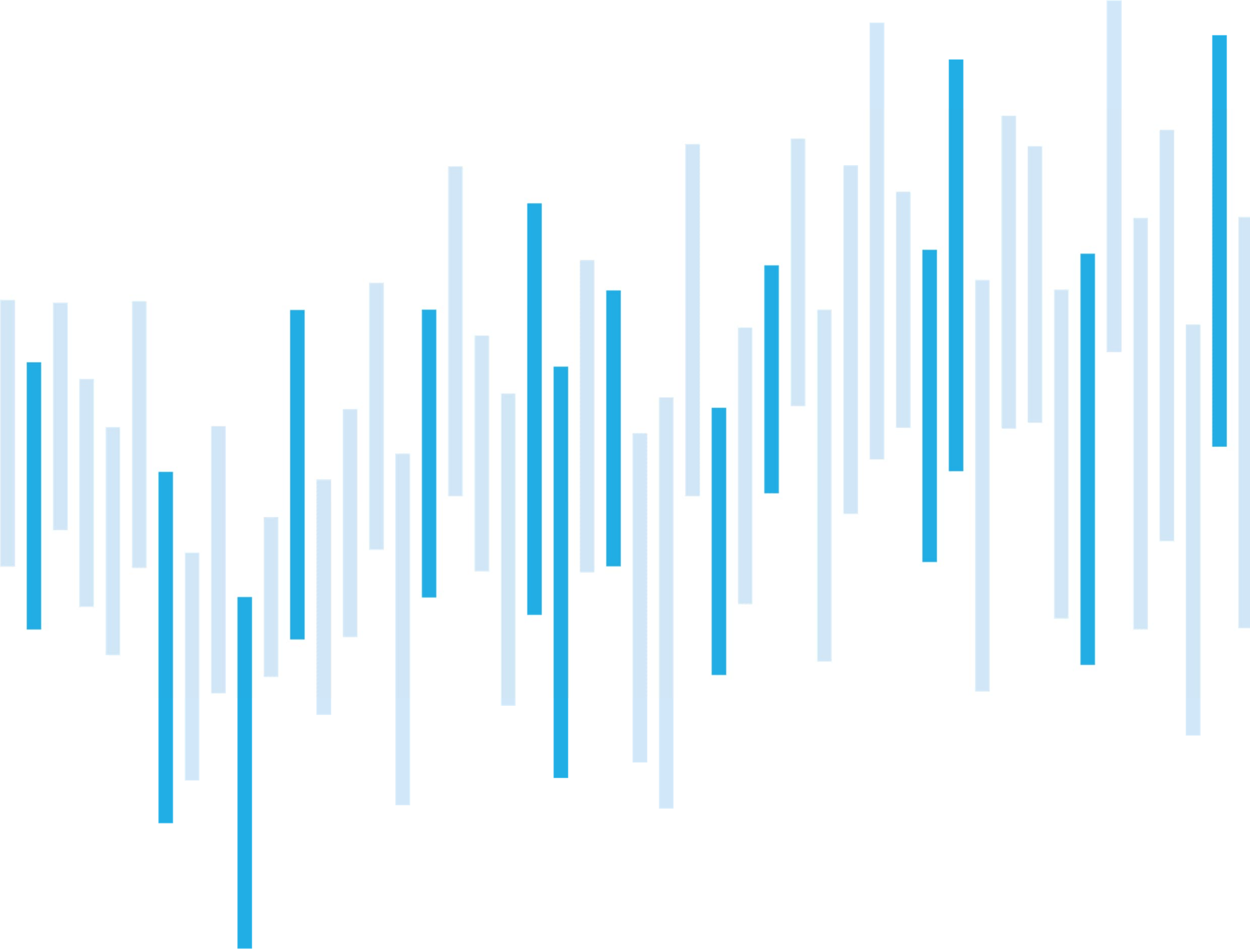
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

DECEMBER 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

The number of registered cyber incidents in December decreased in comparison to the previous month, reaching below-average values. The severity of registered incidents decreased, too. December is the only 2022 month when no important or very important cyber incident was registered.

In December, incidents reported by regulated entities again prevailed. The victims were mainly public administration and healthcare entities, as well as entities in the digital services and energy sectors. For the first time in 2022, the malicious code category became the most frequent incident type.

Considering the relatively frequent abuse of remote access by attackers as an entry vector in cyberattacks, we focus on the T1133 technique (External Remote Services) in this report.

In the chapter on trends, we focus on cybercrime-as-a-service. It is a business model within which cybercrime actors offer the tools and services intended for carrying out cyberattacks.

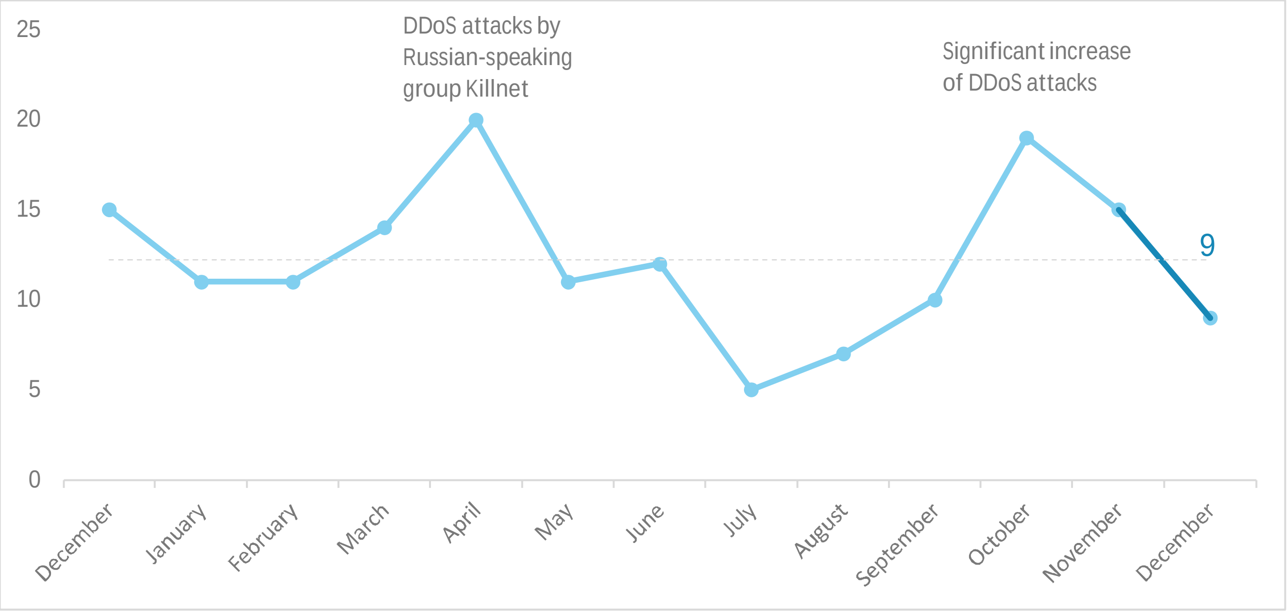
Table of contents

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 such information is always stated.

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

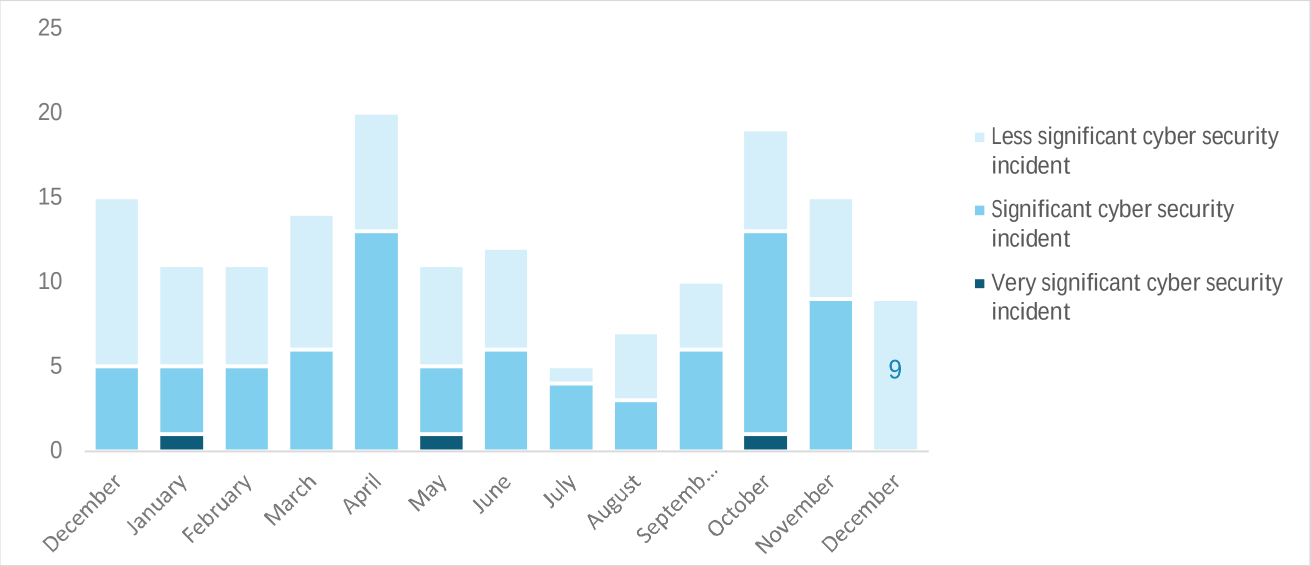
Number of cyber incidents reported to NÚKIB

Similarly to November, December was characterized by a decrease in cyber security incidents. Therefore, the number of incidents moved below average values at the end of the year, with December becoming the month with the third lowest number of incidents for 2022. [1]



Severity of the handled cyber incidents[2]

End of the year was characterised by a decrease of severity of cyber incidents. December is the only 2022 month with no important or very important cyber incident registered.



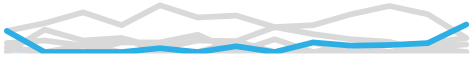
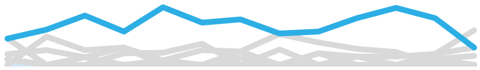
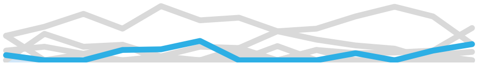
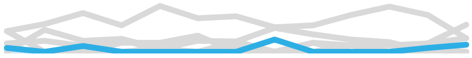
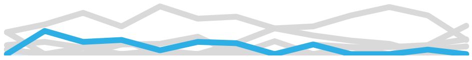
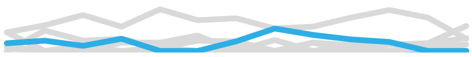
[1] Six incidents were reported to NÚKIB by regulated entities according to the CSA. Three were reported by entities that do not fall under this law.

[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 the December cyber incidents into four categories:

- The most common type of incident was malicious code, which occupied relatively low numbers for most of the year. December incidents involved ransomware and other malware types.
- Two attacks on availability were registered in December, only one of which involved DDos attack. Compared to the two previous months it is a significant decrease of this attack type.
- In December, two incidents related to information security occurred. While one of them was caused by system error, the other was caused by human failure.
- NÚKIB also registered one incident in Others category

	November 2022		December 2022
Availability e.g., availability disruption caused by a DoS/DDoS attack or sabotage	13 %		44 %
Information security e.g., unauthorised access to data, unauth. modification of information	60 %		22 %
Malicious code e.g., virus, worm, trojan, dialer, spy-ware	13 %		22 %
Other	7 %		11 %
Fraud e.g., phishing, identity theft or unauth. use of ICT	7 %		0 %
Intrusion attempts e.g., scanning, sniffing, social engineering	0 %		0 %
Information gathering e.g., scanning, sniffing, social engineering	0 %		0 %
Intrusion e.g., compromising an application or user account	16 %		0 %
Abusive content e.g., spam, cyberbullying, inappropriate content	0 %		0 %

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

Trends in cyber security in December from the perspective of NÚKIB[4]

Phishing, spear-phishing, and social engineering

Phishing and other social engineering techniques represent a continual trend. In December, phishing was used to spread a malicious link in at least one reported case.

Malware

After a few months pause, NÚKIB registered two cases of incidents involving malware. One of the recorded cases involved the use of Redline Stealer malware designed primarily for data collection, which is offered as a service (malware-as-a-service).

Vulnerabilities

As in November, NÚKIB issued one vulnerability alert in December. It was the critical FortiOS vulnerability CVE-2022-42475, whose exploitation by unauthenticated users allows remotely shutting down the machine and executing arbitrary code.

Ransomware

In December, NÚKIB solved two ransomware attacks in total, both at unregulated subjects. The ransomware types were PLAY and FAUST. The latter belongs to the Phobos family, which has appeared in incidents several times this year.

Attacks on availability

In contrast to the previous months, when DDoS campaigns against Czech entities were registered, there was a significant decrease in the category of attacks on availability. Merely one DDoS attack was registered in December. Although this attack was successful, it only resulted in a short-term outage of the entity's web portal.

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

Technique of the month: External Remote Services

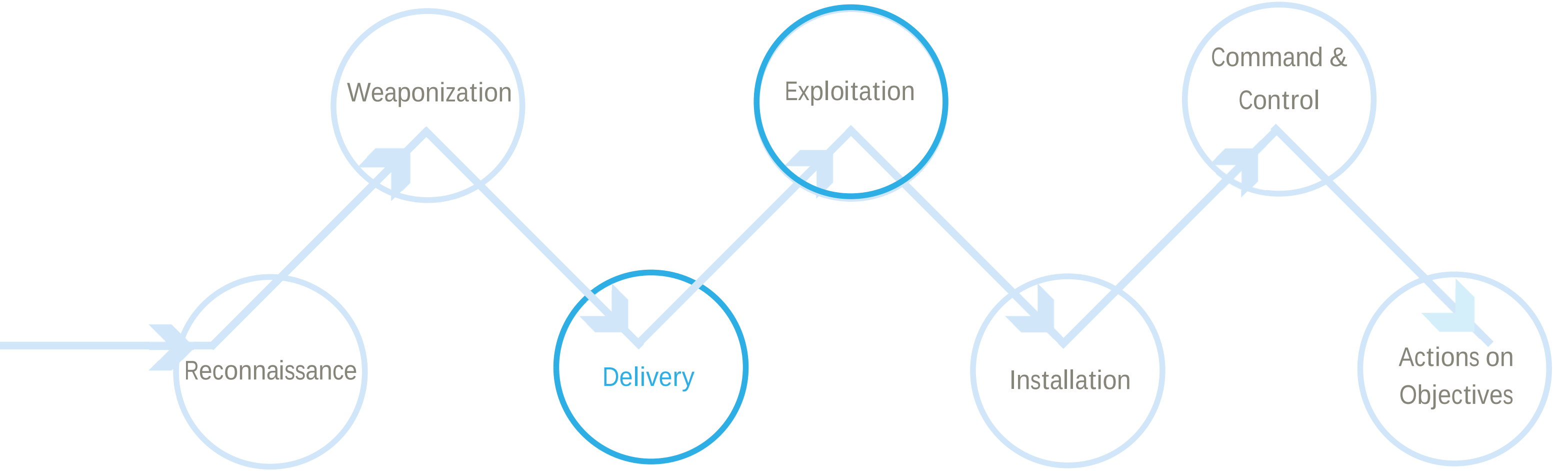
Among others, NÚKIB evaluates cyber incidents also on the basis of MITRE ATT&CK framework, which serves as an overview of known techniques and tactics used in attacks. Attackers often use remote access as an entry vector for an attack. On that ground, we focus here on T1133 technique: External Remote Services.

MITRE ID: T1133

External Remote services technique within MITRE ATT&CK falls into two phases because it may be used to acquire primary access to victim´s network and to get subsequent persistence as well. For this purpose, attackers can exploit remote services with external access (e.g. VPN, Citrix) that allow users to connect to internal corporate network resources from external locations. Connecting usually requires entering credentials that can be obtained by attackers through a variety of other techniques. In some specific cases the access can be acquired also using services not requiring authentication.

Mitigace: One of the basic mitigation measures is to disable or block remotely accessible services that are not necessary. It is also advisable to restrict access to remote services through centrally managed concentrators, such as VPN networks and other managed remote access systems. More generally, multi-factor authentication and network segmentation are also appropriate mitigation measures.

Representation of T1133 in the kill chain showing when attackers use the technique:



Focused on the trend: cybercrime-as-a-service

In December, NÚKIB registered an incident involving the use malware which operates on a malware-as-a-service model. This incident thus corresponds to the trend when various cybercrime actors offer their tools and services for sale under the so-called cybercrime-as-a-service model. Although it is currently widely discussed in the context of ransomware, it is a model under which a range of tools and services can be purchased. They may include not only ransomware, but also other malware types, accesses to previously compromised systems, complex services for phishing campaigns or vishing (for more please see Fig. 1).

Obr 1: Examples of cybercrime services and tools.

DDoS-as-a-service

Offers access to infected devices connected to the Internet (so-called botnet) in order to carry out DDoS attacks.

Access-as-a-service

Offers accesses to compromised accounts or systems.

Malware-as-a-service

Offers malware for further utilization within cyberattacks.

Phishing-as-a-service

Offers complex phishing services ranging from detailed tutorials to pre-prepared emails or legitimate-looking malicious sites.

Vishing-as-a-service

Offers renting of voice systems intended for carrying out of vishing actions.

Cybercrime-as-a-service is therefore a business model enabling virtually any person with sufficient funds to exploit the tools or services for cyberattacks. Due to the growing popularity of this model, which brings with it large profits, competition is also growing, which in turn leads to a wider range of products, but also to a reduction in price. And this again makes the provided services available to a wider group of potential clients.

In many cases, this model also benefits more experienced malicious actors, who can add the malware, ransomware or other tools into their toolsets and use them in more sophisticated attacks or entire campaigns.

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.