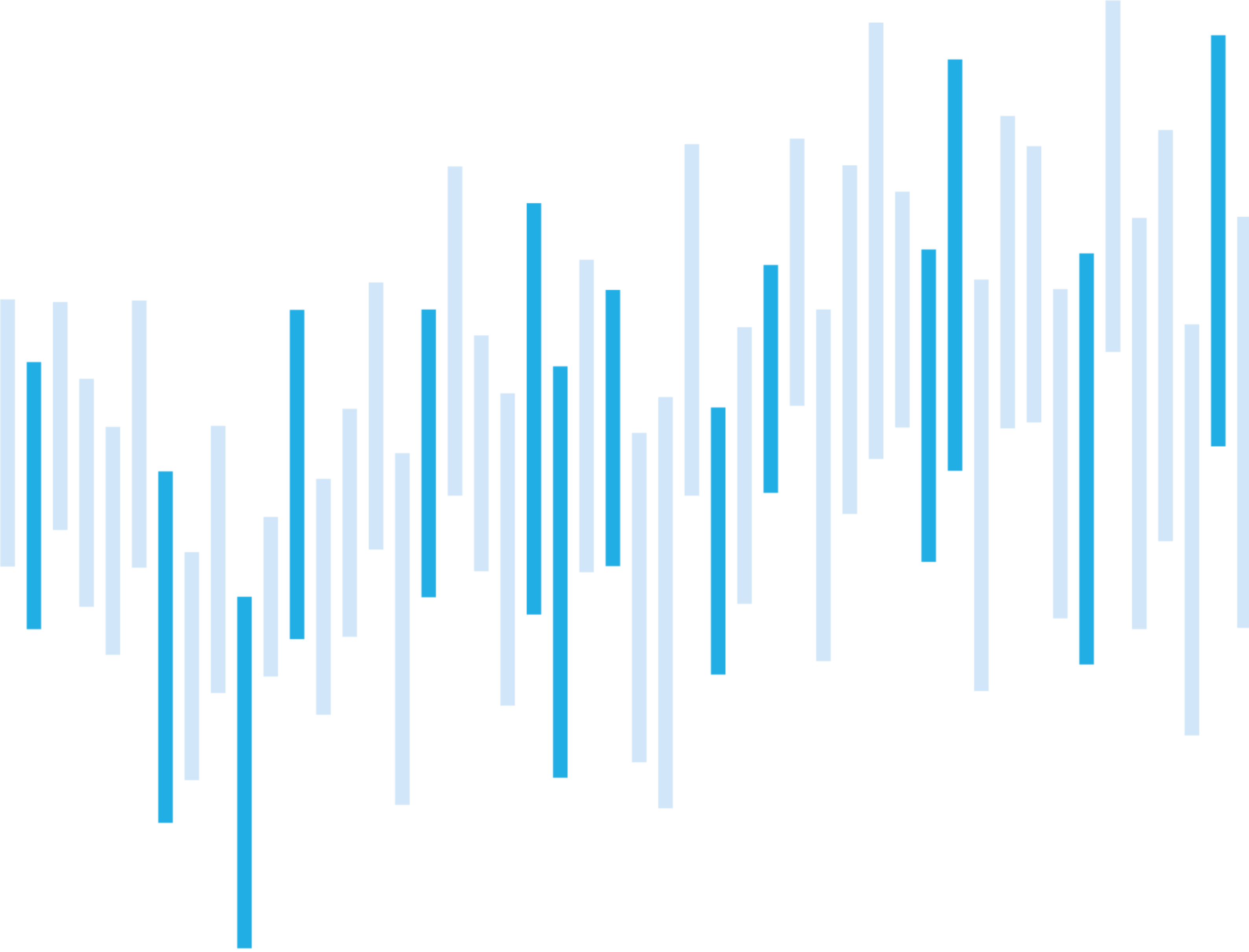
CYBER SECURITY INCIDENTS FROM THE NÚKIB’ S PERSPECTIVE

JUNE 2023



National Cyber
and Information
Security Agency

Summary of the month

The number of June incidents was above the average of the last 12 months. In addition to DDos attacks, which have consistently increased the number of incidents in the last six months, this time there was also an increase in ransomware attacks.

Ransomware PLAY was most frequently utilized in the incidents. Out of the six June cases handled by NÚKIB, PLAY was responsible for three. PLAY is characterized by its high operational tempo. In just one year of its existence, it has had more than hundred victims, and their numbers continue to grow. Moreover, the geographical distribution of attacked organizations clearly indicates that the Czech Republic is a high-priority target for its operators.

Since it is likely (55-70%) that attackers will continue their activities against Czech targets in the short term, the warning about the increased risk of ransomware attacks, which NÚKIB published on its website during June, remains valid. This warning includes, among other things, a list of critical vulnerabilities that are currently being exploited by ransomware actors in Czechia and worldwide, and we recommend verifying them.

Table of content

Number of cyber security incidents reported to NÚKIB

Severity of the handled cyber security incidents

Classification of incidents reported to NÚKIB

June trends in cyber security from NÚKIB's perspective

Technique of the month: Exploit Public-Facing Application

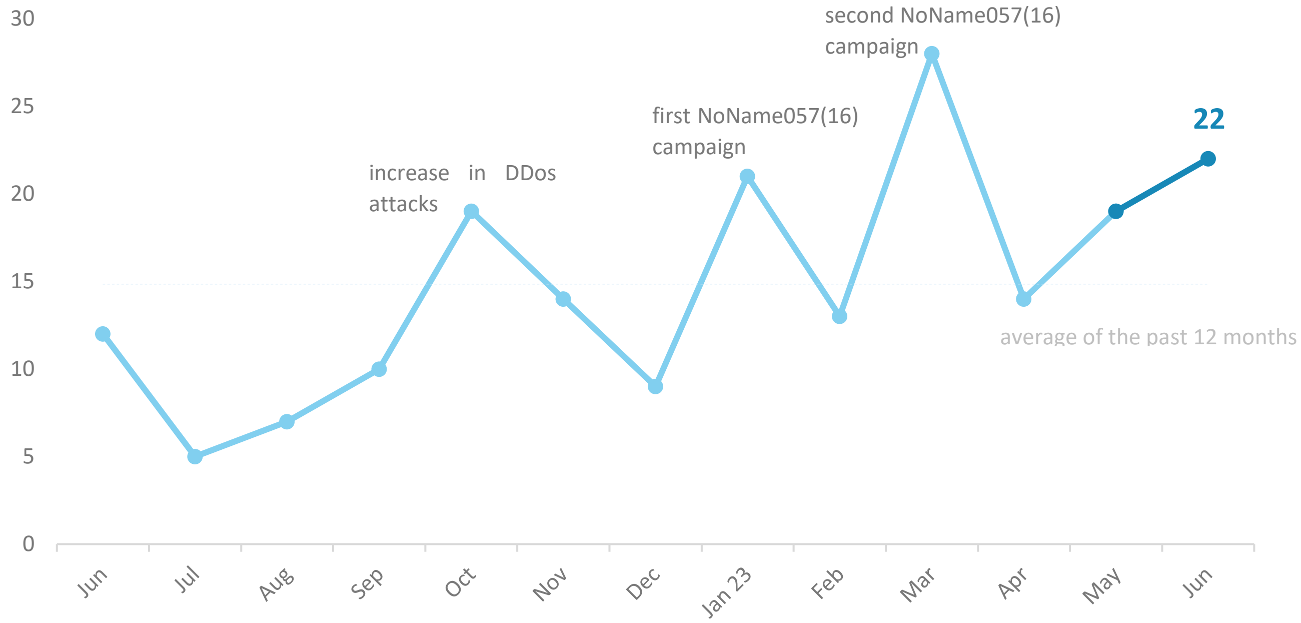
Focus on a threat: Ransomware PLAY targets Czech organisations

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

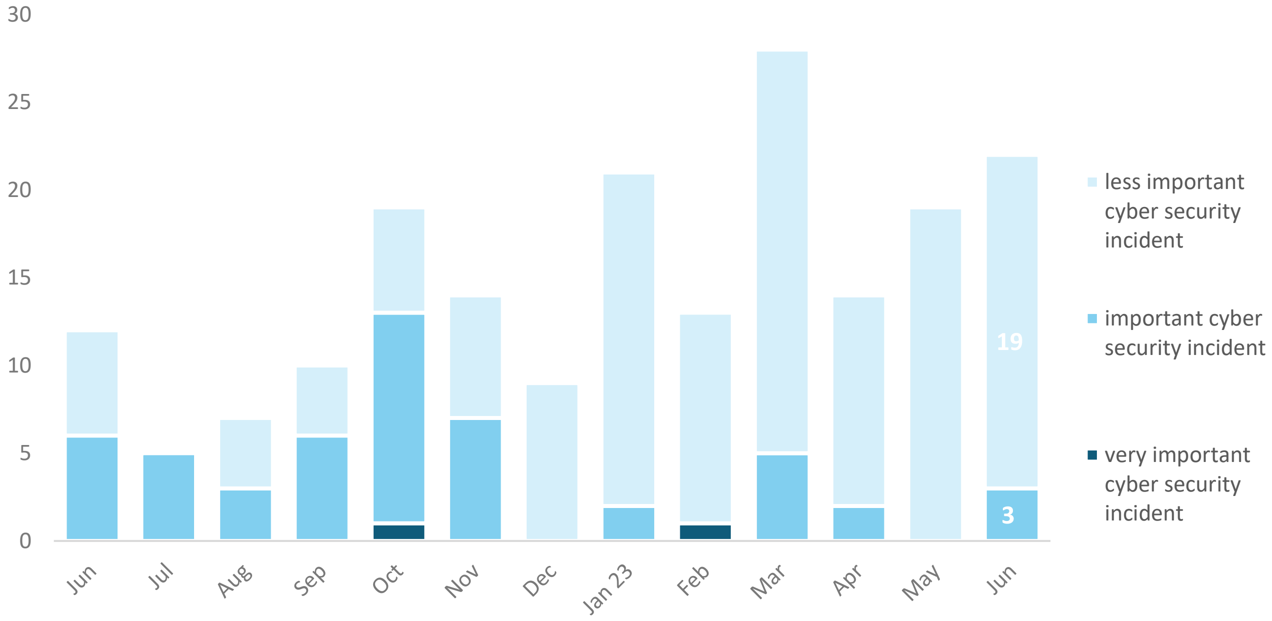
Number of cyber security incidents reported to NÚKIB

The number of incidents, similarly to last month, remained significantly above average. [1]



Severity of the handled cyber security incidents[2]

Ransomware attacks have also deepened the severity of cyber incidents. Since two of them deleted backups from the affected organizations and hindered their quick recovery, NÚKIB classified them as significant incidents.



[1] NÚKIB registered 16 incidents in total with liable entities according to Cyber Security Act. The remaining six incidents reported not regulated subjects to NÚKIB.

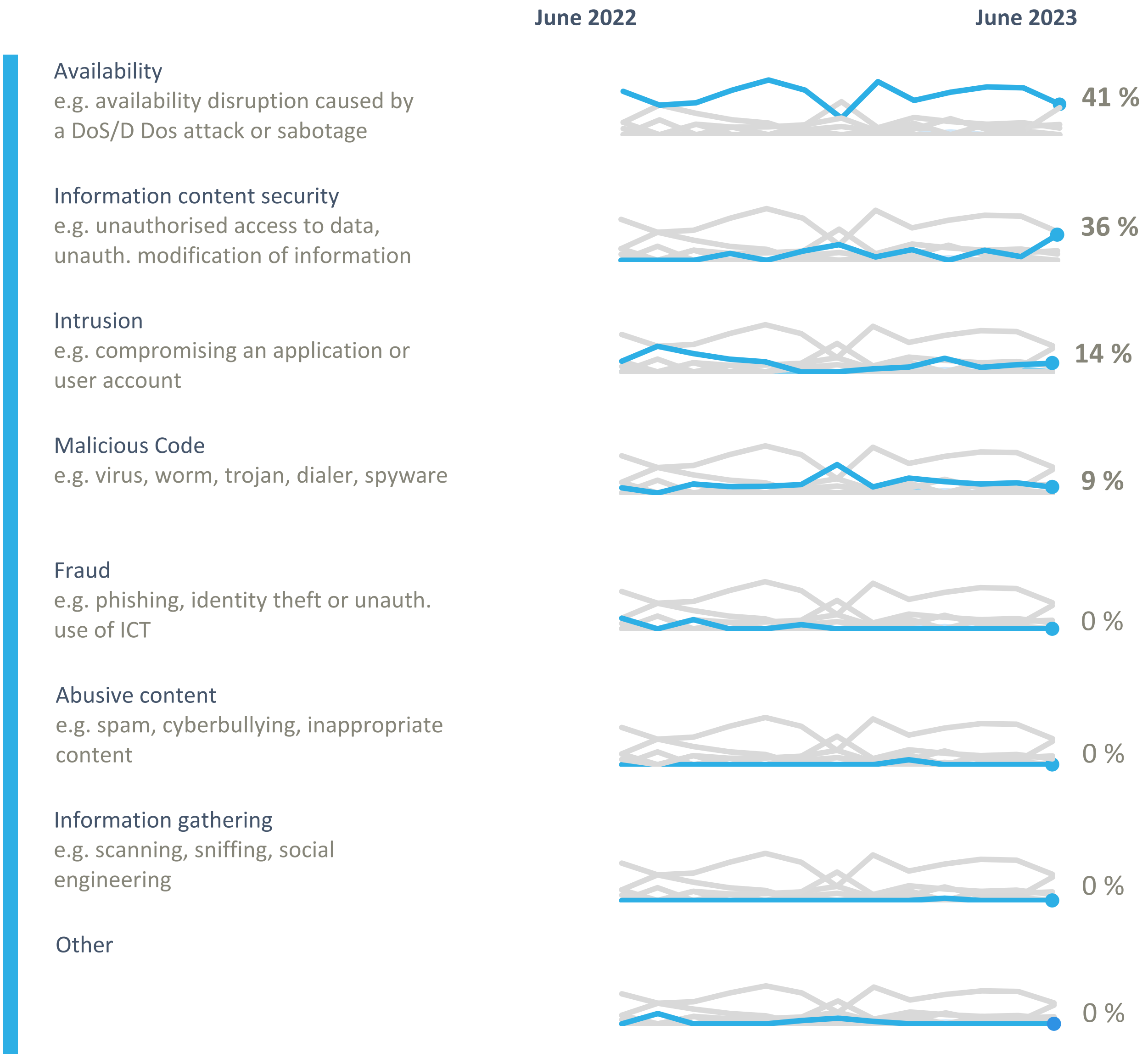
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [3]

In June, NÚKIB once again most frequently recorded service availability disruptions, mainly due to DDos attacks. However, their percentage share in cyber incidents decreased compared to the last six months. This is partly due to the increase in ransomware attacks, of which there were six, which we classified as information security breaches.

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

- In three cases of "penetration," login credentials were stolen for various systems and databases, resulting in attackers gaining temporary access to them.
- Two incidents, where malware was found on user workstations, were classified as malicious code.



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

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

Phishing, spear-phishing and social engineering ↘

After several months of intensive efforts by NÚKIB to address phishing campaigns against Czech strategic targets, the situation calmed down in June. NÚKIB recorded a spear-phishing case targeting a Czech company in the defence industry, but no compromise occurred. Another, less sophisticated phishing attempt, targeted one of the Czech universities.

Malware ↘

In one of the June incidents, the phishing attachment triggered malicious code upon opening, which began downloading a .zip file from a malicious domain. Based on the URL information, it is likely (55-75%) that the malware in question is QakBot, which would probably proceed to download ransomware into the user's system. However, the EDR (Endpoint Detection and Response) technology intercepted QakBot and placed the downloaded file in quarantine.

Vulnerabilities ↗

The ransomware targeting Czech entities in June often exploits vulnerabilities as an attack vector. The ransomware variant called PLAY exploits vulnerabilities such as FortiOS (CVE-2018-13379, CVE-2020-12812) and MS Exchange (CVE-2022-41080, CVE-2022-41082) to compromise networks. These and other critical vulnerabilities that are currently being exploited by ransomware actors in the Czech Republic and worldwide have been identified in our alert on the NÚKIB website and we recommend verifying whether the vulnerable applications are not used.

Ransomware ↗

Although ransomware has been a persistent threat, and NÚKIB has been dealing with it almost every month since 2018, cybercriminal activities against Czech targets intensified in June. NÚKIB dealt with six cases of ransomware attacks, two of which had significant impacts on the affected organizations' operations.

The ransomware variant PLAY had the most notable increase in attacks, which we describe in detail in the last chapter. Additionally, actors also targeted organizations using the ransomware BlackBasta and LockBit

Attacks on availability →

June with eight DDos attacks is comparable to the previous month. The DDos campaign, led by an unknown attacker, targeting exclusively Czech government institutions, continued. The attacks have begun in February of this year and have been targeting DNS servers of the institutions each month in an attempt to overwhelm them. Unlike hacktivist campaigns, no actor has claimed responsibility for these attacks.

DDos attacks by the hacktivist group NoName057(016) also continued.

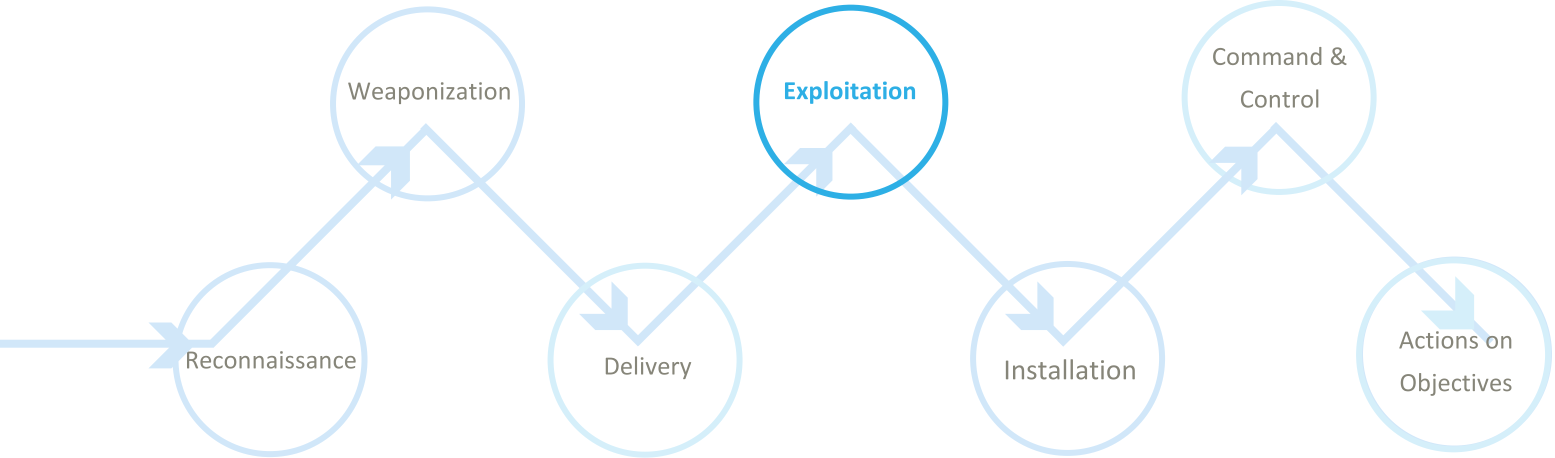
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

Technique of the month: Exploit Public-Facing Application

The ransomware PLAY, which targets Czech entities, infiltrates its victims' networks by exploiting vulnerabilities. This technique corresponds to "Exploit Public-Facing Application" in the MITRE ATT&CK matrix. The vulnerabilities exploited by the ransomware PLAY are FortiOS and Microsoft Exchange ones.

> **Exploit Public-Facing Application** is a technique where attackers exploit weaknesses in systems exposed to the Internet. These systems can include web servers, e-mail servers, or applications for remote data management. If attackers notice improper security settings on the victim's side or errors made by the program's developer, they can exploit them and gain access to the victim's networks. Successful compromise can result in data theft or encryption followed by extortion.
>
> **MITRE ID:** T1190
>
> **Mitigation:** Organizations can mitigate the risk of exploiting this technique by only exposing necessary services to the Internet. Regularly installing updates for operating systems and applications, along with maintaining protocols for managing these updates, is also necessary. These measures make it more difficult for actors to exploit software vulnerabilities. For remote access services (VPN, RDP, SSH), we recommend using the multi-factor authentication (MFA). Using MFA on all accounts, especially VPN, webmail, and accounts with access to critical systems, hinders lateral movement by attackers within the network.

Representation of the T1190 technique in the Cyber Kill Chain showing the attack phase in which the cyber actors use the technique:

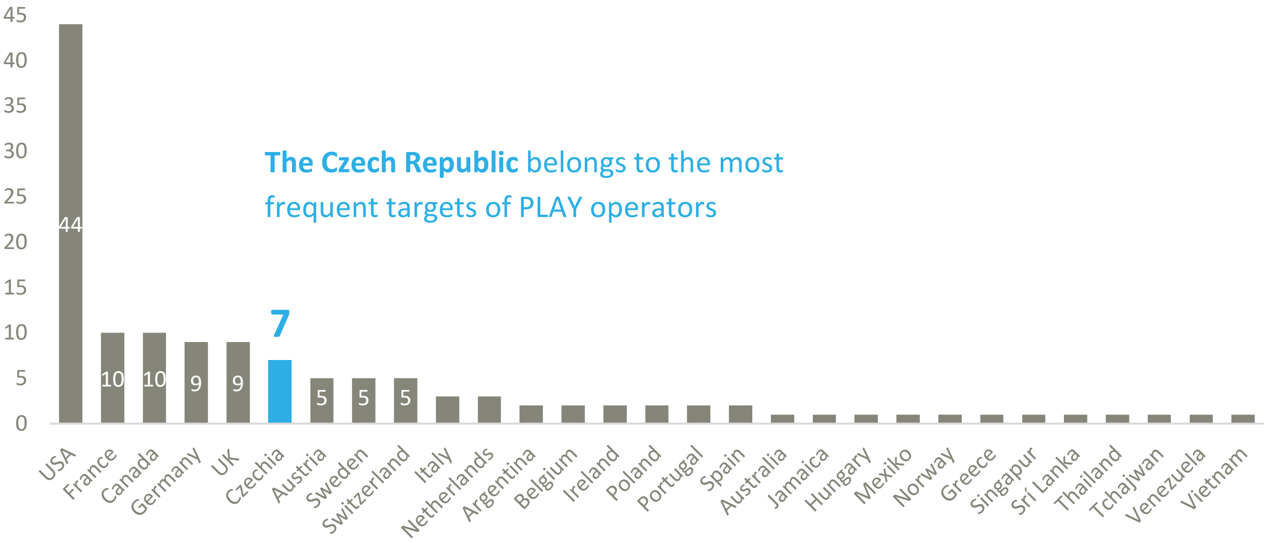


Focus on a threat: Ransomware PLAY targets Czech organisations

During June, NÚKIB observed an increased activity by cybercriminal groups in the Czech cyberspace. Ransomware PLAY played the most significant role in this increase. Among the six ransomware attacks that NÚKIB dealt with in June, three were attributed to PLAY. As shown in the graph below, the operators of the ransomware PLAY ranked the Czech Republic high on their list of targets.

Ransomware PLAY has been active since at least June 2022 and a number of its victims is growing rapidly. It has accumulated over a hundred victims in one year. The operators of the ransomware have published information about nearly 150 victims, including seven from the Czech Republic, on their dark web pages. These organizations rank among transportation, energy, and defence industries, which are essential for the functioning of the state.

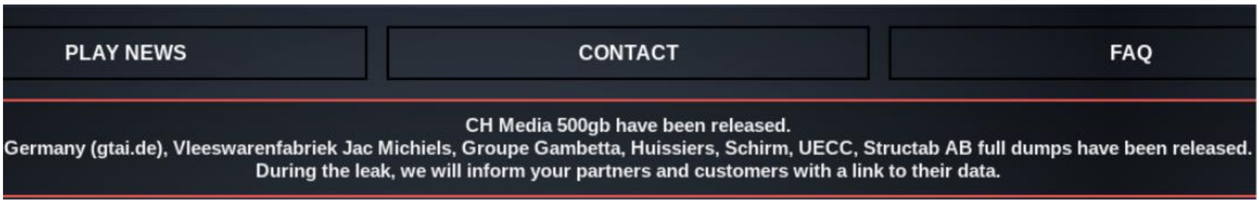
Graph 1: Geographical distribution of ransomware PLAY victims[5]



The Czech Republic belongs to the most frequent targets of PLAY operators

The group is characterized by the use of so-called **intermittent encryption** which encrypts only partial blocks of target files. This method allows significantly higher encryption speed (lower hundreds of MB/s) while complicating detection. PLAY operators also employ **a triple extortion technique**, where in addition to encryption and the threat of data disclosure, they also threaten to contact the victims' customers to motivate payment.

Fig. 1: Example of triple extortion by ransomware PLAY operators (screenshot dated June 13, 2023)



CH Media 500gb have been released.
Germany (gtai.de), Vleeswarenfabriek Jac Michiels, Groupe Gambetta, Huissiers, Schirm, UECC, Structab AB full dumps have been released.
During the leak, we will inform your partners and customers with a link to their data.

It is likely (55-70%) that the attackers will continue their activities against Czech targets in the following months. The warning on increased risk of ransomware attacks issued by NÚKIB on 20th June 2023 on its web , remains still topical.

[5] Data updated to 11th June 2023

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.