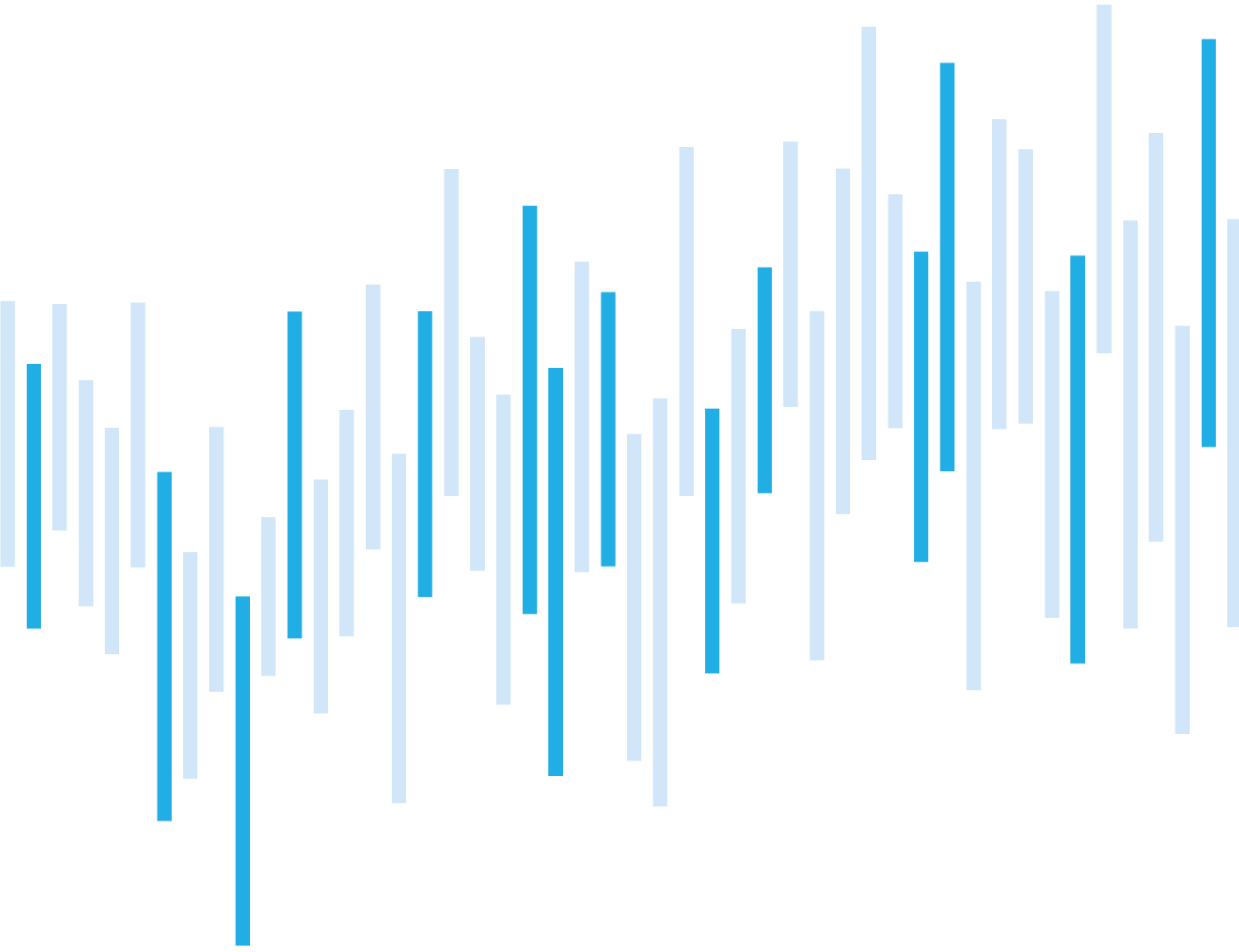
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

AUGUST 2024



National Cyber and Information Security Agency

Summary of the month

In August, 31 incidents were recorded, one fewer than in July. The trend of an above average number of incidents continued for the second month. The high number of incidents during August is mainly due to a DDoS campaign by the Russian-speaking hacktivist group NoName057(16) against public and financial sector entities. However, there were other availability attacks where the attacker could not be identified.

Most of the incidents fell into the category of less important, however, one of the recorded ransomware attacks against a public sector institution was assessed as significant.

In the Focus on a Threat chapter, this time we deal with the NGate malware and fraud campaign that was discovered by the cybersecurity company ESET. Its originators are trying to obtain sensitive data and financial resources of victims, and they were supposed to be active within the Czech Republic.

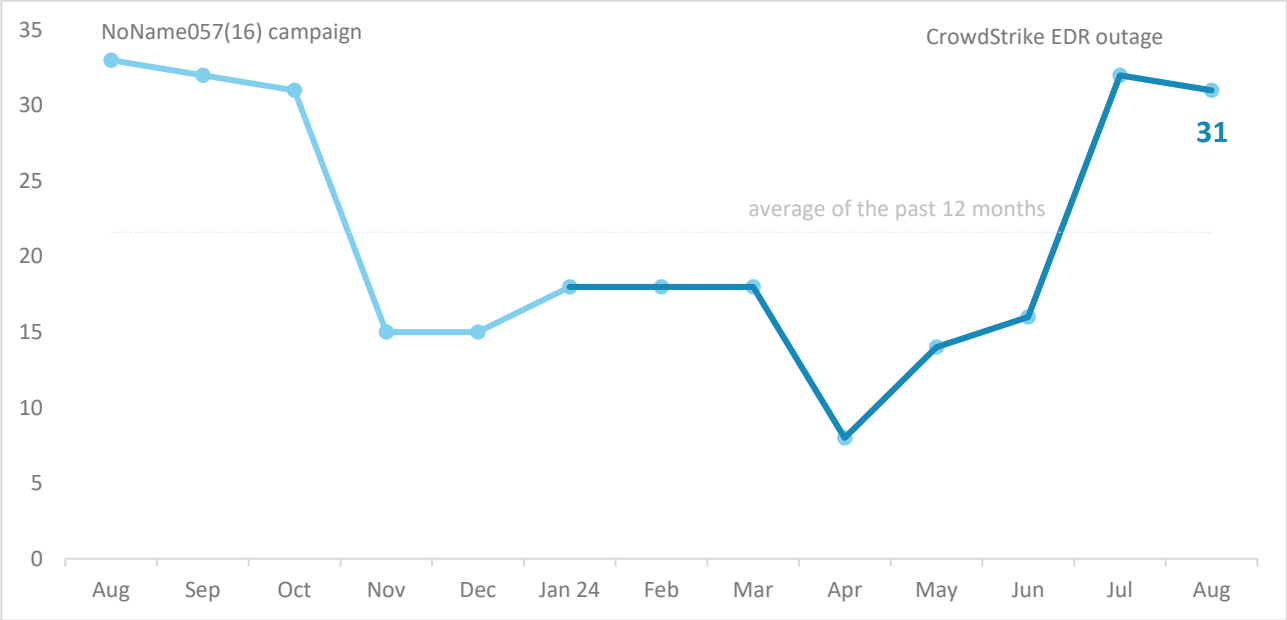
Table of content

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.gov.cz

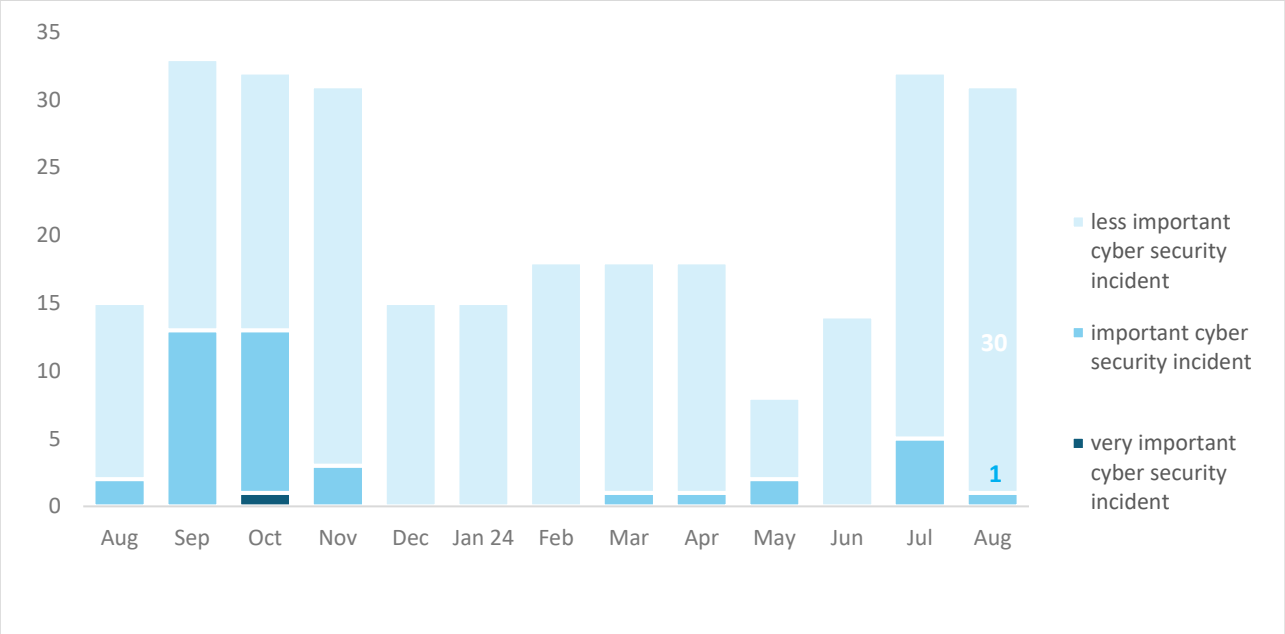
Number of cyber security incidents reported to NÚKIB

In August, 31 incidents were recorded, meaning both summer months were significantly above average in the number of incidents. July's increase was due to an outage of CrowdStrike EDR software, while August's elevated number was due to a DDoS campaign conducted by Russian-speaking hacktivists.



Severity of the handled cyber security incidents[1]

Only one of the recorded incidents was assessed as important, the remaining 30 fall into the category of less important. This again shows the trend that despite the high number of individual DDoS attacks, these cases do not have significant impacts on their victims.



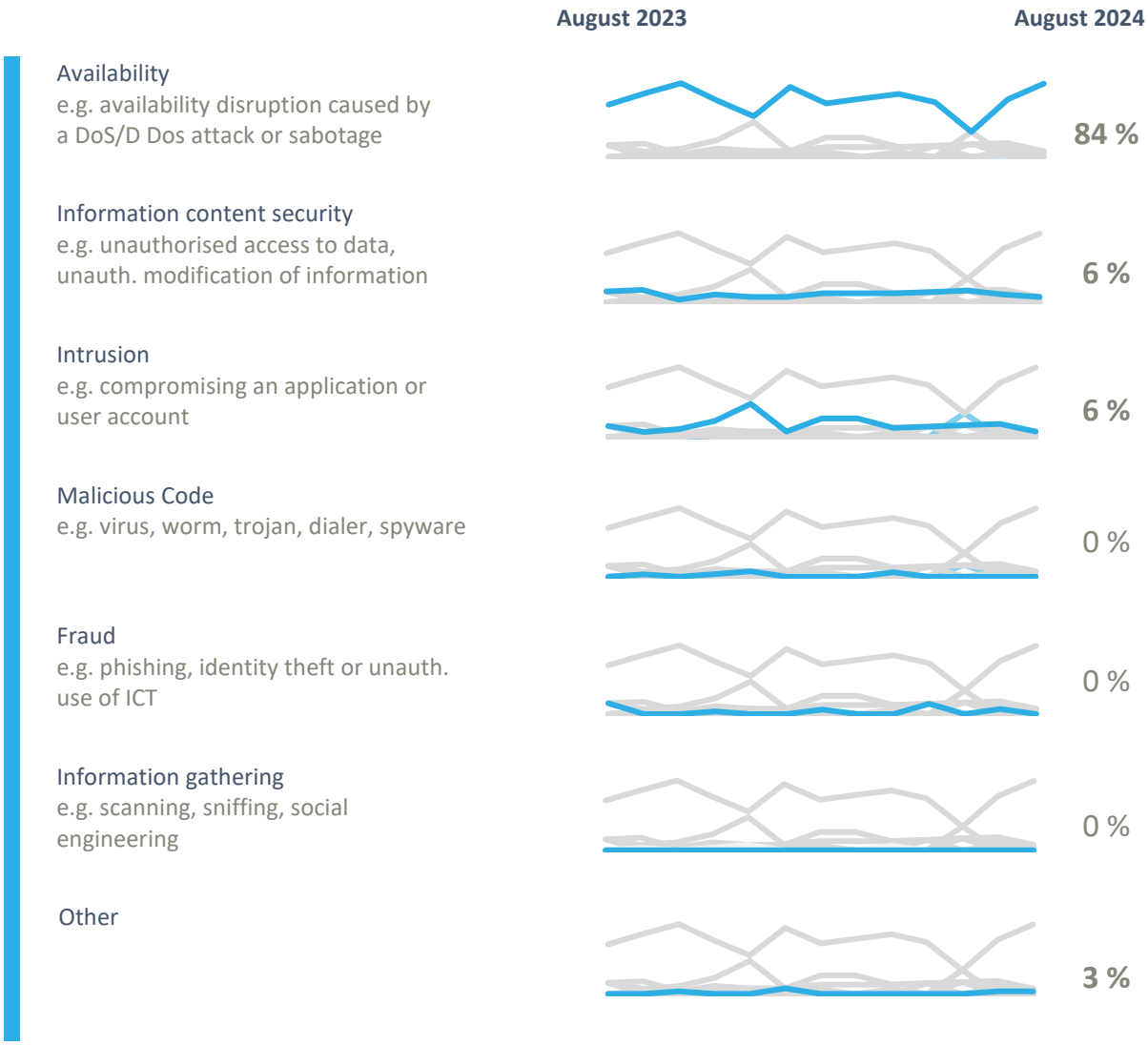
[1] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [2]

Due to the high number of DDoS attacks in August, and on the contrary a smaller number of other incidents, the Availability category dominates the August overview. In addition to more than twenty DDoS or DoS attacks, it also includes 4 outages due to technical failures.

NÚKIB also dealt with incidents in two categories:

- Two incidents fell into the Information content security category, both of which were ransomware attacks. One of the attacks was conducted against a public sector institution and is attributed to the White Rabbit group. The second attack was carried out by the RansomHub group.
- Within the category of Intrusion, NÚKIB recorded two incidents of user accounts being compromised. In one case, the attacker successfully convinced a foreign client of the compromised company to authorise payment of a fake invoice, while in the other case, the attacker merely spread spam.



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

August trends in cyber security from the NÚKIB's perspective [3]

Phishing, spear-phishing and social engineering

In August, NÚKIB did not record any phishing incidents.

Malware

In August, as in the previous months, there were continuous activities regarding malware analysis in connection with some previously recorded incidents.

Vulnerabilities

During August, NÚKIB continued to publish vulnerabilities through its X social media channel, where the Digital Information Agency (DIA) also published information about a malicious campaign to spoof government websites to obtain sensitive information and funds from victims.

In addition, there was also a statement issued by the NÚKIB in cooperation with the Personnel Data Protection Office (ÚOOÚ) warning of e-commerce applications collecting non-standard amounts of user data.

Ransomware

In August, two ransomware-related incidents were recorded. One of them was perpetrated by the White Rabbit ransomware group and was conducted against a public sector institution, while the second incident is connected to the RansomHub group.

Attacks on availability

During the month of August, the NÚKIB registered more than twenty DDoS and DoS attacks targeting mainly state institutions. The Russian-speaking hack-tivist group NoName056(17) was behind most of them, while the attacker of the rest is unknown.

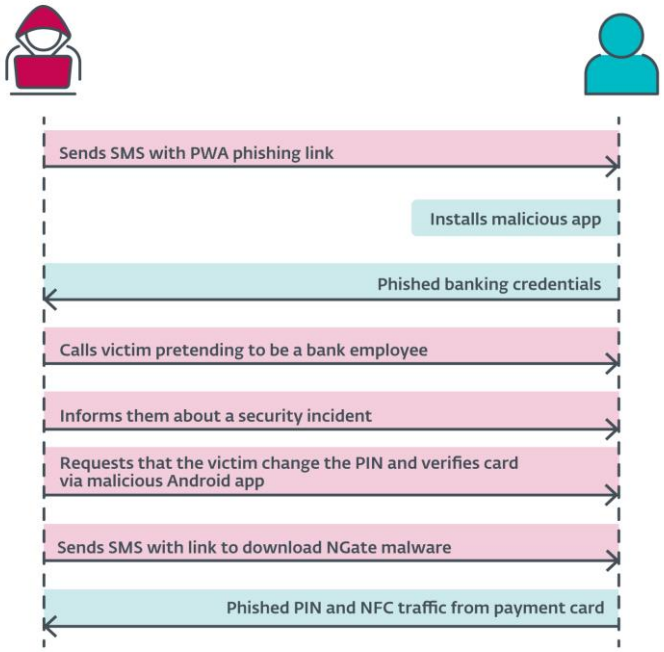
[3] The development illustrated by the arrow is evaluated in relation to the previous month.

Focus on a threat: NGate malware and fraud campaign targeted Czech citizens

Researchers at ESET have spotted a new mobile malware called NGate, which targets Android phone users to obtain the victim's banking details. Although the campaign has reportedly been stopped after the arrest of one of the group's members, **it cannot be ruled out (40-50%) that it will be resumed or replicated by other actors in the future.**

This malware has been reported in the Czech Republic, Hungary and Georgia. In the Czech Republic, clients of three unnamed banks were targeted. The attackers trick the victim into installing the malware on their device by phishing. Once NGate is launched, it displays a fake web page that extorts the victim's bank details. What makes this malware particularly risky is the NFCGate feature, which can also obtain other banking details through the NFC technology used for contactless payments on mobile phones. With this data, attackers can completely spoof the victim at ATMs and then withdraw cash from their account. Alternatively, they can mimic NFC communications for smaller contactless payments. Through NFC functionality, the malware can be used without installation on the victim's device as a card reader copying payment data. The data obtained would only allow for smaller contactless payments not requiring a PIN.

Pic. 1: NGate campaign scheme



Source: eset.com

According to ESET, the campaign involves sophisticated phishing in several phases to trick the victim into installing a malicious app. The best way to defend against this malware is to download apps only from verified and legitimate sources. You should also be cautious when entering your banking or other login details. Last but not least, it is advisable to set low limits on ATM withdrawals or card payments to limit the amount of money an attacker can steal. It's also a good idea to keep an eye on your contactless payment cards so that they can't be scanned, as NFC doesn't work at distances greater than 5cm.

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	40–50 %
Unlikely	20–35 %
Highly unlikely	0–15 %

Traffic Light Protocol

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website https://ww.first.org/tlp/). 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.