulnerability last August, as confirmed by webshell findings. Nevertheless, it cannot be ruled out that these are separate attacks and the attacker got into the victim's network in a different way.

[5] Some data from the incident overlaps with this analysis: Exchange Exploit Leads to Domain Wide Ransomware (thedfirreport.com)

Exploitation

If an attacker accessed the victim's network by exploiting the ProxyShell vulnerability, then it would enable him to run a code with administrator privileges on the server and create a persistence account in the next step. NÚKIB is currently analysing whether this hypothesis is true.

Installation

The attacker created a *DefaultAccount* in the system, which is natively present in new versions of Windows. It did not legitimately exist in the older version of the Server used by the victim, and the attacker probably named it that way so that his presence did not arouse immediate suspicion. The attacker then transferred into the system a *dllhost.exe* file containing the functionality of a commonly available *Fast Reverse Proxy* tool and launched it to initiate connections to control servers and to lateral movement in the network.

Two hours after creating the account, the attacker transferred the tool to a domain controller and obtained domain administrator privileges. It is likely that the domain administrator's login details were dumped from the LSASS process after a service technician logged on to the controller.

Then, the attacker created persistence using Task Scheduler and the CacheTask.bat script to automatically install and run the *Fast Reverse Proxy* tool to communicate with the control serve

Command and Control

Thanks to the installed *Fast Reverse Proxy* tool, the attacker could repeatedly return to the compromised network and take further action in it. The attacker communicated with the control server through an RDP connection tunnelled through port 443 from addresses *148.251.71[.]182* and *107.173.231[.]114*.

Actions on Objectives

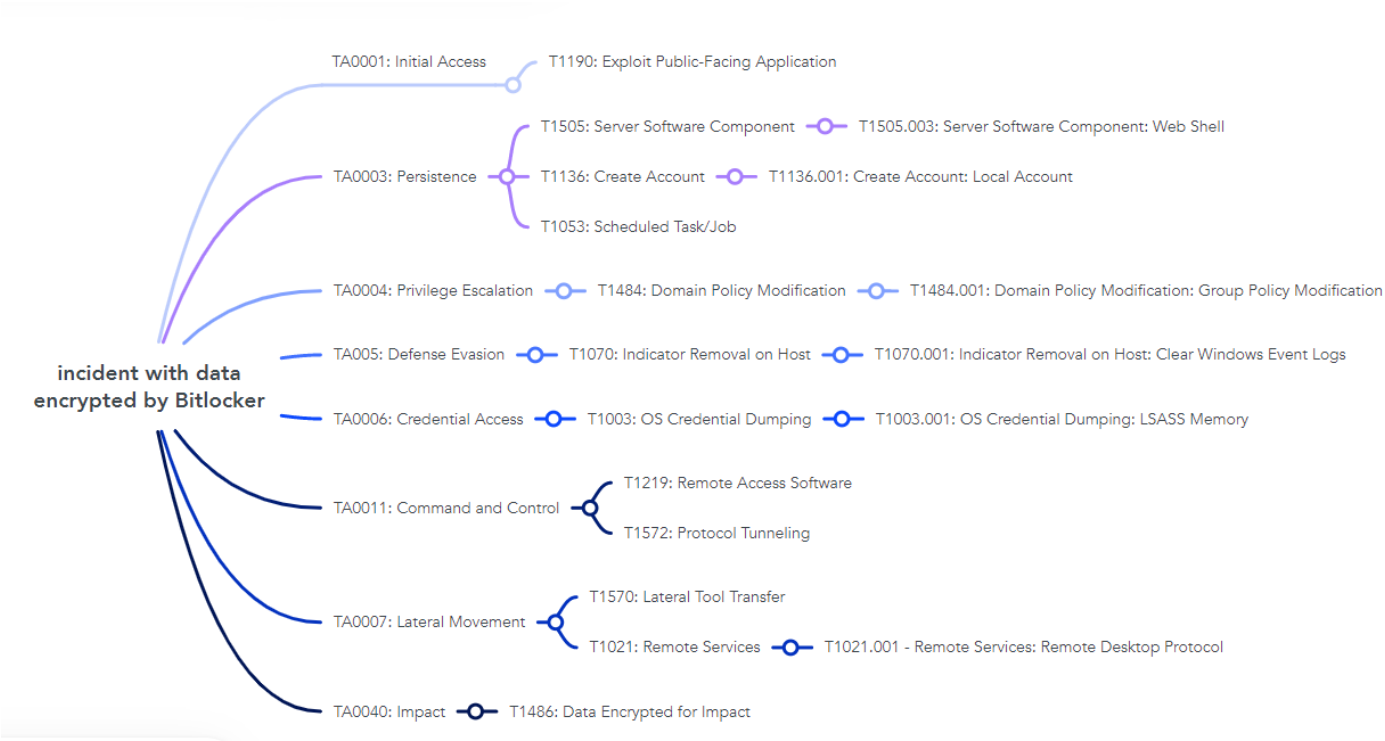
The attacker deleted event logs from the domain controller under the domain administrator's account.

In March, the attacker started encrypting domain machines using a legitimate Bitlocker tool. The administrators quickly noticed the encrypting thanks to the heavy network load and successfully stopped it on most machines. Meanwhile, the attacker managed to decommission approximately 10% of user stations and several servers.

During the encrypting, the attacker left behind a ransom note with the contact email *jolyoga@yandex.com*. However, the note did seem convincing, and it cannot be ruled out that its aim was not to enforce payment but only to cause damage and destroy traces.

It is not clear from the data available so far whether the data have been exfiltrated. In the meantime, an analysis of the activities is being performed from gradually restored logs of older backups.

Following is a list of MITRE ATT&CK techniques that the attacker used in the activities against the Czech public administration institution:



Probability terms used

Probability terms and expression of their percentage values:

Term	Probability
Almost certain	90–100 %
Highly likely	75–85 %
Likely	55–70 %
Realistic probability	25–50 %
Unlikely	15–20 %
Highly likely	0–10 %

Conditions for the information use

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website www.nukib.cz). The information is marked with a flag, which sets out conditions for the use of the information. The following flags are specified that indicate the nature of the information and the conditions for its use:

Colour	Conditions
TLP:RED	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.