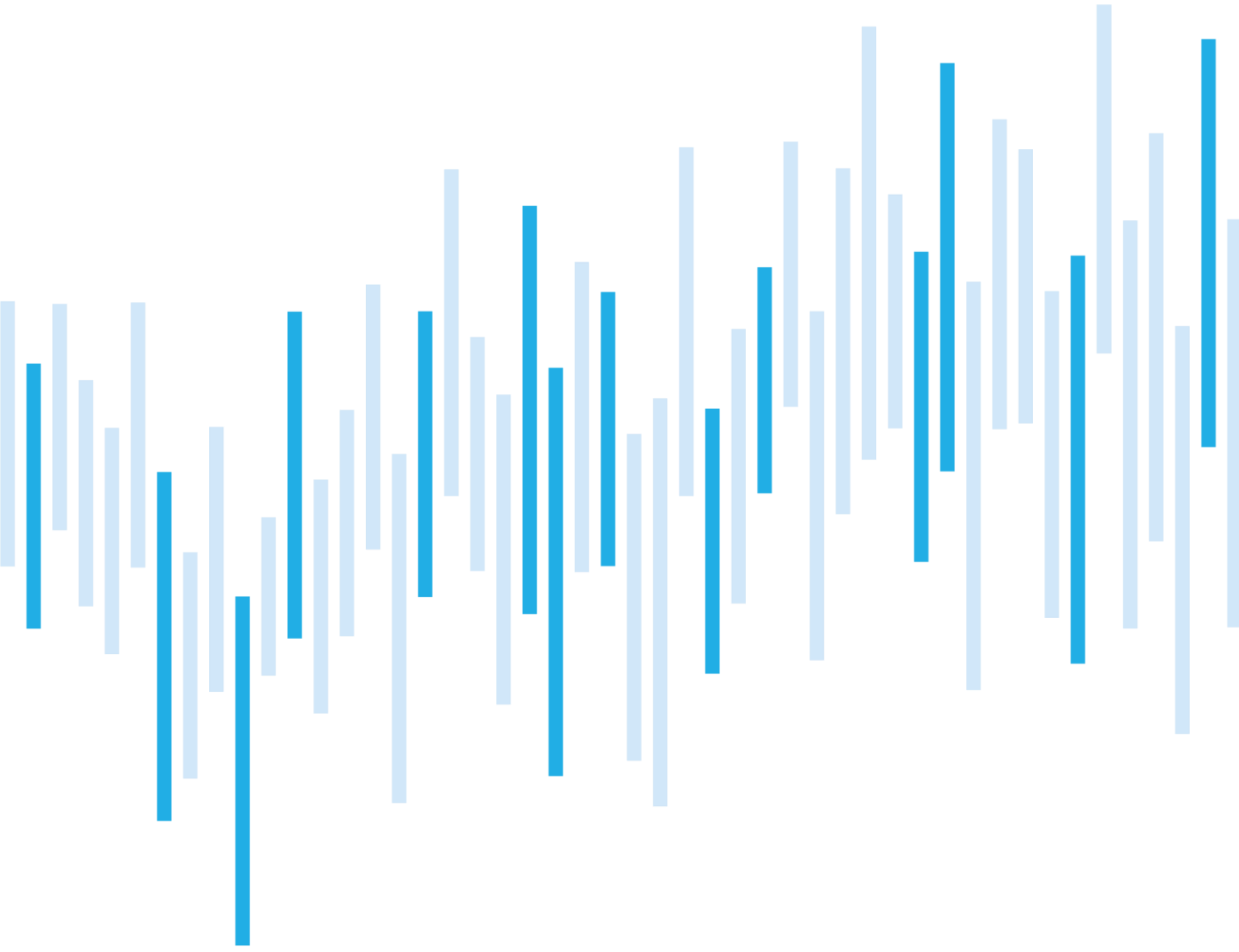
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

MAY 2024



National Cyber and Information Security Agency

Summary of the month

In May, the number of recorded cyber incidents rose again to a total of 14. However, the resulting figure is still below the long-term average.

The incidents recorded during May were quite diverse and almost all categories of incidents were recorded. In terms of impact, however, all were categorised as less important.

The Focus on an event chapter refers about the political attribution of the cyber espionage operations of the Russian state-sponsored group APT28 (also known as Fancy Bear or Forest Blizzard). Attribution was made by the Czech Republic and Germany in early May, along with support from the EU, NATO, and the United States, the United Kingdom, and France. The statement referred to the group's long-standing malicious activities against strategic government institutions, but also specifically to its recent campaign exploiting a vulnerability in Microsoft Outlook to obtain sensitive data.

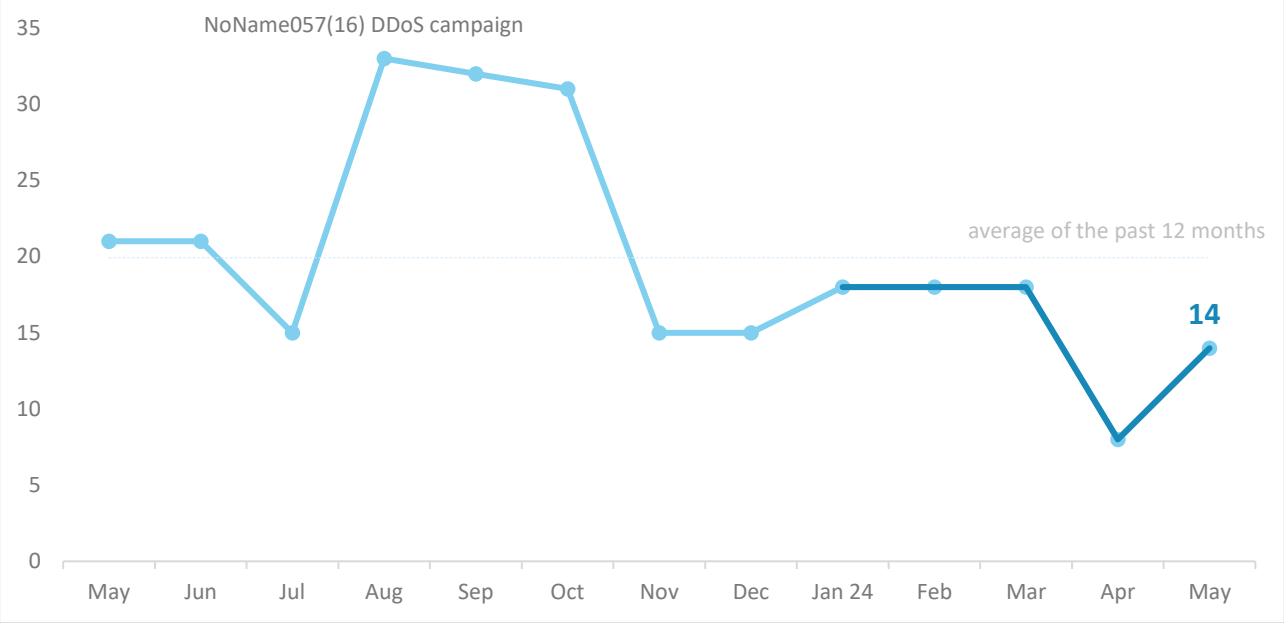
Table of content

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

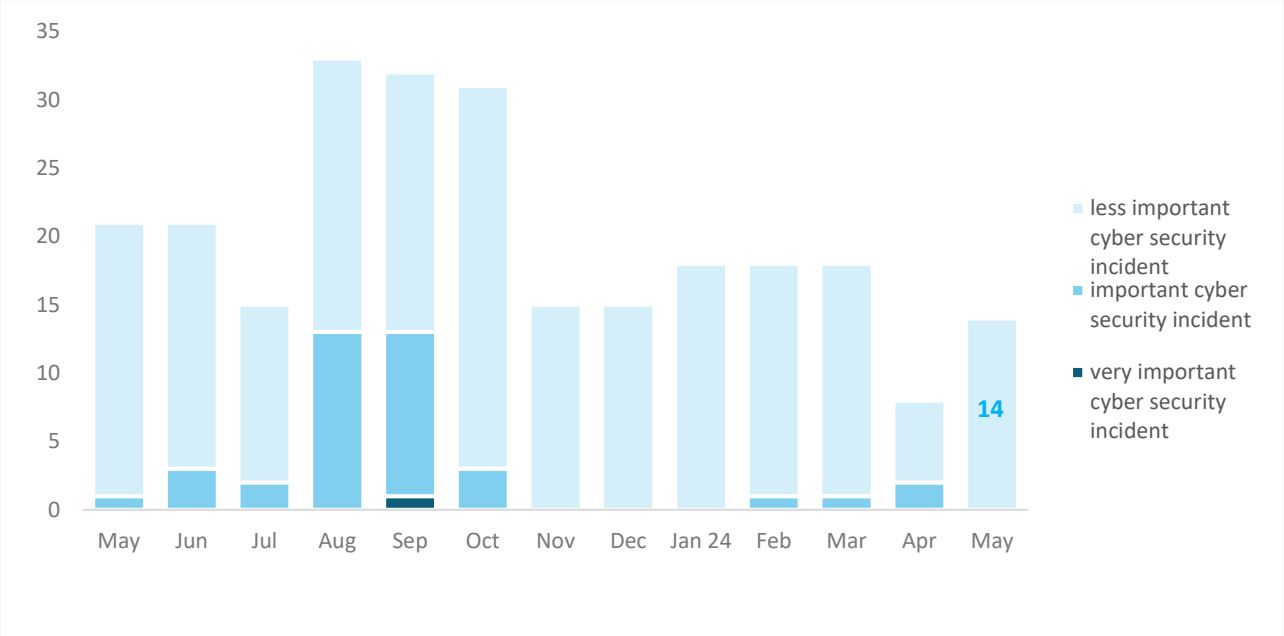
Number of cyber security incidents reported to NÚKIB

During May, a total of 14 incidents were recorded, which represents a gradual return to the average values of the previous year. As in April, NÚKIB did not register any DDoS attacks, which historically significantly increased the average number of incidents.



Severity of the handled cyber security incidents[1]

All 14 of May's cyber incidents fall into the less important category.

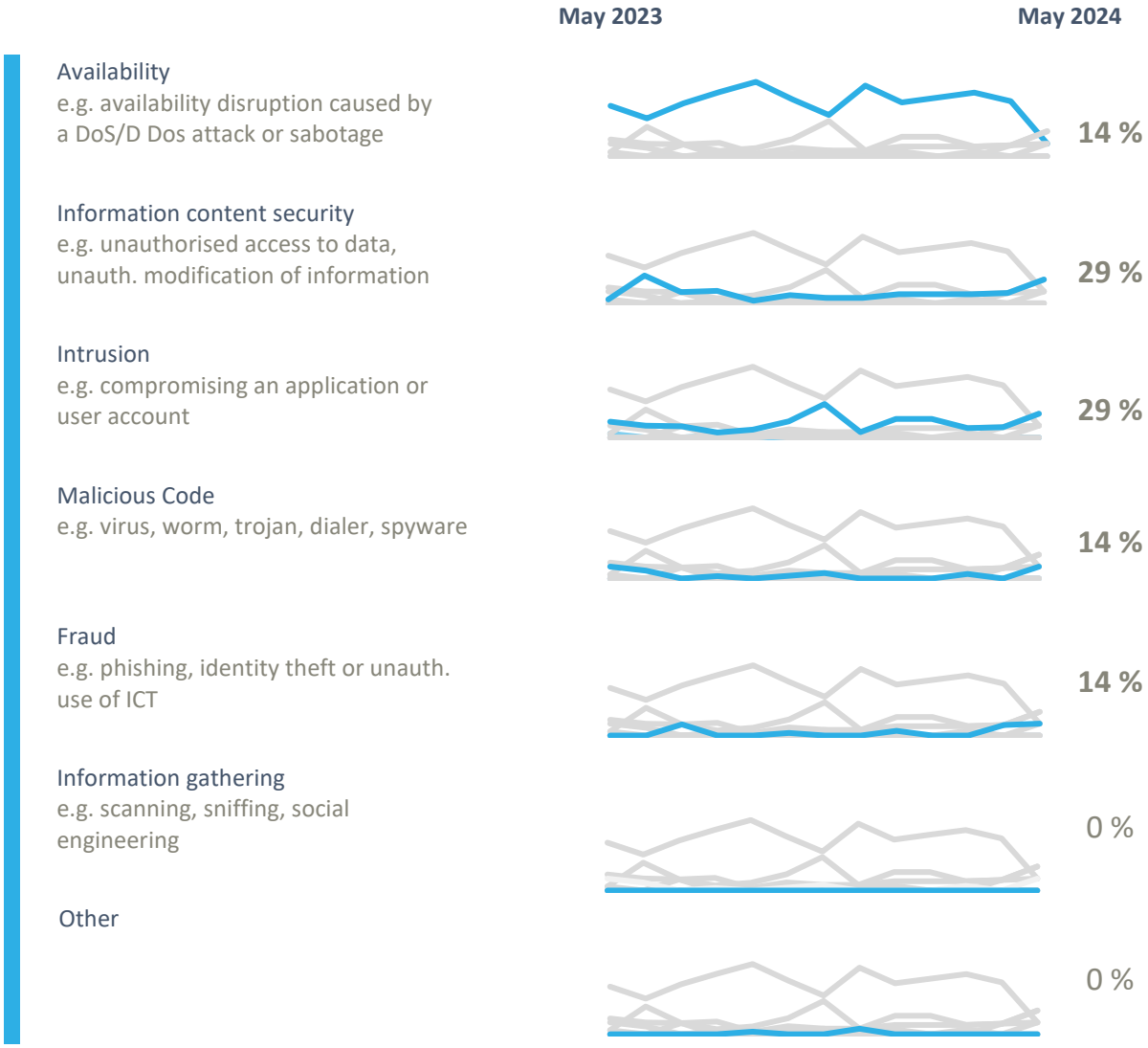


[1] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [2]

A number of different types of incidents were recorded in May. From malicious code and service outages to intrusions and various types of fraudulent behaviour, including fraudulent CEO e-mails with the aim of stealing funds. Specifically, NÚKIB dealt with incidents in the categories of Fraud, Information Security, Availability, Malicious Code and Penetration.

- There were two ransomware attacks, among others. One is the responsibility of the RansomHub group operating in RaaS (Ransomware as a Service) mode, and the other is the responsibility of the Akira Ransomware group.
- The two incidents in the Availability category were caused by a technical fault in the infrastructure.
- In the Penetration and Fraud category, there were mainly successful phishing campaigns that either leaked login credentials or further sent malicious messages. In one case, however, payments from clients of the compromised company were successfully redirected to the financial account of the attacker, resulting in financial damage.



[2] 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 [3]

Phishing, spear-phishing and social engineering

In May, the NÚKIB recorded four incidents in which phishing techniques were used. In all cases, however, the impact of the incidents was low. However, in one case, a fake CEO e-mail resulted in a payment being sent to the attacker's account. However, the fraud was promptly detected and the payment reversed.

Malware

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

Vulnerabilities

During May, NÚKIB did not issue any vulnerability alerts.

Ransomware

In May, two ransomware-related incidents were recorded. One of them was caused by the RansomHub group operating in RaaS (Ransomware as a Service) mode, while the other incident was caused by the Akira Ransomware group.

Attacks on availability

During May, NÚKIB recorded two incidents in the category of Availability, which were caused by a technical fault. In one case, the service outage involved two critical information infrastructure systems.

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

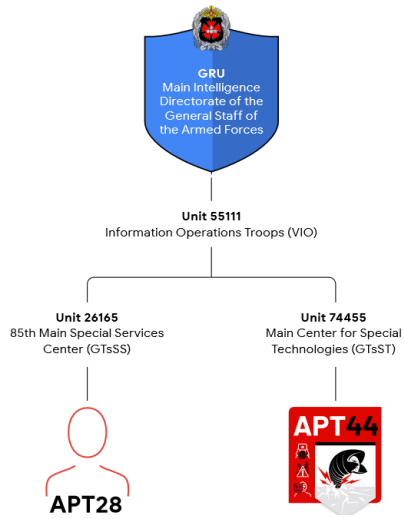
Focus on an event: Attribution of malicious activities in cyberspace to the Russian Federation

On Friday, May the 3rd, malicious activities in cyberspace were attributed to the Russian Federation by the Czech government. Specifically, the attribution of cyber espionage attacks to the Russian state-sponsored group APT28 (also known as Fancy Bear or Forest Blizzard), which operates under the Russian military intelligence service (GRU) command. **APT28 has long targeted the government sector of Western countries, including the Czech Republic.** As a result, Germany has made a similar attribution alongside the Czech Republic, with both public statements accompanied by expressions of support from the European Union, the North Atlantic Treaty Organization, and, at the national level, the United States, the United Kingdom, and France.

The main attacks attributed include the exploitation of the CVE-2023-23397 vulnerability in the Outlook email application or the execution of attacks through the network of compromised Ubiquiti routers. This network was targeted in February in an operation called Dying Ember, in which the Czech military intelligence service (VZ) also participated.

APT28 is one of two known units under the GRU command, the other being APT44 (also known as Sandworm). APT28's primary focus is on long-term cyber espionage operations, with some of the more significant ones including the interference in the 2016 US presidential election and the 2017 French presidential election. **A high percentage of the group's current activity, then, has been concentrated towards Ukraine in the context of the conflict.**

Fig. 1: Diagram of the expected structure of GRU cyber units according to Mandiant



Political attribution of cyber-attacks is an important tool for states to deter attackers from further malicious activities, but also to demonstrate their ability to detect and willingness to attribute such activities to specific attackers. It can also serve as a basis for possible retaliation or demonstration of unity.

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.