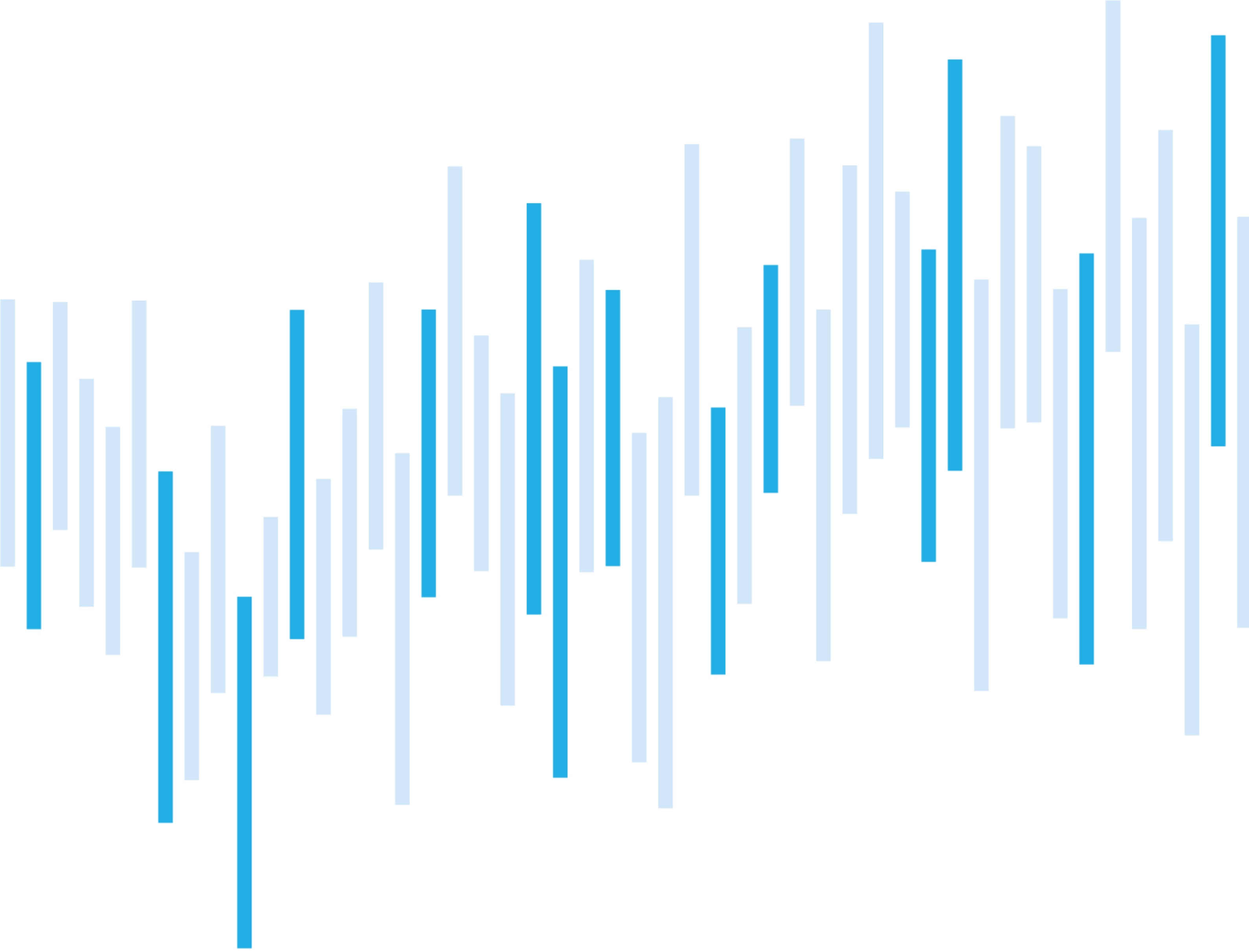
Cyber Incidents from of the NÚKIB’s Perspective

FEBRUARY 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

In February, the cybersecurity community turned its attention to events in Ukraine. The Czech Republic has not yet confirmed any incident that has been demonstrably linked to the war. However, around the time of the Russian invasion, there was widespread port scanning in the Czech Republic, including scanning of government organizations and critical infrastructure. Attackers were very likely looking for weaknesses in Czech targets' infrastructure that could later be exploited for follow-on cyber-attacks. As we argue on page 6, it cannot be ruled out that this scanning is related to the war in Ukraine.

Due to the Czech active support of Ukraine, the threat of cyber espionage, DDoS or ransomware attacks has increased. It cannot be ruled out that a cyber-attack on Ukrainian targets (e.g. by a wiper) will unintentionally spill over to the Czech Republic. In view of these threats, on 25 February, NÚKIB issued a Warning in which it gives recommendations to organisations on how to defend against these specific cyber threats. The Warning also includes a list of the techniques most commonly used by Russian and Belarusian groups in their attacks, including links on how to mitigate these techniques.

Table of Contents

Number of cyber incidents reported to NÚKIB

Severity of the handled cyber incidents

Classification of incidents reported to NÚKIB

February trends in cyber security from NÚKIB's perspective

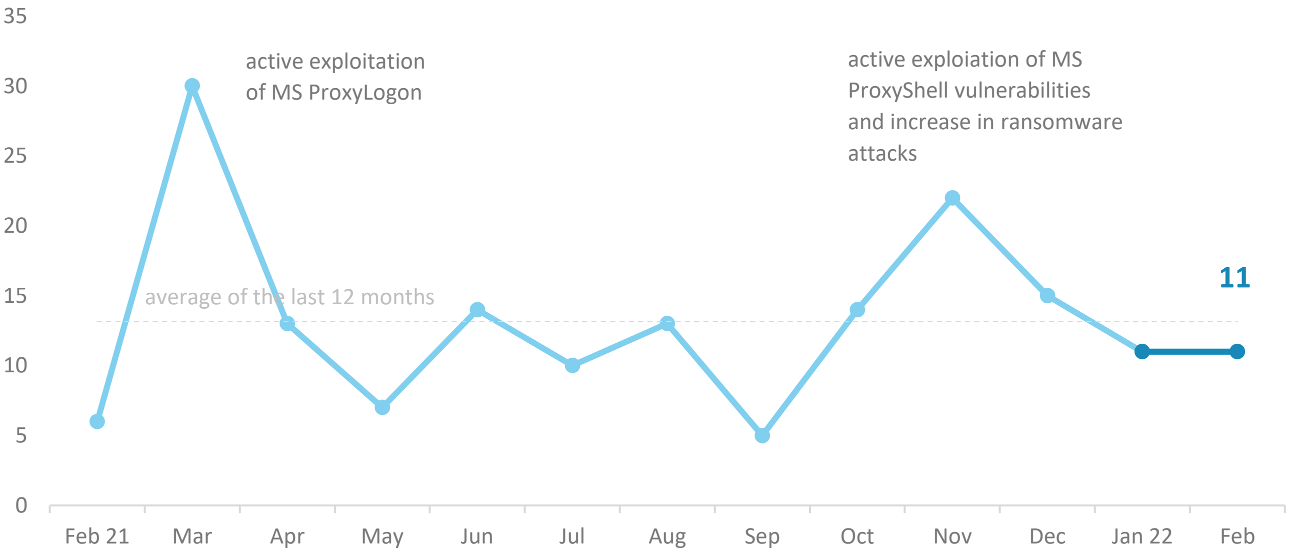
Technique of the month: Phishing

Focus on threat: Cyber-attacks relatied to Russian invasion of Ukraine

The following report summarises the events of the month. The data, information and conclusions contained herein are primarily based on cyber incidents reported to the National Cyber and Information Security Agency (NÚKIB). Where the report contains information from open sources in some parts, the origin of this information is always indicated. Comments and suggestions for improving the report can be sent to komunikace@nukib.cz.

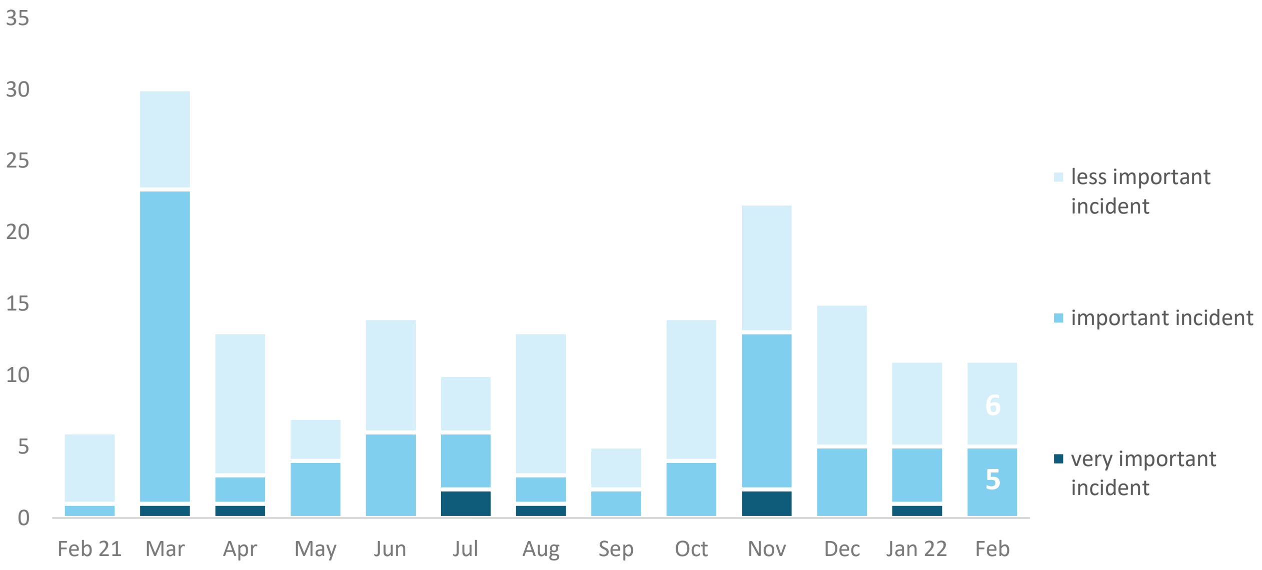
Number of cybersecurity incidents reported to NÚKIB

With 11 cyber incidents, February remained a slightly below average month in terms of number.[1]



Severity of the handled cyber incidents[2]

NÚKIB did not classify any of the February incidents as very significant. The incidents with more significant impacts included primarily ransomware attacks that limited the functioning of the attacked entities.



[1] Four incidents were reported to the NÚKIB by persons obliged by the Cyber Security Act. The remaining seven incidents were reported to the NÚKIB by entities that are not covered by the Act and therefore, do not have to inform NÚKIB.

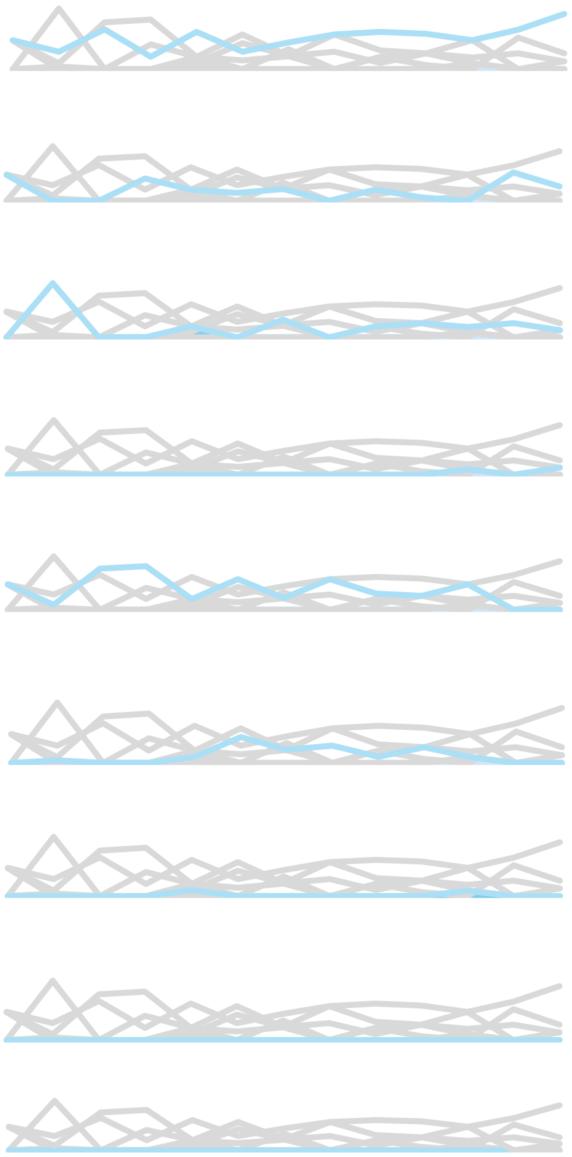
[2] The severity of cyber incidents is defined in Decree No. 82/2018 Sb. and in the internal methodology of NÚKIB.

Classification of incidents reported to NÚKIB[3]

February incidents were divided into four categories:

- Nearly two-thirds of the incidents resulted in unavailability of services. In February, ransomware affected the functioning of compromised systems, encrypting also victims' backups. In addition, DDoS attacks or a technical error affected availability;
- Fraud was the second most common category with two incidents. Due to successful phishing campaigns in two organizations, attackers were able to obtain login credentials of organizations' employees and to send phishing to other recipients from the compromised mailboxes;
- The last two incidents were classified by the NÚKIB as penetration and "other“.

	February 2021	February 2022
Availability e.g. availability disruption caused by a DoS/DDoS attack or sabotage	33%	**64%**
Fraud e.g. phishing, identity theft or unauthorised use of ICT	33%	**18%**
Intrusion e.g. compromising an application or user account	0%	**9%**
Other	0%	**9%**
Malicious code e.g. virus, worm, Trojan, dialer, spyware	33%	0%
Information security e.g. unauthorised access to data, unauthorised modification of information	0%	0%
Intrusion attempts e.g. attempt to exploit a vulnerability, attempt to log in, etc.	0%	0%
Information gathering e.g. scanning, sniffing, social engineering	0%	0%
Abusive content e.g. spam, cyberbullying, inappropriate content	0%	0%



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

February trends in cyber security from the NÚKIB’s perspective[4]

Phishing, Spear-Phishing and Social Engineering

Employees of a Czech government institution received a Ukrainian-themed phishing email at the end of February. However, none of them opened the malicious link with the .zip file and no compromise occurred. The attacker masqueraded as an employee of the European Council and referred to an analysis of the current situation. Based on information from partners and our own analysis, we know that the same attacker sends phishing emails also to other European government organizations. Given the current issues, it is very likely that phishing campaigns with a Ukrainian theme will continue to increase.

Malware

ESET uncovered two destructive malwares, HermeticWiper and IsaacWiper, which attacked Ukrainian targets on 23 and 24 February. According to ESET's, the attacks are characterized by careful preparation and malware artifacts suggest that the attacks had been planned for several months. No activity of these malicious codes was detected in the Czech Republic in February, but such a possibility cannot be ruled out in the future, whether as an inadvertent spillover to other systems or as a targeted attack against countries actively supporting Ukraine. HermeticWiper was also discovered in Latvian and Lithuanian systems.

Vulnerabilities

As the threat of cyber-attacks from Russian and Belarusian groups is increasing, so is the likelihood of vulnerabilities being exploited. In a Warning released on February 25, NÚKIB identified 14 most common vulnerabilities frequently exploited by these actors. In relation to the vulnerabilities, in the Warning, NÚKIB recommends that Czech organizations examine the presence of the listed potentially vulnerable systems in their infrastructure and make sure they are up to date.

Ransomware

NÚKIB handled three ransomware-related incidents in February. The victims were a Czech private company and a medical facility.

Even in the case of ransomware, there is an increased risk related to the war in Ukraine. Some ransomware groups have joined the Russian side and threaten the countries that will poses a threat to Russia through cyberspace.

Availability Attacks

In February, NÚKIB registered two DDoS attacks. The first one, which was an HTTP flood, resulted in a two-hour unavailability of the web server of the attacked organization. The second attack was a SYN flood and rendered the victim's website inaccessible for half an hour. Neither of these attacks are linked to events in Ukraine. However, given the current proliferation of DDoS attacks against Ukrainian targets, we cannot rule out their possible use against Czech organizations within the next month.

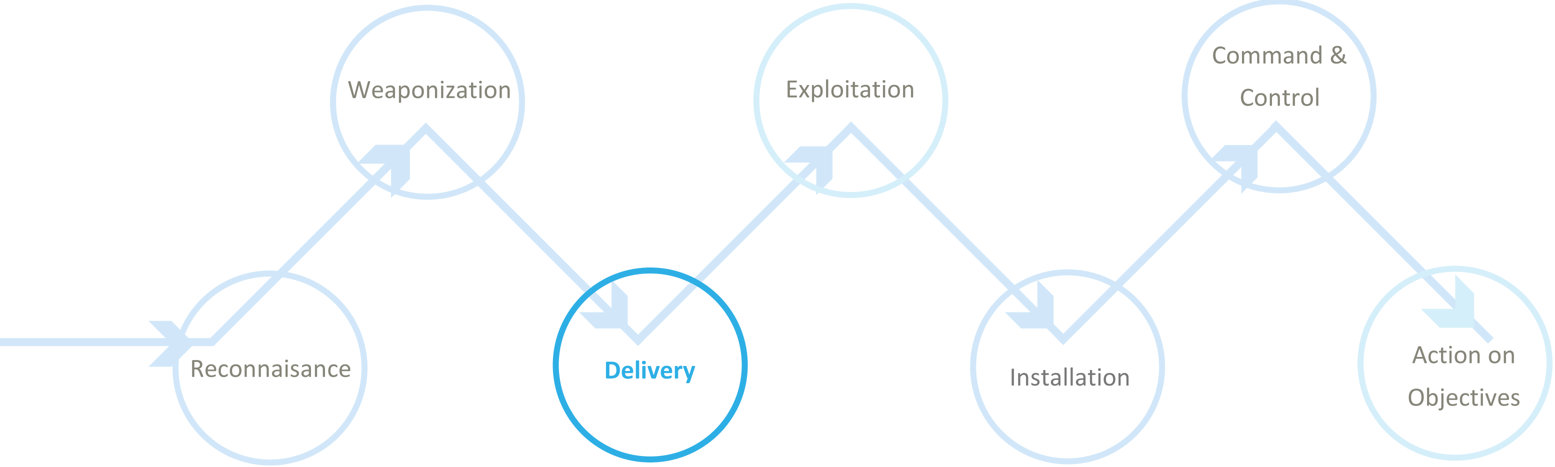
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

Technique of the Month: Phishing

NÚKIB also evaluates cyber incidents based on the MITRE ATT&CK framework, which is a curated knowledge base of techniques and tactics used in cyber-attacks. Phishing was the most common among February incidents handled by NÚKIB. Moreover, it is likely that phishing campaigns will increase in the coming months. Phishing is often a gateway for attackers to enter victims' systems. Therefore, it is likely that as the threat of cyber espionage and destructive attacks is growing, so will the number of phishing emails.

> **Phishing** is a technique in which attackers send phishing emails to their victims in an attempt to gain access to systems. All forms of phishing are electronically delivered forms of social engineering. Phishing can be either indiscriminate or targeted (spear-phishing). Typically, it contains attachments or links that either execute malicious code when opened or prompt the user to enter login details.
>
> **MITRE ID:** **T1566**
>
> **Mitigations:** The mitigation of this offensive technique runs on two levels. On a technical level, a significant amount of phishing relying on spoofed sender identities can be filtered out if the mail server supports and performs incoming mail screening according to the NÚKIB protective measure. Sandboxing of attachments, at least for potentially problematic file types (zip, exe, ps1, js), and warnings for encrypted archives are also appropriate countermeasures. Macros in Office documents are still the most commonly exploited method for malware delivery. This attack vector can be most easily prevented by technical measures by blocking macro functions to users who don't necessarily need them to do their jobs, using domain policies. However, such technical steps alone are not enough. Users need to be continuously trained, alerted to the risks associated with social engineering and the latest phishing trends so that they are able to detect it themselves.

Representation of phishing in a kill chain, showing at which stage the attackers use the technique:



Focus on threat: Cyber-attacks related to the Russian invasion of Ukraine

The attention of the cyber security community, as well as of the whole world, has been focused on what is happening in Ukraine. As tensions escalated during February, cyber threats against the Czech Republic grew proportionately. In the wake of active Czech diplomatic and material support, targeted attacks by Russian and Belarusian groups or unintentional spillover attacks on Ukrainian targets, such as those caused by destructive malware, are likely. The likelihood also increases in light of the cyber-attacks against Lithuania and Latvia by HermeticWiper wiper (see Page 4).

What cyber events related to the Russian invasion of Ukraine have been recorded in the Czech Republic?

In February, the NÚKIB did not record any cyber incidents that were demonstrably linked to the Russian invasion of Ukraine. However, from February 21 to 25, massive port scanning was conducted across the country. Two Russian IP addresses targeted Czech IP addresses across the board, including addresses of the Czech state administration and critical infrastructure.

```
92.63.197.97          45.143.203.5
```

It cannot be ruled out that this port scanning is linked to the war in Ukraine. By scanning open ports, the attackers were very likely looking for weaknesses in the security of Czech organizations that could later be exploited for follow-up cyber-attacks. The mere fact that the IP addresses, from which the scans were conducted, are registered in Russia is not sufficient proof that the activity originated there. With a little effort, an attacker can arrange to host his infrastructure almost anywhere. However, the time horizon of the scans is consistent with rising tensions in Ukraine and increased activity by Russian hacking groups. In addition, the same IP addresses were also scanning other European countries supporting Ukraine.

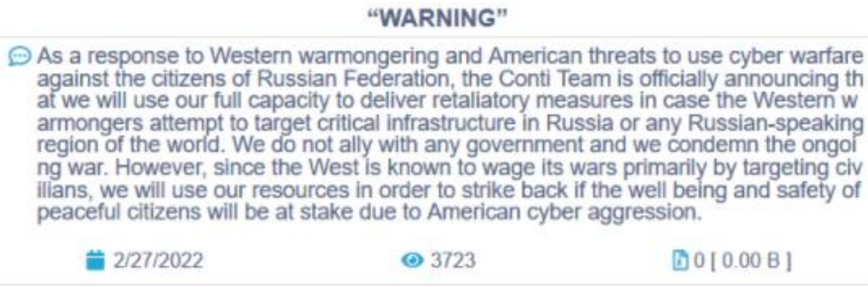
Threat of cyber espionage, DDoS and ransomware attacks is increasing

In late February, NÚKIB did not record any cyber-attacks that were linked to these scans or that were demonstrably linked to Russian aggression in Ukraine. However, caution remains in order. Given the Czech Republic's active support for Ukraine, the threat of cyber espionage, DDoS or ransomware attacks has increased:

- Cyber espionage: With the war in Ukraine, the need to obtain information about the upcoming actions of Western countries has very likely increased on the Russian side. Therefore, it cannot be ruled out that NATO member countries, including the Czech Republic, are already or will soon be the target of intensified cyber espionage operations by Russian APT groups. NÚKIB has not detected such espionage in recent months, but detection of such activities is highly problematic. The espionage is typically carried out by sophisticated APT groups that seek to remain undetected on their victim's networks in order to exfiltrate as much data as possible;
- DDoS: The events in Ukraine are accompanied by DDoS attacks. For example, they preceded the deployment of the destructive HermeticWiper malware and disabled the websites of Ukrainian government and financial institutions. The websites of the Ukrainian Parliament or the Ministry of Foreign Affairs have been targeted. Given the current prevalence of DDoS attacks against Ukrainian institutions, their possible use against Czech organizations cannot be ruled out;

- Ransomware: Cybercriminal groups are also gradually joining the Russian side, some of which are threatening attacks against Ukraine and those who will attack Russia through cyberspace. The most prominent of these is the Conti group, which has been one of the most active ransomware groups globally over the past year. Its operations and links to other cybercriminal groups have been exposed by leaks of its internal communications.

Figure: Conti statement released on February 27



"WARNING"

As a response to Western warmongering and American threats to use cyber warfare
against the citizens of Russian Federation, the Conti Team is officially announcing th
at we will use our full capacity to deliver retaliatory measures in case the Western w
armongers attempt to target critical infrastructure in Russia or any Russian-speaking
region of the world. We do not ally with any government and we condemn the ongoi
ng war. However, since the West is known to wage its wars primarily by targeting civ
ilians, we will use our resources in order to strike back if the well being and safety of
peaceful citizens will be at stake due to American cyber aggression.

2/27/2022 3723 0 [0.00 B]

Source: The Record

In connection with the above-mentioned threats, on 25 February, NÚKIB issued a Warning in which it provides further guidance on how to defend against these specific cyber threats. The Warning also includes a list of the techniques most commonly used by Russian and Belarusian groups in their attacks, including links on how to mitigate such techniques.

Probability Terms Used

Probability terms and expressions of their percentage values:

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

Conditions of Use of Information

The use of the information provided shall be in accordance with the Traffic Light Protocol methodology (available on the website (www.nukib.cz). The information is flagged to specify the conditions of use of the information. The following flags have been set out, indicating 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.