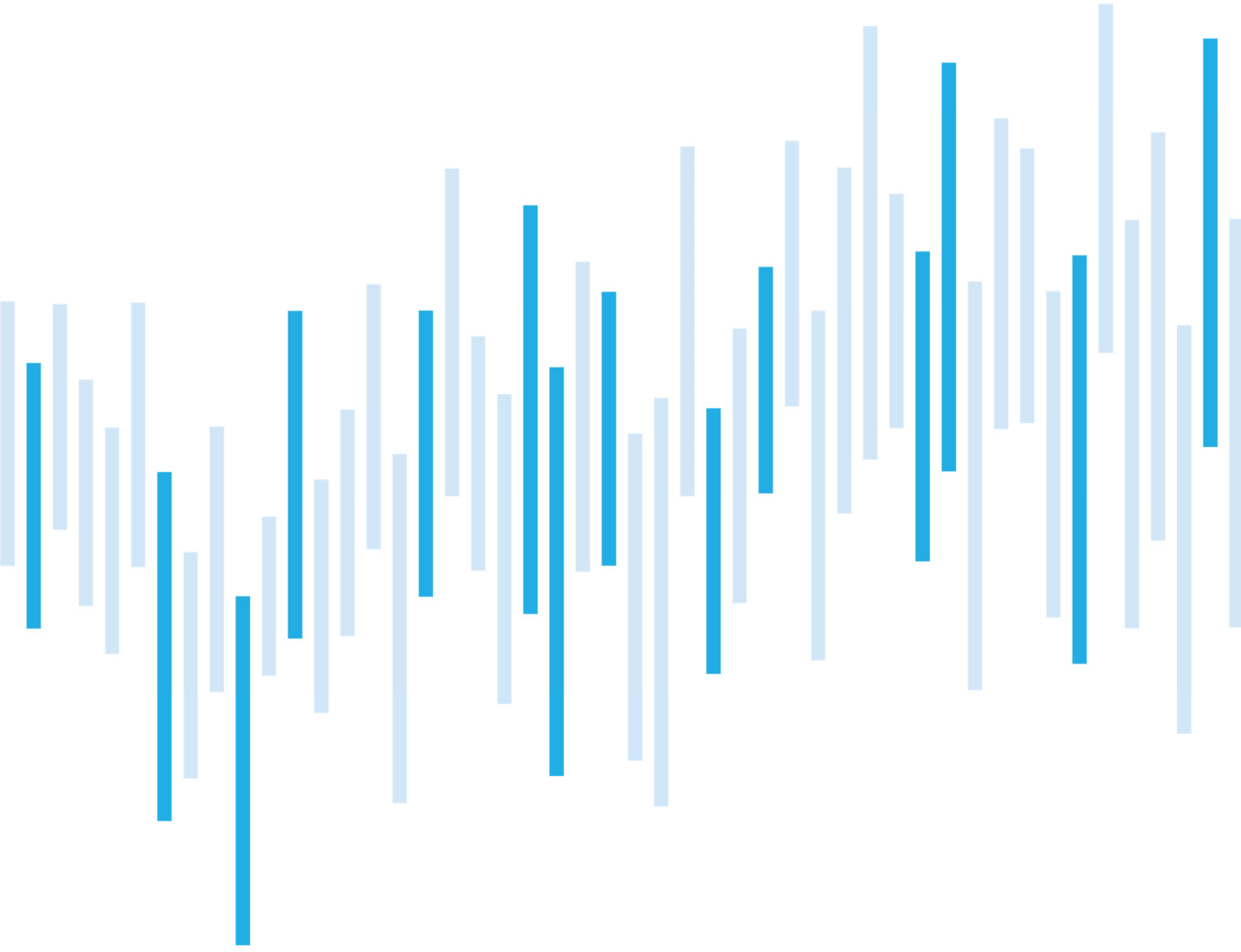
CYBER SECURITY INCIDENTS FROM THE NÚKIB' S PERSPECTIVE

NOVEMBER 2023



National Cyber
and Information
Security Agency

Summary of the month

In November, there was a significant decrease in registered incidents. Although there was no reduction in DDoS attacks by the NoName057(16) group compared to previous months, most of these did not meet the criteria of a cyber security incident. A positive trend could also be observed in terms of incident severity, with only less important cyber incidents registered for the whole of November.

Although there was a significant decrease in the number of incidents from the Availability category compared to previous months, it was again the largest category in terms of proportion. Similarly to the previous months, this number included DDoS attacks and some operational failures. Further NÚKIB dealt with incidents from the Information Content Security and Intrusion categories.

Within the chapter Focus on a threat, this time we are focusing on actors using the Phobos ransomware, which has been recorded many times in the past in the NÚKIB's records.

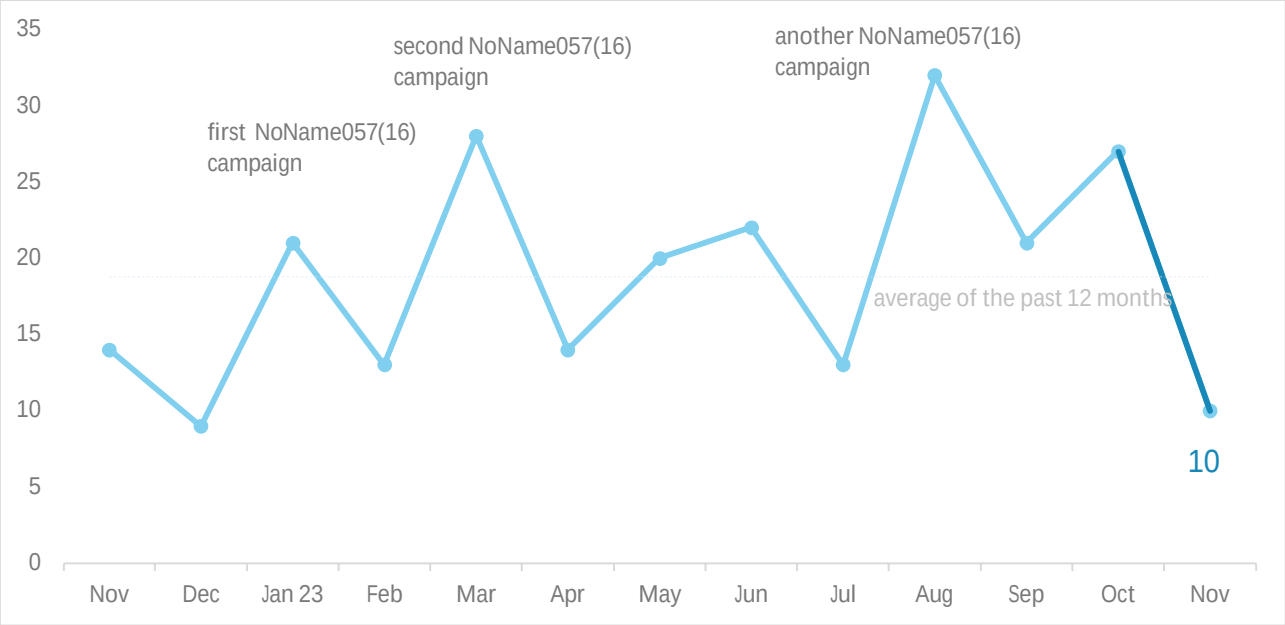
Table of content

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

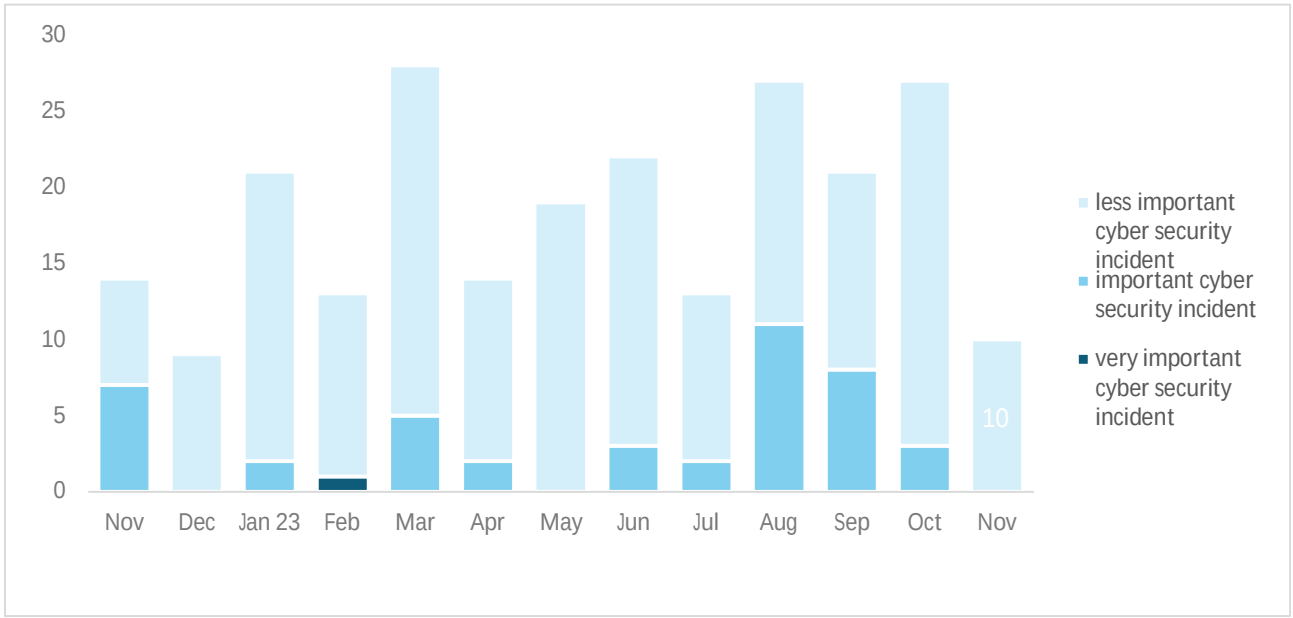
Number of cyber security incidents reported to NÚKIB[1]

In November, there was a significant decrease in registered incidents. Although there was no reduction in DDoS attacks by the NoName057(16) group compared to previous months, most of these did not meet the criteria of a cyber security incident.



Severity of the handled cyber security incidents[2]

During November, NÚKIB did not register any important or very important incident, making it only the second month this year when only less important cyber security incidents were registered.



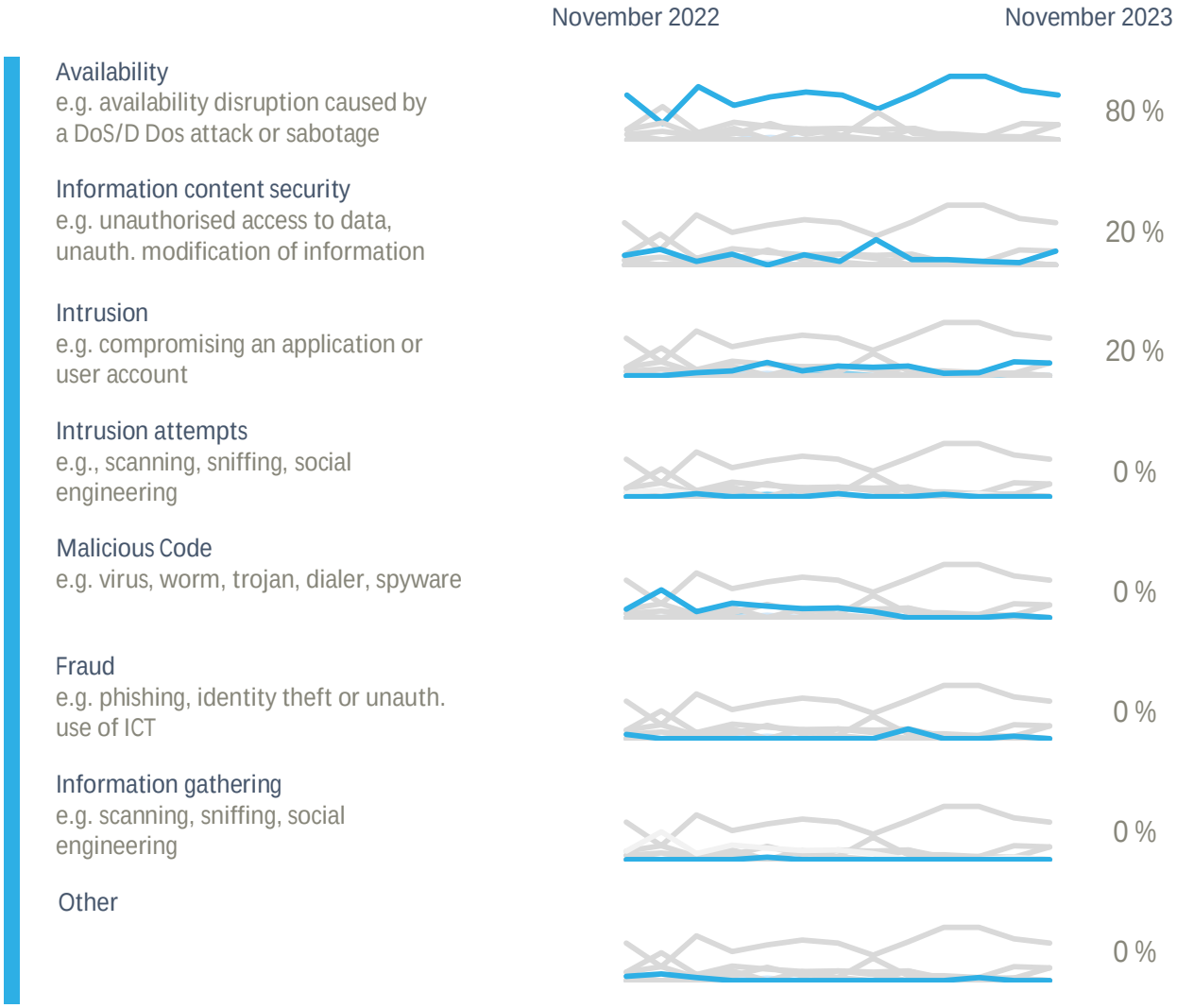
[1] NÚKIB registered 10 incidents in total with liable entities according to Cyber Security Act.
[2] NÚKIB determines the severity of cyber incidents based on Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [3]

Although there was a significant decrease in the number of incidents from the Availability category compared to previous months, it was again the largest category in terms of proportion. Similarly, to the previous months, this number included DDoS attacks and some operational failures.

NÚKIB responded to incidents in two other categories in November:

- During November, NÚKIB recorded two intrusions in total that involved the use of not very sophisticated phishing with several recognizable elements typical for social engineering. Despite this, the attackers were successful in both cases and managed to compromise the targeted accounts.
- Within the Information Security category, there were two successful ransomware attacks at regulated entities (see the section below).



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

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

Phishing, spear-phishing and social engineering

In November, NÚKIB registered only two incidents in which the use of phishing was confirmed. Both cases resulted in the subsequent compromise of the accounts and the access gained was consequently used to further distribution of phishing emails from the compromised accounts.

Malware

In November, there were continuous activities in the area of malware analysis, not only in relation to registered incidents, but also as part of NÚKIB proactive activities.

Vulnerabilities

NÚKIB did not issue any alerts regarding new vulnerabilities in November. However, a security advisory related to the use of the mobile app WeChat and its Chinese version Weixin was issued this month.

Ransomware

In total, NÚKIB registered two incidents involving the Phobos and Cuba ransomwares. While Phobos targeted Czech targets many times in the past, this is the first time that the Cuba ransomware has been recorded.

Attacks on availability

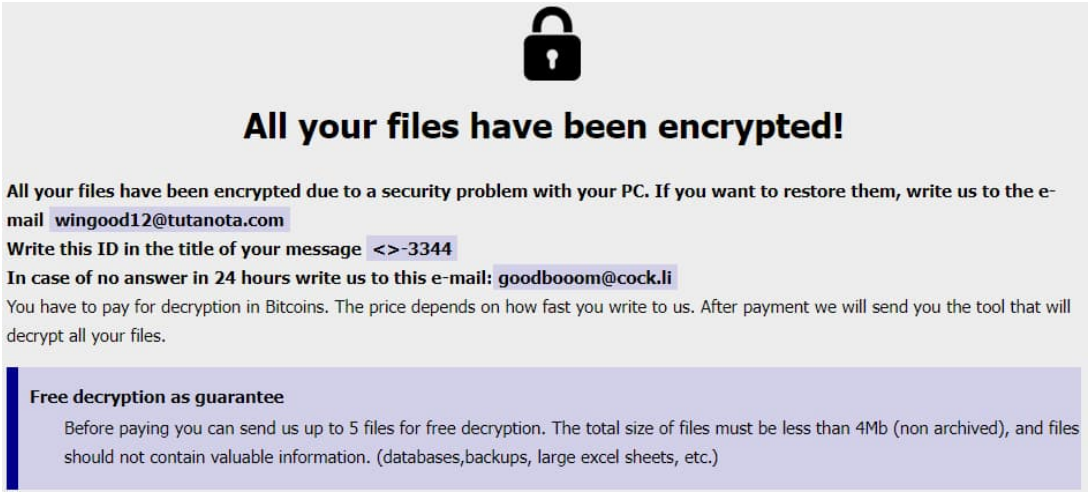
Attacks by the pro-Russian hacktivist group NoName057(16) also continued in November. Although NÚKIB recorded almost thirty of these attacks, only a minimum of them resulted in a cyber incident

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

Focus on a threat: Analysis of actors using Phobos ransomware

In November, NÚKIB registered an incident related to the Phobos ransomware. This is a ransomware, whose variants occurred many times in recorded incidents in the past. The Phobos ransomware family is well known in the community and has been used by a variety of actors since at least 2019. The Cisco Talos Intelligence Group (CTIG) security team has come up with a new analysis focusing specifically on actors using the Phobos ransomware.

Fig. 1: Screenshot of Phobos ransomware ransom note



Source: blog.talosintelligence.com

According to CTIG's findings, it is likely that at least 5 of the most used variants of Phobos ransomware (namely Eking, Eight, Elbie, Devos and Faust) are centrally managed by a single actor. Two facts in particular support this finding. Phobos commonly avoids encrypting files that were previously encrypted by this ransomware, based on blocklists present in its configuration settings. These blocklists are continuously updated with new files that have been used in previous Phobos campaigns. This means that given variants might be managed by a central authority that monitors the use of ransomware variants and tries to prevent mutual collisions.

The use of the same public key in the configuration data within the analysed samples represents the second factor indicating the central management of the aforementioned Phobos variants. The CTIG assesses that only one actor holds the private key to the samples and that this may be the developer of the ransomware offering it as a service (Ransomware-as-a-Service, RaaS). This hypothesis is also supported by the high number of contact emails and other contact details used in Phobos ransomware attacks, suggesting the existence of a widespread affiliate base typical for RaaS. The above-mentioned findings may help in understanding the activities of the actors using the Phobos ransomware and thus may assist in efforts to prevent and mitigate their future attacks.

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.