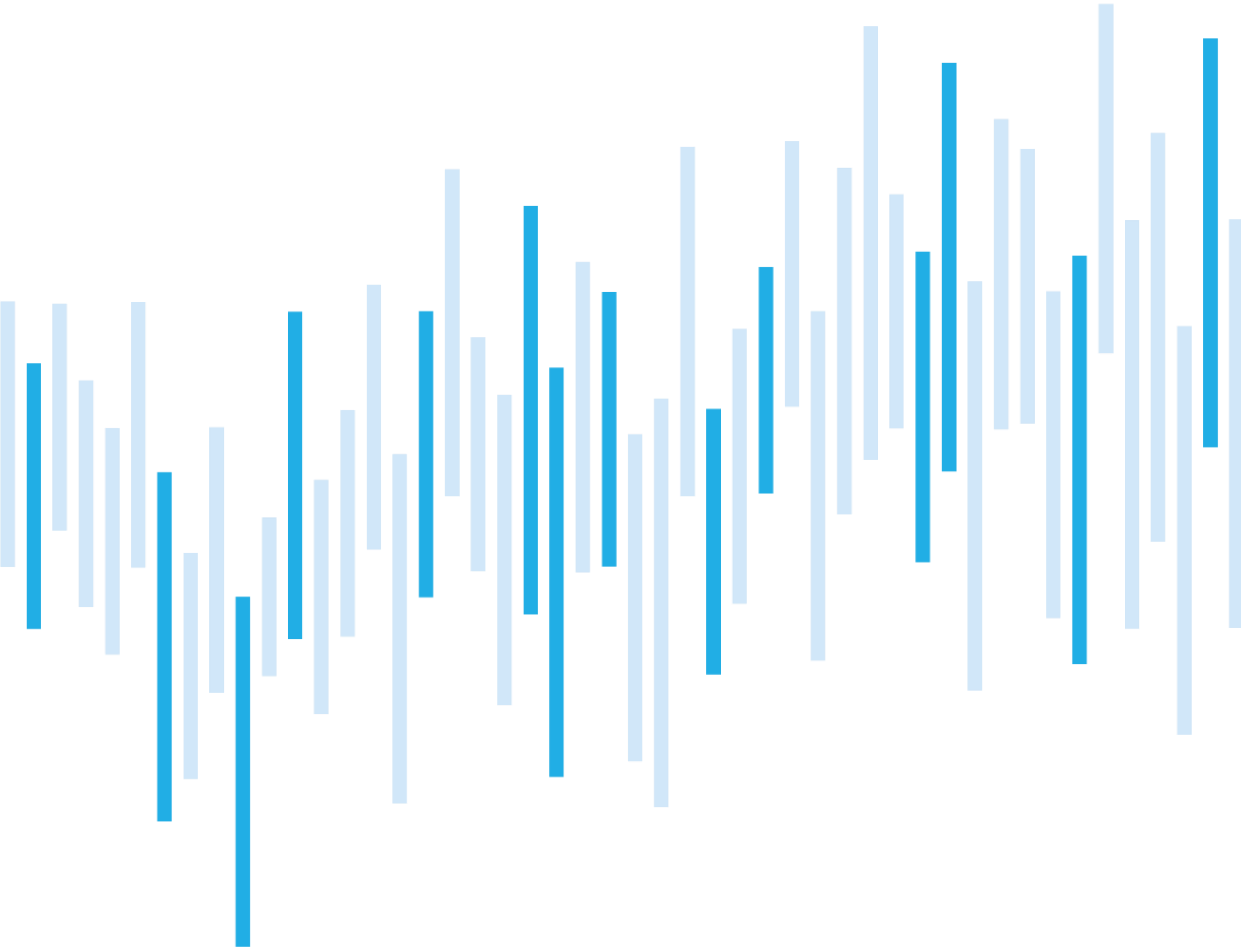
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

MARCH 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

In terms of the number of cyber incidents recorded by NÚKIB, March 2023 became a record month. This number was surpassed only in March 2021, when attackers widely exploited at-that-time-new vulnerability in MS Exchange Server. However, NÚKIB records the majority of incidents as less important. This is mainly due to the high number of DDoS attacks, which had no serious impact and only briefly disrupted the availability of the victims' websites.

In our March report, we outline an ongoing campaign targeting the general public with the aim of obtaining citizens' bank identity data. The attackers imitate the domains and websites of the Czech Ministry of Labour and Social Affairs, Czech Social Security Administration, Citizen Portal and Czech Post. The campaign is problematic because of its persistence and the relatively high activity of the attackers. The attacks began in August 2022 and continue to this day. Every month the attackers create dozens of new domains, which they use for their malicious activities. Taking into account the difficulty of mitigating of the ongoing attacks, we particularly recommend caution on the part of the user and careful examination of domain names. You can report any new fraudulent domains on the StopOnline.cz website, operated by the CZ.NIC association, and also to the Police of the Czech Republic.

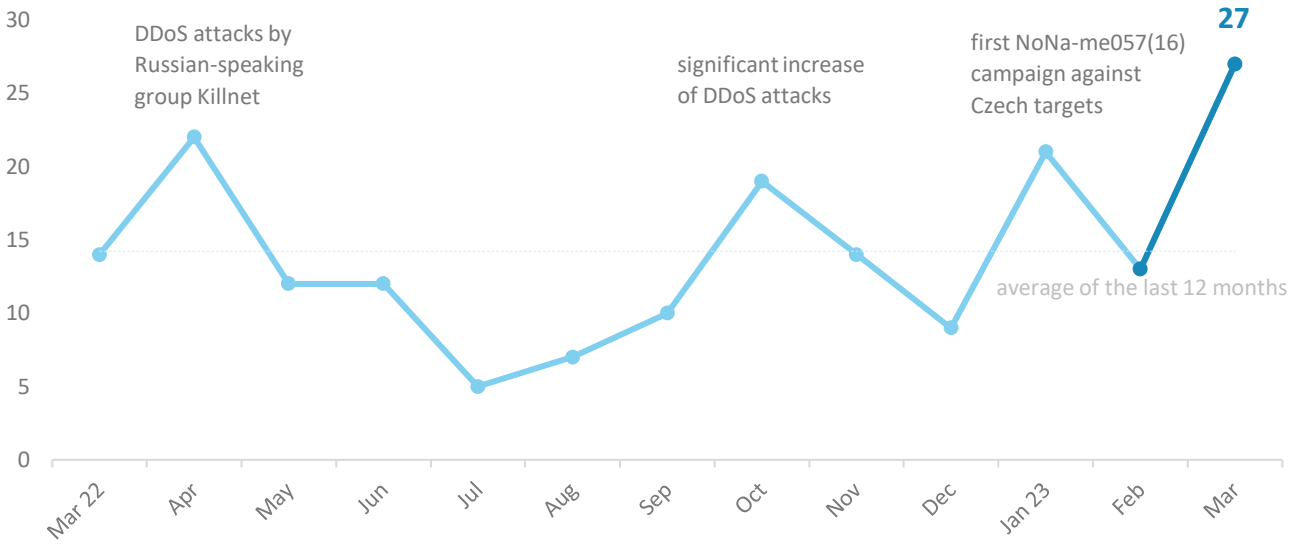
Table of content

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.

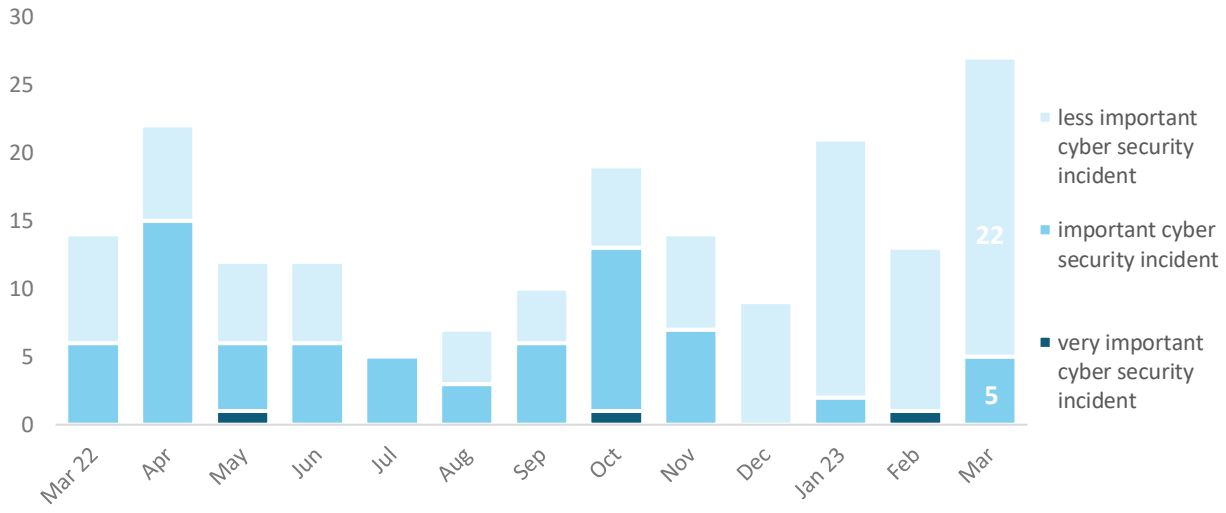
Number of cyber security incidents reported to NÚKIB

Considering the cyber incidents number, March was a record month. It was surpassed only in March 2021, when attackers widely exploited at-that-time-new vulnerability in MS Exchange Server.[1]



Severity of the handled cyber security incidents[2]

Despite the high number of recorded cyber incidents, the absolute majority of them fell into the category of less important incidents, which is mainly given by the high number of DDoS attacks that mostly do not have serious impacts and result in temporal inaccessibility of attacked organizations websites.



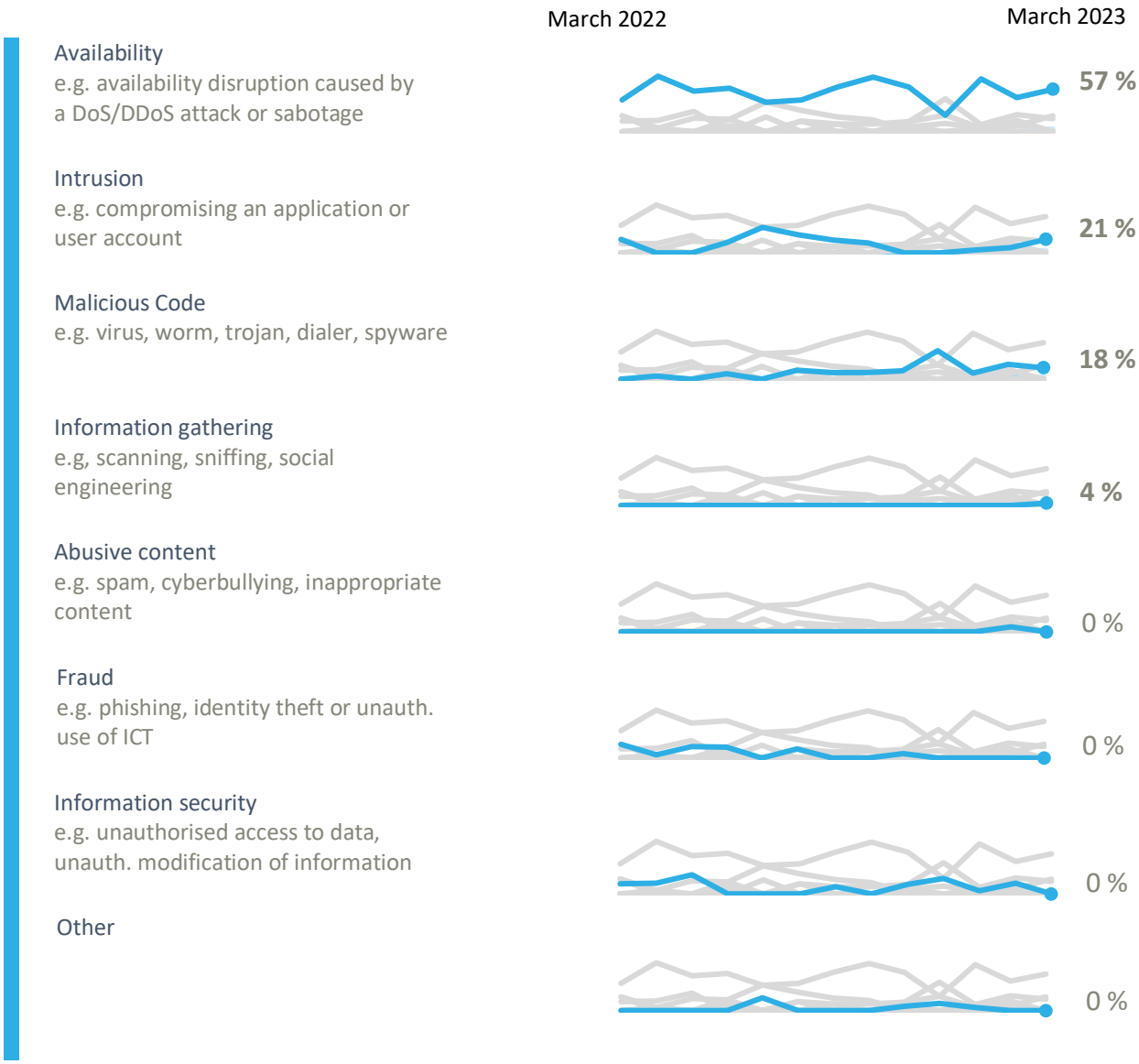
[1] NÚKIB registered 11 incidents in total with liable entities according to Cyber Security Act. Remaining 16 incidents reported not regulated subjects to NÚKIB.

[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB[3]

NÚKIB classified March incidents into four categories:

- More than half of all incidents were caused by DDoS attacks that negatively affected service availability on the victim side. As it is shown in the chart below, the availability disruption has long been at the forefront of cyber incidents recorded by NÚKIB;
- Six organizations reported their user accounts being compromised in March. In several cases, the compromise was preceded by a brute-force password attack, where attackers tried every possible combination of passwords until they hit the right one. Weak passwords may thus be broken within seconds;
- Malicious code is the third most frequent category. All incidents connected to it were caused by ransomware;
- NÚKIB classified the latest incident as information gathering. In this case, the attacker tried to obtain information about the intellectual property of a private company by creating a bot sending hundreds of queries a day to the company's service trying to crack its algorithm.



[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 a social engineering

The smishing campaign imitating websites of Czech state institutions continued in March. First attacks appeared in August 2022 and since then NÚKIB has been continually registering them. The predominant attack vector is smishing, i.e. a form of social engineering, when users receive SMS messages with a link to a fake website. The attackers send the messages to public for financial gain. You can find more information on the whole campaign in the last chapter herein.

Malware

Several organizations in the healthcare sector intercepted phishing messages with an attachment containing Agent Tesla malware. However, according to the text of the phishing e-mail, it was probably a generic campaign that instead of precisely targeted phishing against medical facilities aimed rather generally. Agent Tesla is Malware-as-a-Service, which is used by a wide range of actors and which has long been one of the most frequently used malicious codes in the Czech Republic.

Vulnerabilities

NÚKIB drew attention to a new vulnerability related to the Microsoft Outlook application. The CVE-2023-23397 vulnerability allows attackers to send their victims a specially modified email message that requires no interaction from the victim while allowing the attacker to move within the attacked organization's network. NÚKIB has not yet handled any incidents caused by this vulnerability, however, has already recorded attempts to exploit it. The vulnerability itself is detailed with its mitigation at NÚKIB website.

Ransomware

Number of ransomware attacks reported to NÚKIB increased in March. While NÚKIB dealt with an average of two ransomware incidents per month during the last year, this month there have been a total of five incidents. LockBit 3.0, LokiLocker and MedusaLocker were among the recorded ransomwares. LockBit, ransomware provided as a service, is the one which NÚKIB deals with most often in its incidents.

Attacks on availability

Russian-language hacktivist group NoName057(16) launched another wave of DDoS attacks against Czech targets. Its attacks accounted for more than a third of all incidents recorded by the NÚKIB in March. According to the group's statement on their Telegram account, the actions are retaliatory measures towards Czech actions supporting Ukraine, such as arms supplies. The recorded DDoS attacks did not have serious consequences and only led to the temporary unavailability of the attacked entities websites.

OT – operational technologies

The European Union Agency for Cyber Security (ENISA) released a report on 21th March mapping cyber security threats in the transport sector, where OT components are frequently deployed. The report maps and analyses incidents within the air, sea, rail and road transport between January 2021 and October 2022. The report also provides an assessment of threat actors, attacker motivations and main trends for particular subsectors. You can download the report from the following link of ENISA Transport Threat Landscape.

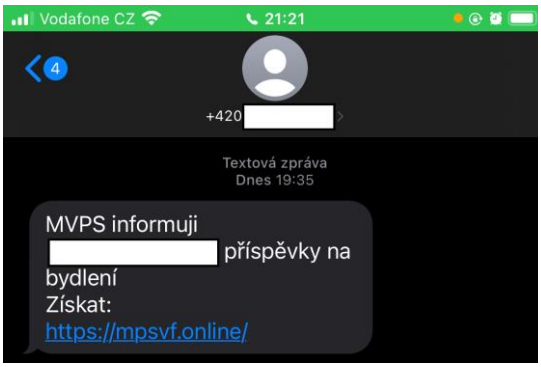
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

Technique of the month: Smishing

Smishing is the predominant attack vector in the currently active campaign in the Czech Republic, which imitates the websites of Czech state institutions and seeks to extract victims' banking login credentials from the general public. The campaign itself is detailed in the following chapter.

Smishing: Smishing is a form of social engineering. The name of this technique, created by combining the words "phishing" and "sms", suggests its nature. Attackers send their victims a text message, often with a link to a website from a seemingly trustworthy source such as a bank or post office. Once a victim opens the link, the attack continues as normal phishing. The victim is redirected to a fake site where he/she is either asked to enter login details or a malicious code is downloaded to the phone.

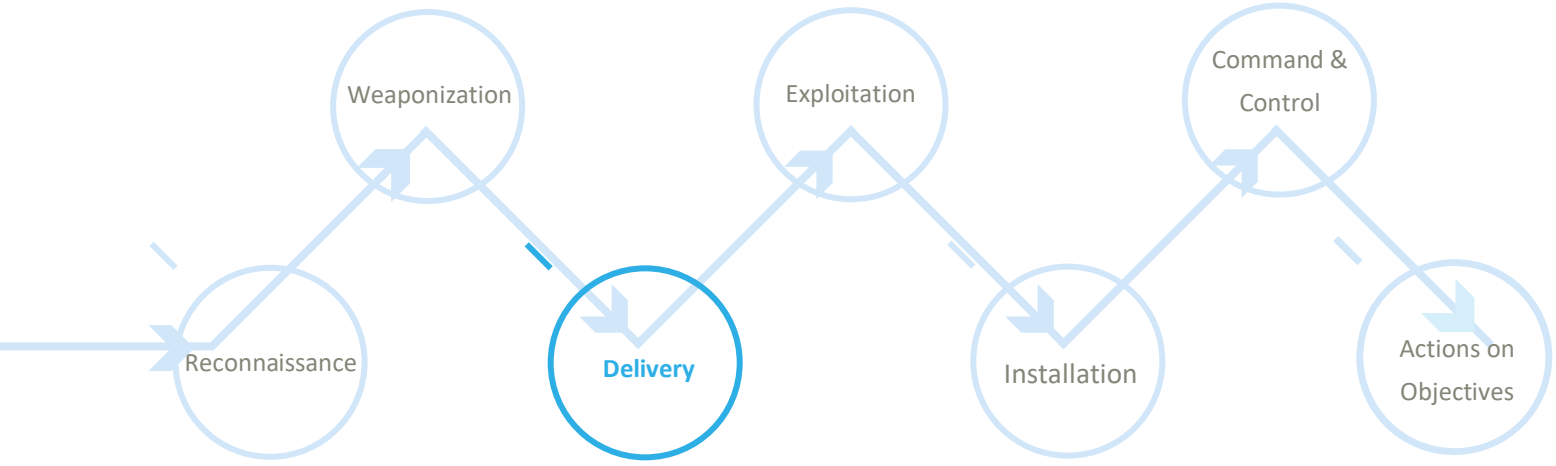
Fig. 1: Redacted phishing SMS message sent in the campaign described in the next chapter. In this case, the attackers tried to increase trustworthiness of the message by addressing the victim by name.



MITRE ID: T1566

Mitigace: Due to difficult mitigation, we strongly recommend caution on the part of the user. We recommend that you pay close attention to incoming messages and alert your family to the risk. When logging in (especially for banking), please always double check that it is indeed a legitimate address. If not, please report it to the CZ.NIC association, which blocks malicious domains.

Representation of smishing in a kill chain showing the attack phase in which the cyber actors use the technique:



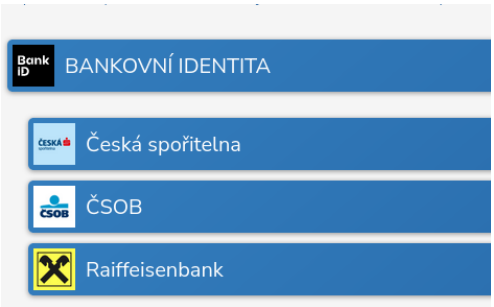
Focus on a threat: Smishing campaign imitating websites of the Czech state institutions

NÚKIB has long been registering the financially motivated smishing campaign targeting the general public with primary goal to obtain citizens' bank identity data. Within the campaign, the attackers imitate the domains and websites of the Czech Ministry of Labour and Social Affairs, the Czech Social Security Administration, the Citizen Portal and the Czech Post. In doing so, they abuse, for example, the motives of offering housing allowances, payment of social benefits or invitations to establish a data box.

The attackers mostly proceed as follows:

1. Attackers start their attacks by sending messages with various themes containing hyperlinks (see Fig. 1 on the previous page). Typically, these links imitate domains of Czech state institutions. For instance, domains with various variations such as ceska-mpsv[.]cz, mpsv-egov[.]online, mpsv[.]info, etc. are created in case of MSPV.
2. Having clicked on the attached link, the victim is redirected to a fake page imitating the website of the relevant institution with the option of logging in via a bank identity (see Fig. 2). Fake websites are graphically very well prepared and contain not only the official logos of the institutions, but also almost identical graphic design.

Fig. 2: Screenshot from the malicious website



3. If the victim logs into the fake banking identity, attackers will use the victim's credentials to log into its legitimate banking, prompting a two-factor authentication. The possibility of successful misuse of your online banking login details is not very likely (15-20%) thanks to two-factor authentication at login. However, there is a real possibility (25-50%) that attackers may resell this data. The victim was also redirected to another page asking them to enter their credit card details in some cases. After entering entering these details, the attackers then transferred the funds through the selected payment gateway.

The campaign is problematic because of its persistence and the relatively high activity of the attackers. In August 2022, NÚKIB called attention to the campaign when attackers started to target Czech citizens. However, the campaign still continues. Attackers are constantly creating new domains for malicious sites, and in March alone they created more than seventy of such domains. Though the newly created domains are gradually blocked by CZ.NIC association, the attackers continue in creating new ones. In addition to that, a large part of new pages is created outside the Czech national (.cz) domain, out of CZ.NIC competence to block them.

Considering the difficult mitigation, we particularly recommend caution on the part of the user. The official website for applying for housing allowance can be found only at https://www.mpsv.cz/web/cz/-/prispevek-na-bydleni. You can report any new fraudulent domains on the StopOnline.cz website, operated by the CZ.NIC association, and possibly also to the Police of the Czech Republic.

Probability terms used

Probability terms and expressions 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 unlikely	0–10 %

Traffic Light Protocol

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 of use
TLP: RED	For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP: AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP: AMBER+STRICT	Restricts sharing to the organization only.
TLP: GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.
TLP: CLEAR	Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.