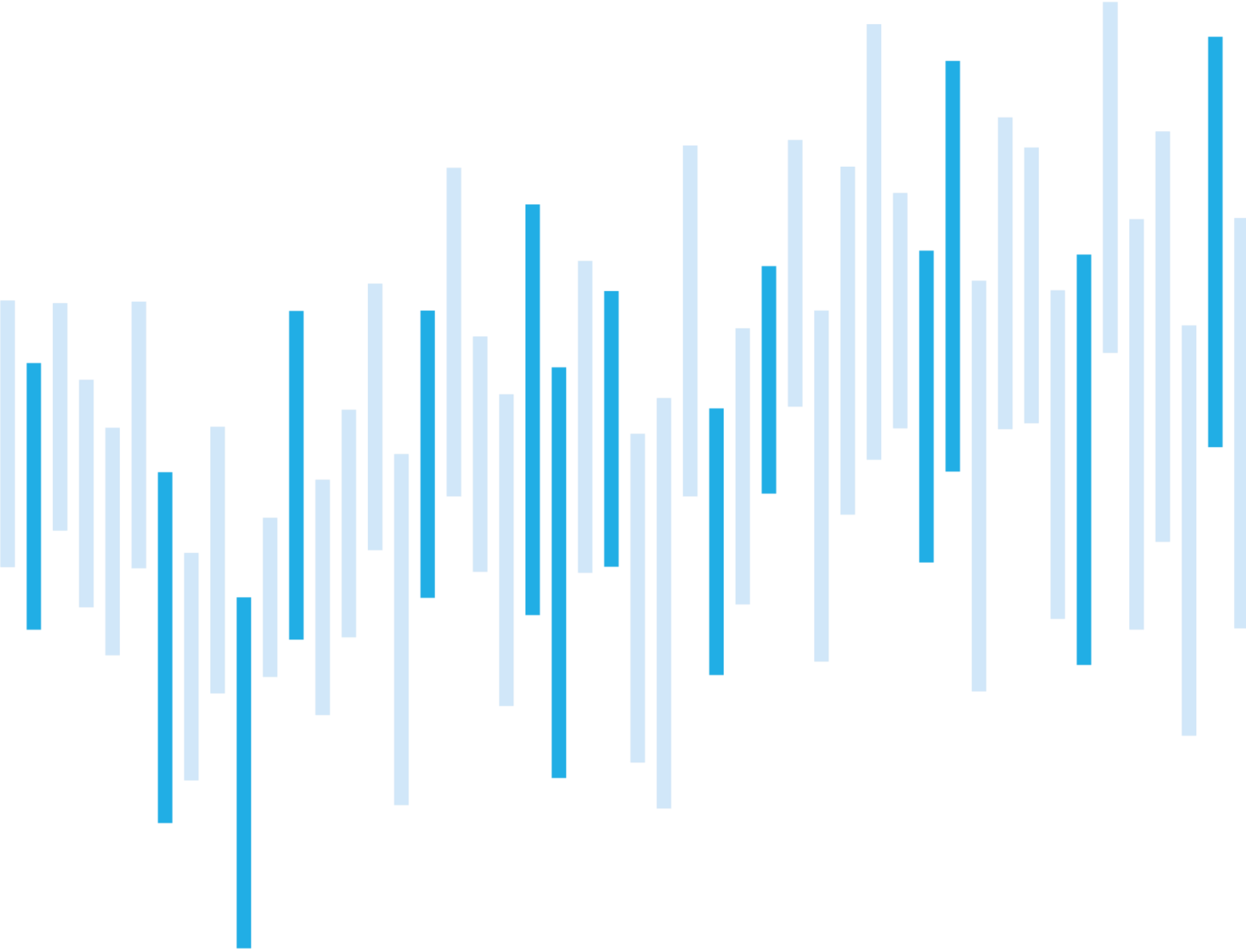
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

JUNE 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

The number of cyber incidents that occurred in June remained within the average values. Like every year, we record fewer incidents during summer, though their severity is currently relatively high.

Attacks against regulated entities prevailed notably. Nevertheless, no sector was affected more significantly than the others.

In June, NÚKIB concentrated on CZ PRES as an event of particular significance. At the beginning of July, the Czech Republic began to preside over the Council of the European Union (so-called CZ PRES) for the rest of this year, with cybersecurity being one of its five priorities. Moreover, it cannot be overlooked that CZ PRES is a tempting target for attackers, primarily with respect to possible espionage, ransomware/wiper attacks, and attempts to paralyse CZ PRES through DDoS attacks.

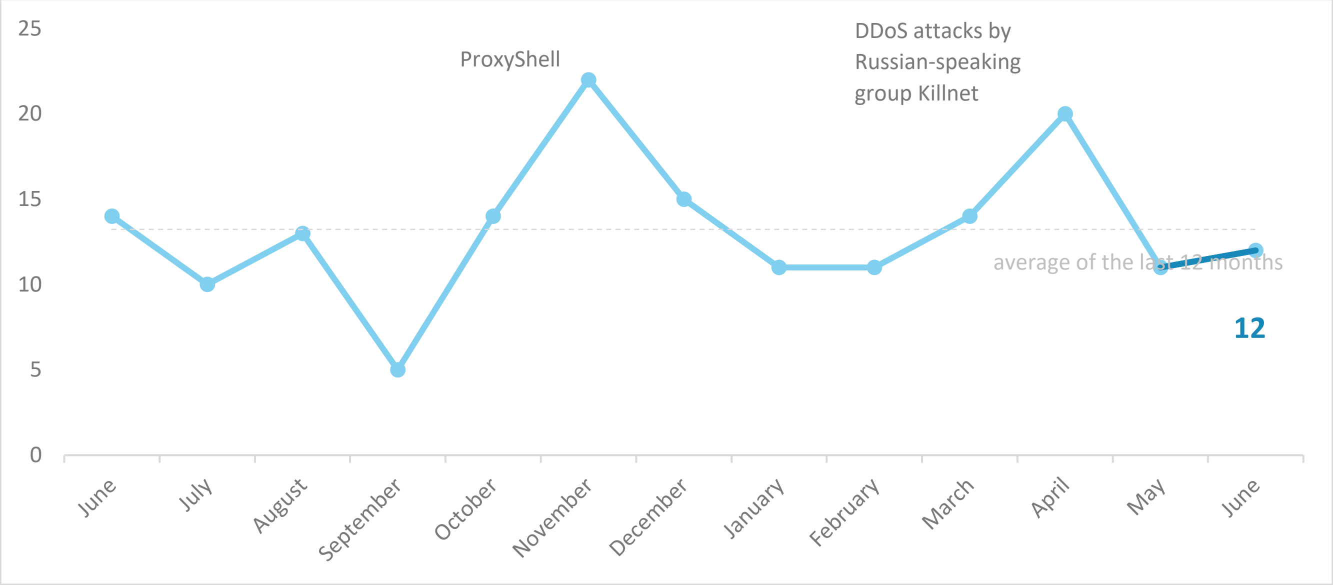
Table of contents

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.

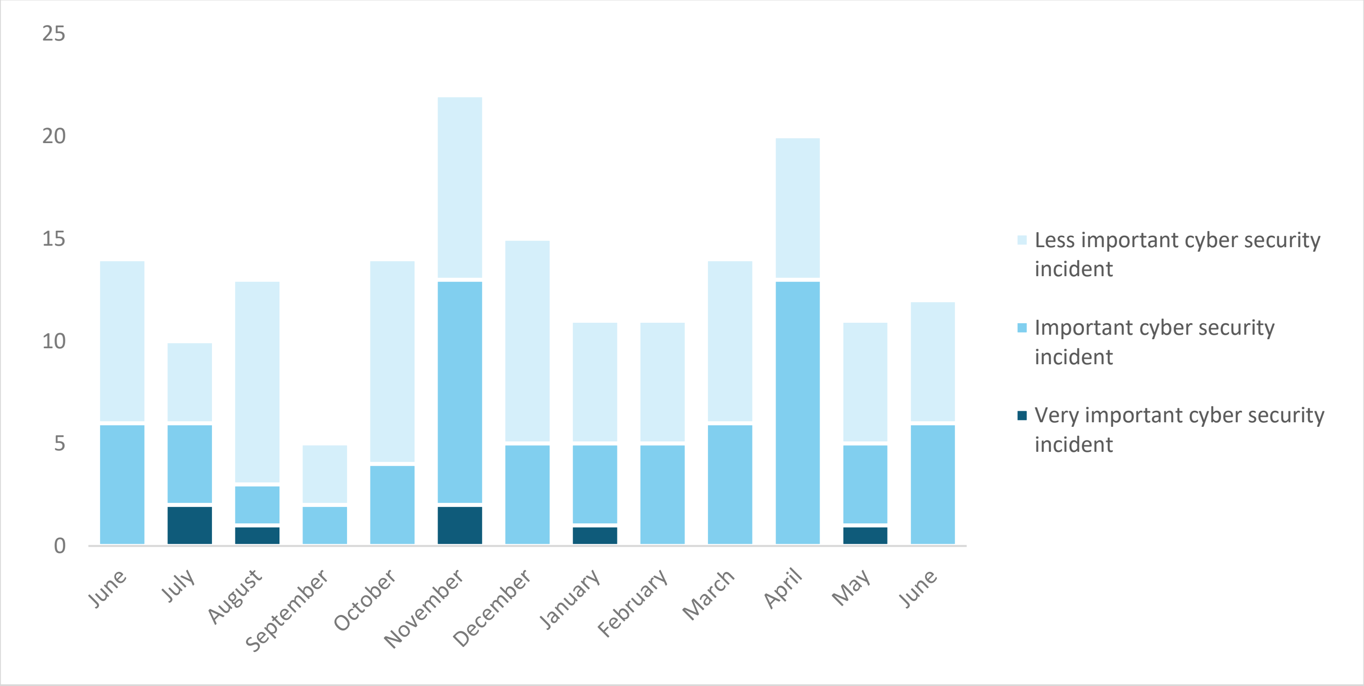
Number of cyber incidents reported to NÚKIB

The number of incidents remained at an average level in June. During summer, their number is usually lower.[1]



Severity of the handled cyber incidents[2]

The ratio of less significant incidents to significant incidents was almost balanced in June. In contrary to the preceding month, there was no very significant incident.



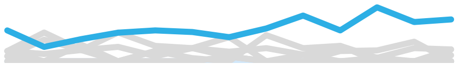
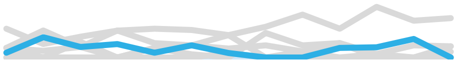
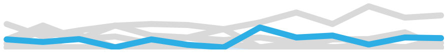
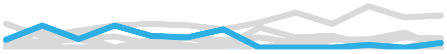
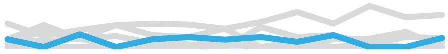
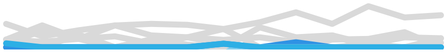
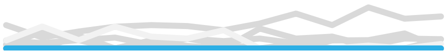
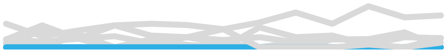
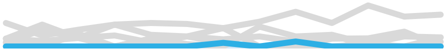
[1] Ten incidents were reported to NÚKIB by obligated persons according to the Cyber Security Act. The remaining two incidents were reported by entities that do not fall under this law.

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

Classification of the incidents reported to NÚKIB[3]

NÚKIB classified June's incidents within the following four categories:

- Although incidents associated with availability continued to prevail, they were caused primarily by technical errors resulting in the system unavailability but for two cases. In one case, the unavailability was caused by ransomware. The most interesting case involved cutting of optical fibre cabling that resulted in the entity's system being unavailable.
- There were also several incidents classified as intrusion. However, none of them was serious.
- Incidents categorised as fraud included a phishing attack against one state institution. The institution's employees received an e-mail with a message in Czech but signed in the Serbo-Croatian language. The phishing was sent from an account belonging to the telecommunications company based in Bosnia and Herzegovina.
- NÚKIB also registered an incident categorised as malicious code.

	June 2021		June 2022
Availability e.g., availability disruption caused by a DoS/DDoS attack or sabotage	43 %		**58 %**
Information security e.g., unauthorised access to data, unauth. modification of information	7 %		0 %
Fraud e.g., phishing, identity theft or unauth. use of ICT	14 %		**17 %**
Malicious code e.g., virus, worm, trojan, dialer, spyware	14 %		**8 %**
Intrusion e.g., compromising an application or user account	14 %		17 %
Intrusion attempts e.g., scanning, sniffing, social engineering	7 %		0 %
Information gathering e.g., scanning, sniffing, social engineering	0 %		0 %
Abusive content e.g., spam, cyberbullying, inappropriate content	0 %		0 %
Other	0 %		0 %

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

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

Phishing, spear-phishing, and social engineering

Phishing and phishing attempts have been a permanent trend. The most interesting case in June was an incident during which employees of one state institution received an e-mail written in quite good Czech but with the Serbo-Croatian signature. The e-mail was highly likely sent from a compromised account of the company in the sector of telecommunications, which is based in Bosnia and Herzegovina.

Malware

Since Microsoft disabled launching macros in the Office suite by default, there has been a noticeable decline in the usage of this technique in phishing campaigns spreading Emotet, AgentTesla, or Qakbot, for example. In reaction, these malware families occur in new versions, mainly delivered through misused LNK files.

NÚKIB also found a spear-phishing campaign spreading PlugX malware. Nevertheless, none of the reported cases resulted in an incident.

Vulnerabilities

A new critical vulnerability CVE-2022-26134 appeared in June associated with products by Atlassian, namely Confluence Server and Data Center. An attacker can launch a code remotely (RCE), which has potentially devastating impacts on victims. If the vulnerability is abused successfully, the attacker can install a backdoor, ransomware, or stealer that steals data from the victim.

Ransomware

Although the proportion of ransomware in the overall number of incidents was minimal in June, the trend of extortion attacks continued.

Attacks on availability

Similarly, as in the preceding month, none of the incidents was caused by a DDoS attack. Still, there were cases of availability disruptions due to technical errors.

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

Technique of the month: Spear-Phishing Attachment

Among others, NÚKIB evaluates cyber incidents based on the MITRE ATT&CK framework, which serves as an overview of known techniques and tactics used in attacks. Among the incidents in May, the "Spear-Phishing Attachment" technique prevailed.

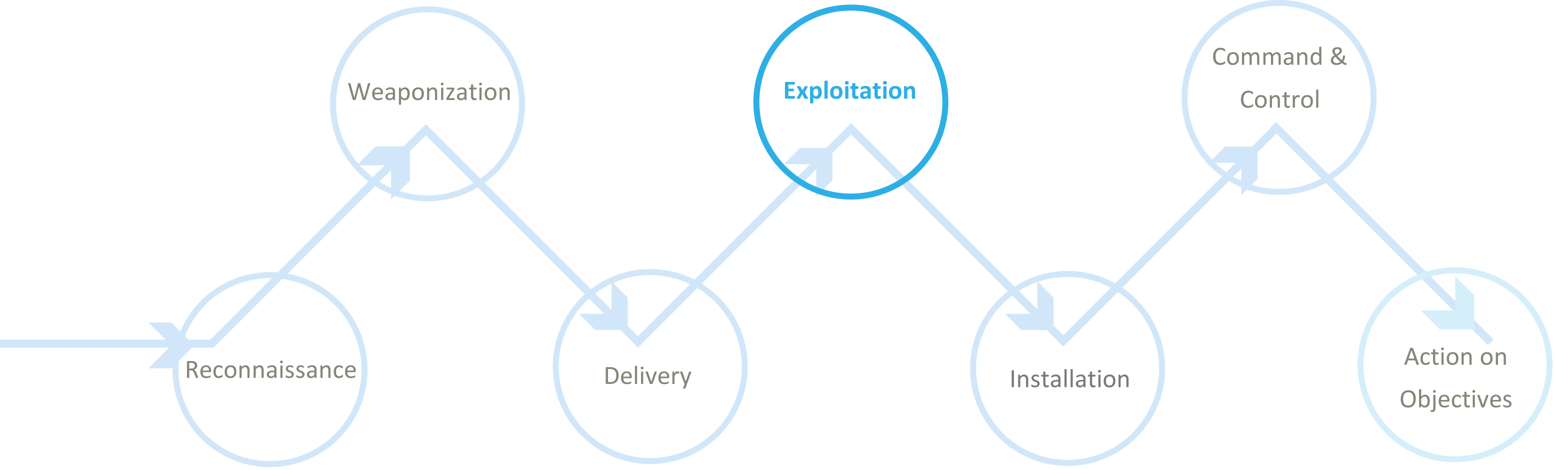
MITRE ID: T1566.001

Since Microsoft has already disabled launching macros in files downloaded from the Internet in the basic configuration of the current versions of the Office suite, several malware families have changed the delivery methods in reaction.

The most widely used technique to make a user launch macro is now using an .LNK shortcut file. It is commonly used for links to files, but a broader functionality can be set in the link parameter. Usually, an attacker masks it using a double extension and an icon modified to look like a PDF or Word document or a legitimate programme installer that the user launches. The most widely used method is setting a shortcut to run PowerShell or a command line to directly perform commands, such as download malware from the Internet and running it directly in the memory. The technique is widely used by Emotet and Ursnif trojans, for example.

Mitigation: Detection and disabling LNK files in e-mail attachments, setting of command line and PowerShell logging, and strict controls of the actual file type by the user.

A representation of the T1566.001 using a kill chain showing at which point attackers use the technique:



Focused on an event: CZ PRES

On 1 July 2022, the Czech Republic assumed historically second Presidency of the Council of the European Union; cybersecurity, together with strengthening of European defence capabilities, is one of the five main priorities of the so-called CZ PRES. Besides cyberspace security, ensuring the cybersecurity of the actual six-month event also plays an essential role in the presidential priorities.

NÚKIB has set following priorities for CZ PRES:

1) Proposal of a regulation to ensure a high common level of cybersecurity of the EU bodies, agencies, and institutions

2) Proposal of security regulation of ICT products and associated services

3) Cybersecurity of the ICT supply chain

Fig. 1: Homepage of the CZ PRES website

There is a realistic probability that the agenda will be affected by the Russian aggression against Ukraine and potential threats resulting from it. The most serious threats include cyber espionage focused on gaining sensitive data from the information and communication systems used for the needs of CZ PRES, attacks deploying wiper/ransomware, and DDoS attacks that would eventually result in the unavailability of critical systems or abusing of cyberspace for information operations (so-called cyber-enabled operations).

Cyber espionage: It must be noted that the volume and sensitivity of the forwarded information increase notably during the presidency. For attackers, it is a rare opportunity to gain valuable about the strategies and processes of the EU.

Wiper/ransomware: A massive attack deploying wiper or ransomware could cause unavailability of a prolonged nature.

DDoS: Contrary to wiper and ransomware, DDoS attacks would primarily cause short-term unavailability, which usually does not have serious consequences. The Czech Republic has recently experienced such attacks when several entities fell victims to the Russian-speaking group Killnet during April.

Cyber-enabled operations: Cyberspace can be used to spread disinformation, for example, via compromised legitimate accounts or websites. The main consequence is a damaged reputation.

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 %

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.