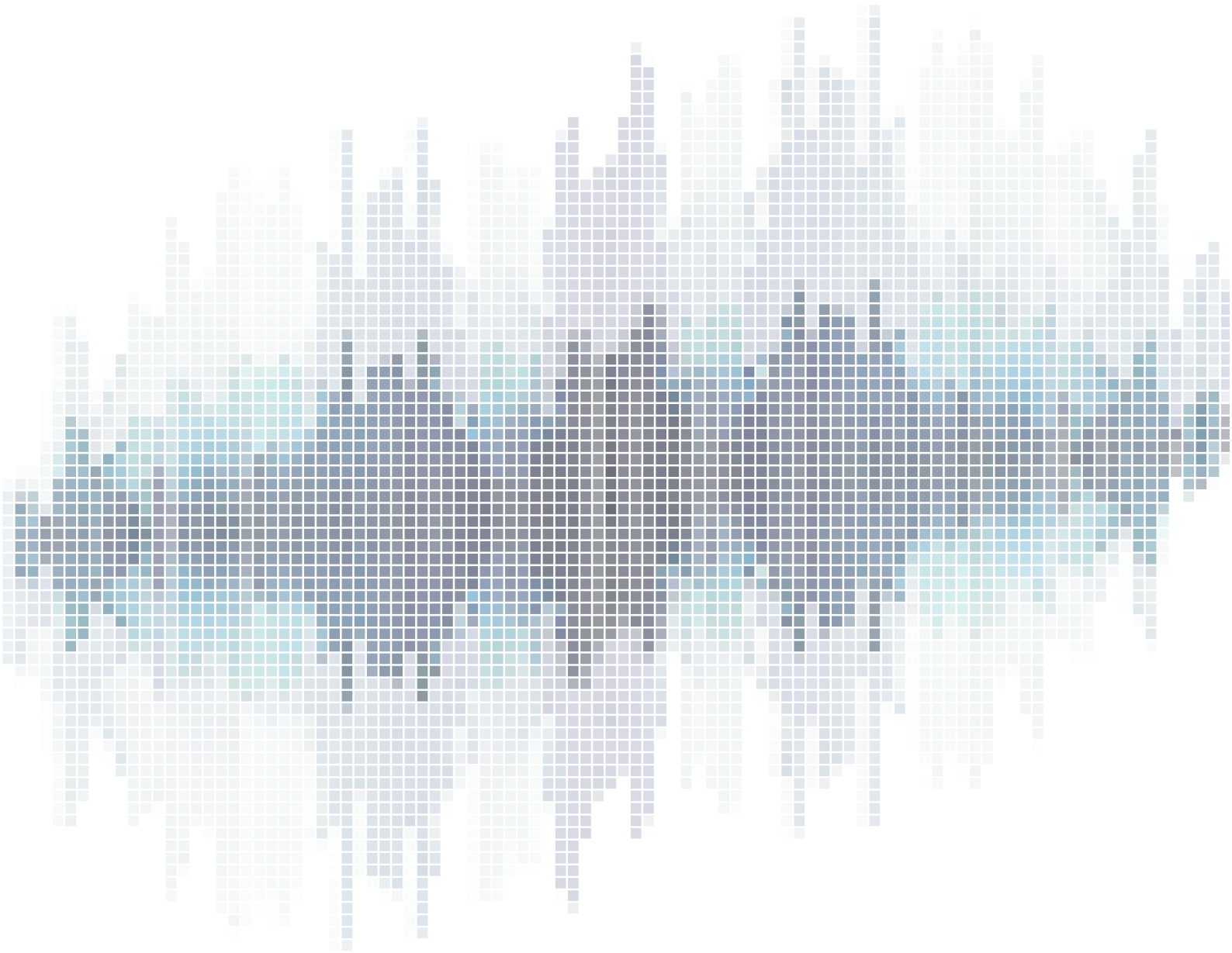
NÚKIB QUARTERLY

Cyber Threat Landscape Q4/2025



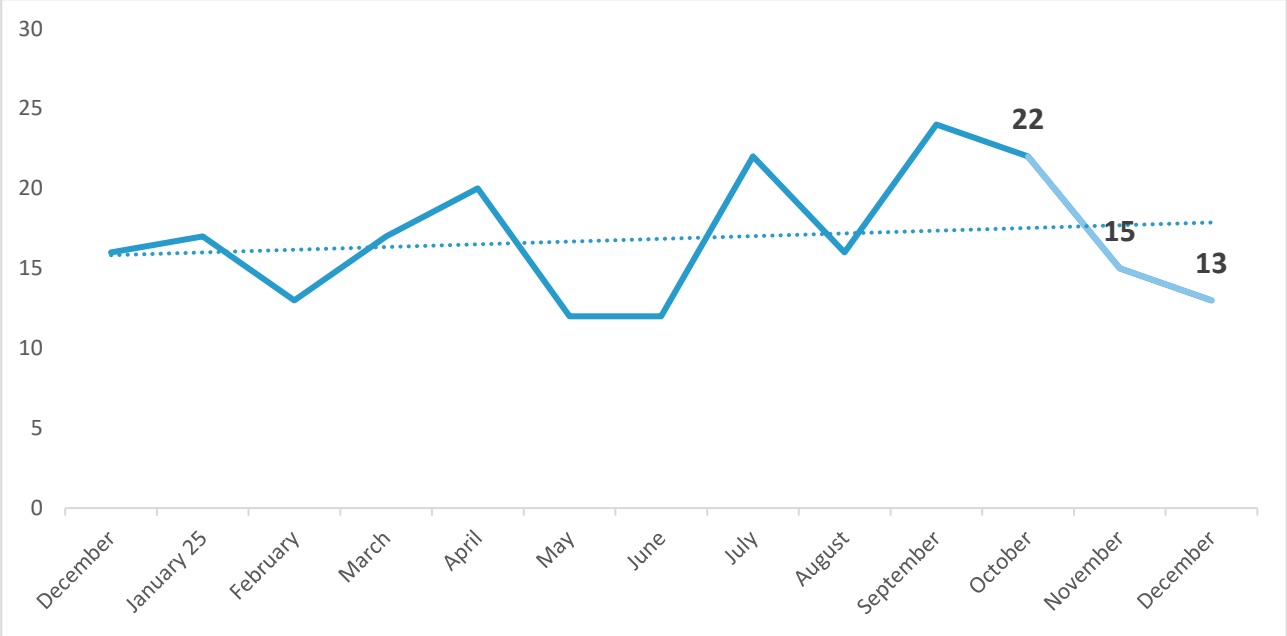
Summary of the Past Quarter[1]

In the last quarter of 2025, NÚKIB recorded a slight decrease in reported incidents. This was due, among other things, to a lower number of recorded DDoS attacks, which decreased approximately fourfold compared to the previous quarter. The most numerous types of incidents in the given period were outages and ransomware attacks. Despite the frequency, none of the ransomware attacks were classified as important or very important incidents. They were carried out by a number of different groups, including the Qilin, Inc. Ransom, Warlock, J Group, and Obscura gangs. NÚKIB also recorded several phishing attacks, account and system compromises, and instances of malicious code. NÚKIB recorded only five incidents related to DDoS attacks for the entire quarter.

NÚKIB responded to a number of different threats in the fourth quarter. **One example is the Joint Cybersecurity Advisory against the activities of pro-Russian hacktivists, which NÚKIB joined together with other Czech and international partners. In December, NÚKIB issued a statement in support of the United Kingdom's warning about the malicious cyber activities of the Chinese companies I-S00N and Integrity Tech.** The ecosystem of private entities in the People's Republic of China, which, among other things, develop offensive tools for local intelligence and security agencies and carry out cyber operations against other countries, poses a significant threat to Czech entities as well.

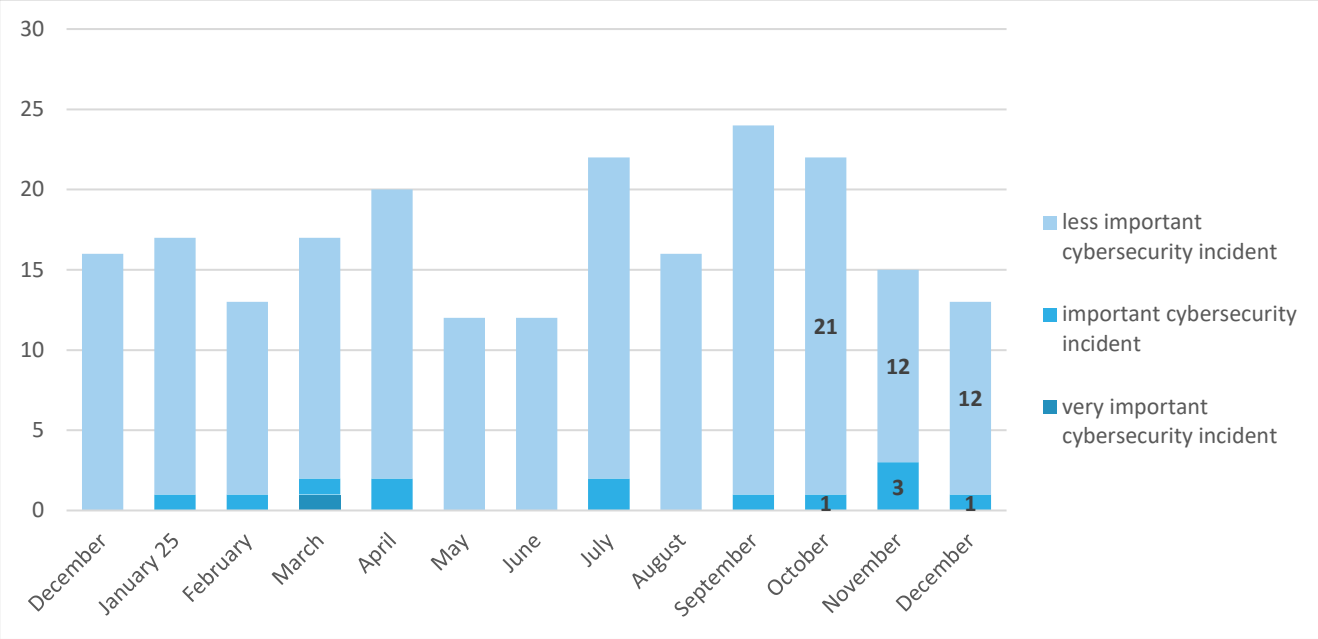
The report also includes a broader overview of cyber threats relevant to the Czech Republic and the activities of NÚKIB in the area of international cooperation.

Number of Cyber Security Incidents Registered by NÚKIB



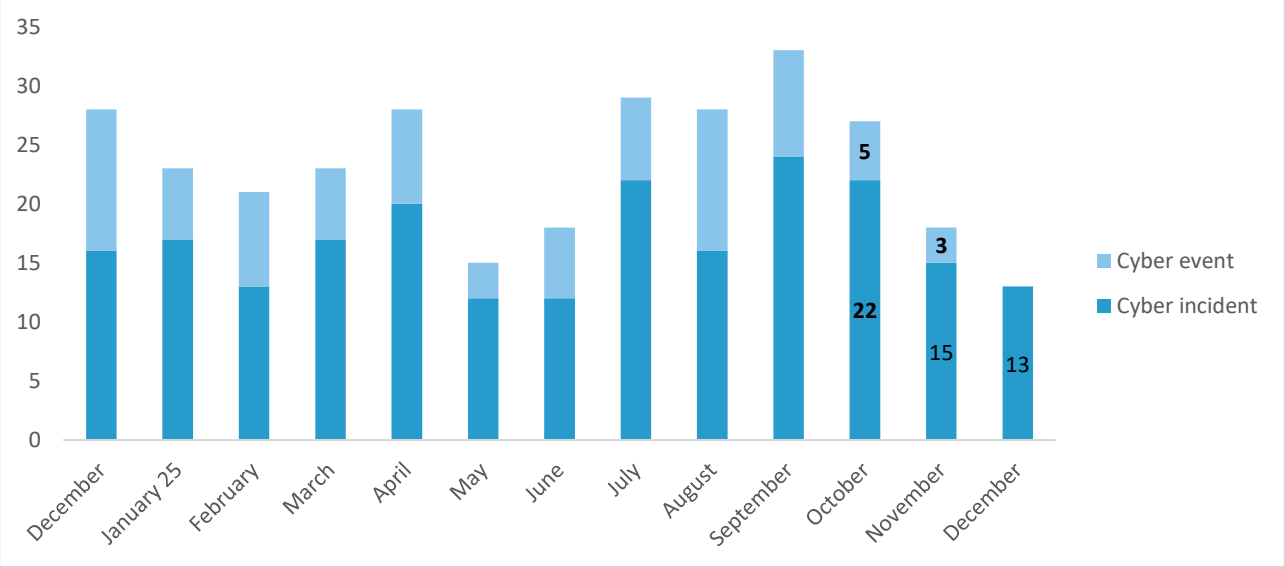
[1] The following overview summarizes the events of the past quarter. The information and conclusions contained in this analysis are based on publicly available information and information obtained by NÚKIB at the time of publication. Comments and suggestions for improving the report can be sent to komunikace@nukib.gov.cz.

Severity of Cyber Incidents Registered by NÚKIB[2]



Incidents vs. Events Registered by NÚKIB[3]

As part of its activities, NÚKIB receives, processes, and evaluates reports of cyber incidents. Based on the analysis performed, a report may be classified as a cyber incident, a cyber event, or an irrelevant report. The graph below shows the proportion of cyber incidents and cyber events.



[2] The severity of cyber incidents is defined in Decree No. 82/2018 Coll., on cyber security, and in NÚKIB's internal methodology.

[3] A cyber security incident is a breach of information security in information systems or a breach of service security or the security and integrity of electronic communications networks as a result of a cyber security event.
A cyber security event is an event that may cause a breach of information security in information systems or a breach of the security of services or the security and integrity of electronic communications networks.
Both terms are defined by the Cybersecurity Act.

Cyber Threats with a Direct Impact on the Cyber Security of the Czech Republic

NÚKIB joined the Joint Cybersecurity Advisory on pro-Russian hacktivist groups attacking critical infrastructure entities

NÚKIB, together with other Czech and international partners, joined a Joint Cybersecurity Advisory on pro-Russian hacktivists issued by the US Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA). The advisory relates to the Cyber Army of Russia Reborn (CARR), Z-Pentest, NoName057(16), Sector16, and other associated actors.

These entities are likely financially supported by the Russian state and act in its interests, however they are not advanced state actors (APTs), as evidenced by their less sophisticated methods with less impact. The groups are known, for example, for their DDoS attacks, which in the past have also targeted Czech institutions.

These groups have been very active since the start of the Russian invasion of Ukraine in 2022, carrying out attacks mainly against Ukraine and NATO member states. In this context, it is worth mentioning that in the United States, Ukrainian citizen Victoria Dubranova has also been charged with supporting the aforementioned CARR and NoName057 groups(16) and faces up to 27 years in prison.

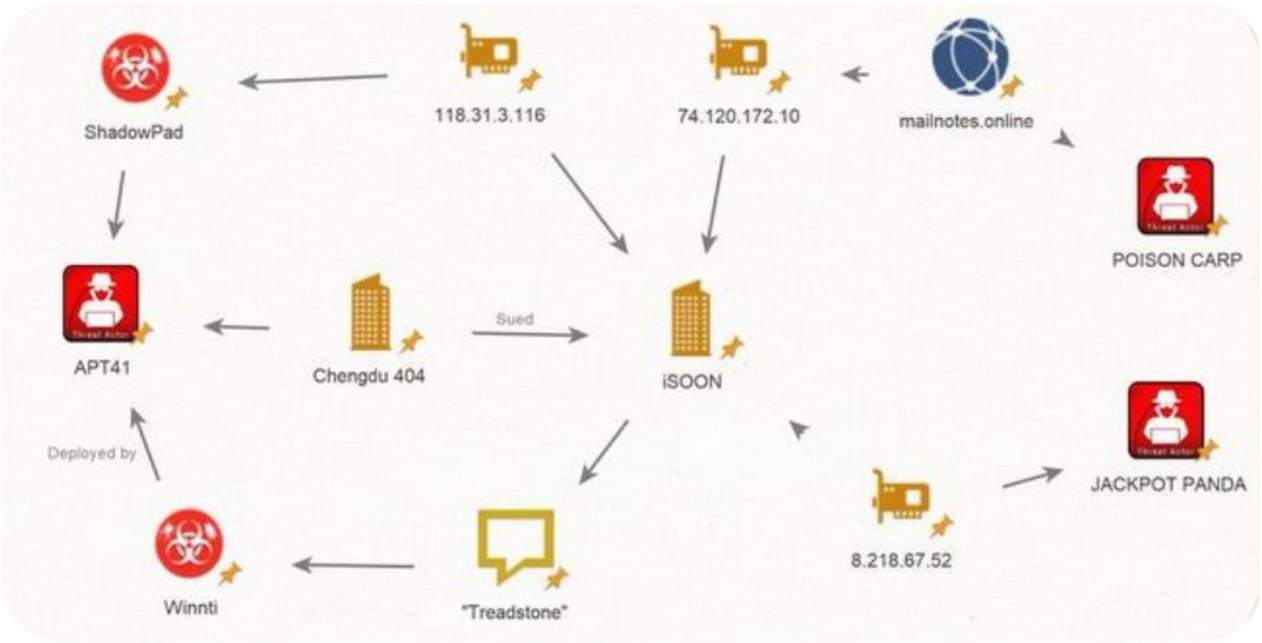
NÚKIB supported the UK in calling out malicious cyber activities of Chinese companies I-S00N and Integrity Tech

On December 10, NÚKIB issued a statement supporting the statement by its partners in the United Kingdom, who drew attention to the malicious activities of Chinese companies Anxun Information Technology (also known as "I-S00N") and Beijing Integrity Technology (also known as "Integrity Tech"). These companies are part of a complex ecosystem of private entities in the People's Republic of China (PRC) that, among other things, develop offensive tools for local intelligence and security agencies and, with the knowledge of the Chinese government, carry out cyber operations against other countries, including the Czech Republic. The United Kingdom has imposed sanctions on both companies.

Based on its own findings and information from domestic and foreign partners, NÚKIB has repeatedly warned against activities originating from this ecosystem and from state actors. These activities pose a growing threat to the Czech Republic, as evidenced by the APT31 cyber campaign, which the Czech government publicly attributed to the PRC in 2025, as well as joint analyses prepared with foreign partners, particularly those from September 2025 focusing on the actor Salt Typhoon.

In parallel with expressing its support, NÚKIB published its own analysis of I-S00N, which provides a detailed look at its functioning within the ecosystem of private companies whose malicious activities are enabled, supported, and exploited by the PRC.

I-S00N's links to other Chinese threat actors



Situation Overview of Cyber Threats Relevant to the Czech Republic

NÚKIB continuously monitors relevant threats that do not have an immediate impact on the security of the Czech Republic. However, even these threats may have a direct or indirect impact on the cyber security of Czech entities, either now or in the future. Maintaining situational awareness of current threats is therefore a key part of NÚKIB's activities.

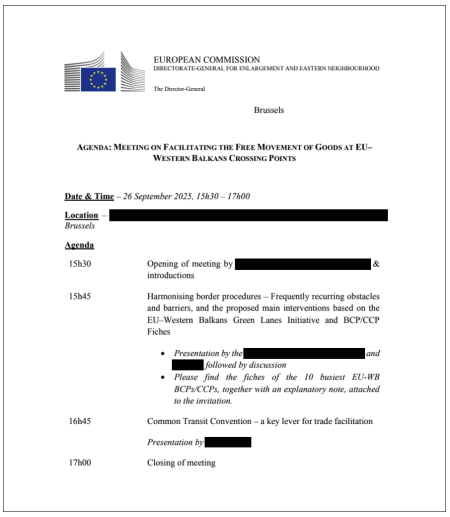
North Korean actor Lazarus engages in cyber espionage against companies involved in unmanned aerial vehicles

ESET has detected new attacks as part of a long-running campaign by the North Korean state actor Lazarus. The group targeted several European companies operating in the defense industry, some of which are involved in the development and manufacturing of unmanned aerial vehicles (UAVs). The attacks are part of a long-running campaign called Operation DreamJob, which relies on social engineering techniques, specifically fake offers of prestigious or important job positions. In the above-mentioned cases, the use of ScoringMathTea malware, already used in a number of previous attacks, was recorded. Given the entities targeted, ESET estimates that the operation may be related to North Korea's current efforts to develop its UAV program. It also adds that developments to date have relied heavily on intellectual property theft.

Chinese actor spied on diplomatic missions in Hungary, Belgium, and other European countries

Arctic Wolf Labs has uncovered a new espionage campaign by Chinese actor UNC6384 targeting diplomatic entities in Hungary, Belgium, Serbia, Italy, and the Netherlands. Spear-phishing emails themed around European Commission and NATO meetings tricked victims into downloading malicious files containing a compromised legitimate Canon Printer Assistant tool that launched PlugX malware. The attackers exploited the ZDI-CAN-25373 vulnerability in Windows shortcut files (LNK), which allows hidden code to be executed. They also demonstrated detailed knowledge of the diplomatic environment and used European meeting calendars in real time. At the same time, they demonstrated a high level of social engineering skills, which gave the campaign an air of credibility.

Example of a spear-phishing lure (higher resolution)



EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENLARGEMENT AND EASTERN NEIGHBOURHOOD
The Director-General

Brussels

AGENDA: MEETING ON FACILITATING THE FREE MOVEMENT OF GOODS AT EU–WESTERN BALKANS CROSSING POINTS

Date & Time – *26 September 2025, 15h30 – 17h00*

Location – [redacted]
Brussels

Agenda

15h30	Opening of meeting by [redacted] & introductions
15h45	Harmonising border procedures – Frequently recurring obstacles and barriers, and the proposed main interventions based on the EU–Western Balkans Green Lanes Initiative and BCP/CCP Fiches • *Presentation by the* [redacted] *and* [redacted] *followed by discussion* • *Please find the fiches of the 10 busiest EU-WB BCPs/CCPs, together with an explanatory note, attached to the invitation.*
16h45	Common Transit Convention – a key lever for trade facilitation *Presentation by* [redacted]
17h00	Closing of meeting

The UNC6384 group has long focused on diplomatic entities, previously targeting diplomats in Southeast Asia and recently expanding its activities to European diplomatic targets. It specializes in deploying variants of PlugX malware, which has been actively used since at least 2008 and remains a popular tool among Chinese actors. According to Google analysts, there is overlap between this actor and the Mustang Panda group in terms of infrastructure, targeting, and TTPs.

New phase of Operation ENDGAME successfully disrupts another part of cybercriminal infrastructure

In mid-November 2025, the latest phase of Operation ENDGAME took place, leading to the neutralization of more than a thousand servers and twenty domains. During this operation, the Elysium botnet was disrupted, as was the spread of the Rhadamanthys Stealer and Venom RAT malware families. In the case of Venom RAT, the main suspect, who was in Greece at the time, was also arrested. The affected infrastructure was used to infect hundreds of thousands of devices around the world.

Operation ENDGAME 3.0, involving police authorities from nine countries across continents, is a continuation of international cooperation in the fight against cybercrime, coordinated by the European institutions Europol and Eurojust, which began in 2022. This international operation achieved a significant success in May 2024, when four people were arrested and over a hundred servers and two thousand domains were neutralized.

Endgame operation logo

Germany accused Russia of a cyberattack on air traffic control and an attempt to influence elections

The German government has accused the Russian Federation of a cyberattack on air traffic control in 2024 and of attempting to influence the last federal elections through a disinformation campaign. Following this move, it also summoned the Russian ambassador.

According to the German government, the cyberattack on Deutsche Flugsicherung (DFS), the company responsible for air traffic control in Germany, was carried out by the Russian state-sponsored group APT28 (also known as Forrest Blizzard or Fancy Bear). DFS confirmed the compromise but stated that flights were not affected by the attack.

A spokesperson for the German Foreign Ministry also said that Russia had attempted to influence and destabilize the last federal elections and internal affairs of the state through a disinformation campaign called Storm-1516. As an example of these activities, the German government cited fake videos that claimed, just days before the elections, that votes had been manipulated.

Cooperation and Information Sharing

Ensuring cybersecurity does not only involve monitoring threats and responding to cyber incidents. An important part of this activity is also mutual cooperation, its development, and the sharing of experiences and information about current threats and ways to effectively counter them.

NÚKIB participated in the 17th edition of Cyber Coalition 2025

NÚKIB participated in Cyber Coalition 2025, one of the most important international cybersecurity exercises organized by NATO in cooperation with NATO CCD COE. The main objective of Cyber Coalition was to practice cooperation, coordination, and information sharing in responding to cyber incidents that could threaten critical infrastructure, allied operations, and international organizations.

Participants responded to realistic scenarios based on the "train as you fight" principle, including technical attacks, procedural processes, and legal aspects of crisis management. In addition to NATO member states, Austria, Australia, Japan, the Republic of Korea, Switzerland, Ukraine, representatives of the European Union, academia, and the private sector also participated in the exercise. The Czech Republic was traditionally represented by NÚKIB and by colleagues from the Cyber and Information Warfare Command of the Czech Army.

NÚKIB Director Lukáš Kintr visited Australia and discussed strengthening cybersecurity cooperation

Lukáš Kintr, Director of the National Cyber and Information Security Agency (NÚKIB), and Roman Pačka, Director of the Cabinet, traveled to Australia in October to develop bilateral cooperation in the field of cybersecurity. This was the first official visit by NÚKIB leadership to Australia, confirming the growing importance of the Czechia-Australia partnership in cybersecurity.

The main topics of discussion included threats to critical infrastructure from state-sponsored actors, issues of secure technologies, and the impact of the rapid development of artificial intelligence on cybersecurity. The discussions also touched on the protection of energy infrastructure and the security of connected vehicles, areas of growing importance in both Europe and the Indo-Pacific region.

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 on the NÚKIB website. The information is marked with a TLP label, which sets out terms and conditions for the use of the information. The individual TLP labels are specified below and indicate the nature of the information and the terms and conditions for their use:

Color	Conditions of use
TLP:RED	The information is for the eyes and ears of individual recipients only. It cannot be provided to any person other than the person to whom the information was addressed unless the other persons are explicitly identified. If the recipient finds it important to disclose the information to other bodies, this has to be done only with the consent of the originator of the information.
TLP:AMBER+STRICT	The information can only be shared and spread within the organization of the recipient and only to those individuals who meet the need-to-know[1] principle.
TLP:AMBER	The information can only be shared and spread within the organization of the recipient and its partners and only to those individuals who meet the need-to-know principle.
TLP:GREEN	The information can be shared and spread within the organization of the recipient and, where appropriate, with partners of the recipient. However, not via publicly available channels; the recipient must ensure the confidentiality of the communication when passing the information.
TLP:CLEAR	The information can be disclosed without restriction. Restrictions based on the intellectual property rights of the originator and/or recipient, or third parties are not affected by this provision.

[1] Need-to-know - a principle that states that only individuals who absolutely need the information for their work should have access to it.