CYBER SECURITY INCIDENTS FROM THE NÚKIB’ S PERSPECTIVE

MAY 2023

Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

The number of incidents in May was well above the average of the past year. Again, the cases involving the disruption of services, including DDoS attacks, dominated. NÚKIB is also monitoring additional phishing campaigns against Czech strategic targets.

During one of the May incidents, NÚKIB registered a relatively new trend in the behaviour of ransomware attackers. The attackers did not encrypt the victim's data, but instead exfiltrated it and threatened to publish it. This is known as the "extortion-only" approach. These new trends in the behaviour of ransomware operators are changing the way organizations should prepare for ransomware.

Considering the dynamic nature of the ransomware environment, NÚKIB has decided to update the public document Ransomware: Recommendations for Mitigation, Prevention, and Response. The behaviour of ransomware operators is changing and the approach of defenders is shifting. Therefore, the new version of the document takes into account the new techniques used by attackers, the latest recommendations from our partners or the most common issues that organisations deal with in relation to ransomware.

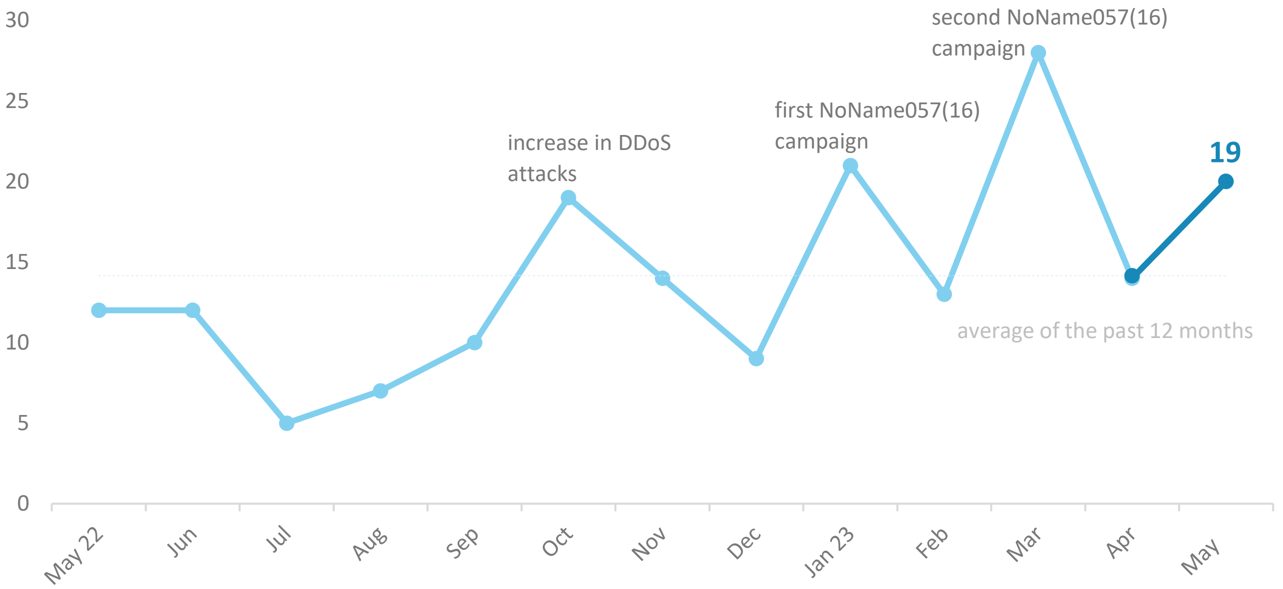
Table of content

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

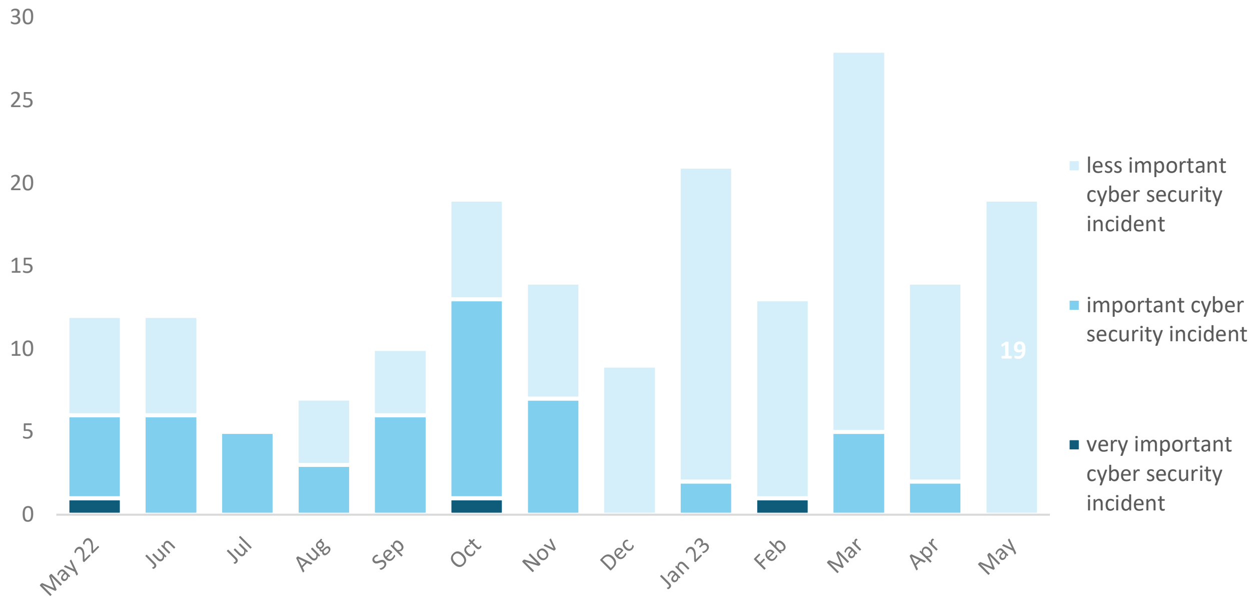
Number of cyber security incidents reported to NÚKIB

In May, NÚKIB registered 19 cyber incidents. As shown in the graph, the number of incidents in the last six months has been fluctuating between average and significantly above-average values. DDoS attacks on state institutions again contributed significantly to the above-average values.[1]



Severity of the handled cyber security incidents[2]

All May cyber incidents occurred without significant consequences that would notably affect the operations of the attacked organizations, and therefore NÚKIB classifies them as less significant.



[1] NÚKIB registered 15 incidents in total with liable entities according to Cyber Security Act. Remaining four 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]

The trend of the past year where incidents were dominated by disruptions to service availability continued in May. NÚKIB classified 11 incidents as such, which is nearly two-thirds of all May incidents. Except for two cases, the availability of services was disrupted by DDoS attacks, primarily targeting state institutions.

In addition to availability, NÚKIB also dealt with incidents in the following categories, among others:

- Two incidents involving data encryption by ransomware were classified as malicious code by NÚKIB.
- Other of ransomware incidents falls under the category of information security. Within this incident, the attackers did not encrypt the data, but only exfiltrated it, threatening to disclose it to the victims.
- NÚKIB classified one of the solved incidents as an intrusion attempt. Nearly thirty employees of a government institution opened a malicious attachment in a phishing email, but the malicious code was already non-functional, and no compromise occurred in the end.

Availability
e.g. availability disruption caused by a DoS/DDoS attack or sabotage

Malicious code
e.g. virus, worm, trojan, dialer, spyware

Intrusion
e.g. compromising an application or user account

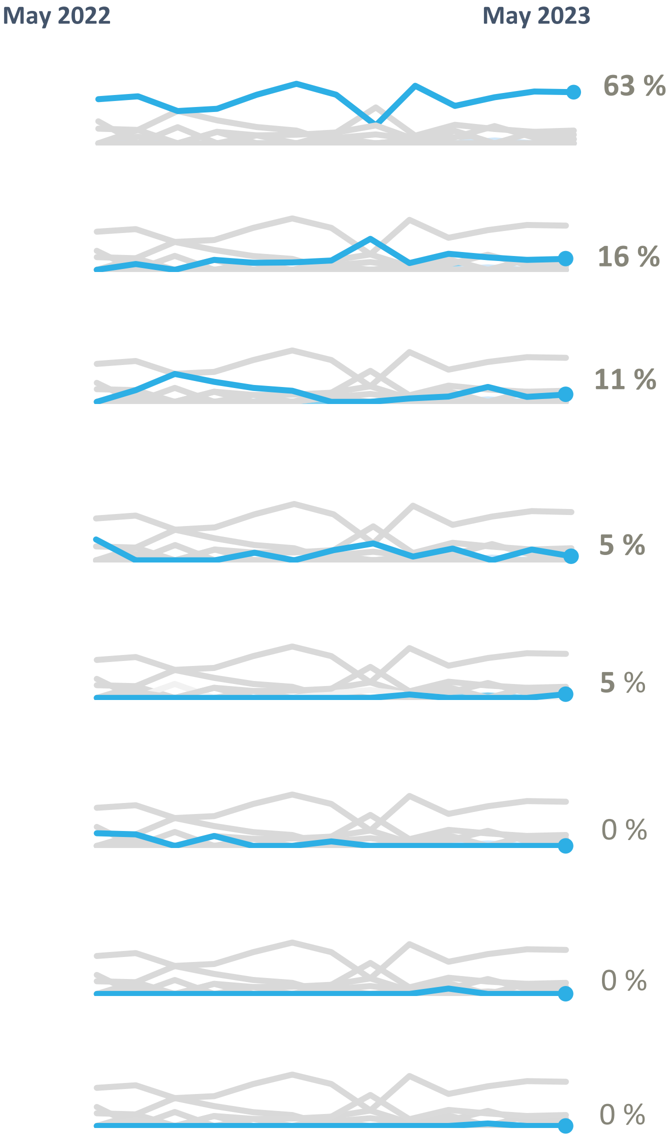
Information content security
e.g. unauthorised access to data, unauth. modification of information

Intrusion attempt
e.g. attempt to exploit a vulnerability, attempt to log in, etc.

Fraud
e.g. phishing, identity theft or unauth. use of ICT

Abusive content
e.g. spam, cyberbullying, inappropriate content

Information gathering
e.g. scanning, sniffing, social engineering



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

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

Phishing, spear-phishing and social engineering

We continue to register ongoing phishing campaigns targeting Czech strategic government objectives. In the phishing campaigns we intercepted in May, the attackers exploited European themes and sent phishing emails under a seeming heading of the European External Action Service (EEAS). The affected organizations did not report any compromising incidents but given the prolonged and high intensity of similar campaigns, it is likely that the attackers will succeed in the short term, deceiving users and compromising some of their targets. The success of their activities will depend on detection speed of the affected organizations.

Vulnerabilities

In May, no new serious vulnerabilities emerged that we would expect to be widely exploited and that could be exploited across NÚKIB liable entities.

Attacks on availability

The number of hacktivist DDoS attacks against Czech targets increased again in May. DDoS attacks accounted for nearly half of all incidents in May, with attackers primarily targeting government institutions. In addition to the ongoing NoName057 group (16), which has been attacking Czech targets for four consecutive months, the incidents also involved the Anonymous Russia group, whose activity was registered last in October of the previous year.

Malware

During the analysis of one of the May phishing campaigns, NÚKIB encountered the malware PlugX, which has been known since 2008 being often part of phishing campaigns. PlugX is a modular malware with various functionalities. It can establish a connection with a control server, gather information about the victim's system, capture screenshots, or download additional files.

Mainly Chinese espionage actors use PlugX as a backdoor in their campaigns. However, speculation suggests that the source code of PlugX has leaked and is now available to a wider range of actors. For example, a few months ago, the ransomware group BlackBasta started using it.

Ransomware

In May, NÚKIB solved four cases of ransomware attacks, which is two more than the previous month. The attacks were attributed to the ransomware Monster, Snatch, DarkTrace, and Trigona.

In the incident involving the Snatch ransomware family, the attackers employed the so-called "extortion-only" approach, where they did not encrypt the victims' data but instead exfiltrated it and blackmailed them with its disclosure. Snatch is a ransomware group that has been active since 2018. They generally use a double-extortion technique in their attacks, encrypting the data and then publishing it. However, this was the first instance where data was disclosed without encryption. You can find more information in the last chapter herein.

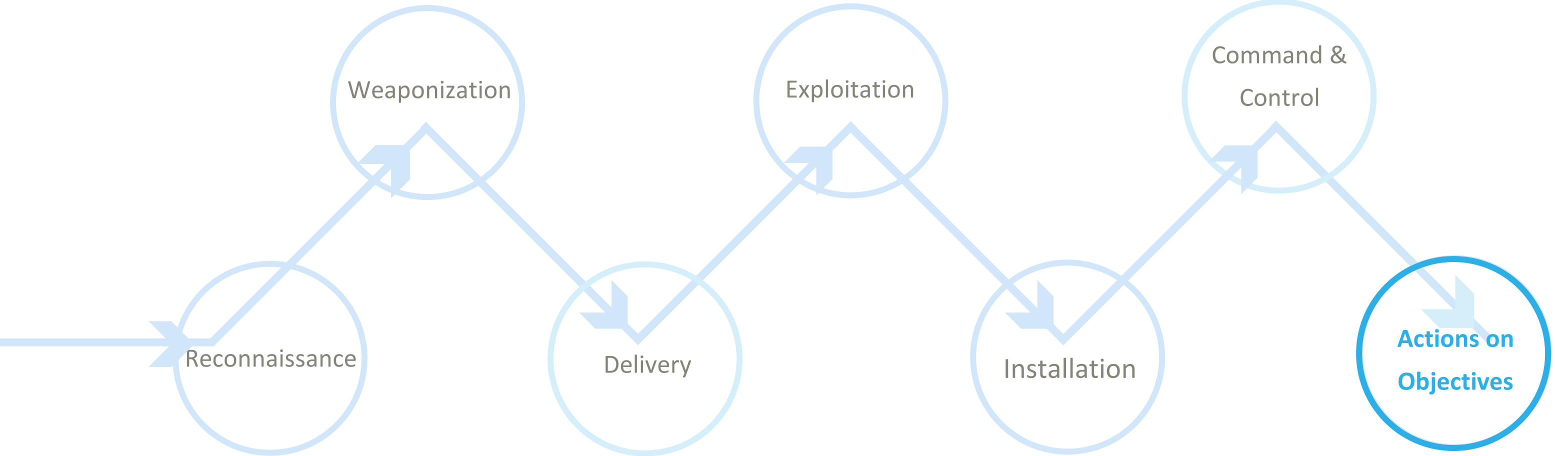
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

Technique of the month: Exfiltration over C2 Channel

In one of the May incidents, the Snatch ransomware operators exfiltrated data from a Czech company without subsequently encrypting it. NÚKIB currently does not have sufficient information to determine the exact method of data exfiltration. However, since ransomware groups most commonly use the Exfiltration over C2 Channel technique for this purpose, we focus on it in this chapter.

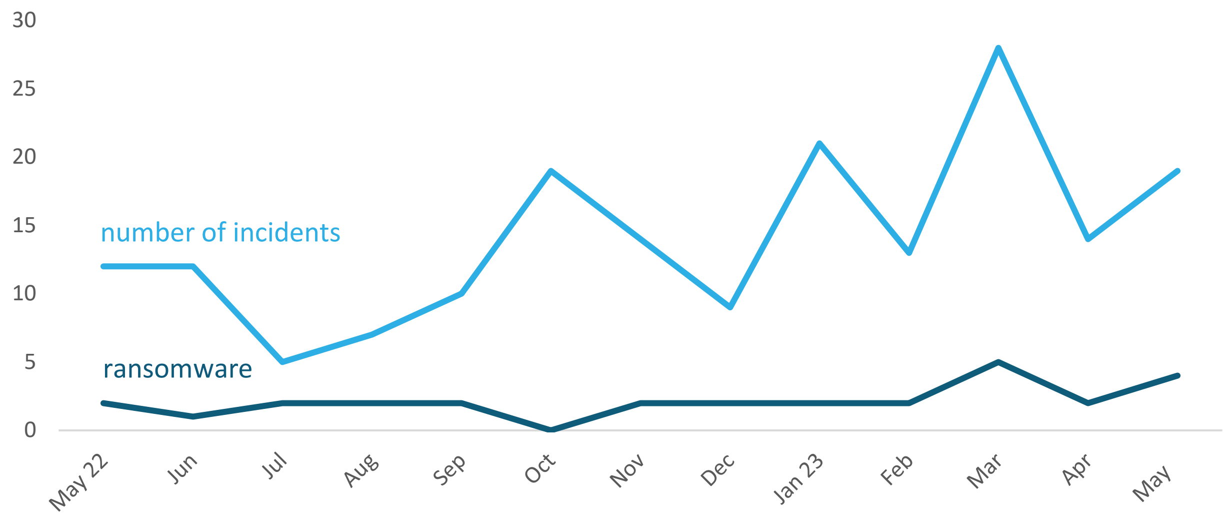
> **Exfiltration over C2 Channel:** This technique describes the process in which attackers utilize an existing command-and-control (C2) channel for data exfiltration. They utilize the communication channels or protocols already permitted within the victim's network. The stolen data is encoded within a regular communication channel using the same protocol as the C2 communication. Examples can include HTTP or various less common protocols. In this manner the attackers can transfer the stolen data without the need to create a new channel, reducing the likelihood of their activities being detected.
>
> **MITRE ID: T1041**
>
> **Mitigation:** Mitigation requires a combination of preventive measures and network traffic monitoring. Monitoring network traffic and analysing logs can help detect unusual behavioural patterns, large data transfers, or suspicious communication protocols. Implementing IDS/IPS systems capable of detecting anomalies in network traffic, as well as threat detection tools that employ heuristics and machine learning, can assist in identifying unusual communication associated with data exfiltration. It is important to monitor command execution and arguments that could lead to exfiltration, isolate suspicious file types (e.g., .pdf, .docx, .jpg, etc.), and track newly established network connections sent or received by untrusted hosts.

Representation of T1041 in the Cyber Kill Chain showing the attack phase in which the cyber actors use the technique:



Focus on a threat: Ransomware and extortion without encryption of data

Ransomware attacks have been regularly appearing among NÚKIB's incidents since 2018. As seen in the graph below, NÚKIB handles at least two ransomware-related attacks every month. Small and medium-sized businesses and schools have been the primary targets in the last year.



The ransomware environment is dynamic, with ransomware groups and their behaviours constantly evolving. As we described in the 2021 Report on Cyber Security in the Czech Republic, attackers no longer solely encrypt data. During attacks, they also exfiltrate data and demand ransom from the victim, threatening to publicly disclose the stolen information. This tactic is aimed at increasing pressure on organizations and raising the likelihood of payment.

In one of the May incidents, NÚKIB observed a new development. A Czech IT company fell victim to the Snatch ransomware. However, unlike typical ransomware attacks, the attackers did not encrypt the company's data. Instead, they exfiltrated it and threatened to start publishing it unless the Czech company paid the ransom. The company RedCanary described it as an "extortion-only" approach.

These new trends in the behaviour of ransomware attackers are changing the way organizations should prepare for ransomware. In addition to protection against ransomware itself, organizations should also consider protection against techniques used by ransomware attackers to exfiltrate data from victims' networks. The most common techniques among these are Exfiltration over C2 Channel (T1041), which we described in the previous chapter, and Exfiltration to Cloud Storage (T1567.002). These are the two most common techniques, used by large ransomware groups like Lockbit, Hive, or Conti, which often target Czech victims to exfiltrate data.

Considering the changing nature of ransomware attacks, NÚKIB has decided to update the public document on Ransomware: Recommendations for Mitigation, Prevention, and Response. The behaviour of ransomware operators is changing and the approach of defenders is shifting. Therefore, the new version of the document takes into account the new techniques used by attackers, the latest recommendations from our partners or the most common issues that organisations deal with in relation to ransomware.

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.