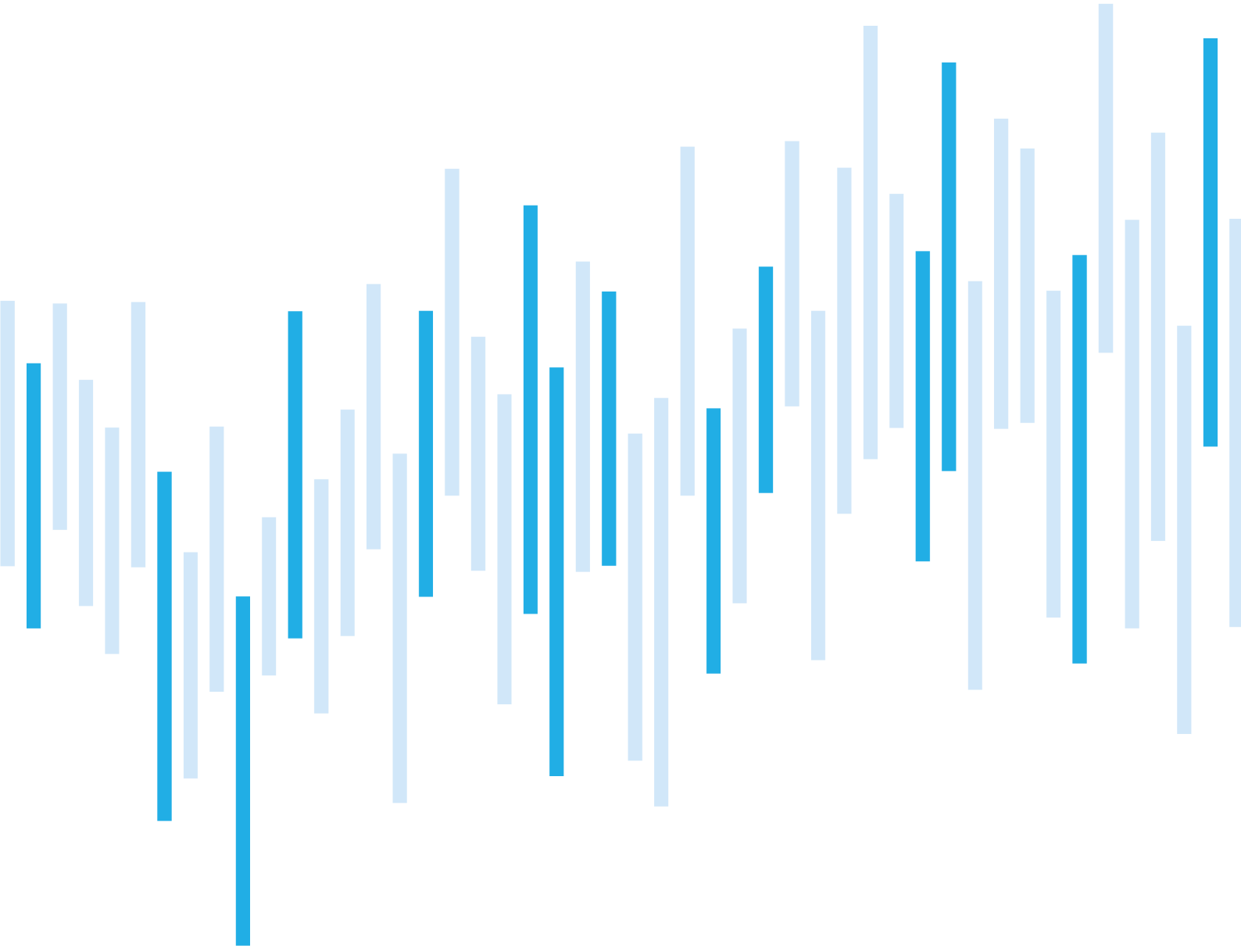
CYBER SECURITY INCIDENTS FROM THE NÚKIB' S PERSPECTIVE

DECEMBER 2023



National Cyber and Information Security Agency

Summary of the month

Although there was a slight increase in recorded incidents in December compared to the previous month, the resulting figure was still relatively low, below the annual average of around 19 incidents per month. As in November, NÚKIB recorded only less important cyber security incidents during December. This category accounted for more than four-fifths of all recorded incidents in 2023.

As was the case throughout the year, the Availability category dominated the incident classification in December. Incidents in this category accounted for nearly two-thirds of all recorded incidents in 2023. Furthermore, NÚKIB dealt with incidents from the Information Security and Intrusion categories.

Within the Chapter Focus on a Threat, this time we focus on the CVE-2023-42793 vulnerability in the TeamCity software solution from JetBrains, which has been actively exploited by the Russian group APT29 (also known as CozyBear or NOBELIUM/Midnight Blizzard).

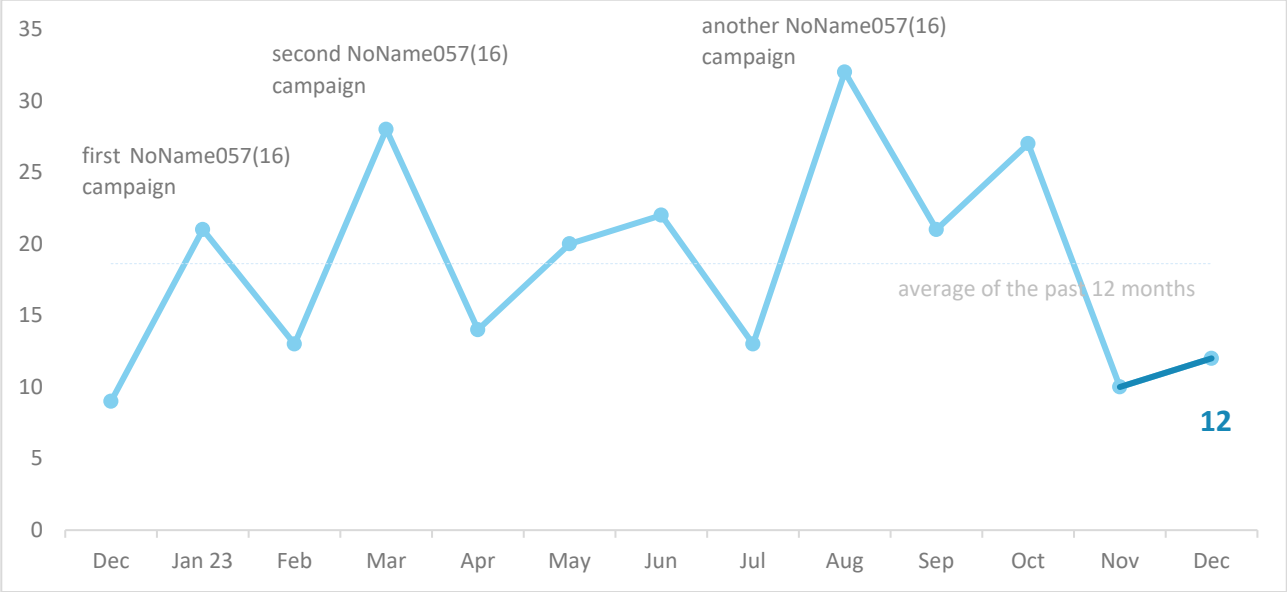
Table of content

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

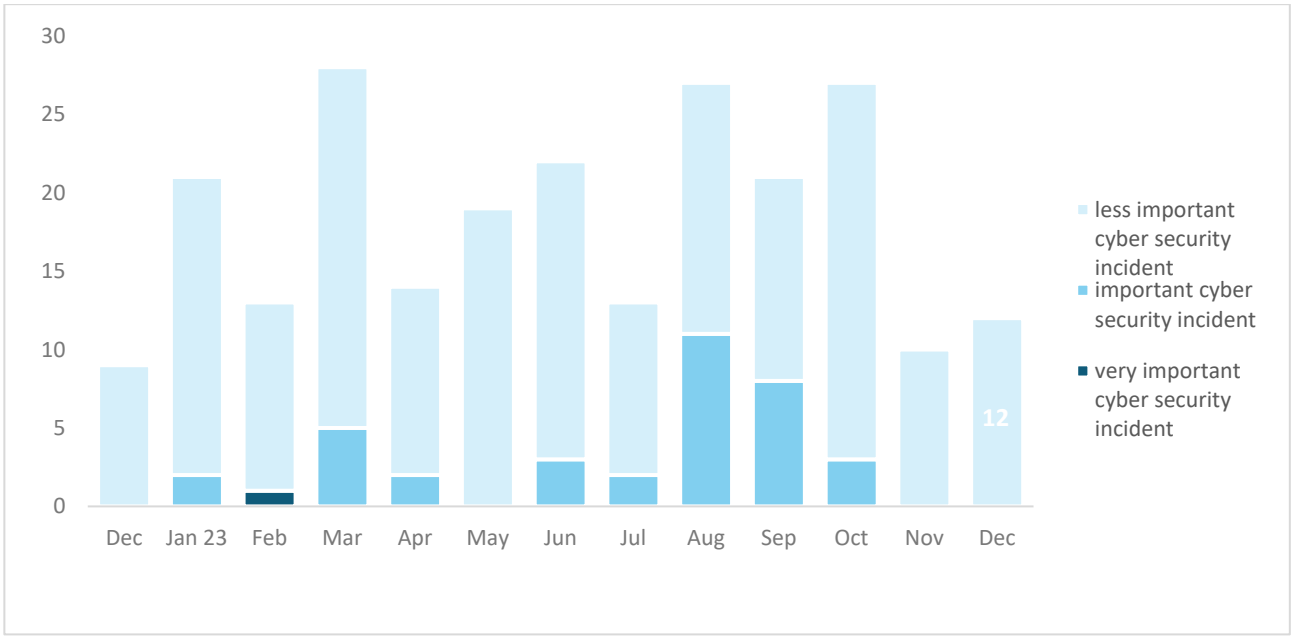
Number of cyber security incidents reported to NÚKIB[1]

Although there was a slight increase in recorded incidents in December compared to the previous month, the resulting figure was still relatively low, below the annual average of around 19 incidents per month.



Severity of the handled cyber security incidents[2]

As in November, NÚKIB recorded only less important cyber security incidents during December, which accounted for more than four-fifths of all recorded incidents in 2023.



[1] NÚKIB registered 9 incidents in total with liable entities according to Cyber Security Act. The remaining 3 incidents involved unregulated entities.

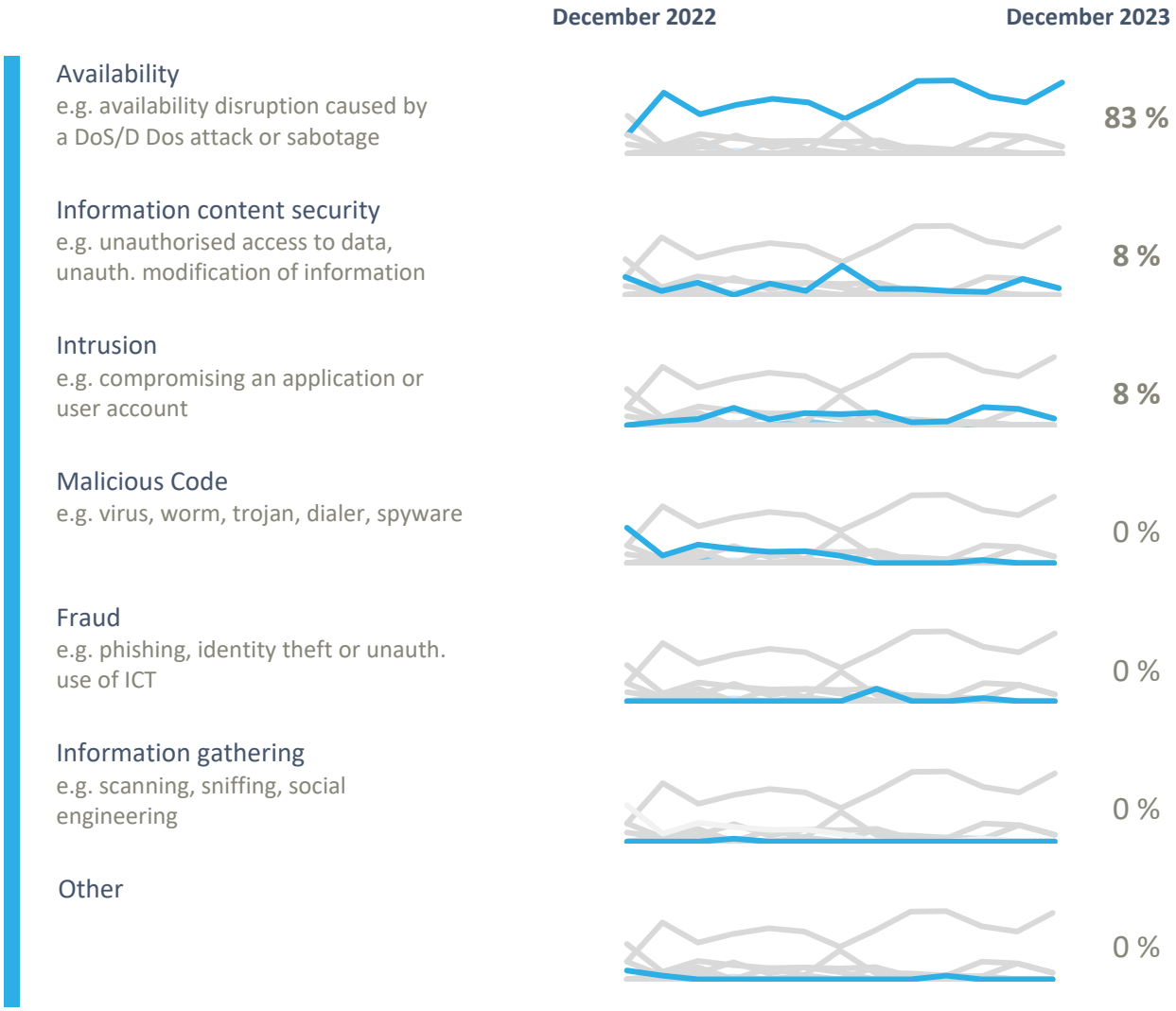
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [3]

As was the case throughout the year, the Availability category dominated the incident classification in December. Incidents in this category accounted for nearly two-thirds of all recorded incidents in 2023. As in previous months, higher numbers of incidents leading to availability disruption were associated with DDoS attacks.

NÚKIB also registered incidents in two other categories in December:

- During December, an intrusion into a regulated entity's system was recorded, resulting in the leakage of customer identification and contact details and some other data. The initial attack vector is unknown at this time.
- Within the Information content security category, NÚKIB recorded an attack by a previously unknown ransomware, during which the attackers encrypted the entity's data and subsequently deleted backups of it



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

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

Phishing, spear-phishing and social engineering

In December, NÚKIB did not register any cases involving phishing or other social engineering methods.

Malware

In December, continuous malware analysis activities were conducted, focusing on selected incidents..

Vulnerabilities

NÚKIB did not issue any advisories regarding new vulnerabilities in December.

Ransom ware

NÚKIB recorded only one incident related to ransomware. The attackers gained access through the Remote Desktop Protocol (RDP) open to the Internet and subsequently encrypted the files and databases of the subject, including their backups.

Attacks on availability

In December, NÚKIB saw a slight increase in DDoS attacks led by various actors, NoName057(16) group, but also by Anonymous Russia, which targeted Czech targets for the first time in more than half a year. For several DDoS attacks, the originator is not yet known.

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

Focus on a threat: Active exploitation of vulnerability in TeamCity

On 13th December, the US Cybersecurity & Infrastructure Security Agency (CISA), along with other US, Polish and UK security agencies, issued a joint warning about a vulnerability in JetBrains' TeamCity software solution. In particular, the institutions warn of vulnerability CVE-2023-42793, which, if exploited, allows an attacker to remotely execute malicious code. According to CISA, this vulnerability is being actively exploited by the APT29 group (also known as CozyBear or NOBELIUM/Midnight Blizzard) associated with the Russian Foreign Intelligence Service (SVR). The attackers use it as an initial attack vector to gain access to the victim's infrastructure, where they then conduct deeper network reconnaissance in an attempt to ensure long-term persistence.

Fig. 1: TeamCity Logo

Source: twitter.com

The TeamCity software solution is mainly a CI/CD (continuous integration & continuous delivery) platform. CI/CD platforms are usually used by programmers and DevOps specialists for writing code, its versioning and then testing and integration. One of the main reasons why development companies deploy such solutions is that it allows them to automate a large number of processes and activities related to software development,

In the context of this campaign, NÚKIB wants to draw attention to the need for supply chain security control. To be able to control the supply chain, it is necessary for each supplier to keep a so-called SBOM (software bill of materials). Within this list of individual software components, it is then easy to track down a vulnerable component, identify its inclusion in the infrastructure and negotiate a remedy.

During the ongoing evaluation of the current campaign, NÚKIB has not registered a high risk of exploitation of the vulnerability in the TeamCity software solution within its constituency, however, despite this, NÚKIB draws attention to the need to control the supply chain and, if a vulnerable version of the TeamCity software solution is detected, to mitigate its exploitation or, in the best case, to update this component.

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://nukib.gov.cz/en/). 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.