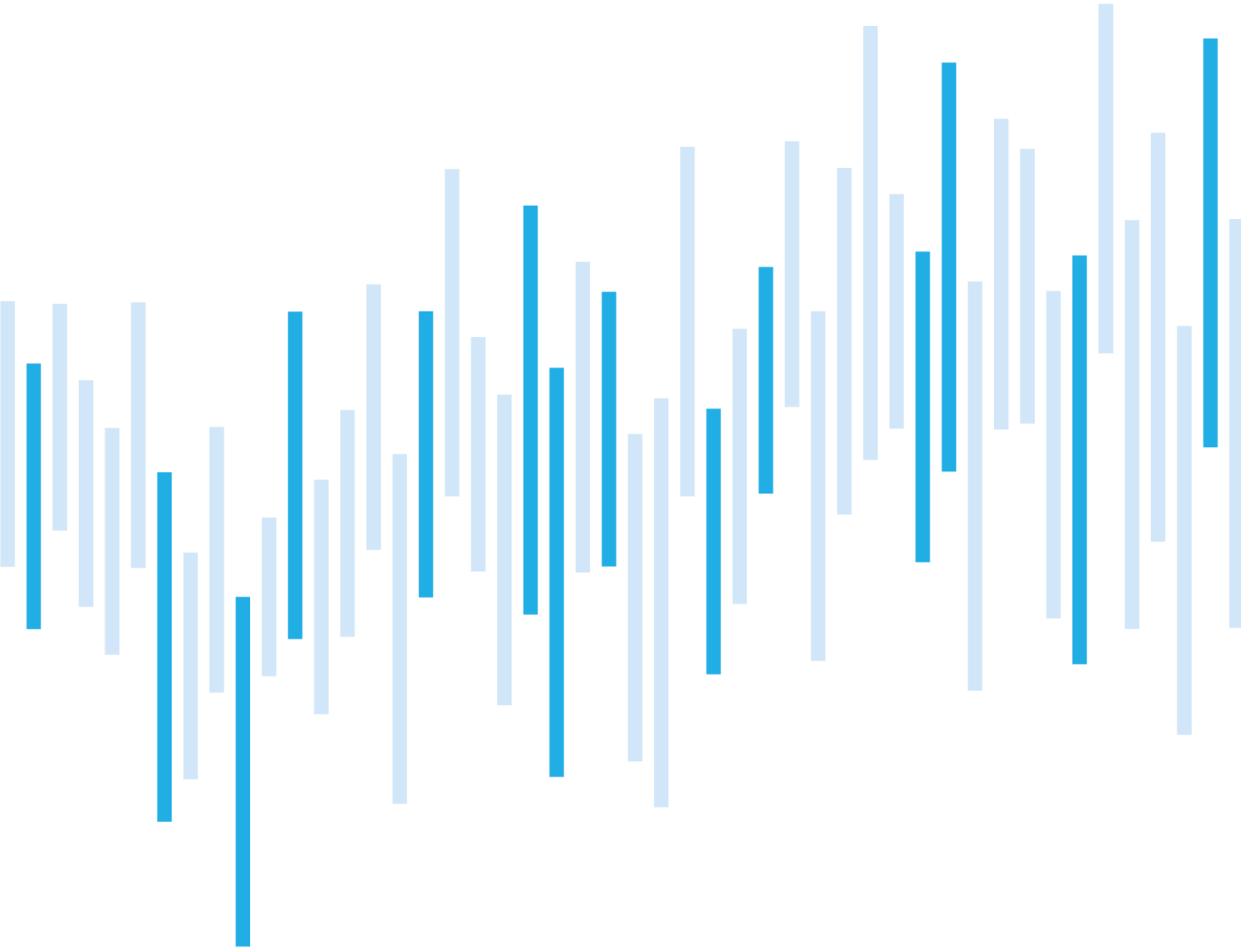
CYBER INCIDENTS FROM NÚKIB'S PERSPECTIVE

NOVEMBER 2021



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary

November was a challenging month in terms of both the number of incidents (22) and their severity. This was mainly caused by expoliting MS Exchange Server vulnerabilities and ransomware attacks.

The MS Exchange Server vulnerability series called ProxyShell first appeared in August this year, but NÚKIB has only now registered its active exploitation when four organisations reported the incident. However, it is likely (55–70%) that the number of Czech compromised targets is much higher considering the prevalence of MS Exchange Server.

November, when ransomware accounted for more than a quarter of all attacks, confirmed the growing nature of this threat. It cannot be ruled out (25–50%) that the return of Emotet malware will be reflected in this negative trend in the coming months. Emotet operators, who began operating their botnets again in November, often leased it to ransomware gangs in the past to serve them as an entry point into organisational networks. The Czech Republic has already experienced such a campaign.

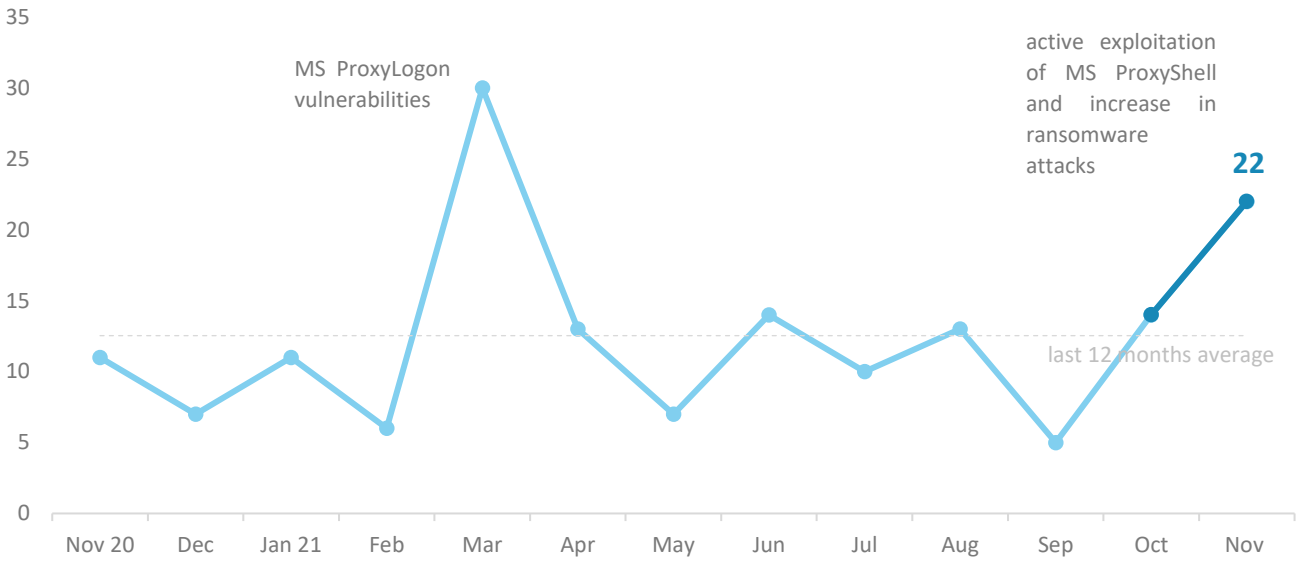
Table of Contents

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, the origin of this information is always stated.

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

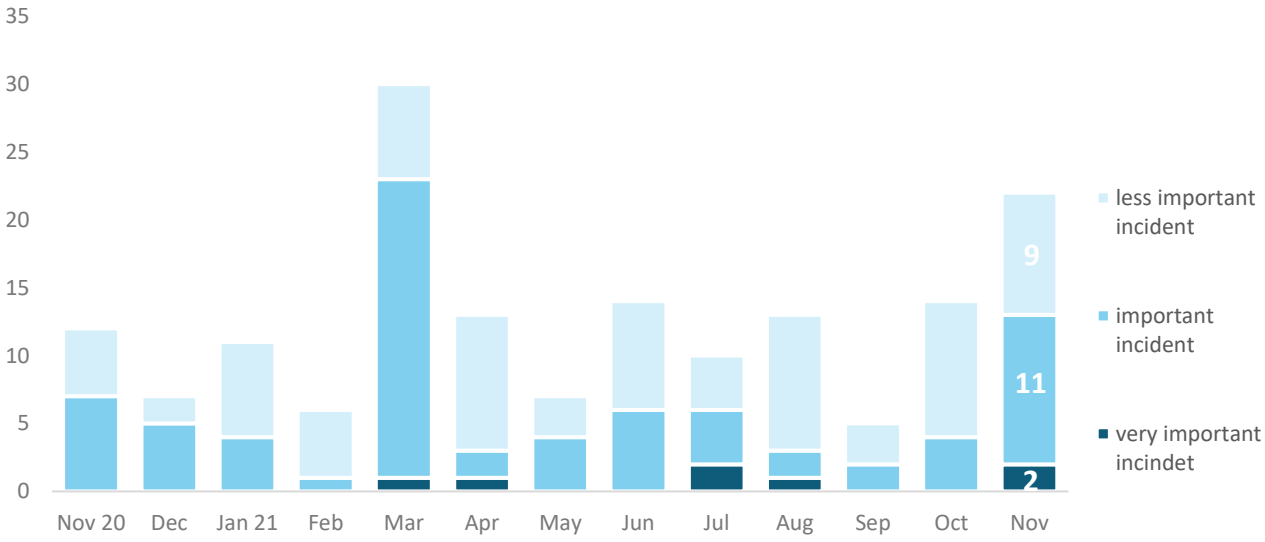
Number of cyber incidents reported to NÚKIB

The number of incidents dealt with by NÚKIB climbed well above this year's average. With 22 incidents, November almost doubled this average.[1]



Severity of the handled cyber incidents[2]

November was also remarkable in terms of the severity of the resolved incidents. In two cases, the cyber incidents were very important and prevented the operators from performing their primary function. At the time of the incident, it was unclear how long it would take to rebuild the networks that contained elements critical to the companies' functioning.

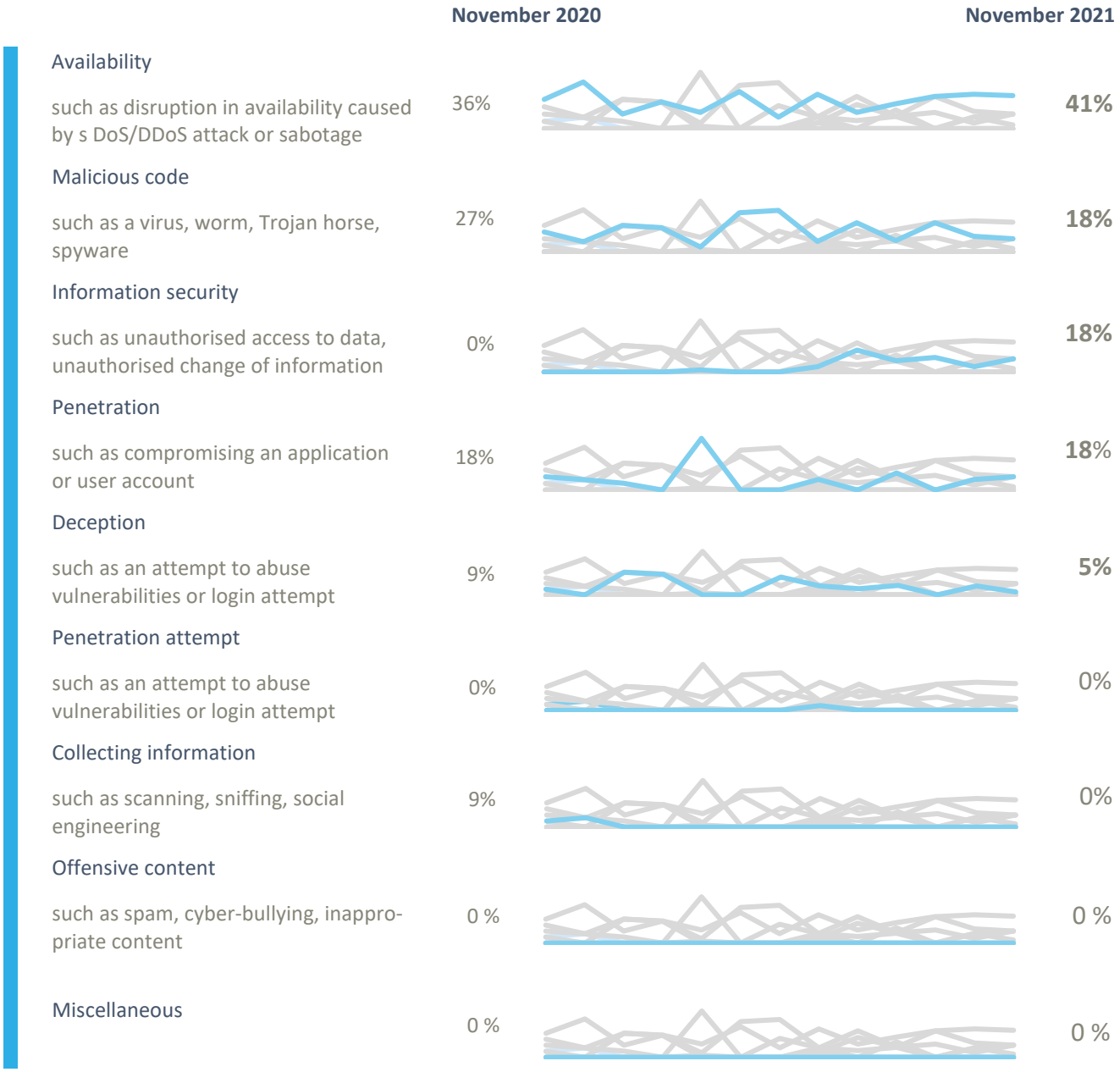


[1] Nine incidents were reported to NÚKIB by obligated persons according to the Cyber Security Act. The remaining 13 incidents were reported by entities that do not fall under this law.
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and internal methodology.

Classification of incidents reported to NÚKIB[3]

Most incidents (9) resulted in the unavailability of services. In four cases, the unavailability was caused by technical errors on the part of the organisations concerned. In another four cases, a partial outage of the service was caused by ransomware. The last unavailability was due to a DDoS attack.

Besides disruptions in availability, NÚKIB also dealt with malicious codes found by four organisations in their networks, four penetrations associated with abusing a series of MS Exchange Server vulnerabilities known as ProxyShell, and four cases of compromised information security. Also in November there were phishing campaigns that compromised user accounts and subsequently sent spams from infected mailboxes.



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

November trends in cyber security from the perspective of NÚKIB[4]

Phishing, spear-phishing, and social engineering

The November MS Exchange vulnerability campaign was closely linked to phishing. In all incidents handled by NÚKIB, the attackers, having gained control of mail servers, downloaded the contents of mailboxes and linked the phishing to their victim's previous legitimate correspondence. They almost certainly (90-100%) did so in the expectation that the recipient would be more likely to open a malicious link if it came in response to a conversation they had with someone they knew.

Malware

Emotet malware has returned to the cyber scene, including the Czech one. This was the first time since January 2021 when Europol, in cooperation with the police forces of several countries, had managed to destroy its infrastructure. Emotet infected one Czech organisation and used its infrastructure as its command and control servers. The return of Emotet is bad news for Czech targets. In 2019 and 2020, they faced several systematic Emotet campaigns, so it cannot be ruled out (25–50%) that another will occur if the malware activity continues to grow.

Vulnerability

In November, the Czech Republic faced active exploitation of the ProxyShell Microsoft Exchange Server vulnerability. ProxyShell first appeared in August this year, but NÚKIB has only now registered its exploitation across the country. The incident was reported by four organisations, both obliged entities and non-regulated organisations. However, considering the prevalence of MS Exchange Server, it is likely (55–70%) that the number of compromised Czech targets is much higher. The probable reason for the active exploitation of the vulnerability is prepared scripts for the attack, which have been available on the dark web since October. You can find more information about this campaign in a public analysis by NÚKIB.

Ransomware

In November, NÚKIB registered six cases of ransomware. In four of those cases, the attackers encrypted part of the infrastructure, making data and services inaccessible to the victims. In the other two cases, they also managed to exfiltrate the data and threatened the attacked organisations with the so-called double extortion.

Organisations were hit by LockBit, Avos Locker, Makop, and Loki Locker, Phobos attacked the remaining two organisations. Phobos is ransomware that has been targeting small and medium-sized businesses throughout the year. LockBit is also a permanent feature in the Czech Republic; this ransomware first appeared in NÚKIB statistics last spring.

Attacks on availability

The November incidents only included one DDoS attack, which made the services of the attacked organisation un-available for eight hours.

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

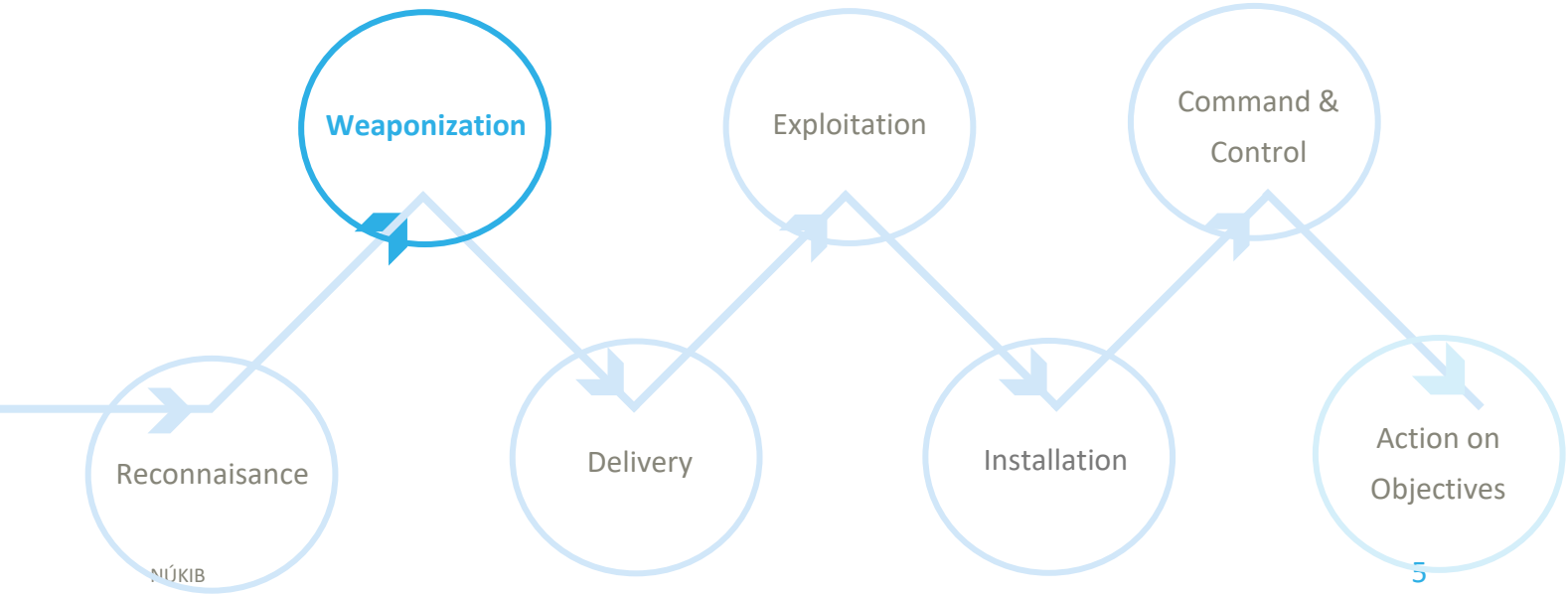
The most used technique of the month: Valid Accounts

NÚKIB also evaluates cyber incidents on the basis of the MITRE ATT&CK framework, which serves as an overview of known techniques and tactics used in cyber attacks. On its basis, NÚKIB determines, among other things, the frequency of the use of techniques/tactics.

MITRE's "Valid Accounts" technique appeared most often in the October incidents. The active abuse of the MS Exchange Server vulnerability was projected into it when the attackers, having compromised the servers, gained access to the victim's mailbox and then sent phishing messages from their legitimate accounts.

> **Valid Accounts** is a technique in which attackers gain access to user accounts, allowing them to move in the infrastructure of the attacked organisation more easily. Access to legitimate accounts makes it easier for them to penetrate various authorisation mechanisms in the system. Legitimate accounts also give them more resilience because the administrator perceives such an account as legitimate and does not pay the needed attention to it. The attackers thus reduce the probability of detection, as their movement is not detected by firewalls, antivirus or other systems that monitor malicious activities.
>
> **MITRE ID: T1078**
>
> **Mitigation:** The mitigation is associated with the recommendations for updating MS Exchange Server. As the "Valid Accounts" technique often goes hand in hand with compromising credentials, its mitigation is also linked to password security. Organisations should enforce strong passwords, require a change after creating a new account, implement multi-factor authentication, and monitor off-hours activity on accounts.

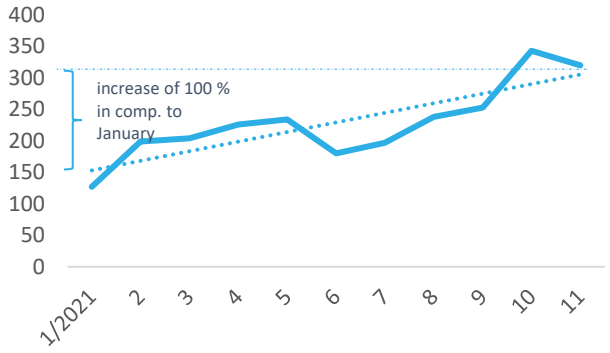
Representation of "Valid Accounts" in the kill chai shows at what stage the attackers use the technique. In NÚKIB incidents, this corresponded to Weaponization, but attackers can generally abuse this technique at most stages of the kill chain.



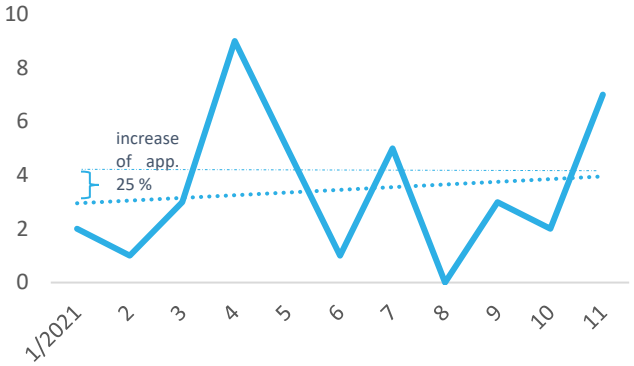
Focus on the threat: Ransomware as a Service

The number of ransomware attacks worldwide and in the Czech Republic is growing. In the last year alone, the number in the world has approximately doubled. In the Czech Republic, it has increased by about a quarter (see the graphs below). Ransomware was widely represented in the November incidents, accounting for more than a quarter of all cyber incidents reported to NÚKIB.

Number of world's ransomware attacks since Jan 2021[5]

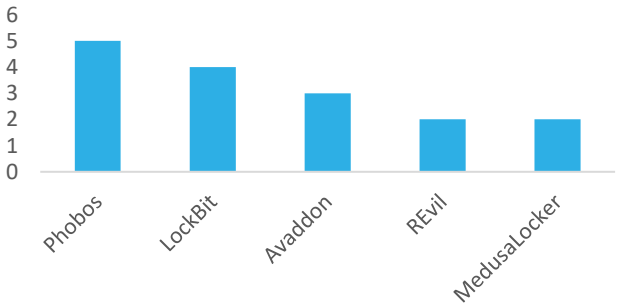


Number of ransomware attacks reported to NÚKIB since Jan 2021[6]



The most active ransomwares in the Czech Republic during 2021 (see chart below) are all leased as a service (ransomware-as-a-service, RaaS).[7] Cybercriminal groups offer their code for a monetary amount to anyone who wants to carry out a ransomware attack. RaaS is, therefore, an ever-changing threat. Unlike APT groups, whose operations are more permanent, some cybercriminal groups operate only for a short time. It often happens that after the demise of one, another appears that uses similar operational procedures.

Five most active groups in the CZE since Jan 2021



Ransomware attacks on Czech targets are very likely (75–85%) to increase further in the short term. There is a realistic possibility (25-50%) that the return of Emotet malware will be reflected in this growing trend. Emotet operators, who began operating their botnets again in November, had in the past often provided access to infrastructure to ransomware gangs to serve as an entry point into organisations' networks. The Czech Republic has already experienced such a campaign in the past. Before Christmas 2019, the Ryuk ransomware spread across the Czech sectors, and Emotet always stood at its beginning.

---

[5] The data in the graph are based on the DarkTracer website, whose administrators monitor dark web and generate statistics based on information from ransomware group sites. Thus, not all ransomware attacks will be included in the statistics, but only the attacks of those groups that publish information about their attacks.

[6] This graph is based on incidents reported to NÚKIB. Based on dark web monitoring, we know about other Czech victims of ransomware groups, but since they have not reported the attack to us (as unregulated entities they were not obliged to do so), we did not include them in the statistics for the sake of the consistency of the data.

[7] ditto

Probability Terms Used

Probability terms and expression 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 Use of Information

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.