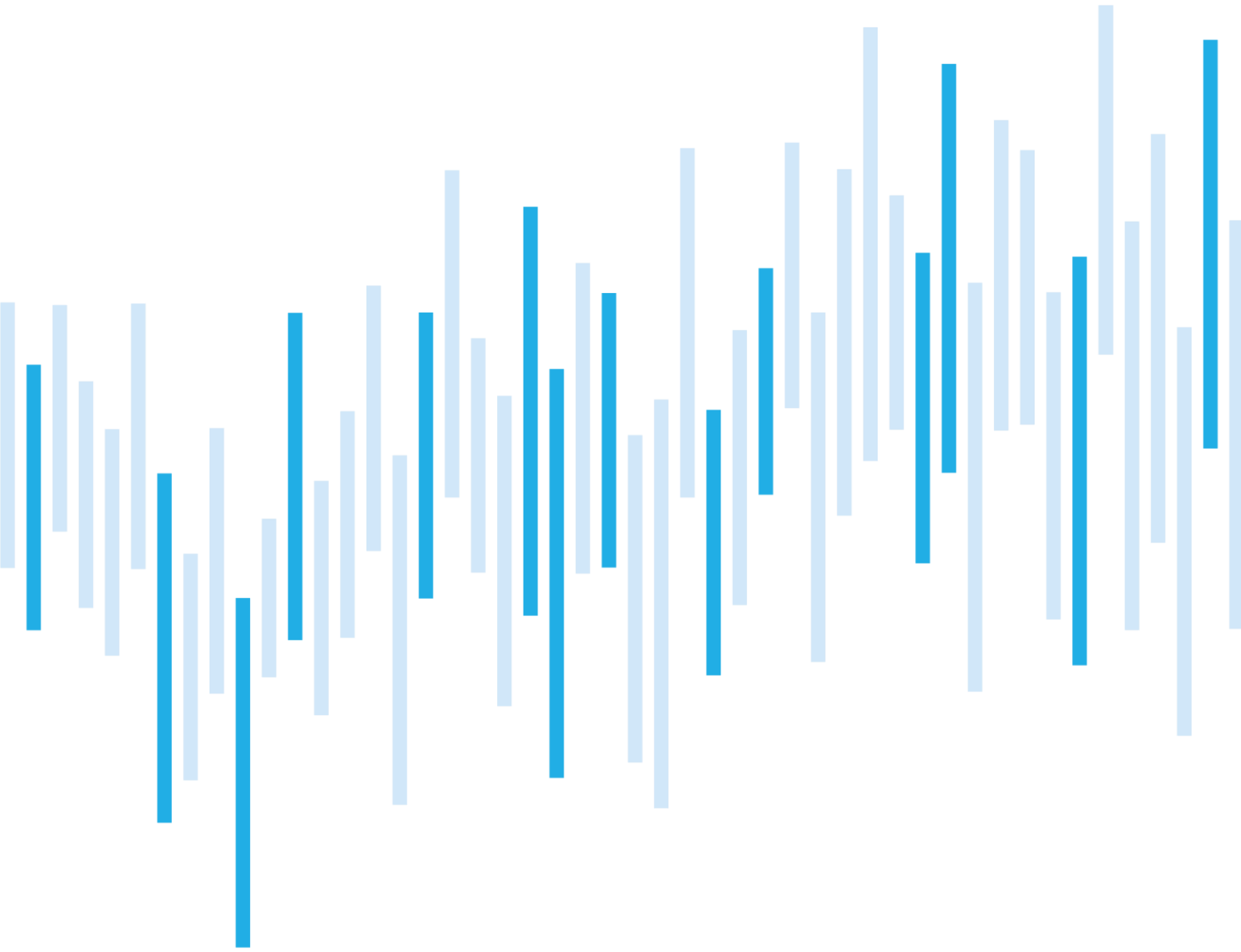
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

OCTOBER 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

During October, the number of incidents reached values well above the average; the highest rate since last April (20 incidents in total). DDoS attacks, whose number almost reached cumulative values since the beginning of this year, are one of factors large share of this increase. Part of the DDoS attacks was performed by the hacktivist group Anonymous Russia, which declared its attacks on the Telegram network.

We recorded the first incident classified as very significant since May. It was an attack on telecommunication services availability. Incidents reported by regulated entities subject to CSA obviously prevailed in October. Public administration and transport sector entities were the most frequently affected ones and involved in half of all incidents.

This time, Direct Network Flood (T1498.001) and Reflection Amplification (T1498.002), are the techniques of the month. The mentioned techniques are closely tied to DDoS attacks applied widely against Czech entities. On that ground we focused on the DDoS attacks and its increased dangers this month.

Table of contents

Number of cyber incidents reported to NÚKIB

Severity of the handled cyber incidents

Classification of the incidents reported to NÚKIB

Trends in cyber security in October from the perspective of NÚKIB

Technique of the month: Direct Network Flood and Reflection Amplification

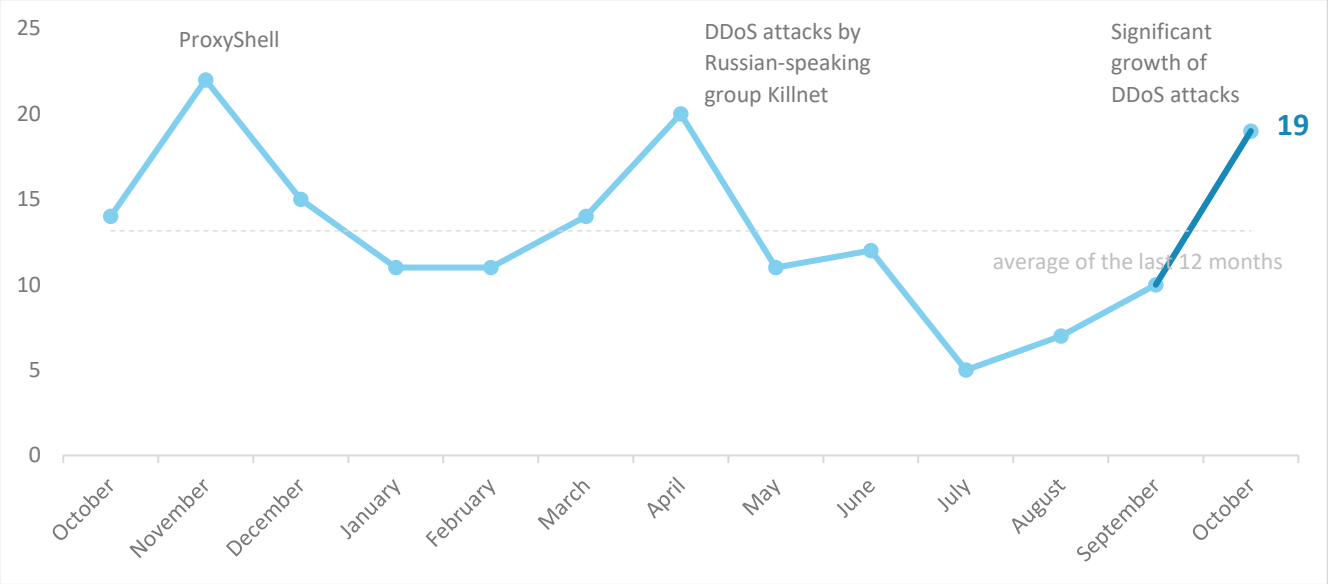
Focus on the trend: increased DDos attack dangers

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.

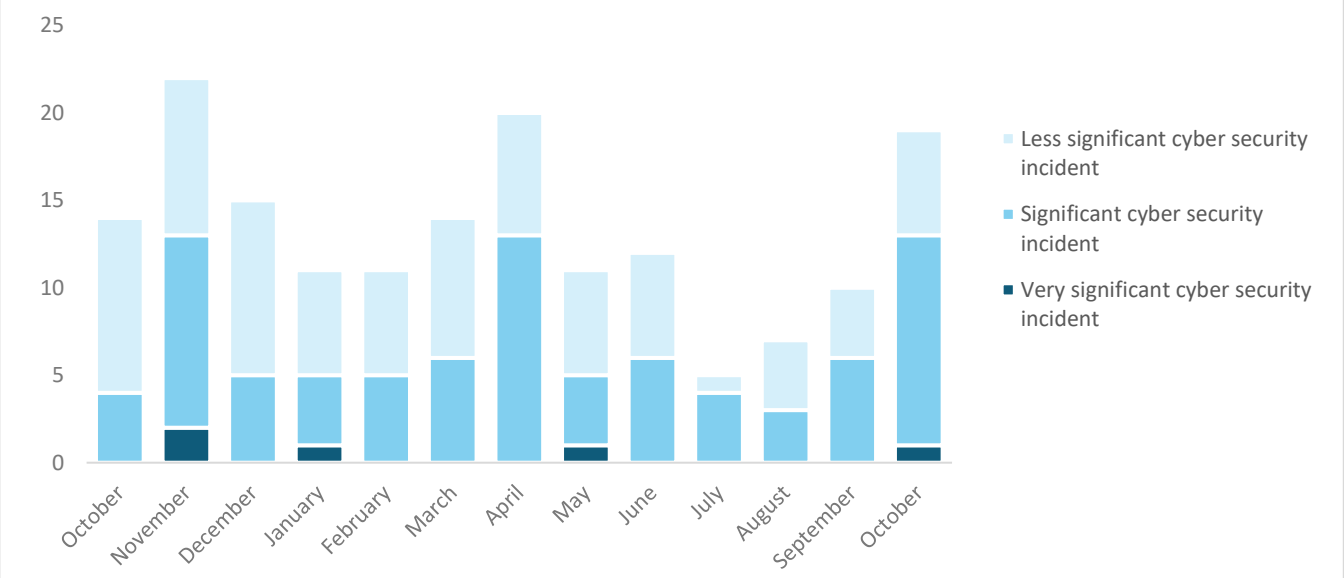
Number of cyber incidents reported to NÚKIB

The number of October incidents highly exceeded average values and almost met the record-breaking number for April this year (20 incidents in total). Like in April, the increase was again caused mainly by the unprecedented growth of DDoS attack numbers. While DDoS attacks were responsible for less than one-third of incidents in the spring, they now account for nearly 70% of them.[1]



Severity of the handled cyber incidents[2]

Incidents classified as significant very slightly predominated during October. For the first time since May, there has been a very significant incident.

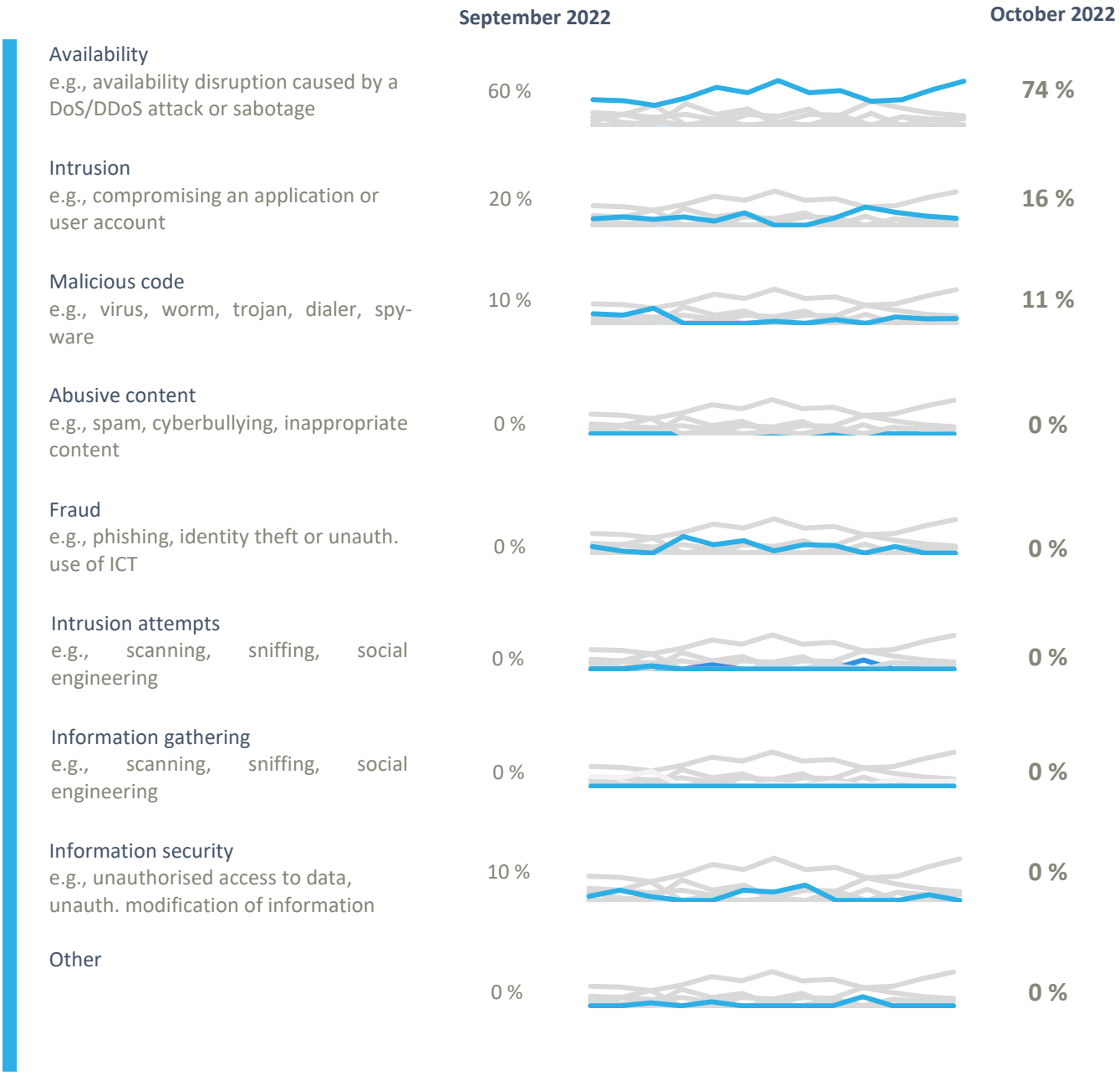


[1] Twelve incidents were reported to NÚKIB by regulated entities according to the CSA. The remaining seven incidents were reported by entities that do not fall under this law.
[2] NÚKIB determines the severity of cyber incidents based on Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB[3]

NÚKIB classified the October incidents into three categories:

1. Though availability attacks represent a permanent trend, their share of total incidents grew from 60% to nearly 75% in a month. The unprecedented increase of DDoS attacks was the reason. Their total almost equalled its actual summary values for the entire year, with Anonymous Russia group attacks against Czech entities being one of the reasons.
2. Network and user account compromises are an ongoing trend. During the past month, the infrastructure of several entities was abused to send phishing and spam, which caused, among other things, damage to the reputation of their domains.
3. Concerning the malicious code, two incidents stood out, namely the using the ProxyNotShell vulnerability with subsequent deployment of malware in one healthcare sector organization and the discovery of crypto-currency mining malware (cryptominer) in the transport sector.



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

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

Phishing, spear-phishing, and social engineering

Phishing or phishing attempts are permanent trend. During October, the infrastructure of several entities was abused for sending of phishing e-mails. Among other issues, the damage of domain reputation was the result.

Malware

NÚKIB did not analyse any malware based on the data from the October incidents. Malware analysts focused on RedLine Stealer malware as well as Mirai botnet within their continuous activities.

Vulnerabilities

NÚKIB issued two vulnerability alerts during October. The first one related to CVE-2022-26113 (CVSS 7.5) in FortiClient. This vulnerability enables to get a remote access to the administrator interface in FortiOS (firewall) and FortiProxy (web proxy). The second one dealt with the vulnerability of Wi-Fi in Linux core.

Ransomware

Ransomware was not reported for the first time this year. Before, ransomware had been the long-term constant trend, particularly when offered as a service (ransomware-as-a-service).

Attacks on availability

Though availability attacks constitute a permanent trend, there was a significant increase in October. Except for one case, these were DDoS attacks, whose number almost equal a cumulative value for the whole year 2022. Attacks by Anonymous Russia group, which announced attacks against Czech entities on its account on Telegram, were one of the causes. Adversaries primarily used less sophisticated HTTP flooding method.

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

Technique of the month: Direct Network Flood and Reflection Amplification

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. Considering the massive increase in DDoS attacks, this time we focus on sub-techniques T1498.001 (Direct Network Flood) and T1498.002 (Reflection Amplification).

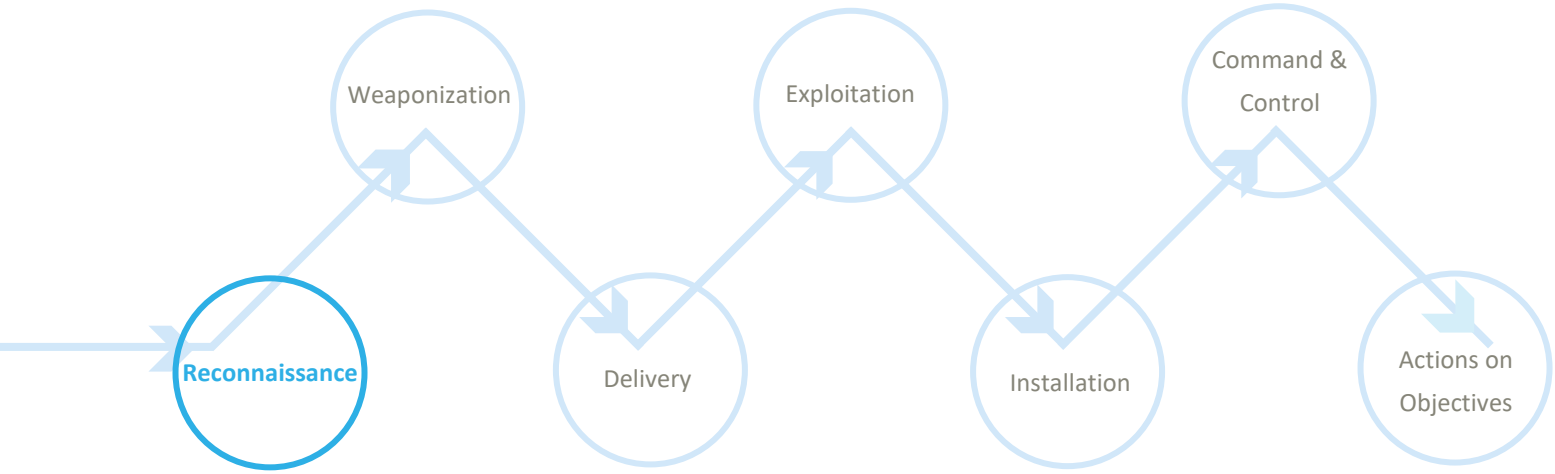
MITRE ID: T1498.001 + T1498.002

Direct Network Flood: Attackers may attempt to deny a service by direct "flooding" the target system with high volume of traffic. Such attack could affect an availability. During this attack, one or more systems are used to send network packets and almost any network protocol can be used to "flood". Usually, UDP and ICMP protocols are used, although also TCP and others can be used.

Reflection Amplification: Attackers can also use a third-party server intermediary that hosts and will respond to the spoofed source IP address. Given type server is known as reflector. The attack is then carried out by sending packets to the reflector with victim's spoofed addresses. During this type of attack, a much larger response is sent to the victim's server due to the size of the query entered by the attacker.

Mitigation: Network traffic filtering is the key mitigation technique. Harmful traffic needs to be filtered from the legitimate one, which is provided by internet service providers (ISP) or third parties. Depending on the volume, on-premises filtering may be possible by blocking IP addresses that are the source of the attack, targeted ports, or protocols used for transmission.

Representation of T1498.001 and T1498.002 techniques in the kill chain showing when attackers use the technique:

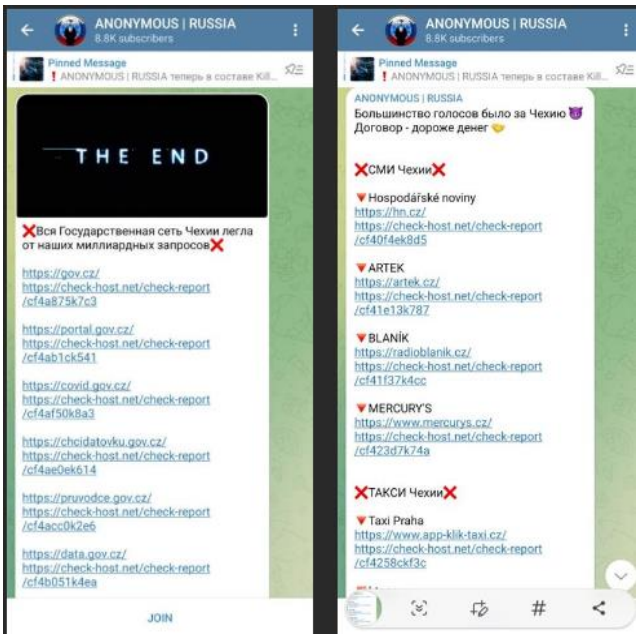


Focused on the trend: increased DDoS attack dangers

Significant increase of DDoS attacks is the trend of October. **As previously said, when the nine months are added together, their number nearly equals the summary values from 2022.** Russian-language group Anonymous Russia has claimed part of these attacks. A similar wave of DDoS occurred in April, when Killnet targeted several Czech entities.

On October 2, Anonymous Russia declared attacks against Czech organizations on the Telegram social network. These included government institutions, media, banks, or airports, but also targets like restaurants. **Despite of that the real impact was rather low and only few of the originally declared targets were hit.**

Fig.1 Objectives declared by Anonymous Russia



This kind of groups are identified as hacktivist and may have a wide motivation scale. Separately issued alert from November 1 mentions that hacktivists or so-called patriotic hackers may attack in connection to political decisions and declarations perceived by them to be hostile. This year, Poland, Lithuania, Latvia, Estonia, Romania, Italy, and Germany faced similar attacks too. **Despite the targeting context, it is not possible to evaluate whether and possibly to what extent these actors are connected to specific states and their power authorities.**

Recommendation: Even though DDoS-type attacks usually have little long-term impact and primarily result in the inaccessibility of websites or related services, it is still desirable to implement certain measures. Warning from February 25, 2022, includes recommendations directly related to DDoS attacks. The measures in 3.1 and 3.2 can be used by any organization, while clauses 3.3 and 3.4 are intended specifically for internet connection providers.

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.