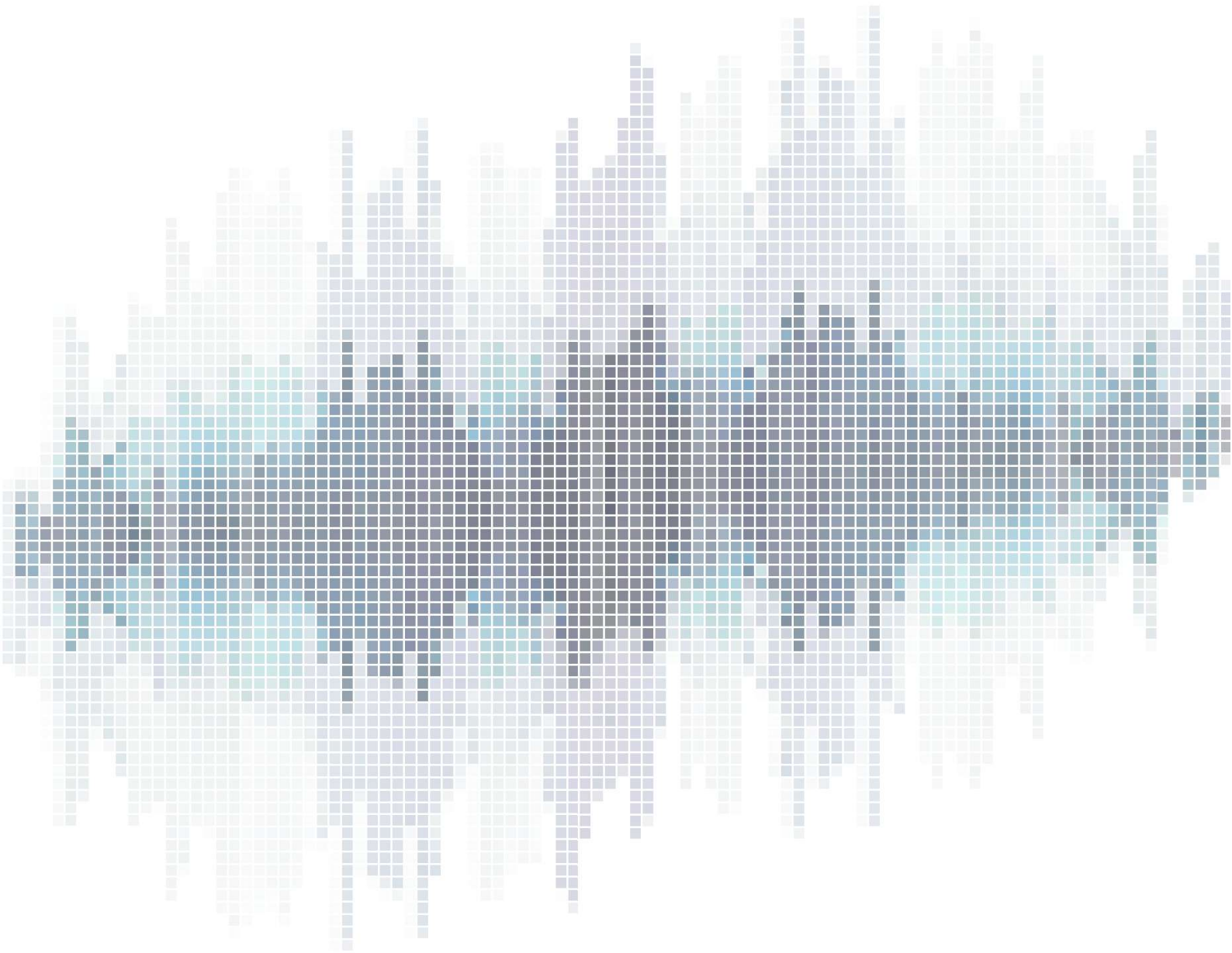
NÚKIB QUARTERLY

Cyber Threat Landscape Q1/2026



Summary of the Past Quarter [1]

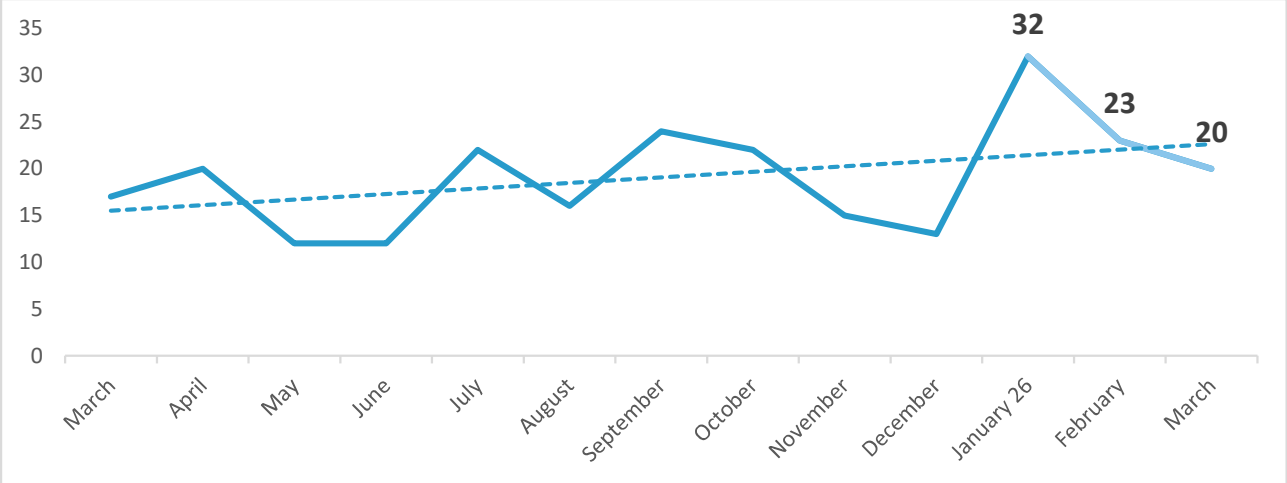
During the first quarter of 2026, NÚKIB recorded more than 70 cyber incidents, which represents the highest value over the past year. This increase was primarily driven by a wave of pro-Russian hacktivist DDoS attacks in January, as well as a relatively high number of incidents classified under the Intrusion category. **The increased activity of hacktivist actors led NÚKIB to issue an alert and mitigation recommendations.** At the same time, NÚKIB also addressed the issue of insufficiently secured VNC services exposed to the internet, which were abused not only by hacktivist actors. Although this problem was not noticeably reflected in incident statistics, NÚKIB strongly recommends implementing adequate security measures for VNC services, especially in cases where they are accessible from the internet and protected by a weak or no authentication mechanisms at all.

While the number of DDoS attacks gradually declined after January, the number of successful intrusions remained stable throughout the quarter. This category included incidents of varying severity, involving compromises of systems, perimeter devices, databases, email accounts, and individual user accounts.

Throughout the entire first quarter, NÚKIB did not register any ransomware attacks against entities subject to the higher-obligation regime under the new Cybersecurity Act. However, ransomware attacks did affect providers of regulated services under the lower-obligation regime, where cyber security incident handling is coordinated through the National CERT (CSIRT.CZ). The Information Security category—where ransomware incidents are typically classified—was therefore represented mainly by data and information leaks.

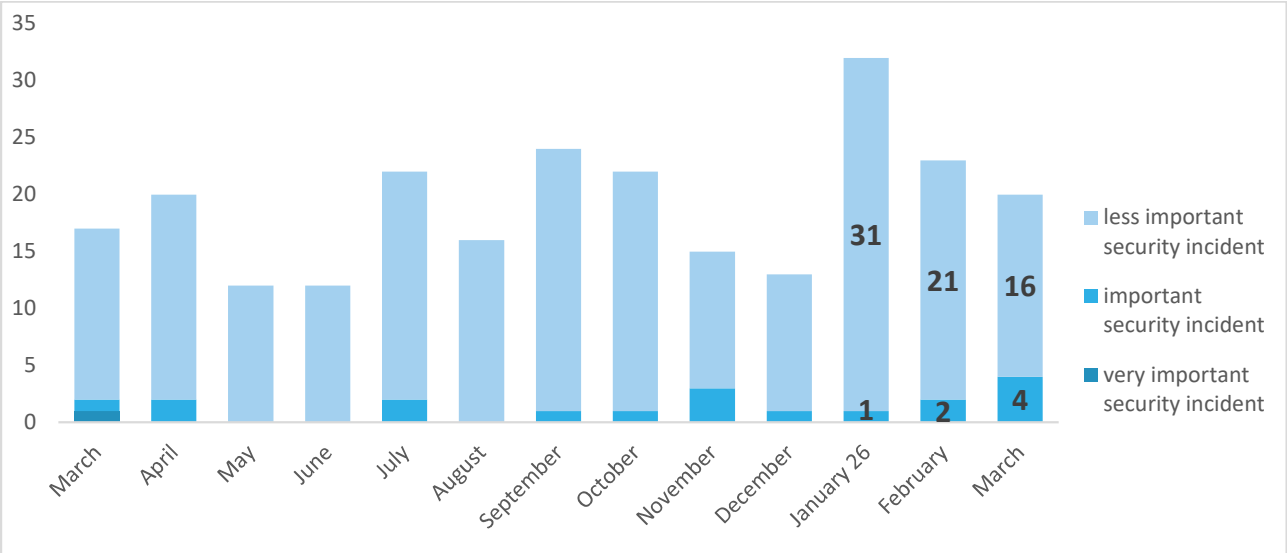
Alongside the overall increase in the number of incidents, the severity of handled incidents also slightly increased. In the past quarter, NÚKIB recorded a total of seven significant incidents, the majority of which affected state institutions. All other incidents were classified as less significant.

Number of Cyber Security Incidents Registered by NÚKIB



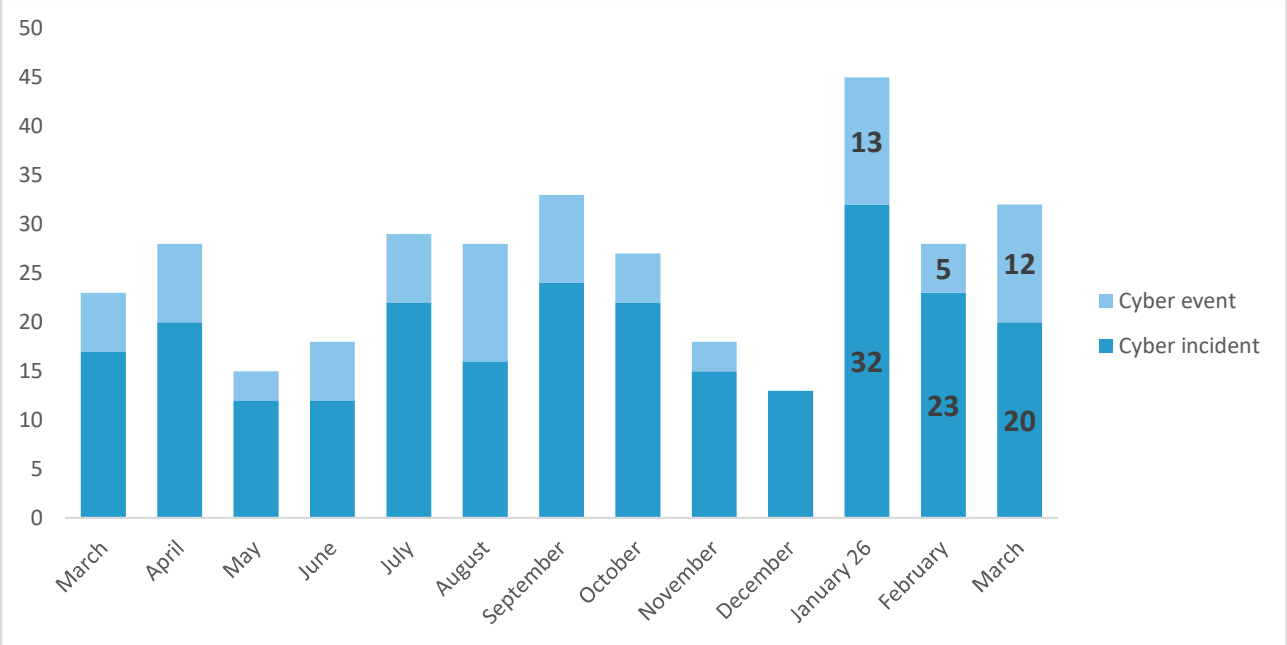
[1] The following overview summarizes the events of the past quarter. The information and conclusions contained in this analysis are based on publicly available information and information obtained by NÚKIB at the time of publication. Comments and suggestions for improving the report can be sent to komunikace@nukib.gov.cz.

Severity of Cyber Incidents Registered by NÚKIB[2]



Incidents vs. Events Registered by NÚKIB[3]

As part of its activities, NÚKIB receives, processes, and evaluated 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

Increased Hacktivist Activity in January

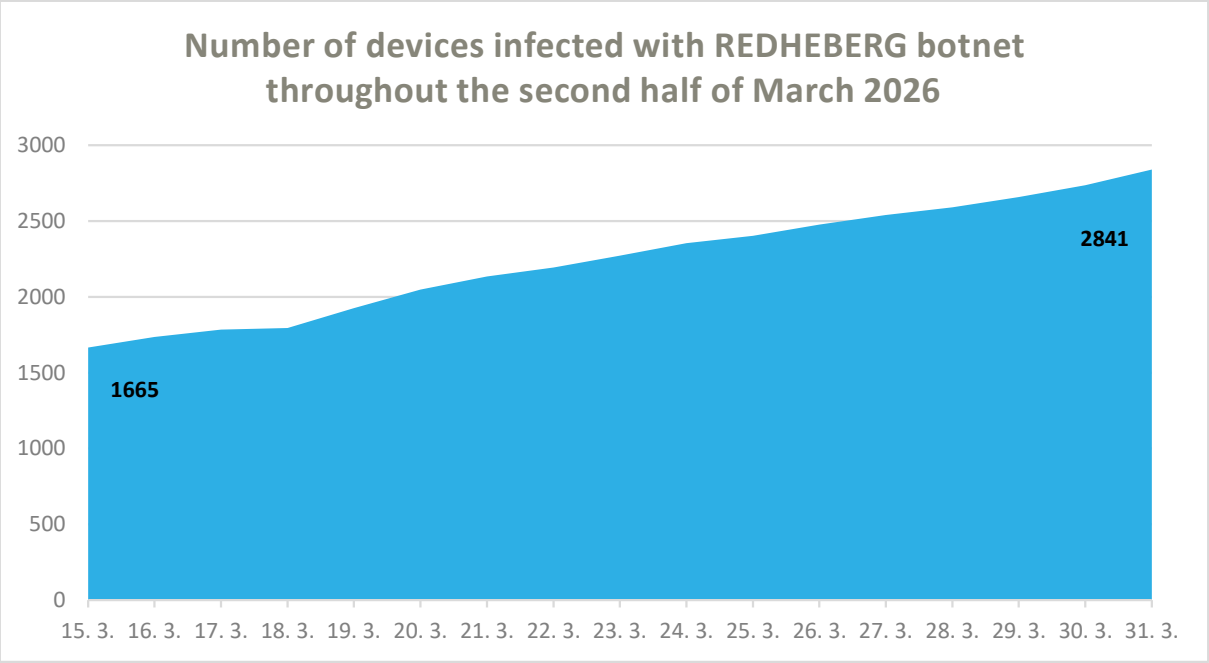
As early as the beginning of January, pro-Russian hacktivist activity in the Czech Republic increased, manifesting primarily in waves of DDoS attacks targeting Czech entities. This activity significantly influenced the total number of incidents recorded by NÚKIB, with DDoS attacks forming by far the largest subcategory of all incidents. In response, NÚKIB issued an alert for regulated entities via the NÚKIB Portal, including recommendations for prevention and mitigation of such attacks.

At the same time, NÚKIB warned of the increased interest of pro-Russian hacktivists in attacks targeting VNC interfaces of PLC devices secured with weak or no passwords, as well as the abuse of other services exposed to the internet. All attacks recorded so far had minimal impact and primarily affected non-regulated entities. Nevertheless, NÚKIB recommends not exposing VNC interfaces directly to the internet, or at the very least using sufficiently strong passwords. Inadequate protection of such devices increases the risk of unauthorized access to operational technologies (OT) and enables easy manipulation of these systems.

In both cases, the activities had no significant impact on Czech entities. Toward the end of January, the activity of these actors gradually subsided and was reflected only minimally in incident statistics.

Alert on Active Spread of the REDHEBERG Botnet in the Czech Republic

Another alert issued by NÚKIB in March was also related to insufficiently secured VNC services exposed to the internet. During this period, there was a significant increase in the number of devices compromised by the REDHEBERG botnet within the Czech Republic. At the time of writing this report, more than 3,200 compromised devices are still registered in the Czech Republic. According to available information, devices are compromised via remote, unauthenticated access to VNC services directly exposed to the internet. Device compromise and subsequent inclusion in the botnet is relatively simple to detect, among other indicators through specific messages and banners with extremist content.



A botnet is typically defined as a network of infected devices that are remotely controlled by an attacker without the users' knowledge. Such devices can be exploited for further cyber attacks, including spreading malicious content, overloading internet services, or further propagation of malware. Even if a device appears to function normally, its participation in a botnet poses a risk not only to its operator but also to other internet users.

NÚKIB strongly recommends the following:

- Do not expose VNC or other remote access services directly to the internet.
- Restrict remote access services to internal networks only, or ensure access via VPN.
- Ensure that remote access is not possible without authentication and use strong authentication mechanisms.
- In case of suspected device compromise, immediately take remedial measures and follow
- Standard cyber incident response procedures.

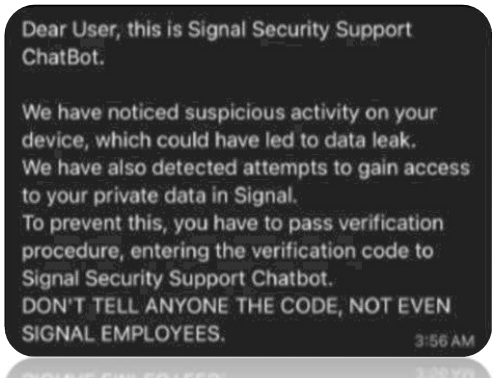
Situation Overview of Cyber Threats Relevant to the Czech Republic

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.

Russia Conducts a Global Cyber Espionage Campaign via the Signal Messaging Application

Dutch intelligence services have warned of a global cyber espionage campaign conducted via the Signal communication platform. The campaign primarily targets political representatives, government officials, and members of the armed forces, although no specific state-sponsored actor was initially identified. Compromises reportedly also occurred within the Netherlands itself, at the level of individual user accounts. The Signal platform as such was not compromised. According to the report, the primary attack vector is phishing, in which attackers impersonate Signal technical support and attempt to trick victims into providing a verification code required to gain access to their accounts. Cases have also been reported of fraudulent abuse of QR codes, which—by exploiting a legitimate application feature—allowed attackers to link their accounts with those of the victims. Most recently, U.S. authorities attributed the campaign to actors linked to Russian intelligence services.

Phishing Message on the Signal Platform



Russian State and Chinese Cybercriminal Actors Used an iPhone Hacking Tool Originally Developed for Western Intelligence Services

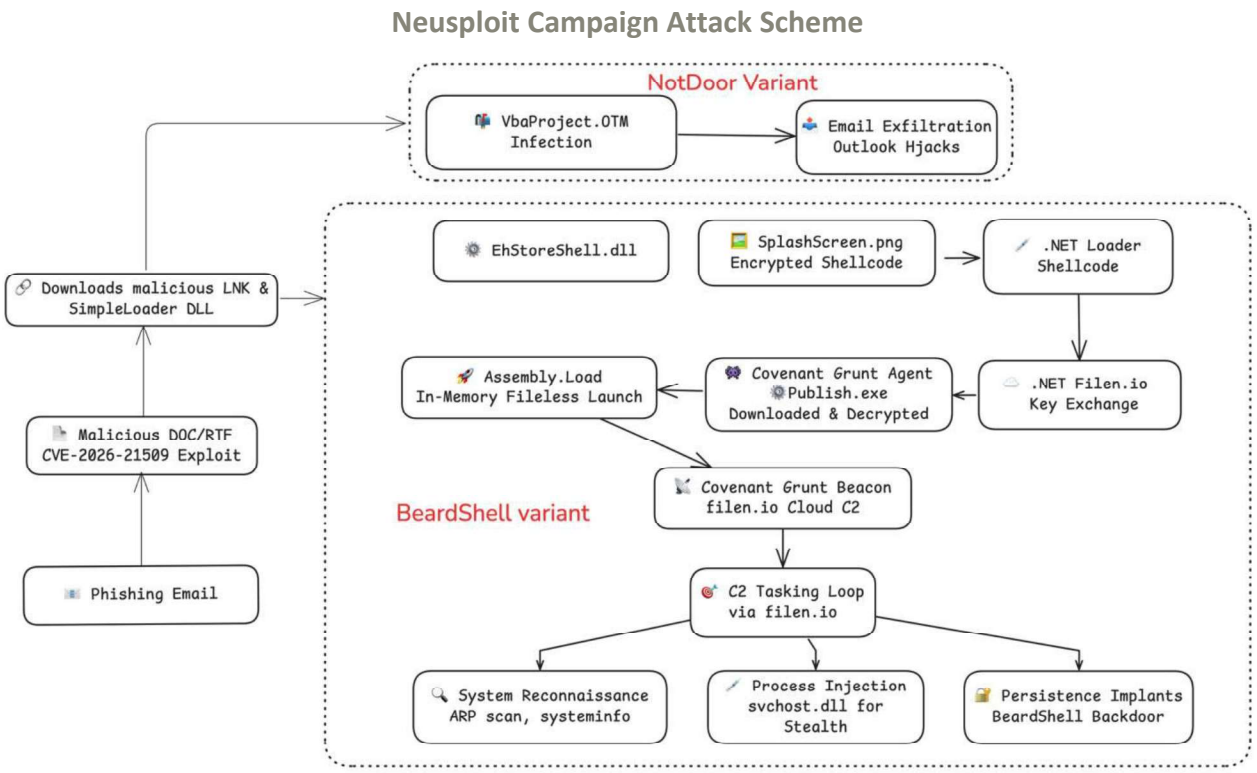
In 2025, researchers at Google monitored the widespread use of an advanced iPhone compromise tool known as Coruna, which was deployed in multiple campaigns worldwide. Analysis by iVerify and testimonies from former employees suggest that parts of the tool may have originated within the Trenchant division of the U.S. defense contractor L3Harris, which supplies offensive cyber technologies to the U.S. Government and its intelligence partners within the Five Eyes alliance. The tools, however, appear to have subsequently spread beyond their originally intended user base. Coruna was later used by the Russian cyber espionage group UNC6353 against selected targets in Ukraine, via compromised websites. Similar tools subsequently appeared in campaigns conducted by Chinese cybercriminal groups, primarily focused on financial fraud and cryptocurrency theft.

Cybercriminal Actor Stole European Commission Data Following Compromise of Amazon Cloud Services

The European Commission is investigating a security incident involving the compromise of Amazon cloud services (Amazon Web Services, AWS) hosting some of its accounts. Cybercriminal group ShinyHunters has claimed responsibility for the incident that was uncovered on March 24. The European Commission confirmed the theft of its data, while stating that its internal systems were not affected. According to additional information, more than 350 GB of data, including several databases, were stolen. The attacker has already published part of the data on a dark web site. According to a report by CERT-EU, initial access was obtained as a result of a supply-chain compromise involving the company Trivy, during which an access key to Amazon cloud services was obtained. This key subsequently enabled attackers to gain control over additional AWS accounts associated with the European Commission.

Russian Actor APT28 Conducted a Cyber Espionage Spear-Phishing Campaign Against European States

The Ukrainian CERT, together with cybersecurity companies Zscaler and Trellix, uncovered a cyber espionage campaign in Europe. The so-called Operation Neusploit is attributed to the Russian state-sponsored actor APT28, which operates under the Russian military intelligence service (GRU). The campaign exploited the CVE-2026-21509 vulnerability in Microsoft Office, enabling attackers to bypass security mechanisms, distribute modified documents, and execute malicious commands. The malware involved reportedly included Covenant and MiniDoor, which enabled data exfiltration, particularly of email communications. The campaign also employed social engineering techniques, with messages written in both English and the national languages of the targeted entities. Initial attacks targeted state institutions in Ukraine, Romania, and Slovakia, followed by attacks against maritime transport and diplomatic entities in Poland, Slovenia, Turkey, and Greece.



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.

Seventh Edition of the International Prague Cyber Security Conference 2026 Held in Prague

In March, the seventh edition of the international Prague Cyber Security Conference (PCSC) took place in Prague. The conference was organized by NÚKIB in cooperation with the Ministry of Foreign Affairs of the Czech Republic. The event welcomed approximately 400 experts from government institutions, academia, and technology companies representing dozens of countries worldwide, reaffirming its role as a key European platform for strategic debate on cybersecurity.

Discussions focused on regulatory approaches to digital products across regions, cybersecurity funding, trust in supply chains, and the impact of emerging technologies, including artificial intelligence and quantum technologies. Attention was also given to lessons learned from the war in Ukraine and the growing scale of state-sponsored cyber operations. The conference underscored the importance of international cooperation as a cornerstone of resilience in cyberspace.

NÚKIB Hosted the Cyber Champions Summit with NATO and Indo-Pacific Partners

In cooperation with the Ministry of Foreign Affairs of the Czech Republic and NATO, NÚKIB organized the Cyber Champions Summit 2026, attended by senior representatives of NATO allied countries and key partners from the Indo-Pacific region (Australia, Japan, South Korea, and New Zealand). The event was opened by the President of the Czech Republic, Petr Pavel, who emphasized the growing security interdependence between the Euro-Atlantic and Indo-Pacific regions and the importance of strong alliances in an increasingly deteriorating global security environment.

The aim of the summit was to strengthen international cooperation in cyber security and cyber defence, particularly through information sharing, exchange of experience, and coordination of approaches to the prevention and response to cyber incidents. Discussions focused on current cyber threats as well as the further development of joint activities at the political, military, and technical levels. The meeting also confirmed NÚKIB's active role in the Indo-Pacific region and the long-term commitment of the Czech Republic to strengthening international cybersecurity cooperation.

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.