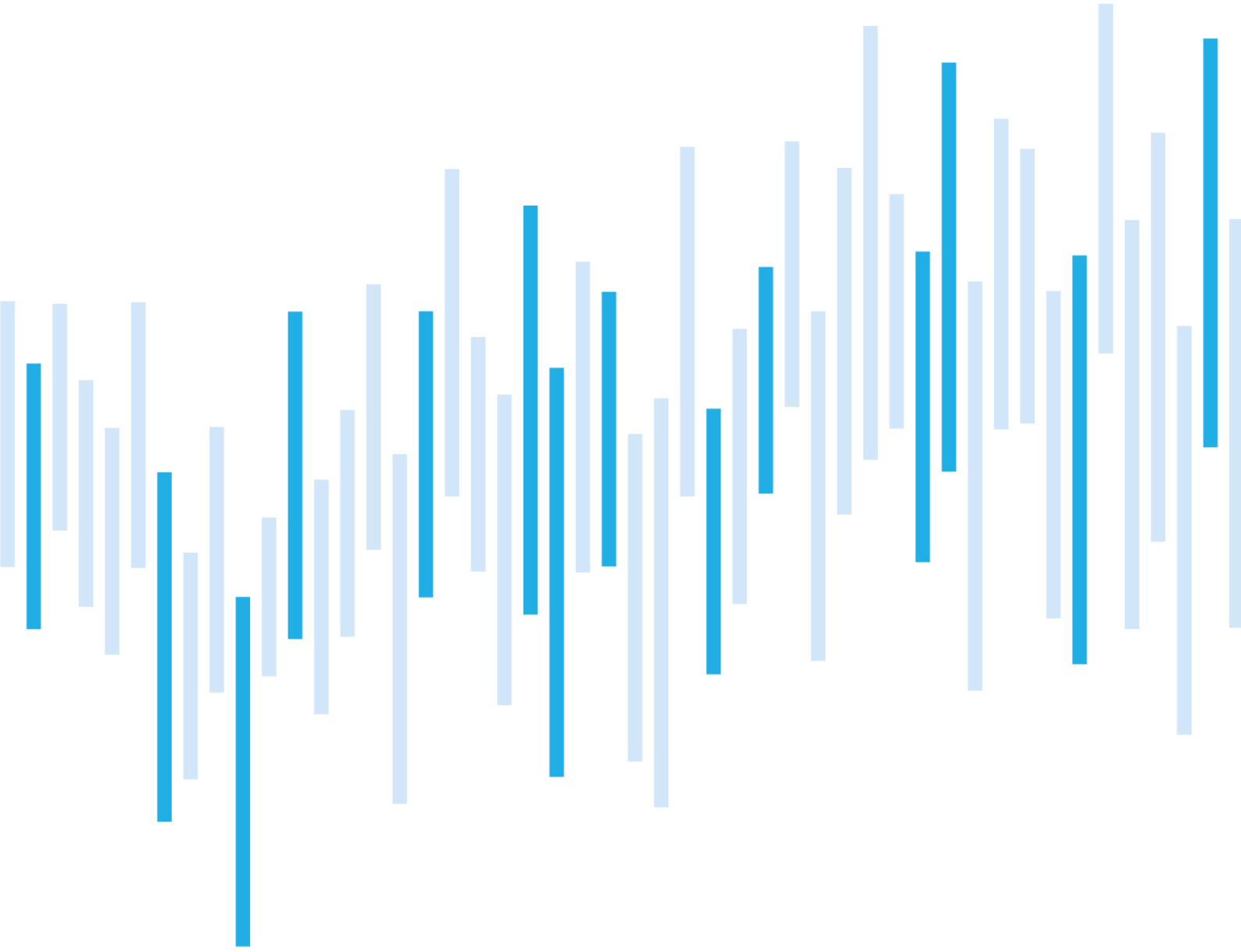
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

JULY 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

In July, the number of cyber incidents remained well below the average. NÚKIB usually records fewer incidents during summer, though their number in July was very low even for this quieter period of year. As for their severity, however, most of them were categorised as significant.

The ratio of incidents at regulated entities to incidents at non-regulated entities was almost balanced in July. Furthermore, no sector was targeted more significantly.

Since a local government was affected in July, this report concentrates on attacks against municipalities and regions. They represent a tempting target not only for the potential of financial profits but also because of their often weaker security.

Table of contents

Number of cyber incidents reported to NÚKIB

Severity of the handled cyber incidents

Classification of the incidents reported to NÚKIB

July trends in cyber security from the NÚKIB's perspective

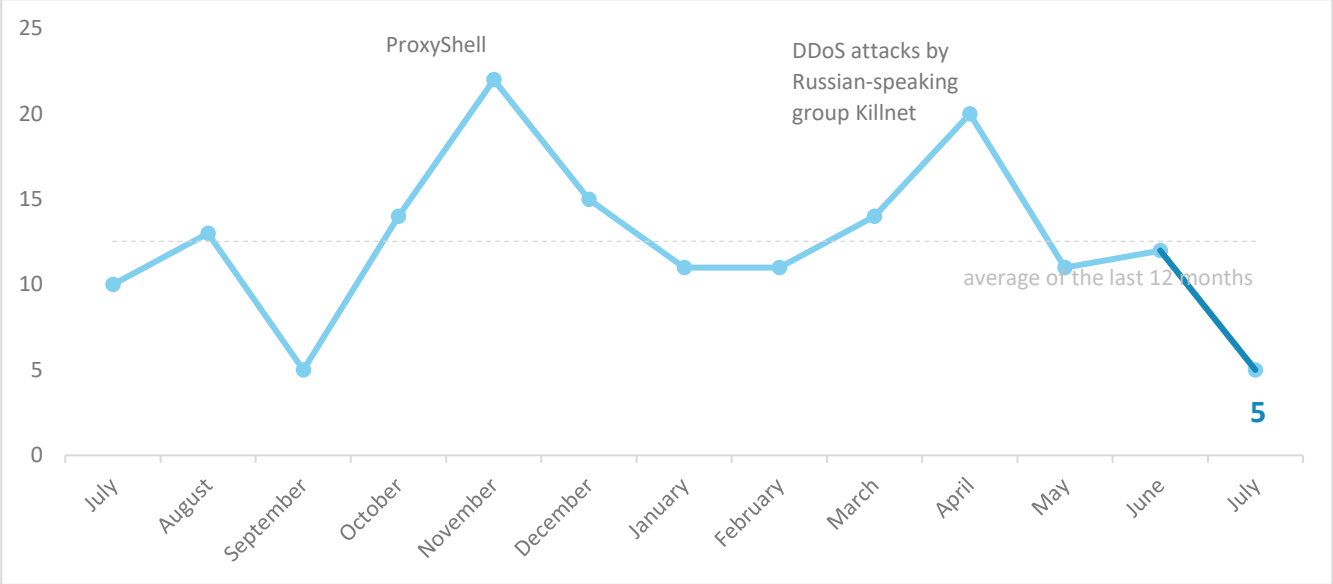
Focused on a trend: Attacks on local governments

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.

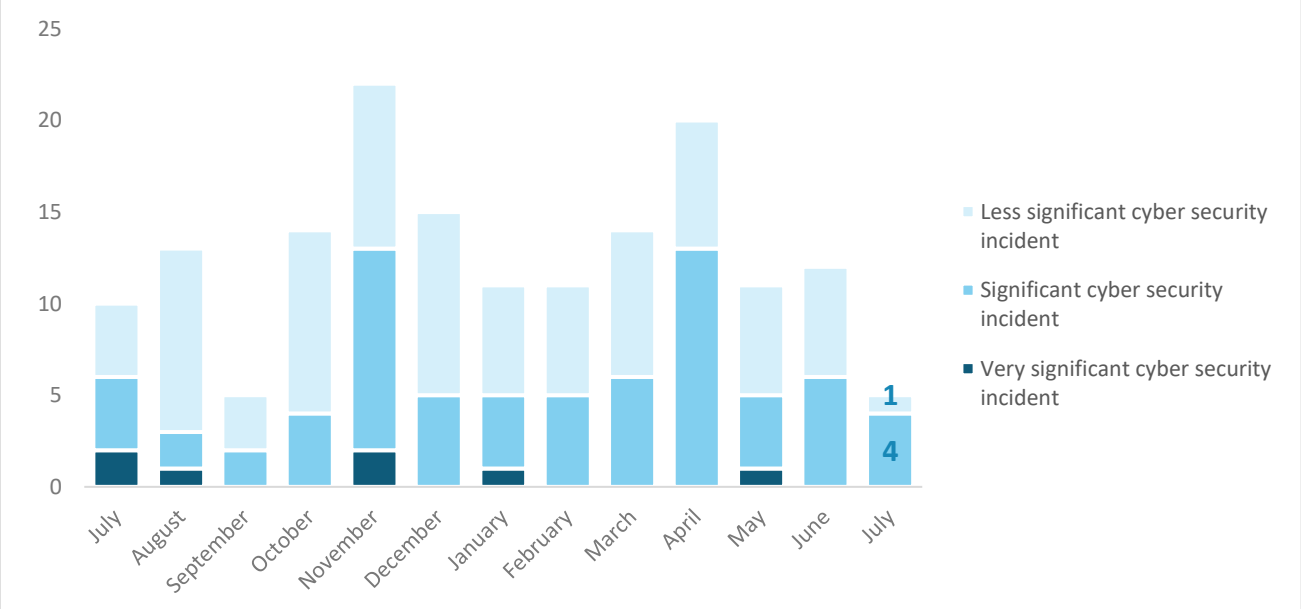
Number of cyber incidents reported to NÚKIB

In July, the number of incidents was well below the average. Their number was low even for the summer months, which are usually quiet.[1]



Severity of the handled cyber incidents[2]

Incidents that were categorised as significant noticeably prevailed in July. In June, there was no incident categorised as very significant.



[1] Three incidents were reported to NÚKIB by regulated entities 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 July's incidents within the following three categories:

- NÚKIB registered two attacks on availability, which have been a lasting trend. In both cases, these were ransomware attacks against non-regulated entities, but the ransomware type is unknown. The victims included local government bodies too.
- Likewise, intrusions also show a steady trend. Their number was the same as in June, but a severity increased.
- The one incident classified as "other" involved short-term unavailability of an application run by a regulated entity. Considering its nature, the incident was categorised as significant.

	July 2021		July 2022
Availability e.g., availability disruption caused by a DoS/DDoS attack or sabotage	20 %		**40 %**
Intrusion e.g., compromising an application or user account	0 %		**40 %**
Other	0 %		**20 %**
Malicious code e.g., virus, worm, trojan, dialer, spyware	40 %		0 %
Information Security e.g., unauthorised access to data, unauth. modification of information	30 %		0 %
Intrusion attempts e.g., scanning, sniffing, social engineering	0 %		0 %
Information gathering e.g., scanning, sniffing, social engineering	0 %		0 %
Abusive content e.g., spam, cyberbullying, inappropriate content	0 %		0 %
Fraud e.g., phishing, identity theft or unauth. use of ICT	10 %		0 %

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

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

Phishing, spear-phishing, and social engineering

Phishing and phishing attempts show a steady trend. Even though no such incident was recorded in July, there is a realistic probability that the vector of the attacks that occurred was social engineering.

Malware

NÚKIB did not analyse any malware based on the data from July's incidents.

Vulnerabilities

NÚKIB did not issue any alert regarding new vulnerabilities during July, nor did it detect any more significant abuse of the specific vulnerabilities known so far.

Ransomware

The ratio of ransomware to the overall number of incidents was relatively low in July, though the trend of these attacks continued.

Attacks on availability

Like in June, none of the incidents was caused by a DDoS attack.

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

Technique of the month: Deobfuscate/Decode Files or Information

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 recorded in July, the "Deobfuscate/Decode Files or Information" technique prevailed.

MITRE ID: T1140

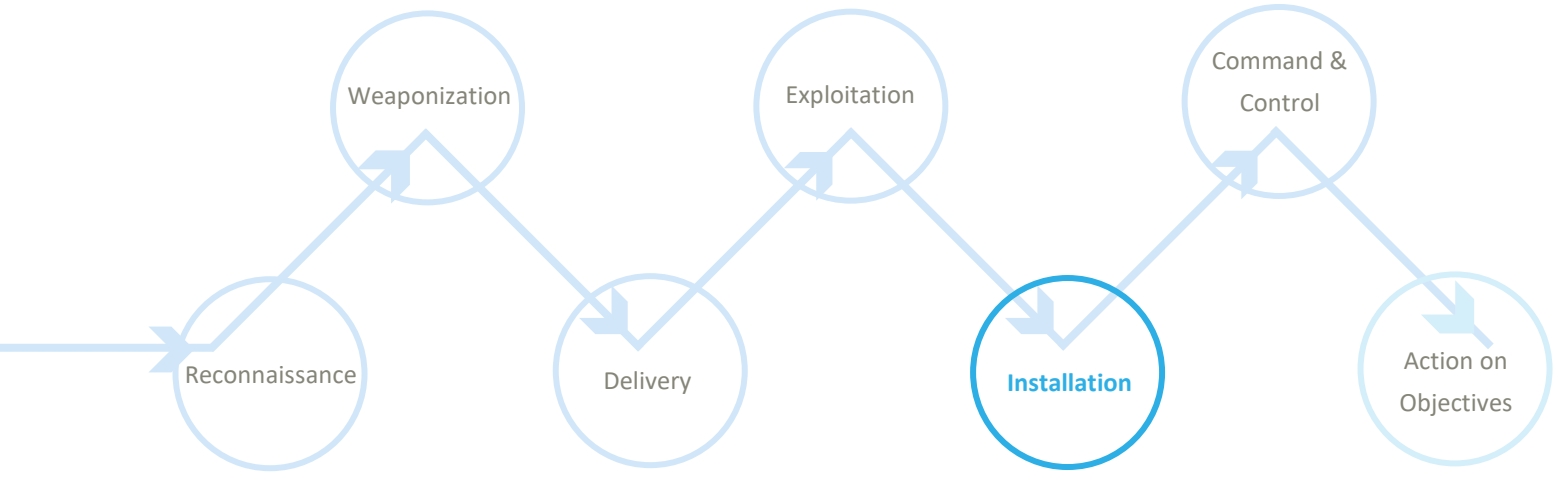
The technique is used to bypass protection or detection systems. An attacker delivers the malware to the system encrypted or encoded into another format or divided into more parts, which makes efficient control difficult. Consequently, the file can be evaluated as non-malicious. Later, the malware is decrypted and restored to its original form by other process, user action or legitimate tool (e.g., certutil). The decrypting and subsequent launching are often made in the memory only to make detection yet more difficult.

The practical use can range from the mere encoding of the malicious code into Base64 to sophisticated types employing multi-level asymmetric cryptography. Moreover, it is frequently combined with the technique T1204: User Execution, when a user receives the malware in an archive for which they enter a password.

Mitigation: The technique cannot be, by its nature, effectively mitigated. However, steps can be made to make their detection more effective. It is crucial to audit launching processes and file modifications, particularly those with a cryptographic tool as their parent process. Users are also recommended to be particularly attentive to password-protected archives downloaded from the Internet or enclosed with emails.

TLS traffic inspection may be appropriate with highly sensitive systems to ensure timely detection.

A representation of the T1140 using a kill chain showing at which point attackers use the technique



Focused on a trend: Attacks on local governments

In July, NÚKIB was informed about an incident in which ransomware targeted a local government. The year 2022 has already seen several such incidents targeted at municipal or regional authorities or entities under their umbrella. Therefore, this month's report focuses on attacks targeting local governments.

Local governments are a tempting target because of potential financial gain; thus, ransomware attacks are one of the most frequent types of attack. Ransomware blocks systems, making the fundamental services provided by municipal or regional authorities unavailable. Experience shows that endangered are both large cities and regional authorities (because of financial profits) as well as smaller towns, where weaker security is often anticipated.

Fig. 1: Illustrative image of a town hall

Besides insufficient IT security, poorly trained staff is often the main problem. **A specific case can be an insider attack when an employee with a broad authorisation intentionally causes damage to their employer for whatever reason or carries out activities that are not in accordance with their standard agenda.**

Recommendation:

NÚKIB has issued several recommendations that local governments can implement. Municipal, metropolitan or regional authorities can apply the Minimum security standard, whose main aim is to help entities not regulated by the Cyber Security Act. Senior representatives of local authorities can apply the Basic security measures for top management. The courses “Dávej kyber” and “Šéfuj kyber” are recommended to ensure elementary training and training of cybersecurity managers, respectively.

NÚKIB has also released a document with recommendations regarding protection against spear-phishing, which is a frequent vector of attacks. Finally, NÚKIB has issued an analysis warning about the ransomware threat, which is still one of the major threats to local governments.

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	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.