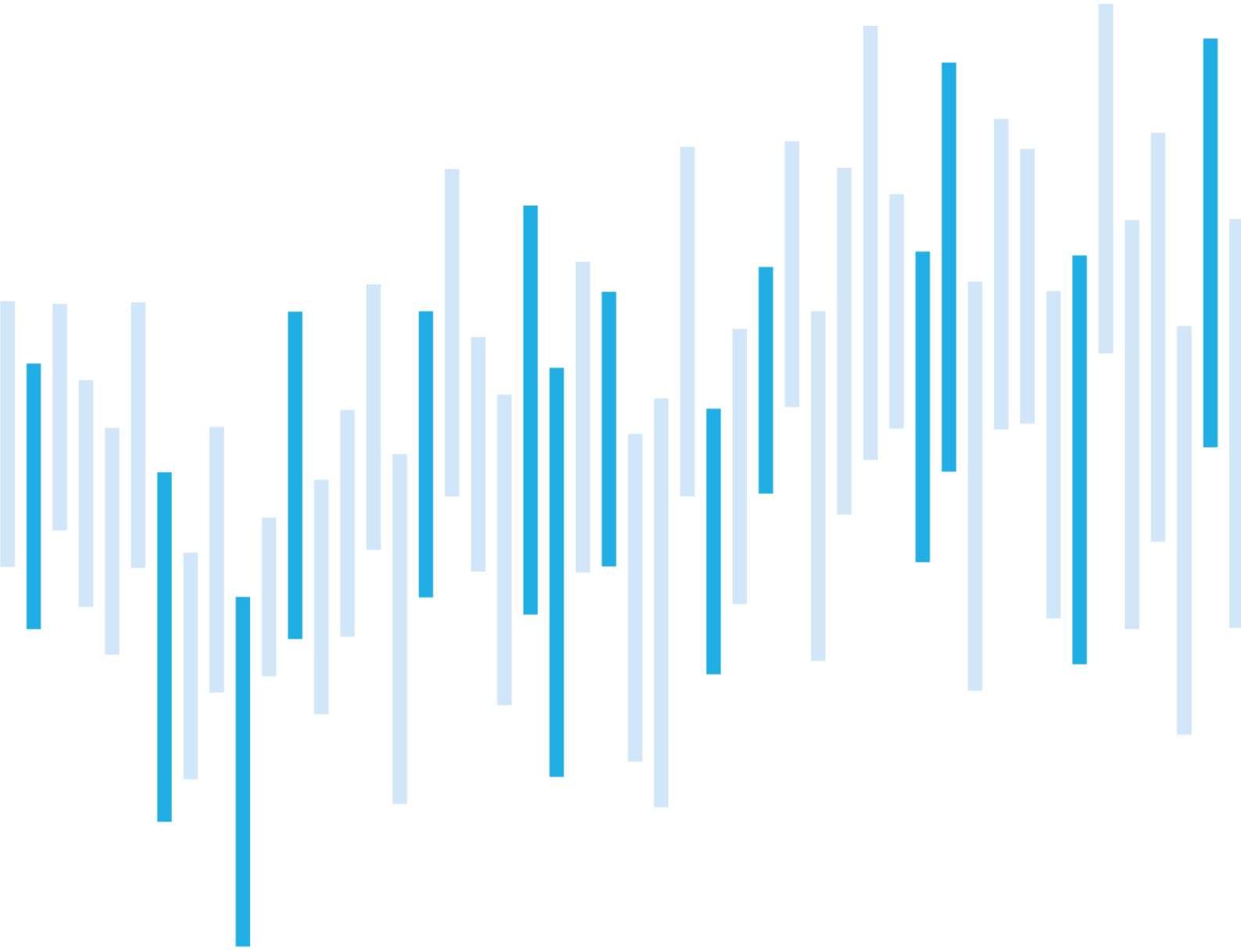
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

SEPTEMBER 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

After a traditionally relatively quiet summer months, the number of incidents in September nearly reached the average value. Contrary to the last year, when the number of incidents did not show a growing trend until October, the growth began already in September this year. An important portion of September's incidents was categorised as significant.

Incidents reported by regulated entities dominated in September. Similarly, as in August, no sector was more affected than the others. Entities of public administration, transportation, healthcare, or financial sector were affected.

This month, we focus on Gather Victim Identity Information technique, which serves as a first stage of the attack.

Given the developing attacks targeted at multi-factor authentication (MFA), the chapter "Focused on a trend" deals with them.

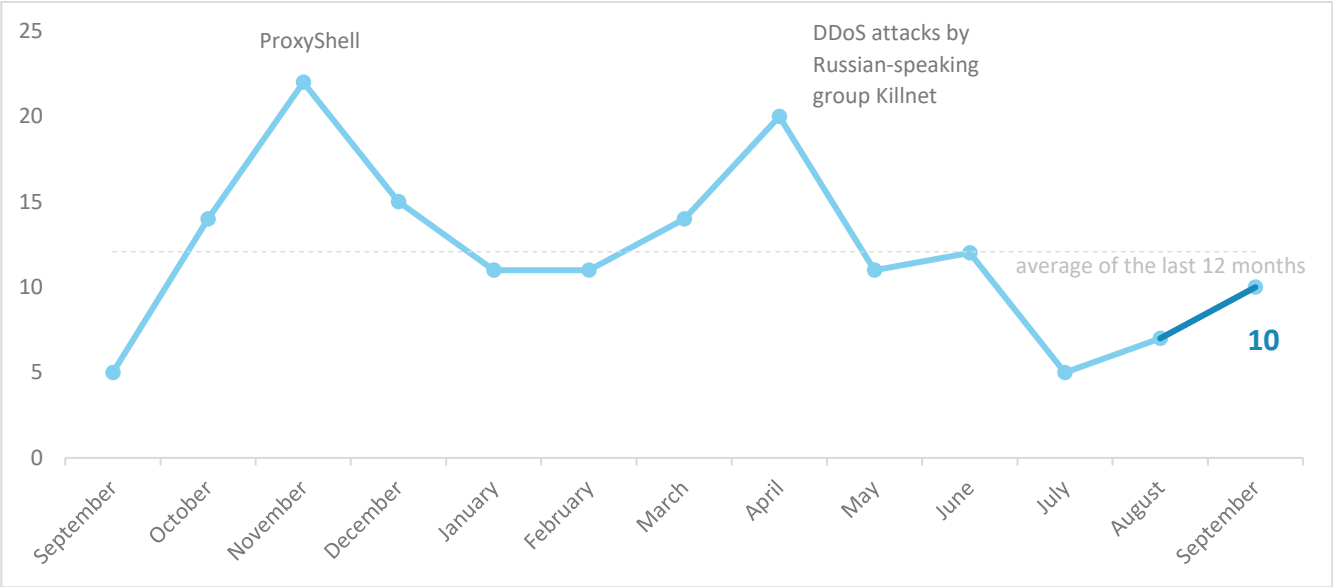
Table of contents

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.

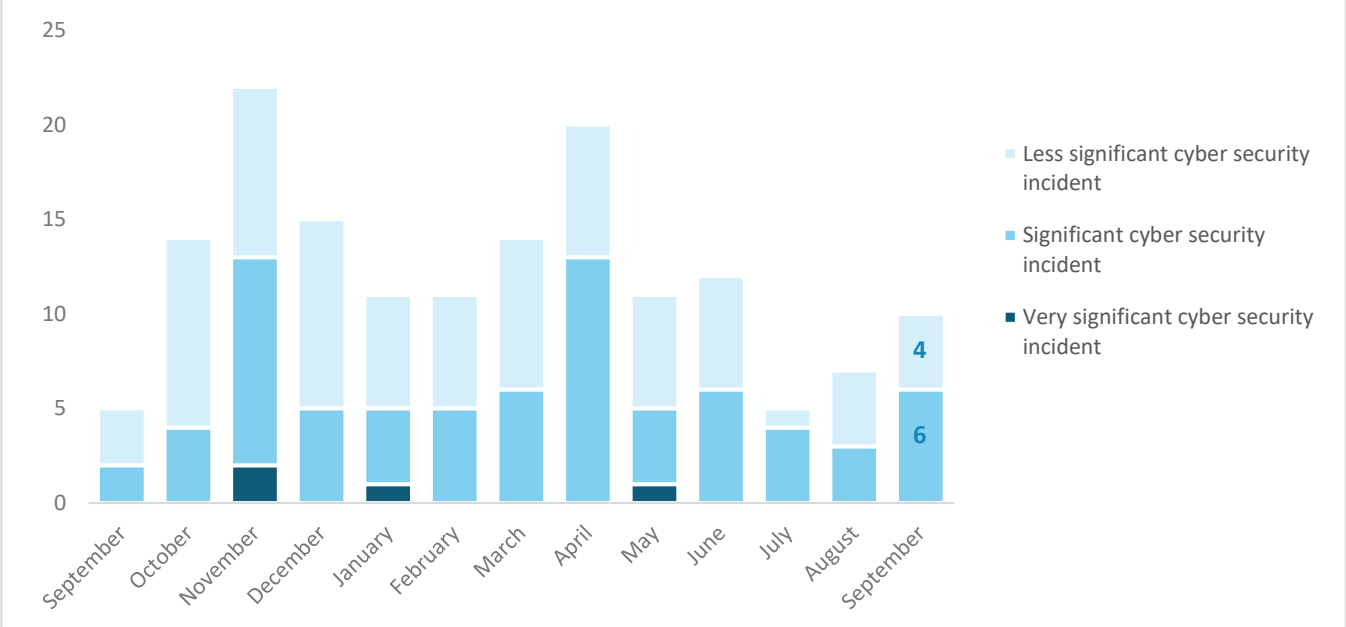
Number of cyber incidents reported to NÚKIB

The number of incidents climbed almost back to average in September. After the relatively quiet summer months, the number of incidents tends to increase every year.[1]



Severity of the handled cyber incidents[2]

Significant incidents very slightly prevailed in September. As in the previous three months, there was no very significant incident.



[1] Seven incidents were reported to NÚKIB by regulated entities according to the CSA. The remaining three 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 the incidents that occurred in September within four categories:

- There were attacks on availability again, which is a lasting trend. Two cases involved a DDoS attack, while another two were linked with ransomware.
- Network and user accounts compromise are another lasting trend.
- In one case, a malicious code was launched on victim's device with following attempt to communicate with adversarial server.
- First time since May, an incident classified as information security occurred. Nevertheless, the victim actively dealt with the incident and prevented unauthorised access.

	září 2021		září 2022
Availability e.g., availability disruption caused by a DoS/DDoS attack or sabotage	40 %		60 %
Intrusion e.g., compromising an application or user account	0 %		20 %
Information Security e.g., unauthorised access to data, unauth. modification of information	0 %		10 %
Malicious code e.g., virus, worm, trojan, dialer, spyware	40 %		10 %
Fraud e.g., phishing, identity theft or unauth. use of ICT	20 %		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 %
Other	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 September from the perspective of NÚKIB[4]

Phishing, spear-phishing, and social engineering

Phishing and phishing attempts are a lasting trend. However, in September, no interesting case was recorded.

Malware

Based on the data from September, NÚKIB did not analyse any malware.

Vulnerabilities

NÚKIB released two alerts against vulnerabilities in September. The first alert was about the CVE-2022-26113 (CVSS 7.5) in FortiClient. This vulnerability enables an unprivileged user with an access to the device on which the FortiClient VPN client is installed to gain SYSTEM user rights. The other alert was about two MS Exchange Server vulnerabilities, namely the CVE-2022-41040 (CVSS 6.3) and the CVE-2022-41082 (CVSS 8.8).

Ransomware

The trend of ransom attacks continued in September. The number of registered attacks remained the same, with Phobos and DeadBolt ransomware used for the attacks.

Attacks on availability

Like in August, DDoS attacks also occurred in September. One of the incidents involved a combination of UDP Flood, IP Fragmentation, and DNS Amplification.

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

Technique of the month: Gather Victim Identity Information

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. During the initial stage of serious attack, attackers must first gain information about the identities of their victims; therefore, this report focuses on the technique T1589: Gather Victim Identity Information.

MITRE ID: T1589

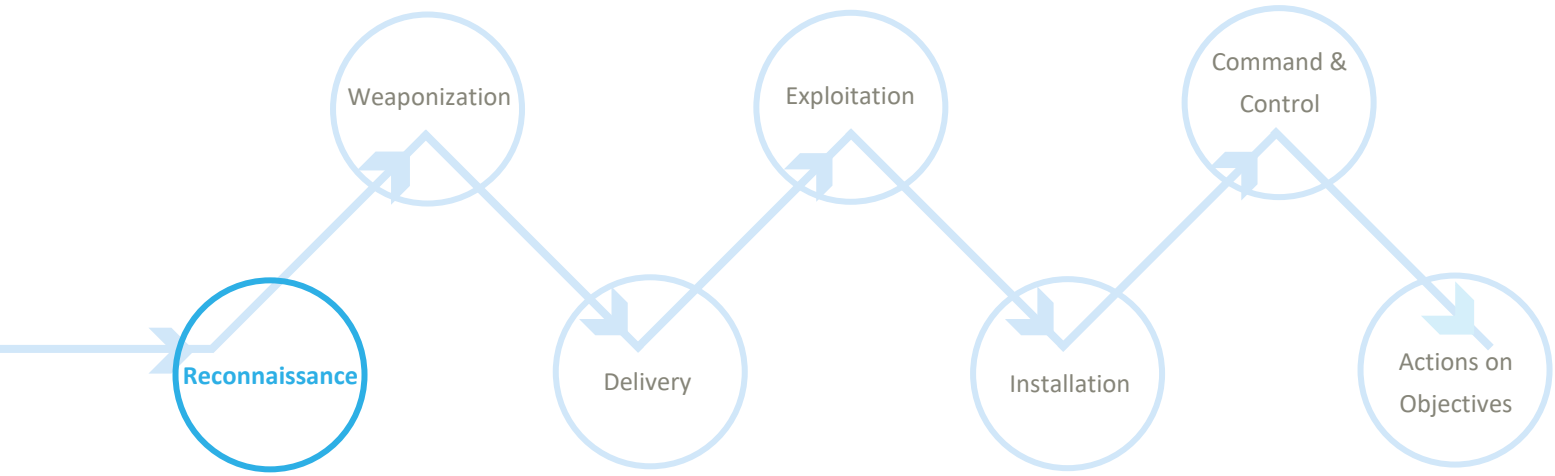
During the first stage of the reconnaissance, attackers concentrate on gathering information about the identities of their potential victims. The information can contain both personal details (such as names of employees) and sensitive data (such as logging details). They can gather information "actively", i.e., through phishing or active scanning, or non-invasively from publicly available sources (from social networks, for example). The latter case is known as Open-Source Intelligence (OSINT).

The gathered information can be used as an excellent basis for further reconnaissance, creation of operational resources, or initial access to the victim's network. The technique further divides into three sub-techniques: the T1589.001: Credentials, the T1589.002: Email Addresses, and the T1589.003: Employee Names.

A very similar technique is the T1589: Gather Victim Org Information. Within this technique, attackers focus on finding physical locations (an infrastructure, for example), assessing the business tempo, business relations, and identifying roles.

Mitigation: The technique is not easy to mitigate. Entities shall primarily concentrate on minimising the amount of data (primarily sensitive data) that are available from outside and thus exploitable through the OSINT.

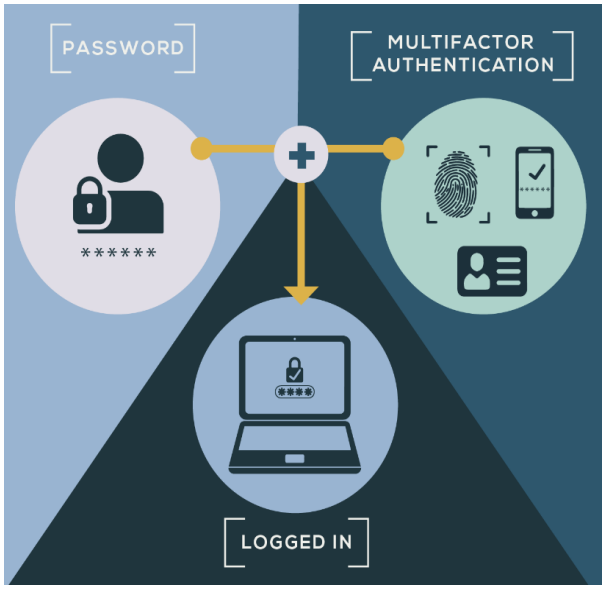
A representation of the T1589 technique in a kill chain, showing at which point attackers use it:



Focused on a trend: Attacks against MFA (multi-factor authentication)

Multi-Factor Authentication (hereafter only MFA) is a recommended practice to secure accounts or remote access. Authentication using a password is deemed to be outdated and not resilient against common attacks such as phishing or brute force password guessing. In addition, password database breaches are not infrequent despite consistent protection, resulting in password being compromised without any fault on the user's side. A requirement of another factor prevents a potential attacker from accessing even if one has the password. We need to bear in mind, though, that it only represents increased protection against attacks on the password rather than uncrackable securing.

Fig. 1: Illustrative image of multi-factor authentication



The number of attacks against MFA has significantly grown over the last months. Attackers quickly adapt to the widespread introduction of MFA. Moreover, many new open-source tools are being created that facilitate circumventions or thefts of authentication tokens. The most frequent types of the attack are the following:

1) Authorisation code interception

Just as a password can be eavesdropped using a keylogger or when communicating over an unsecured channel, an authorisation code can be obtained in the same way. This code protects against cracking the password from the outside, nevertheless it cannot prevent account theft if the end user's device has been compromised.

2) MFA fatigue

One of the MFA methods is a confirmation of access in an application where the user obtains a notification asking them to approve or reject the access. Since no code is copied, this method is eavesdropping resilient. However, it is more vulnerable due to the human factor. With the number of notifications obtained, a user may not pay sufficient attention to notifications and hence allow access unwittingly or by mistake.

3) Adversary-in-the-middle

With this type of attack, a user obtains a link to a visually similar domain owned by the attacker (e.g., g00gle.com), which serves as an intermediary of the actual service (google.com). As the site contains real content of the required service thanks to the redirecting, a scam can only be detected by careful check of the domain and its certificate. This method requires the attacker to register a domain that serves as a proxy sending logging details to the given service. The site indirectly communicates with the real server of the service, so the user obtains a legitimate alert asking for MFA authentication. However, the attacker captures the code immediately and thus gains access.

These attacks may be mitigated by authentication via physical token, for example using a FIDO standard.

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 %

Podmínky využití informací

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.