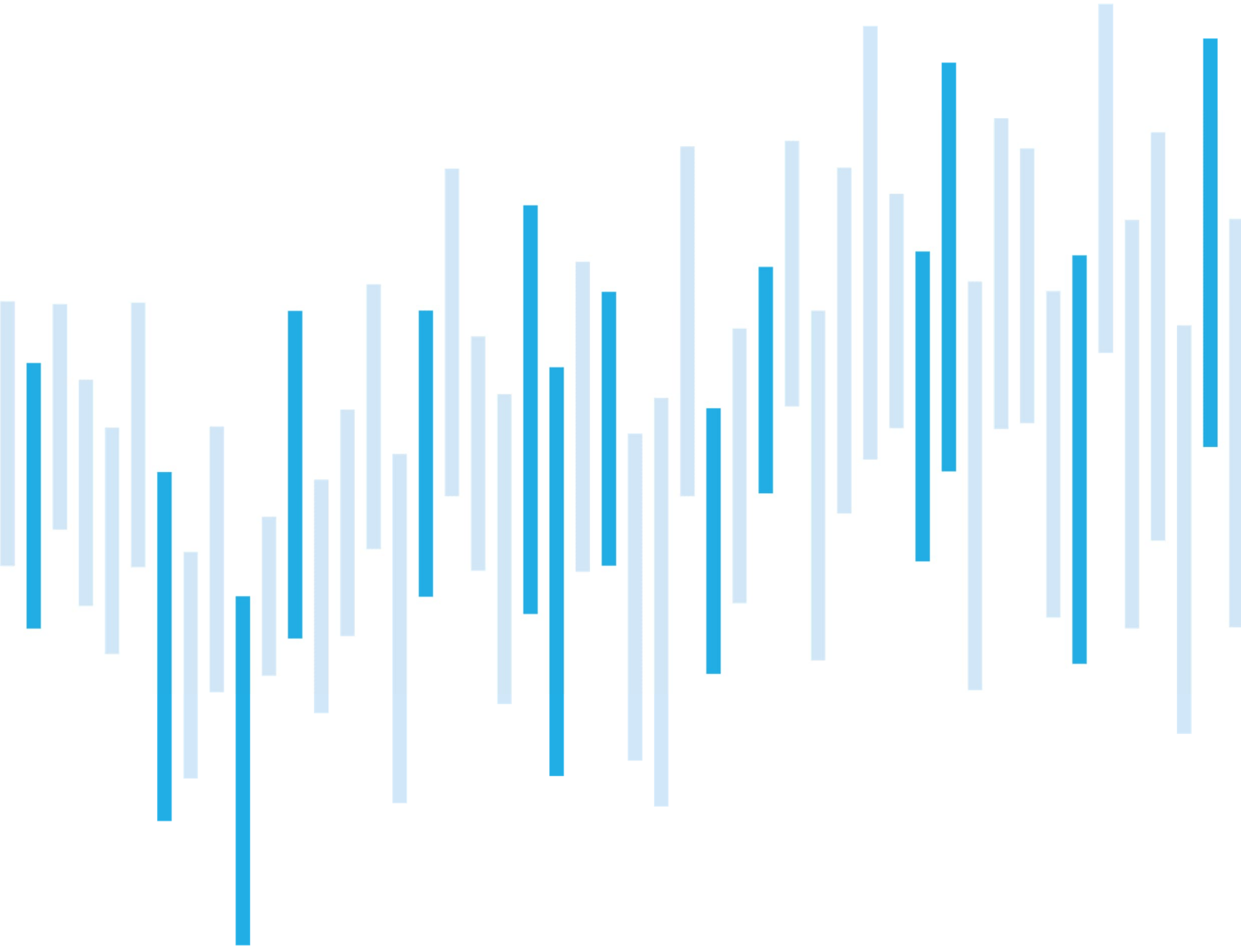
CYBER SECURITY INCIDENTS FROM THE NÚKIB' S PERSPECTIVE

FEBRUARY 2024



National Cyber
and Information
Security Agency

Summary of the month

The number of incidents recorded in February was identical to the previous month. It was the fourth month in a row with below average figures. For the first time in three months, an important cyber incident was registered. The remaining 17 incidents fell into the category of less significant.

Also in February, the long-term trend of dominance of availability-related incidents continued. Incidents from the categories of Intrusion and Information Content Security were also registered.

In the Focus on a Threat chapter, we focus this time on the police intervention against the infrastructure of the LockBit ransomware gang. This crackdown can be considered one of the largest of its kind. LockBit has been one of the most active cybercriminal actors, attacking more than 2,000 victims worldwide since 2020. As part of the operation, security forces gained control of the ransomware gang's infrastructure, data and other information. Within the operation the decryptor to the LockBit 3.0 ransomware was obtained.

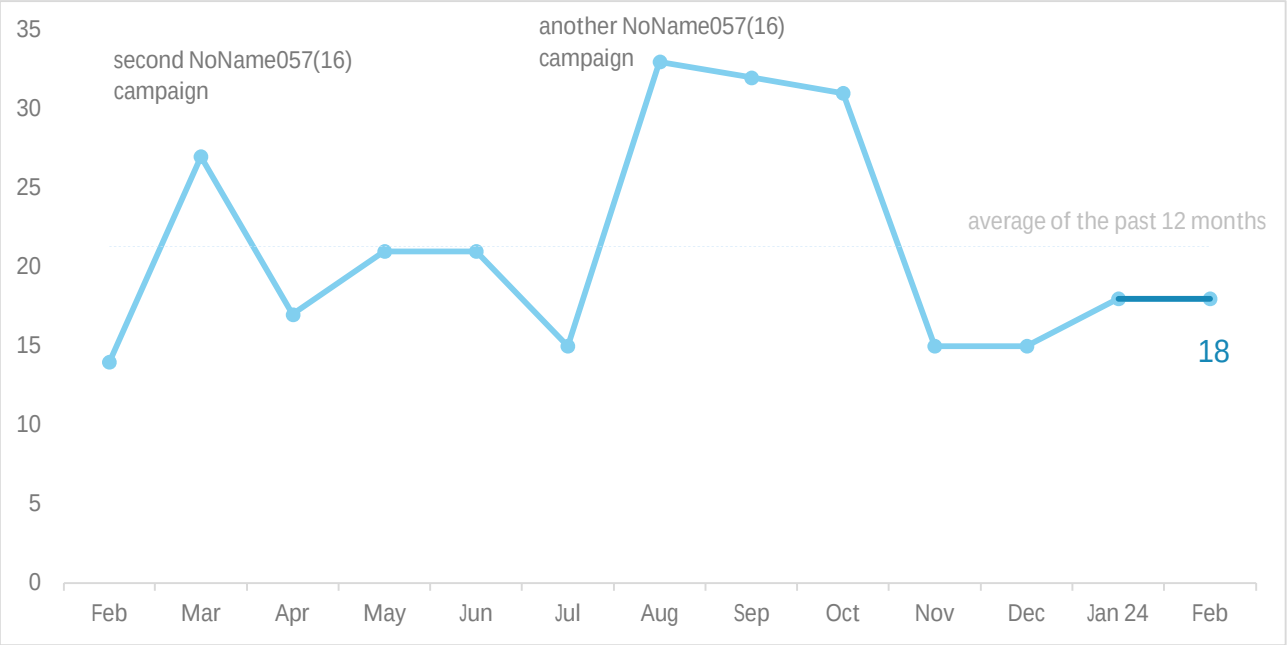
Table of content

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

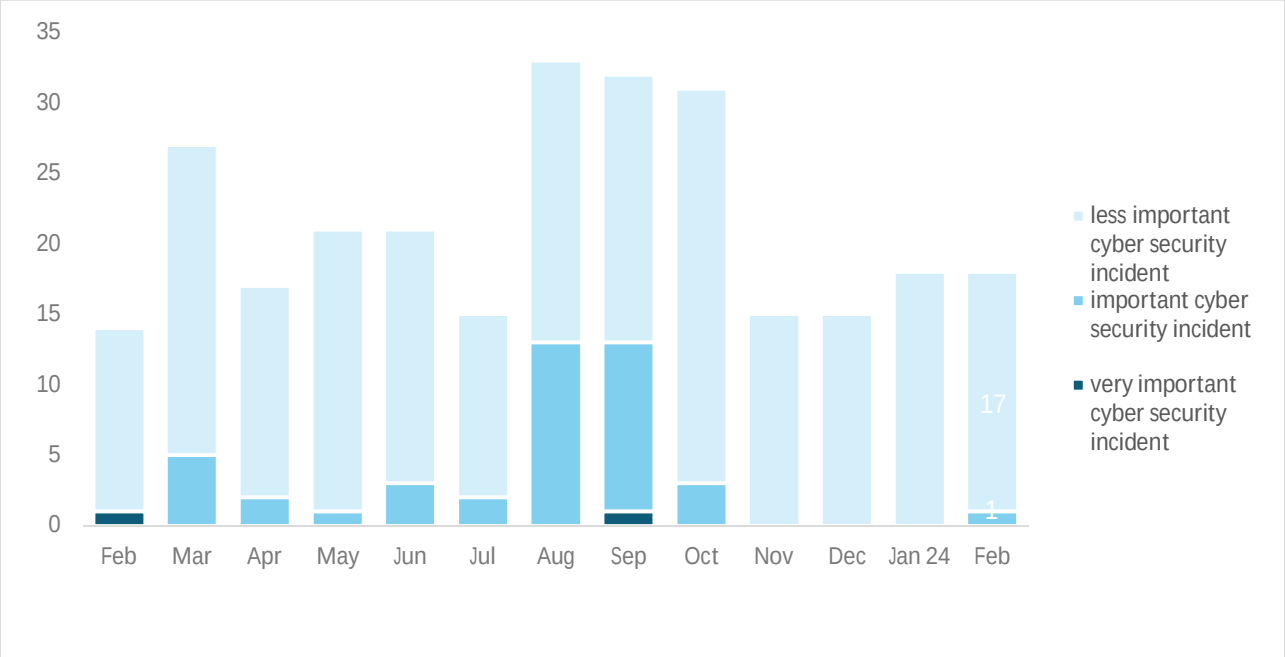
Number of cyber security incidents reported to NÚKIB[1]

The number of incidents recorded in February was identical to the previous month. It was the fourth month in a row with below average figures.



Severity of the handled cyber security incidents[2]

During February, an important cyber security incident was registered for the first time in three months. The remaining 17 incidents fell into the category of less important.



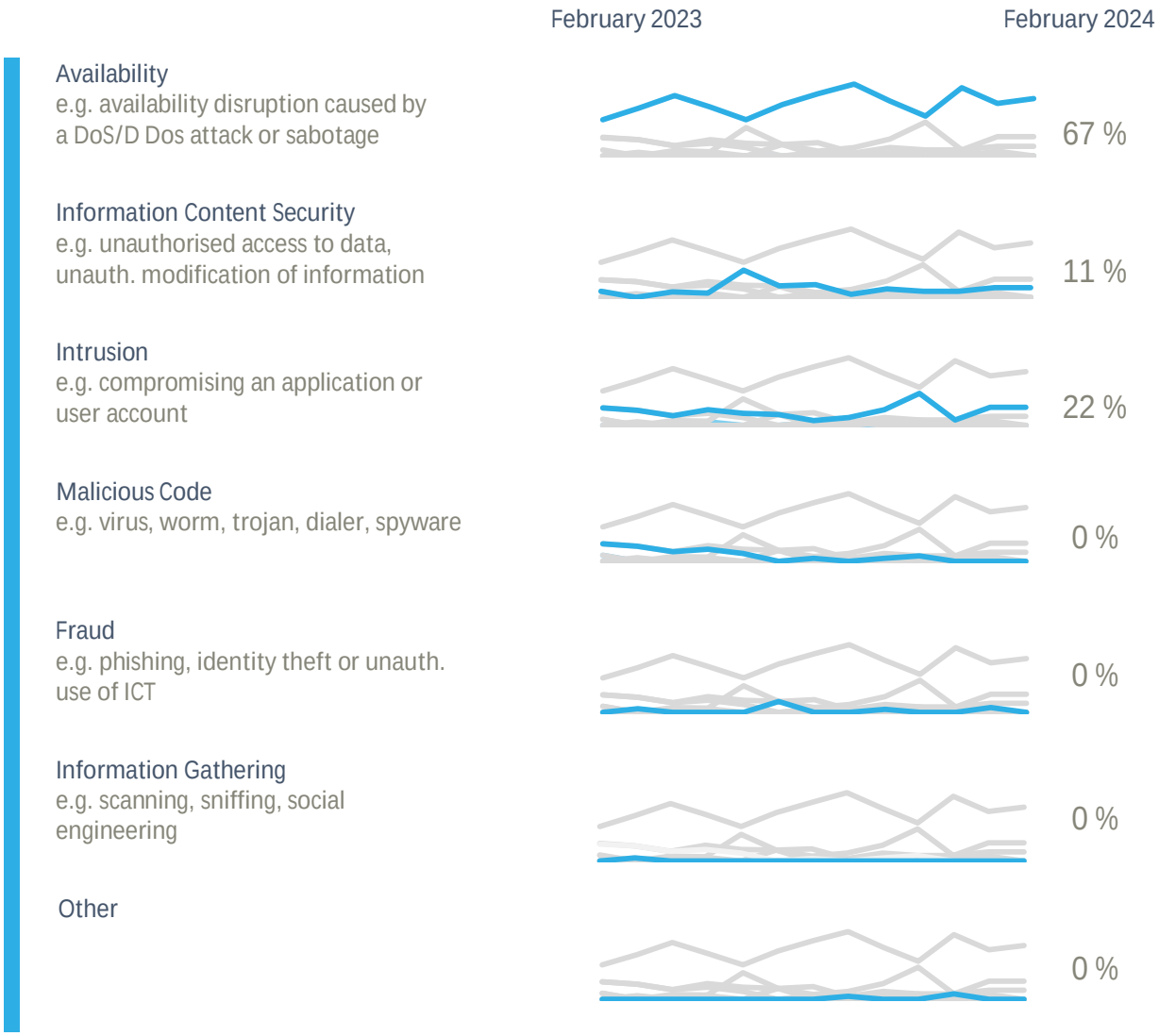
[1] NÚKIB registered 16 incidents in total with liable entities according to Cyber Security Act. The remaining 2 incidents involved unregulated entities.
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [3]

Also in February, the long-term trend of dominance of availability-related incidents continued. As usual, this category consisted primarily of DDoS attacks (see next section) and outages.

NÚKIB further solved incidents in two categories:

- Four cases of Intrusion were registered in February. One incident in this category was related to the Ivanti product vulnerabilities reported in the last month´s summary. For the time being, these vulnerabilities have not yet made a significant contribution to the incidents recorded by NÚKIB, despite open-source information about their widespread exploitation.
- Within the Information Content Security category, NÚKIB recorded one important incident in which sensitive information of a regulated entity leaked. In addition, one incident involving ransomware targeting an unregulated educational institution fell under this category.



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

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

Phishing, spear-phishing and social engineering

In February, NÚKIB registered only two incidents in which the use of phishing was confirmed. The attackers managed to lure the victim into filling in credentials on a fraudulent site and then use these to access other services.

Malware

Like in the previous months, also in February continuous malware analysis activities were conducted in connection with formerly registered incidents.

Vulnerabilities

During February, NÚKIB issued one warning related to vulnerabilities. These were two remotely exploitable vulnerabilities in the FortiOS operating system used in FortiGate firewalls from Fortinet, Inc. NÚKIB recommends that all vulnerable products from this company be updated immediately. If the firewalls do not offer an update, it must be downloaded directly from the manufacturer's website.

Ransomware

In February, as in the previous two months, only one incident related to ransomware was recorded. It was RebornRansomware, through which attackers encrypted virtual servers of an unregulated educational institution.

Attacks on availability

In February, NÚKIB recorded a total of 7 DDoS attacks targeting mainly state institutions. Pro-Russian hacktivist groups were behind only two of these attacks.

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

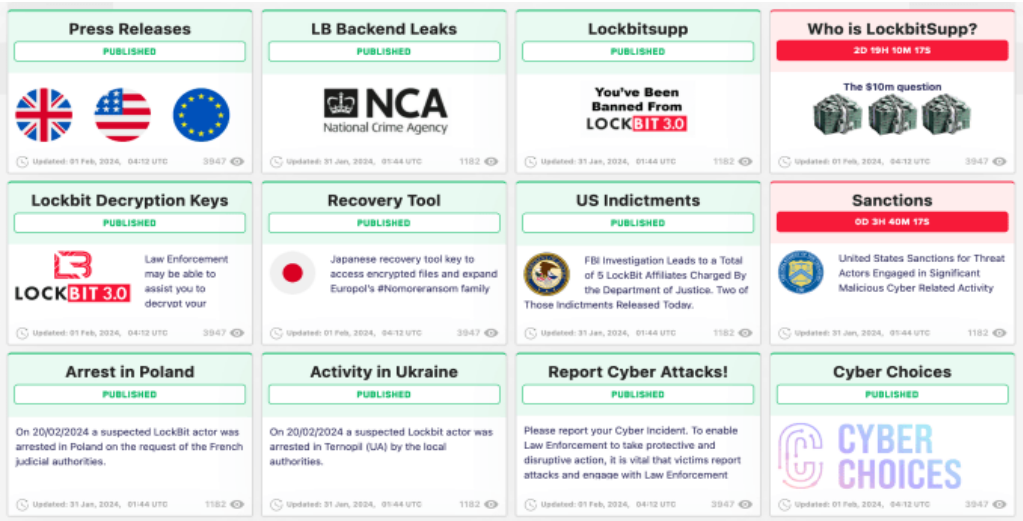
Focus on a threat: The crackdown on the infrastructure of the LockBit ransomware gang

During Monday, February 19, the darkweb site of the ransomware gang LockBit was seized in an international law enforcement operation involving the UK National Crime Agency, FBI, Europol and several international police agencies. As part of the operation, security forces gained control of the ransomware gang's infrastructure, data and other information. Shortly thereafter, they began to announce a variety of information, namely through LockBit's leaksite (see Figure 1). Security forces also recently announced the seizure of more than 14,000 accounts on third-party services belonging to members or partners of the LockBit gang. Other information already made public includes, for example, that LockBit kept victims' data even after it had received ransom payments from them.

Since the announcement of the operation, the first US arrest warrants have already been issued and the first arrests have been made, specifically in Poland and Ukraine. However, the amount of material seized is reportedly enormous and will take time to analyse. Therefore, it is very likely (75–85%) that further interventions against gang members and their partners or new knowledge of their activities can be expected.

Within the operation the decryptor to the LockBit 3.0 ransomware was obtained, too.

Fig. 1: Screenshot of LockBit leaksite after the takeover by the authorities



Source: techcrunch.com

The police crackdown on the LockBit group can be considered one of the largest of its kind. LockBit has been one of the most active cybercriminal actors, attacking more than 2,000 victims worldwide since 2020. The crackdown has led to a disruption of its capabilities, but also damaged the credibility of the group, whose possible future relationships with criminal partners will be accompanied by fears of compromise. Five days later, however, the LockBit group has resumed its activities and issued a statement commenting on the police intervention. The group also posted information about new victims on its new darkweb page. However, it is not yet clear whether these are real victims or merely an attempt to feign continued activity.

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 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.