CYBER SECURITY INCIDENTS FROM THE NÚKIB’ S PERSPECTIVE

SEPTEMBER 2023

National Cyber
and Information
Security Agency

Summary of the month

Even though the number of incidents recorded in September decreased compared to the previous month, it remained above the average of the last twelve months. Most of the incidents were part of the NoName057(16) campaign, which primarily targeted the Czech banking sector and took place in late August and early September.

Considering its importance, this campaign made its way not only into the number of registered incidents but also into the severity statistics. DDoS attacks in September represented almost four-fifths of all registered incidents and most of them were classified as significant.

We take a closer look at the NoName057(16) group this time in the *Focus on a Threat* chapter. The chapter not only describes the campaign of this group, but also focuses on its modus operandi to date, the technical description of its attacks and mitigation possibilities.

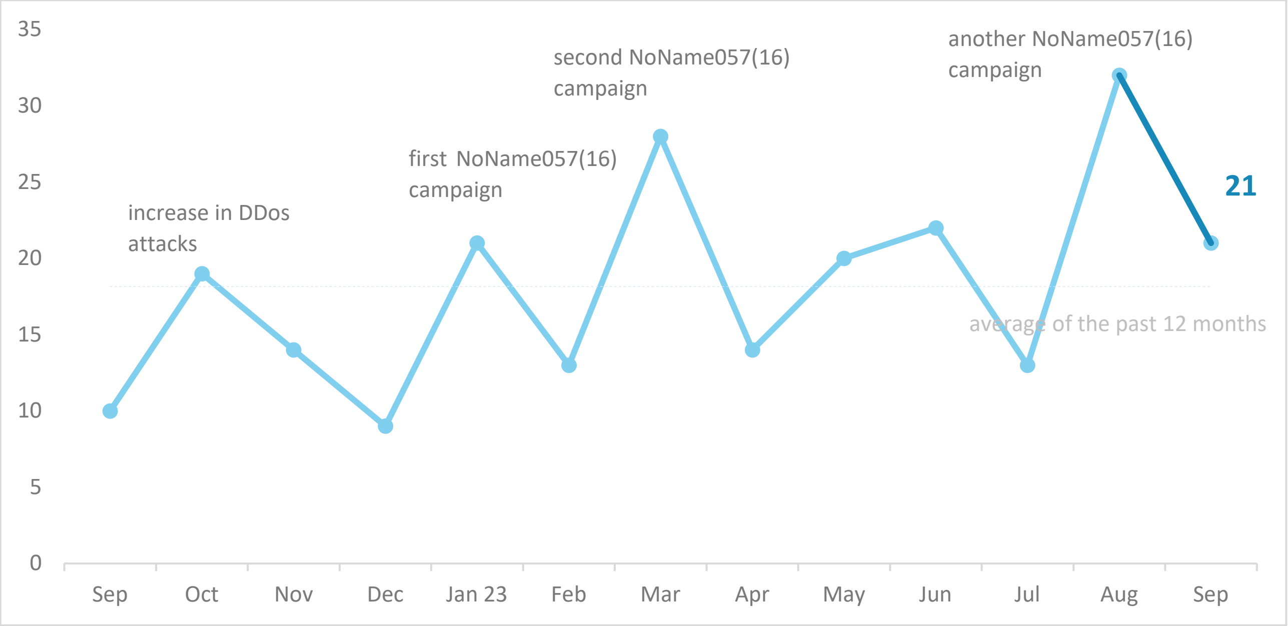
Table of content

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 this information is always stated.

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

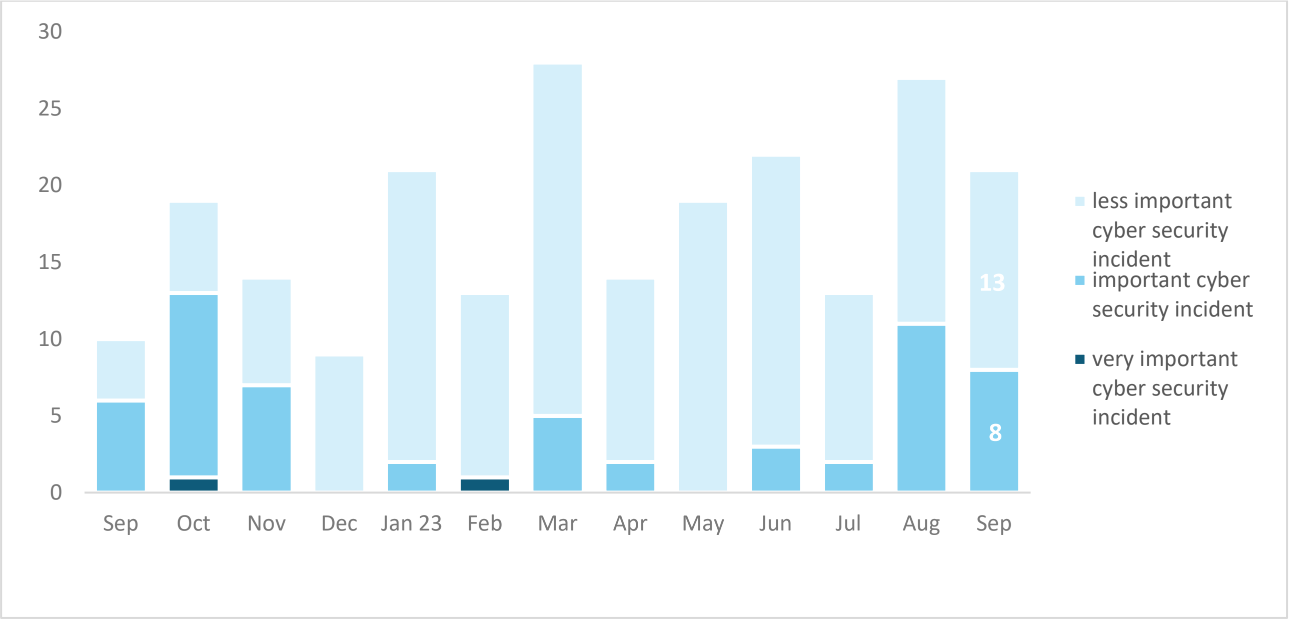
Number of cyber security incidents reported to NÚKIB

Even though the number of incidents recorded in September decreased compared to the previous month, it remained above the average of the last twelve months. Most of the incidents were part of the NoName057(16) campaign took place in late August and early September.[1]



Severity of the handled cyber security incidents[2]

The increased number of significant cyber incidents recorded during September was linked to the continuation of the aforementioned NoName057(16) campaign against Czech banks, which was also reflected in the August statistics.



[1] NÚKIB registered 18 incidents in total with liable entities according to Cyber Security Act. The remaining 3 incidents involved unregulated entities.

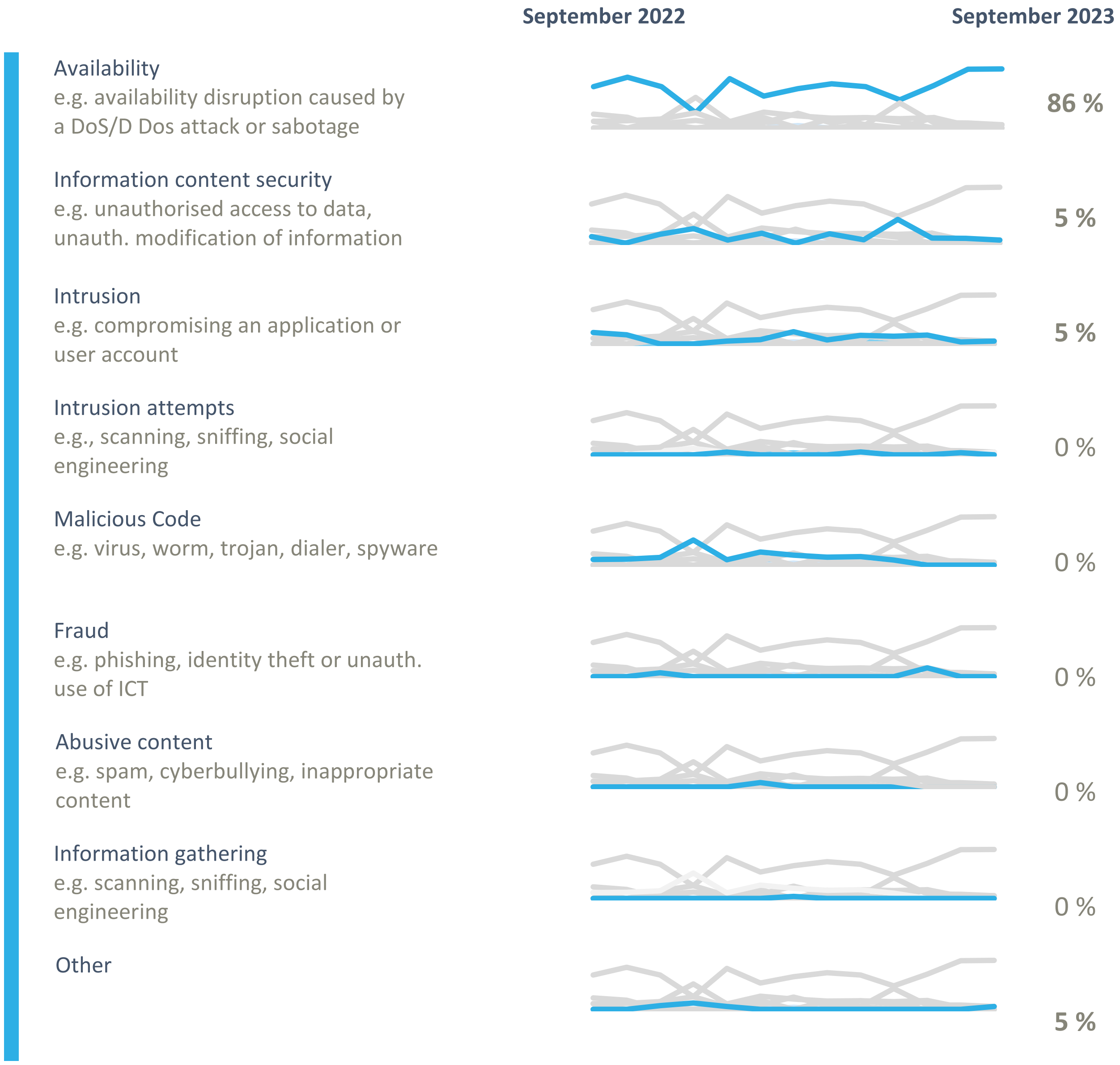
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB[3]

The availability category dominates the incident classification for the ninth month. During September, more than four-fifths of all recorded incidents resulted in an availability disruption. These were predominantly again caused by DDoS attacks.

In addition to this, NÚKIB dealt with incidents in the following three categories:

- ○ One case within the Information Security category was connected to the Monti ransomware attack (see section below).
- ○ There was one incident under the category of Intrusion in September. This involved an attack by a highly sophisticated actor who managed to gain access to the systems of a regulated entity.
- ○ Within the Other category, there was a specific incident caused by the loss of a user's tablet.



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

September trends in cyber security from the NÚKIB's perspective [4]

Phishing, spear-phishing and social engineering

Although phishing has long been a persistent threat that appears within NÚKIB incidents, the number of registered phishing attacks during September was significantly lower than in previous months.

Malware

As in August, NÚKIB did not detect any malware in September, with the exception of the ransomware listed below.

Vulnerabilities

In September, NÚKIB did not issue any advisories about newly discovered vulnerabilities.

Ransomware

NÚKIB in September recorded an incident in which the Monti group used ransomware to attack and then extort an unregulated entity. This group was formed in mid-2022 a few months after the leak of internal data of the Conti ransomware gang. Monti adopted not only the gang's tactics and techniques, but also the Conti ransomware source code, which it then used to create its own. According to Zscaler ThreatLabz the group recently started to use a new variant of Monti ransomware called BIDON.

Attacks on availability

The trend of recent months, when the pro-Russian hacktivist group NoName057(16) has been attacking selected Czech targets in waves still has continued. More information about the group's most recent campaign to date is available in the chapter Focus on a Threat.

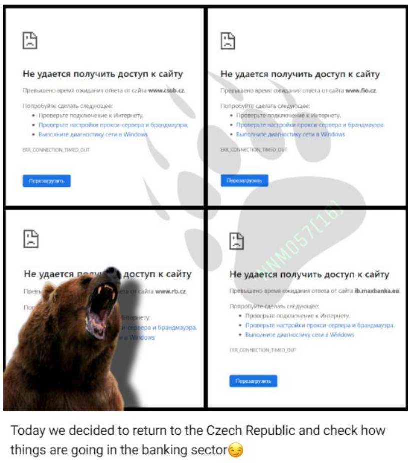
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

Focus on a threat: DDoS campaign by the NoName057(16) group against Czech entities

At the turn of August and September, another wave of DDoS attacks by the NoName057(16) group occurred, primarily targeting the Czech banking sector. As a result of the attacks, several Czech banks experienced problems with unavailability of services. Due to the attacks, bank customers were unable to log in to their banking accounts, however, due to the type of attack, the confidentiality or integrity of their data was not compromised, and their funds were not compromised in any way. The attacks then continued in the following days, when, in addition to banking institutions, industrial and military sector entities were attacked. The group's activity targeting Czech entities ceased after a few days and none of the attacks had longer-term consequences.

With its attacks NoName057(16) often reacts to geopolitical or other events or statements related to events in Ukraine or Russia. However, it is currently unclear whether and, if so, what the impetus was for the wave of attacks on Czech banking institutions. Given the long-term targeting of Czech entities, future occurring of further attacks cannot be ruled out in the foreseeable future. NÚKIB has been monitoring the NoName057(16) group for a long time and proactively contacts the entities identified as targets and provides relevant recommendations.

Fig. 1: Telegram post by NoName057(16)



Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта **www.csob.cz**.

Попробуйте сделать следующее:

- Проверьте подключение к Интернету.
- Проверьте настройки прокси-сервера и брандмауэра.
- Выполните диагностику сети в Windows

ERR_CONNECTION_TIMED_OUT

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта **www.fio.cz**.

Попробуйте сделать следующее:

- Проверьте подключение к Интернету.
- Проверьте настройки прокси-сервера и брандмауэра.
- Выполните диагностику сети в Windows

ERR_CONNECTION_TIMED_OUT

Не удается по доступ к сайту

Превы ета от сайта **www.rb.cz**.

Поп

- Интернету.
- и-сервера и брандмауэра.
- и в Windows

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта **ib.maxbanka.eu**.

Попробуйте сделать следующее:

- Проверьте подключение к Интернету.
- Проверьте настройки прокси-сервера и брандмауэра.
- Выполните диагностику сети в Windows

ERR_CONNECTION_TIMED_OUT

Today we decided to return to the Czech Republic and check how things are going in the banking sector😏

Source: t.me

The Czech Republic is not the only target of NoName057(16). Over the last weeks of August, the group attacked financial institutions in Poland, as well as mainly transport companies in Denmark, Norway and the Netherlands. The latter three countries were targeted following the announcement of F-16 deliveries to Ukraine.

Technical description of the attacks and mitigation options

DDoS attacks of the NoName057(16) group fall under the HTTP GET/POST flood type. The attacks are typically carried out by individual members uploading a JSON configuration file containing the target URL and IP address to the DDoS client, followed by a full HTTP GET/POST request. This request targets a very specific URL, e.g., a random tab in a press release, a specific loan setting in an online form, or a search for specific ATMs in a database. This can be used in mitigation, where the site administrator may decide to block specific requests or less important parts of the site. The JSON file is updated on average twice a day, but only the targets change, not the requirements. NÚKIB sends a portion of the configuration file with these requirements to all marked targets.

Upon internal NÚKIB analyses, user-agent based blocking is recommended. The DDoS client uses Go-http-agent/1.1, Go-http-agent/2 or an empty user agent (-). However, this mitigation measure carries the risk of some services using the GO language not functioning.

Other mitigations include geofencing or limiting access based on the number of requests from a specific IP address per minute.

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+STRICT	Restricts sharing to the organization only.
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: 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/defence 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.