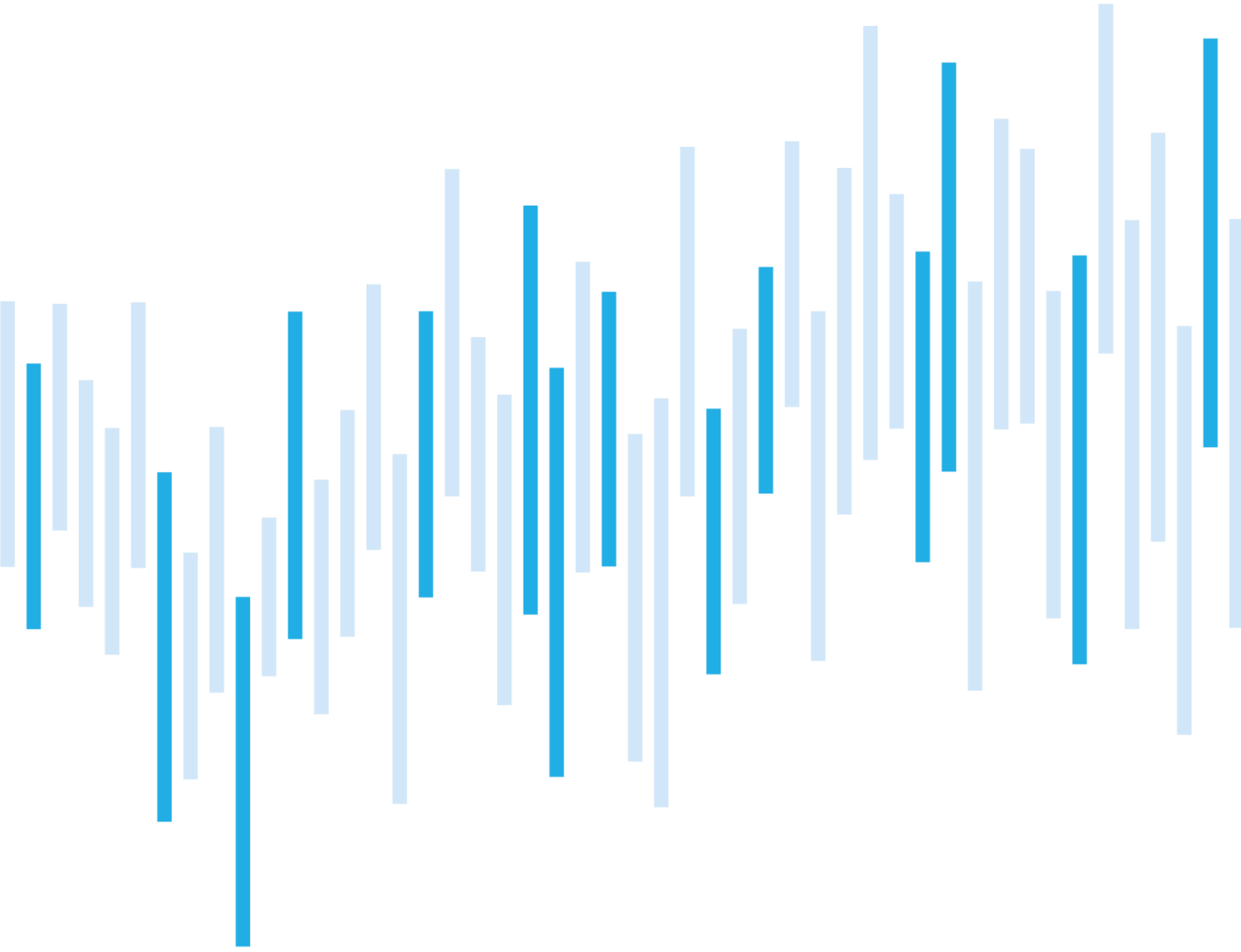
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

NOVEMBER 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

After a rapid growth in October, the number of cyber-attacks returned to slightly higher-than-average values in November. Based on the severity scale, three fifths of the incidents were classified as significant while the rest only as less significant. In comparison with October there were no very significant incidents.

Incidents reported by regulated entities prevailed. The victims were entities from the public administration, healthcare, transport, and banking sectors. Many of the incidents were result of DDoS attacks which indicates a certain extrapolation of the October trend.

Despite the recurring prevalence of DDoS attacks, we focused on the technique known as Email Collection since attackers may collect sensitive information in compromised mailboxes.

Considering the trend, we are focused on ransomware-as-a-service despite the low number of ransomware-related incidents last month. However, it is a long-term and continuously developing threat.

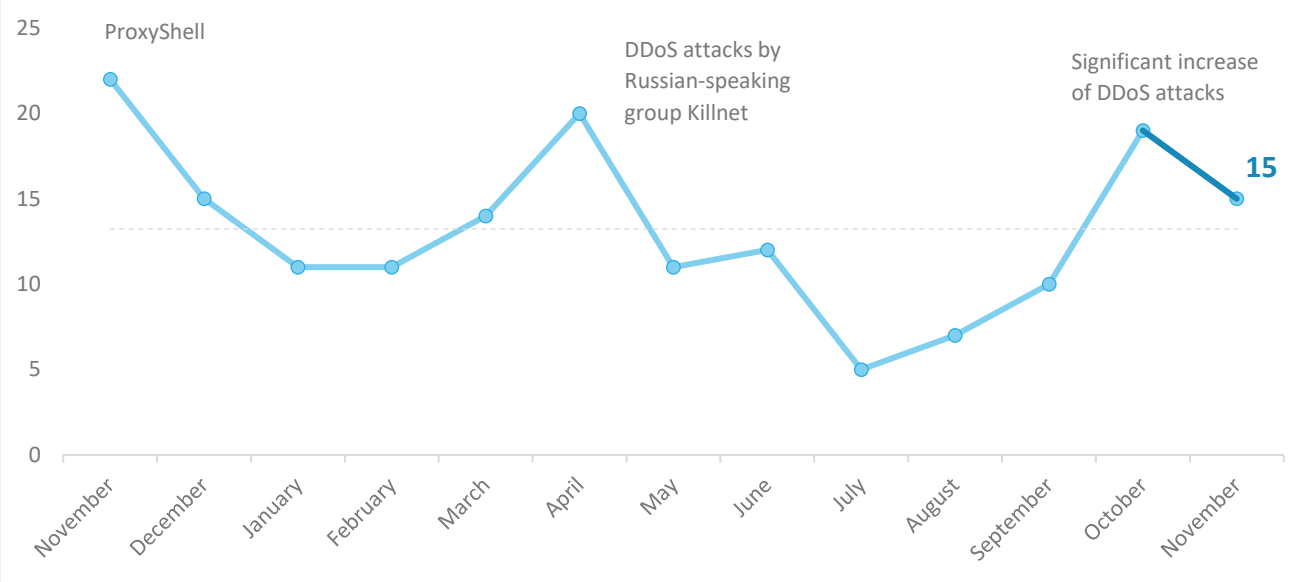
Table of contents

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

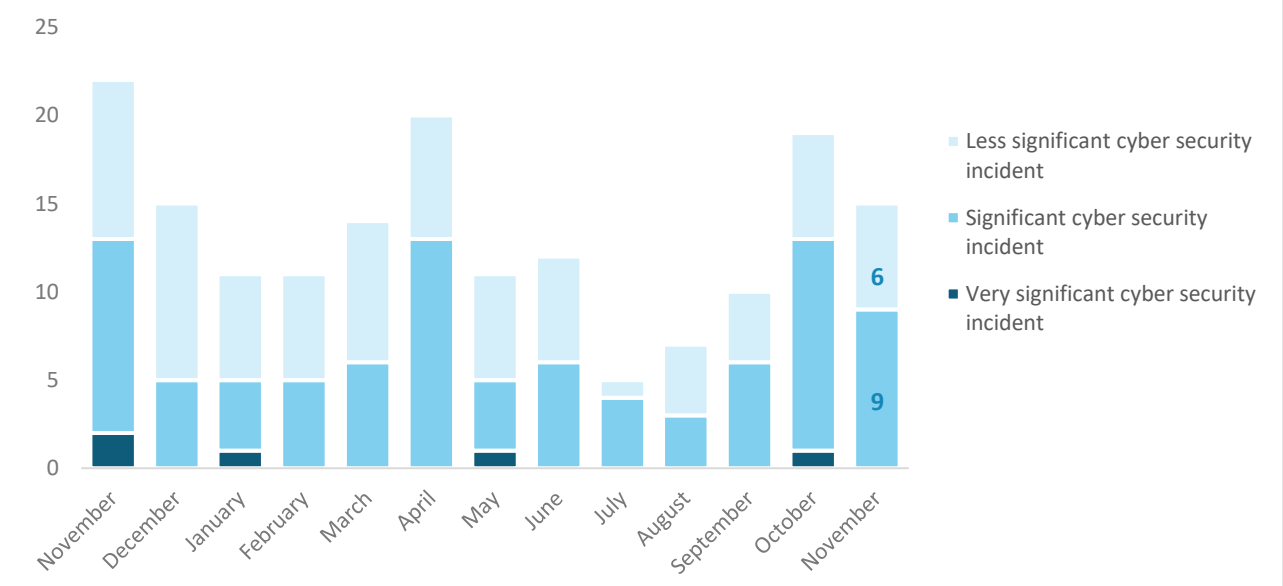
Number of cyber incidents reported to NÚKIB

The number of November incidents slightly decreased in comparison with October; however, it reached higher-than-average values. We detect more incidents during autumn and winter, while compared to previous month, there was no unprecedented increase of DDoS attacks, thus there was a general decrease.[1]



Severity of the handled cyber incidents[2]

Significant incidents prevailed last month. However, compared to October, there was no incident classified as very significant that has occurred three times this year.



[1] Eleven incidents were reported to NÚKIB by regulated entities according to the CSA. Four 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 November incidents into five categories:

- In respect of incident types, attacks on availability still prevailed, with the overwhelming majority being DDoS attacks or, in a minimum of cases, technical errors leading to system outages.
- Two incidents related to information security occurred again after a month's break. Both targets belong to regulated entities active in the healthcare sector. One case was due to data confidentiality breach and in the other a former employee enabled access to the system to unauthorized persons.
- Two of the malicious code incidents involved ransomware attacks.
- One entity became a victim of fraud, when the attackers lured over 900,000 CZK from the victim
- It was the first incident in the category Others since July when the integrity of the application was compromised.

	October 2022		November 2022
Availability e.g., availability disruption caused by a DoS/DDoS attack or sabotage	74 %		**60 %**
Information security e.g., unauthorised access to data, unauth. modification of information	0 %		**13 %**
Malicious code e.g., virus, worm, trojan, dialer, spyware	11 %		**13 %**
Other	0 %		**7 %**
Fraud e.g., phishing, identity theft or unauth. use of ICT	0 %		**7 %**
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 November from the perspective of NÚKIB[4]

Phishing, spear-phishing, and social engineering

Phishing or phishing attempts represent a permanent trend. During November, several entities again faced spear-phishing or its attempts.

Malware

NÚKIB did not analyse any malware based on last month's incident data. However, continuous activities within malware analysis were carried out.

Vulnerabilities

During November NÚKIB issued one vulnerability warning, specifically related to OpenSSL library. Developers originally announced that the vulnerabilities CVE-2022-3602 and CVE-2022-3786 would be marked as critical. Nevertheless, current modern mitigation techniques make difficult or even impossible to exploit vulnerabilities for remote code execution. Eventually, both vulnerabilities were marked as high on the severity scale.

Ransomware

October was the first month this year when no ransomware attack was registered. On the contrary, in November, ransomware appeared again while an unregulated municipal government and a company active in the transport sector were the victims.

Attacks on availability

Comparing the record-breaking October, when DDoS attacks accounted for almost 75% of all incidents, reaching the highest values overall, we saw a decline during November. A major part of the incidents was again related to DDoS attacks. Hacktivists were most likely behind part of the attacks because they considered actions of the targets to be provocative or even hostile, which became the trigger for the attacks.

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

Technique of the month: Email Collection

NÚKIB evaluates cyber incidents, among others, based on the MITRE ATT&CK framework, which serves as an overview of the known techniques and tactics used in cyberattacks. Seeing that the attackers often collect sensitive data from compromised e-mails, we now focus on the technique T1114: Email Collection.

MITRE ID: T1114

During the phase of information collection (within MITRE ATT&CK it is a „Collection" tactics), the attackers may focus on its collection from compromised user e-mails. In addition to confidentiality impairment, the information may be deleted or exfiltrated. Many mailboxes and especially, of senior staff or representatives of organizations with confidential activities, contain strategic character information. The given technique consists of three sub-techniques:

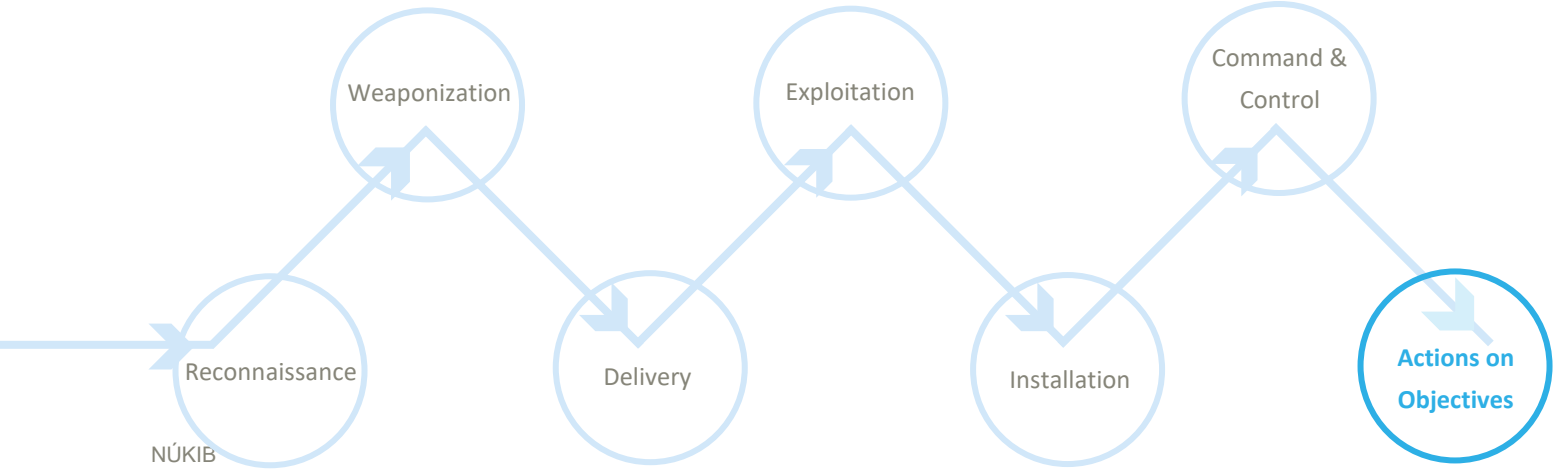
T1114.001 Local Email Collection – Adversaries target local system e-mails. For instance, the files containing data may come from Outlook storage etc.

T1114.002 Remote Email Collection – Adversaries target services like Exchange server or Office 365. Login data may be exploited and an interaction with Exchange server would occur which enables data collection from inside of the network.

T1114.003 Email Forwarding Rule – Adversaries may set rules for message forwarding to collect sensitive data. Misuse of the rules could also bring the monitoring of the victim's activities and further acquisition of valuable intelligence information due to the execution of subsequent harmful activities.

Mitigation: Auditing, sensitive information encryption, or implementation of multi-factor authentication are the basis for mitigation.

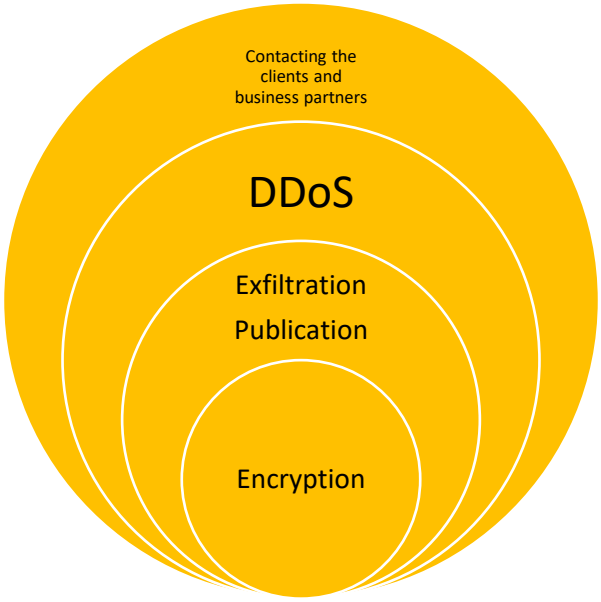
Representation of T1114 in the kill chain showing when attackers use the technique:



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

NÚKIB has been registering ransomware attacks for a long period of time, while the victims fall into a wide range of entities from public administration to private companies and often are not regulated by the Cyber Security Act. **Since 2019-2020 turn the trend known as ransomware-as-a-service (RaaS) prevailed.** It is specific not only by imitating legitimate software and the possibility that malicious software may also be acquired by individuals without the need to develop it or even technical knowledge, but also since it emphasises on multiple extortions.

Figure 1: Multiple extortion



RaaS is a business model where an operator/developer offers its product to clients (malicious actors) for financial profits.

Except for classic encryption, the extortion may be carried out up to four times (quadruple extortion). It may include (not necessarily in this order) exfiltrating data and threats to publish them, DDoS attacks to increase pressure on the victim, and contacting the victim's customers or partners to further increase pressure due to the payment of the ransom. **The stolen data are sometimes published on the darkweb where they are eventually offered to interested parties if the victims have not paid the ransom.** This significantly compromises the data confidentiality, which, apart from not recommended payment of the ransom, also brings possible reputation damage including impacts on victim's business relationships.

Recommendation: Users are recommended to follow basic rules to defend themselves against (spear)-phishing, which remains one of the main ransomware vectors, including for RaaS. Network administrators should also consider implementing tools to limit attackers' access to the victim. NÚKIB issued a recommendation on what to do when attacked by ransomware and an analysis of the ransomware threat. Considering a mitigation, it is recommended to perform regular updates, network segmentation, creating backups, or staff training. It is also recommended that a victim should not pay a ransom. Within the effort to assure comprehensive security, medium to larger organizations can consider the development of Cyber Threat Intelligence or eventually creating teams specifically dedicated to this activity.

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.