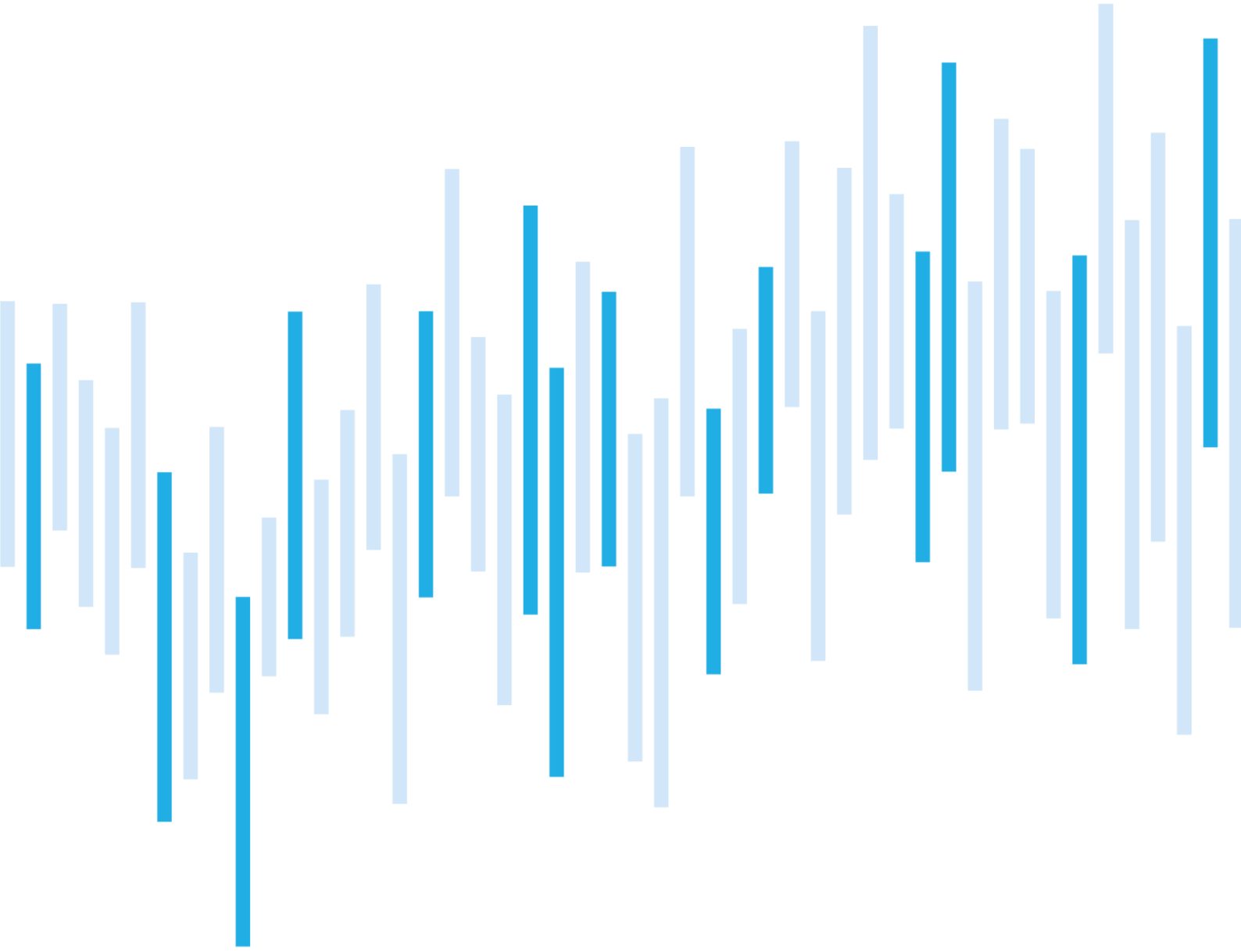
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

JANUARY 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

In January 2023, NÚKIB registered more than a double increase of cyber incidents compared to the previous month. Most of the incidents were reported to NÚKIB by its constituents, many of them from the public administration sector.

Although the number of cyber security incidents increased considerably, their severity remained low. NÚKIB classified most of them as less significant. It was given by the fact that the majority of the cyber security incidents that NÚKIB handled in January were DDoS attacks against victim websites without serious consequences.

Russian-language group NoName057(16) was behind the increased number of DDoS attacks, which hit a number of websites of state and private entities. Therefore, in the final chapter, we focus on this group and its January campaign against the Czech targets.

Also, following the increase in recorded DDoS attacks, this report focuses on the T1498 technique: Network Denial of Service with an emphasis on mitigation options.

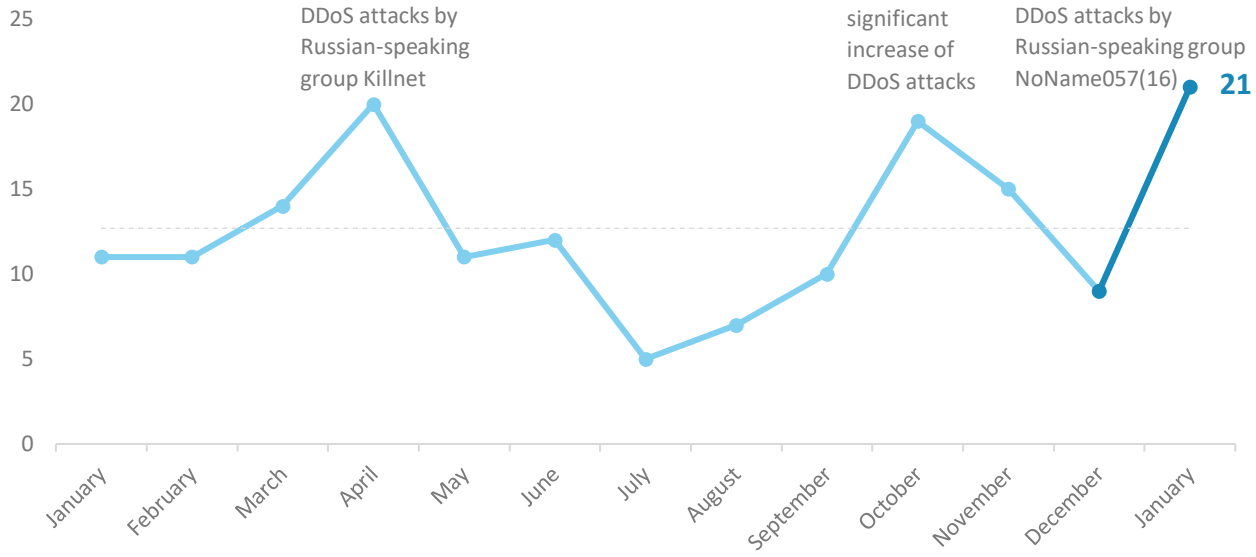
Table of contents

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

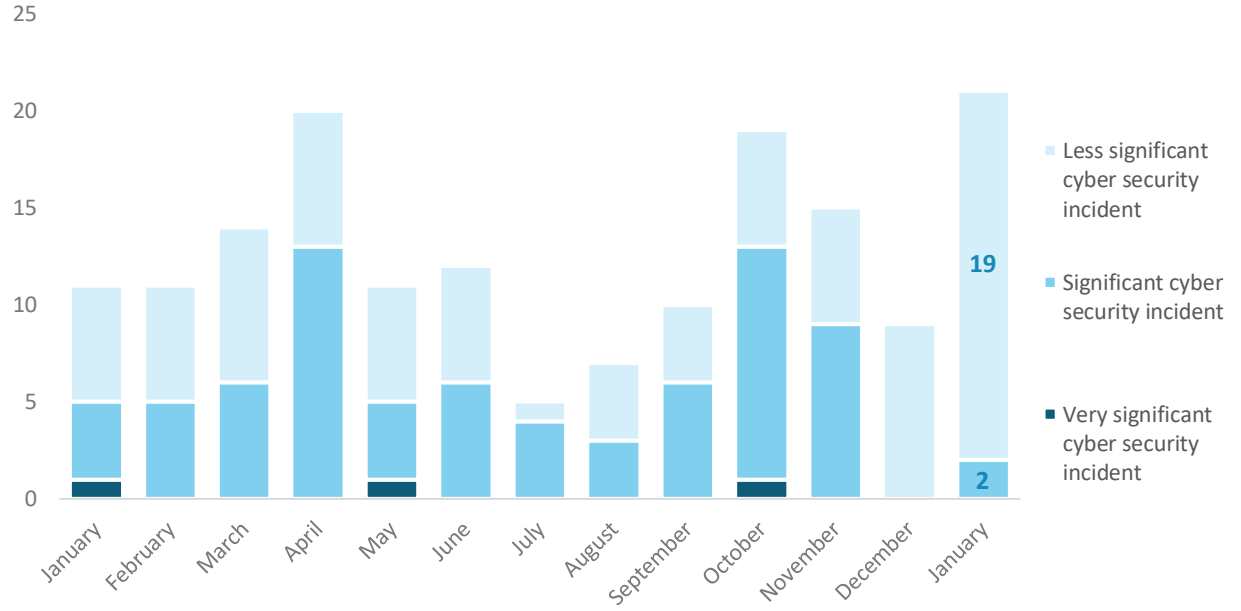
Number of cyber security incidents reported to NÚKIB

In January, NÚKIB recorded a more than a two-fold increase in the number of cyber security incidents compared to the previous month. As early as in the first month of 2023, the attacks almost reached last year's maximum, which was 22 incidents per month.[1]



Severity of the handled cyber security incidents[2]

Despite the high number of cyber incidents, the absolute majority of them fell into the category of minor incidents. Only two significant incidents were registered. As in the previous two months, the absence of recorded very significant incidents continued also in January.



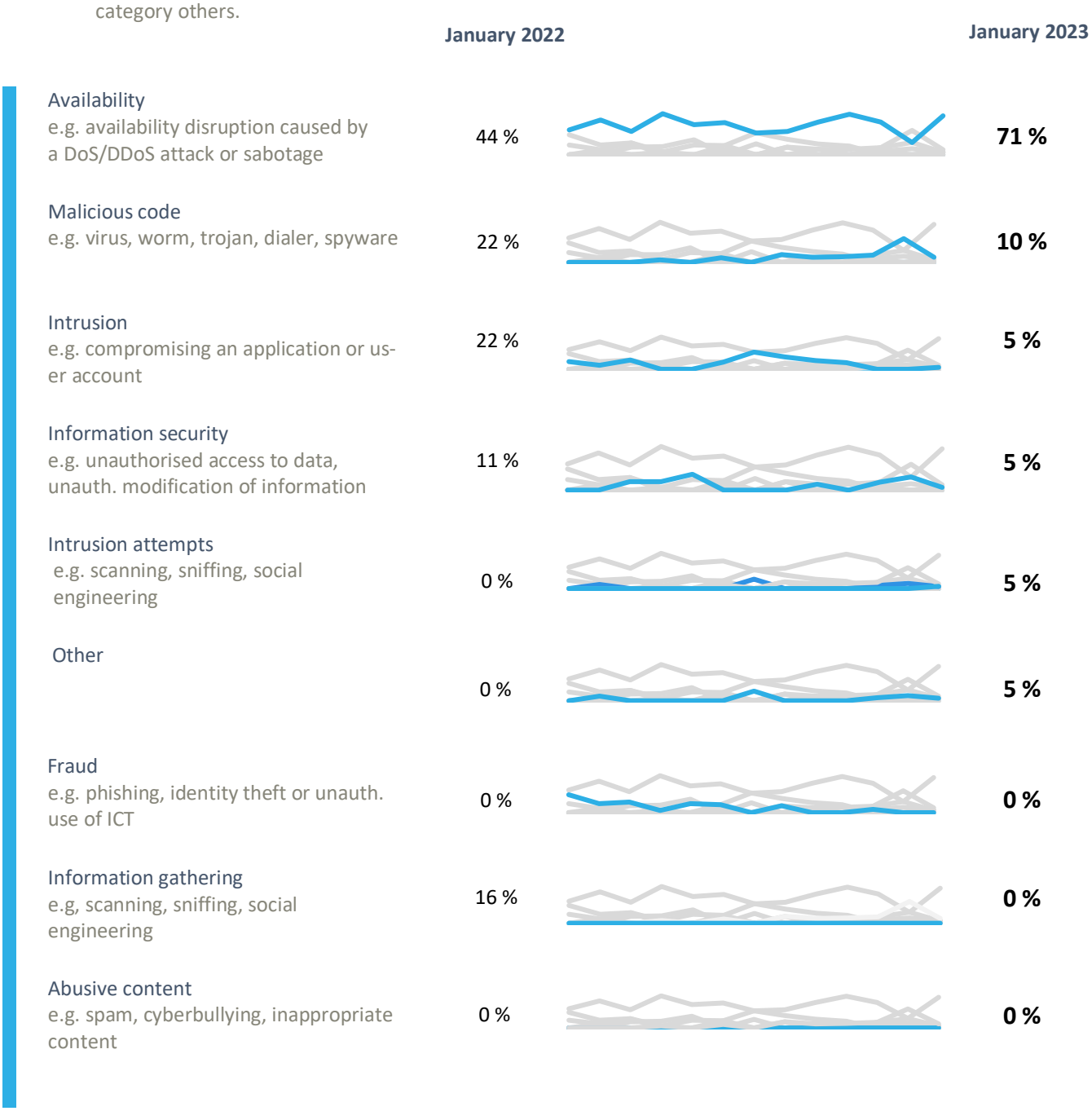
[1] NÚKIB registered 17 incidents in total with liable entities according to Cyber Security Act. The remaining 4 incidents involved unregulated entities.

[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 January cyber incidents into four categories:

- Availability attacks represented the most frequently recorded type of incidents while the decisive majority of them were DDoS attacks on victim websites. The remaining incidents were caused by service outages.
- In the malicious code category, NÚKIB registered two incidents in January. Both were ransomware attacks.
- The January incidents also included one intrusion and one failed intrusion attempt. Both attacks targeted regulated entities.
- In January, the NÚKIB also recorded one incident in the information security and one in the category others.



[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. A successful phishing attack was registered in January in which attackers used a compromised account to send additional phishing emails.

Malware

Except the ransomware cases mentioned below, NÚKIB did not record any incidents involving the use of malware in January. However, NÚKIB continued to carry out malware analysis in connection to December incidents.

Vulnerabilities

During January, NÚKIB did not issue any vulnerability warning, neither detected any significant exploitation of so far known particular vulnerabilities.

Ransomware

In January, NÚKIB registered two ransomware attacks. The PLAY ransomware and now the Dark Power ransomware have been detected again. Both of the attacks targeted non-regulated entities.

Although PLAY is a new ransomware, it has attacked a number of significant victims across the whole world. According to researchers, PLAY is operated by the same actors as Hive and Nokoyawa. DarkPower is also a new ransomware, however, has not been as active PLAY so far.

Attacks on availability

After an one-month pause, there was again a significant increase in DDoS attacks. This increase was due to a campaign by the Russian-language group NoName057(16). Similar to other recorded DDoS campaigns, the effects of the attacks were only short-termed and did not have serious consequences.

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

Technique of the month: External Remote Services

NÚKIB evaluates cyber incidents also on the basis of MITRE ATT&CK, framework, which serves as a summary of known techniques and tactics used in cyber attacks. Within the report we focus on T1498 technique: Network Denial of Service. Although we have covered this technique in our public reports in the past, following the increase in reported DDoS attacks, we are including it again with the emphasis on mitigation capabilities.

MITRE ID: T1498

Attackers can perform Network Denial of Service (DoS) attacks to reduce or block the availability of services. The given type of attacks can then be carried out by exhausting the bandwidth of the network the services rely on. These can be websites, e-mail services, DNS, or web-based applications. This type of attack occurs when attackers "flood" the bandwidth of a network connection with their malicious traffic. The traffic can be generated by one system (Denial of Service, DoS) or many systems (Distributed Denial Service, DDoS). This type of attack leads to a limitation of data availability and usually has no longer-term effects.

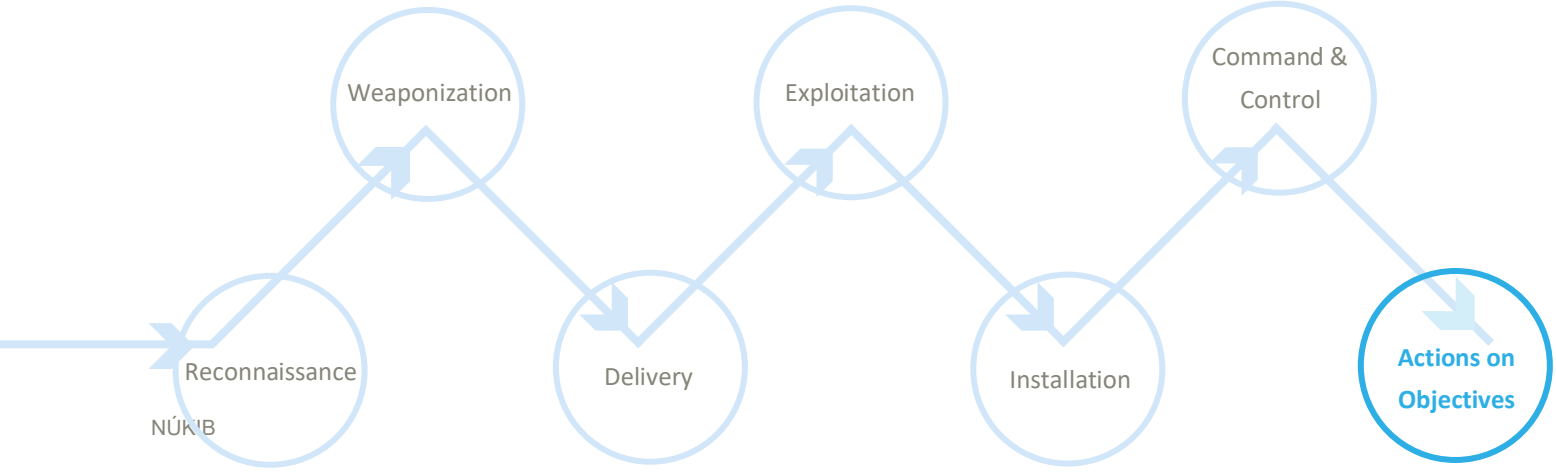
Mitigation: Network traffic filtering is the key mitigation technique. However, defence against DDoS attacks depends to some extent on an attack type. A few examples of attack types and potential mitigation measures are below:

For instance, against HTTP flood type attack conducted from abroad, it is possible to use the so-called geoblocking, i.e. restriction of access based on geographic location. To block a selected ASN, a whole group of IP ranges, can be another operational solution. More advanced mitigation options include real-time traffic monitoring and dynamic rule modification.

During attacks of TCP flood type it is possible to temporarily increase the capacity by increasing the so-called backlog queue or "recycling" of older semi-open connections.

Protection against so called DNS amplification mainly includes the verification and filtering of source addresses and limiting the response time or the number of queries. However, this responsibility lies with DNS server operators themselves and the victim has only limited mitigation options.

Representation of T1498 in the kill chain showing when attackers use the technique:



Focused on the trend: DDoS campaign launched by NoName057(16)

The Russian-language hacker group NoName057(16) carried out a series of DDoS attacks during January, targeting websites of dozens Czech government and private entities.

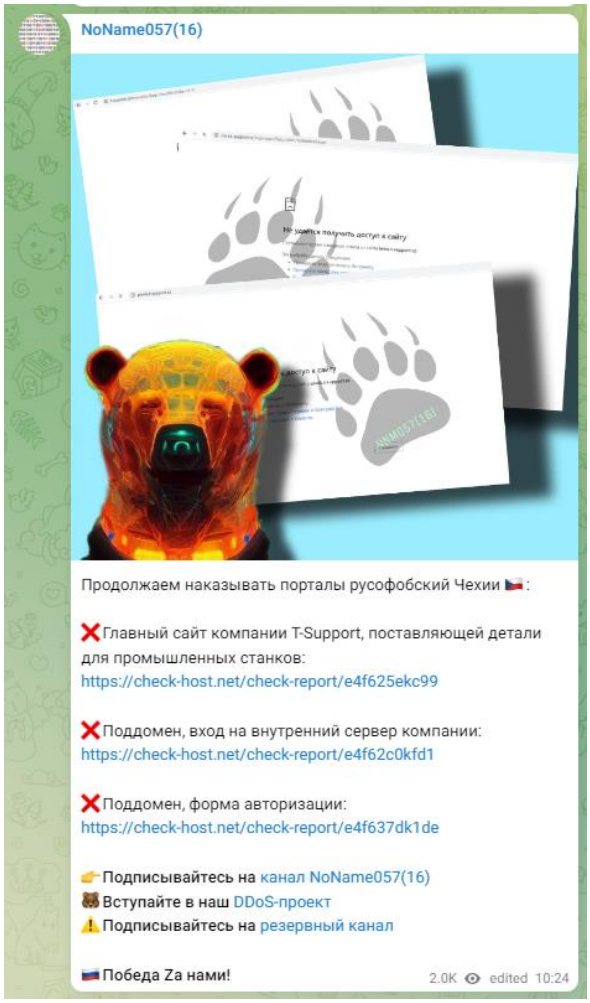
This group was first appeared in March 2022, shortly after the start of the war in Ukraine. Initially, NoName057(16) focused on Ukrainian targets, but later began targeting subjects across sectors in NATO countries. In recent months, the group has focused on targets in Austria, Italy, Great Britain, Lithuania, Poland and Denmark. Starting with 11th January, the group has started attacking also targets in the Czech Republic.

NoName057(16) publishes pro-Russia posts on its Telegram account and condemns Russophobic enemies, whom they also label as their targets. This orientation is also reflected in the choice of targets, which in many cases have a clear political motivation. The group primarily carries out DDoS attacks against selected websites, especially in NATO countries.

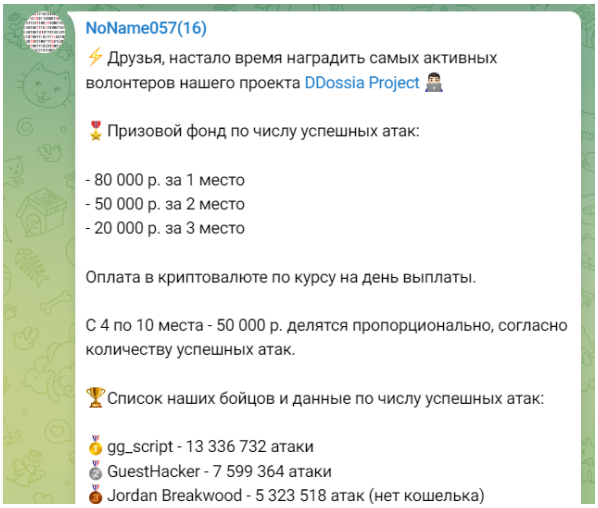
The attacks against Czech targets did not have serious consequences and only led to the temporary unavailability of the attacked entities websites. DDoS attacks generally overwhelm traffic on services accessible from the Internet, but do not compromise information systems of organizations.

To a certain extent NoName057(16) differs from Russian-language groups like Killnet or Anonymous Russia. Particularly it is specific for its DDosia project, through which it offers monetary rewards to interested parties for carrying out as many successful DDoS attacks as possible. The DDosia project is formed by a community of volunteers to whom NoName057(16) offers the DDosia tool, through which he then carries out DDoS attacks. The most productive members then receive financial rewards in cryptocurrencies (see Fig.2).

Obr 1: Telegram post of the NoName057(16) group



Obr 2: Telegram post of the NoName057(16) group announcing the ranking of the most productive attackers



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.