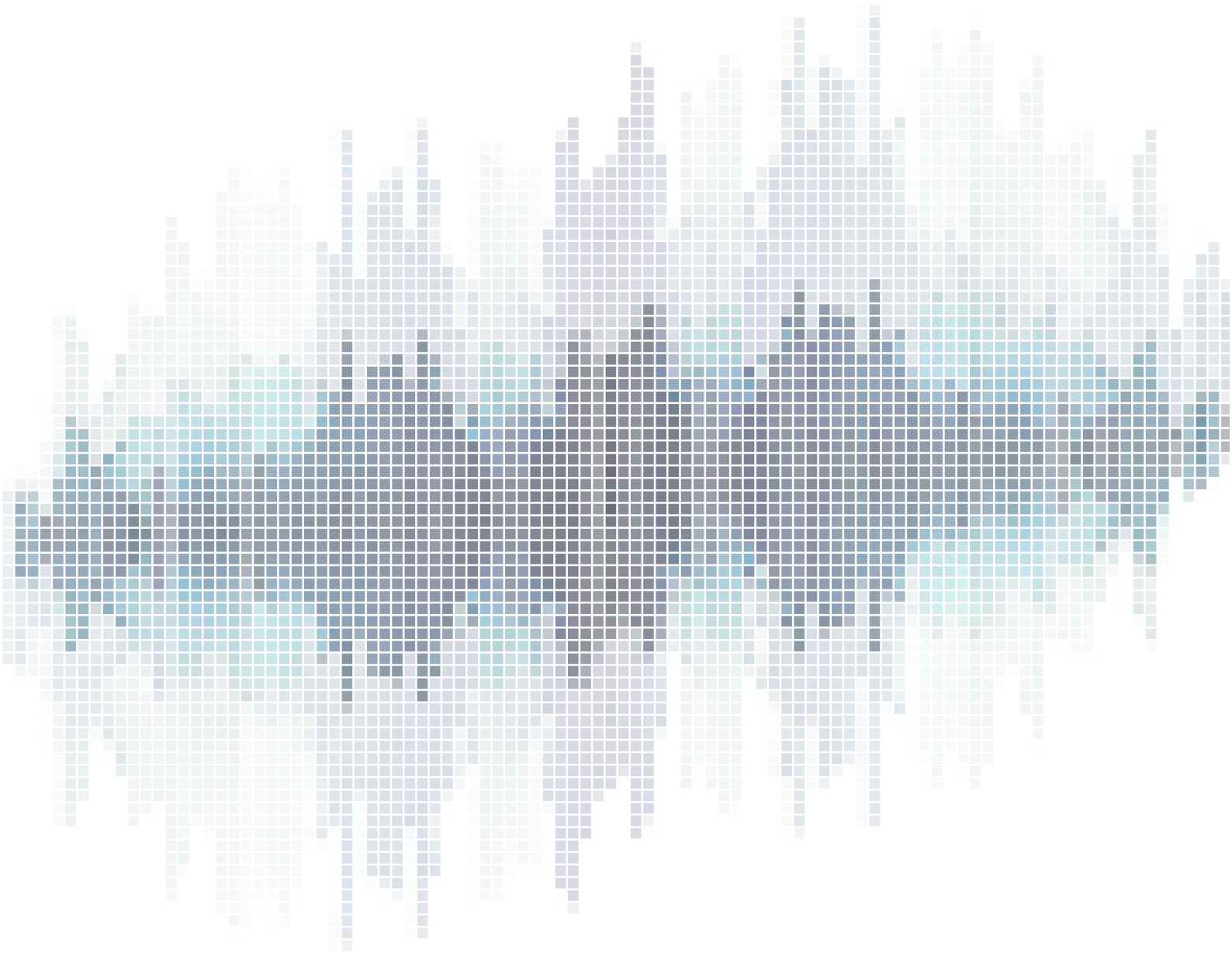
NÚKIB QUARTERLY

Cyber Threat Landscape Q2/2026



Summary of the Past Quarter[1]

In the second quarter of 2026, NÚKIB recorded a total of 44 cyber incidents, representing the lowest quarterly figure in a year. Compared to the first quarter, this marked a decrease of nearly 50 %. Of the recorded incidents, six were classified as important, the same number as in the previous quarter. Unlike the first quarter, when NÚKIB recorded one very important incident, no incident of this severity was reported during the second quarter.

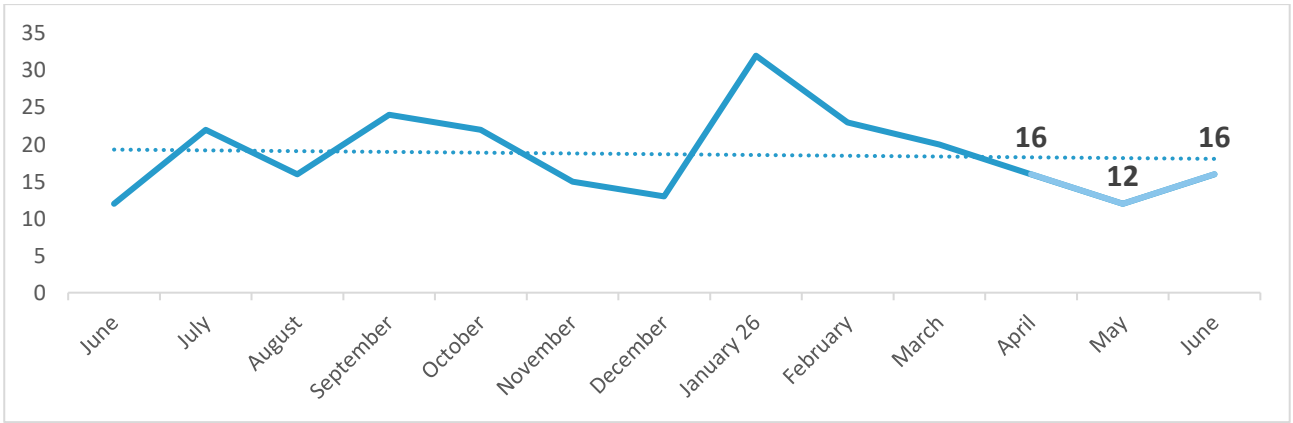
While the absolute number of important and very important incidents has remained at a relatively stable level over time, their proportion increased slightly in the second quarter due to the overall decline in the total number of incidents. **The most pronounced decrease was observed in DDoS attacks, with the last wave of DDoS attacks carried out by pro-Russian hacktivists occurring in January 2026.** Although availability attacks have not disappeared entirely, they have become more sporadic and no longer exhibit the characteristics of coordinated, systematic campaigns.

In contrast, the proportion of incidents classified under the Intrusion category increased significantly, making it the most common type of cybersecurity incident in the second quarter. These incidents involved the compromise of user accounts, firewalls, and application servers. They primarily affected organizations in the public administration, education, and healthcare sectors.

The new Cybersecurity Act, which entered into force on November 1, 2025, has significantly increased the number of entities required to comply with cybersecurity regulations. However, the number of reported incidents has not increased substantially so far. Why is that?

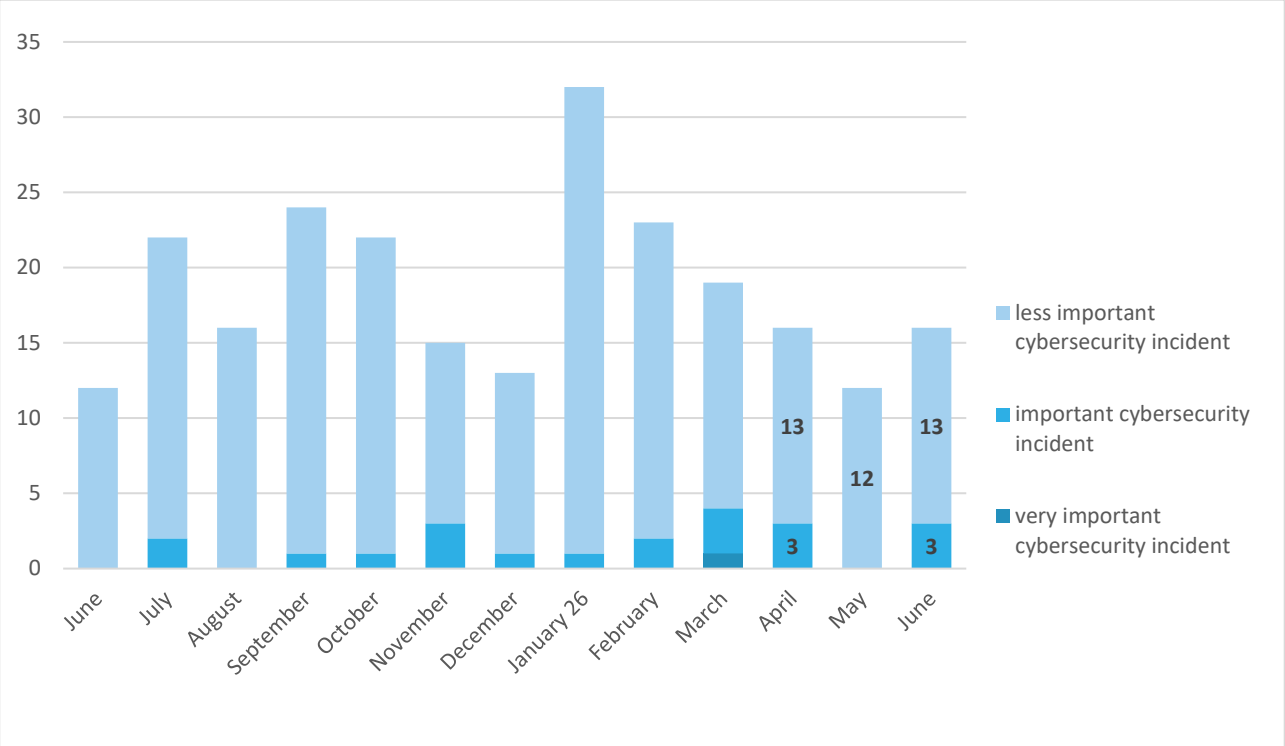
Providers of regulated services have one year from the date they receive their registration decision to begin reporting incidents to NÚKIB. As a result, the impact of the new regulation may not become clearly visible until the turn of 2026 and 2027 at the earliest. Furthermore, the obligation to report all detected incidents applies only to providers of regulated services operating under the higher-obligation regime. Entities subject to the lower-obligation regime coordinate the handling of cybersecurity incidents with the National CERT (CSIRT.CZ). They report incidents to NÚKIB (GovCERT.CZ) only if they themselves assess them as significant.

Number of Cyber Security Incidents Registered by NÚKIB



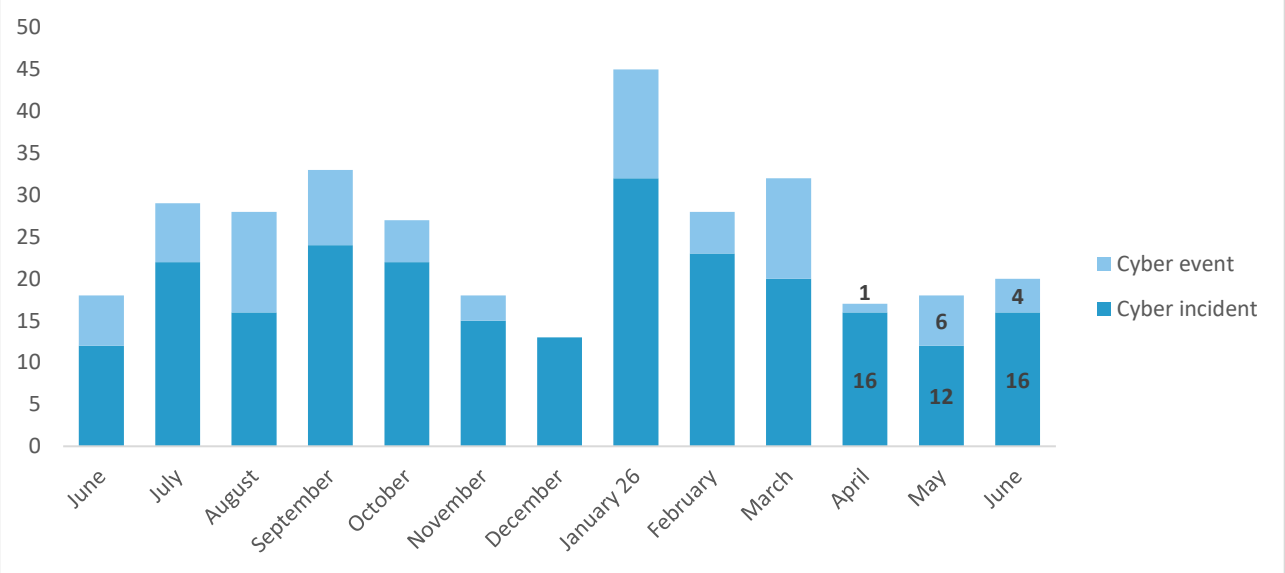
[1] The following overview summarizes the events of the past quarter. The information and conclusions contained in this analysis are based on publicly available information and information obtained by NÚKIB at the time of publication. Comments and suggestions for improving the report can be sent to komunikace@nukib.gov.cz.

Severity of Cyber Incidents Registered by NÚKIB[2]



Incidents vs. Events Registered by NÚKIB[3]

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

Russian state-sponsored actor APT28 compromised TP-Link routers. Czech Military Intelligence carried out an active intervention

APT28, a Russian state-sponsored threat actor affiliated with Russia's military intelligence service (GRU), established a global network of compromised small office/home office (SOHO) routers, according to an announcement by the U.S. Department of Justice and the Federal Bureau of Investigation (FBI). The group's objective was cyber espionage, and the greatest risk involved devices that were using default admin passwords. The Czech Military Intelligence also contributed to the announcement and, as part of a U.S.-led international operation, carried out an active intervention. This intervention involved modifying the configuration of a portion of the globally exploited infrastructure and securing potentially exploitable devices located within the Czech Republic.

The campaign conducted by the 85th Main Special Service Center of the GRU (85th GTsSS), which according to the FBI has been ongoing since at least 2024, differs from previous operations in its method of execution. APT28 (also known as Fancy Bear, Forest Blizzard, or Sofacy Group) exploited vulnerability CVE-2023-50224 in the TP-Link TL-WR841N router model, which allows authentication bypass and unauthorized access to affected devices. By exploiting this vulnerability, the threat actor modified the routers' configuration, which was subsequently propagated to other devices connected to the compromised routers.

The threat actor was then able to monitor domain name system (DNS) queries and, for selected domains and services such as Microsoft Outlook Web Access, return spoofed DNS responses and carry out adversary-in-the-middle attacks against encrypted communications. Through this technique, APT28 obtained passwords, authentication tokens, and other sensitive information, including the contents of emails and web communications, which would normally be protected by SSL/TLS encryption. The group compromised a wide range of devices in the US and other countries, including the Czech Republic. The collected data was used primarily to gather information related to military and government institutions, as well as organizations operating critical infrastructure.

Overview of organizations that contributed to the FBI announcement

The FortiBleed campaign affected 74,000 Fortinet firewalls

Independent Ukrainian researcher Volodymyr Diachenko reported an ongoing campaign conducted by an unidentified Russian-speaking financially motivated threat actor targeting Fortinet firewalls. At the time of disclosure, the attackers had obtained credentials for 73,932 unique firewall URLs, representing approximately half of all internet-exposed Fortinet firewalls. The campaign, dubbed FortiBleed, also targeted Synology network-attached storage (NAS) devices, Sophos firewalls, and Microsoft SQL Server (MSSQL) instances.

Organizations across multiple sectors and regions were affected, including major companies such as Chevron, Samsung, Toyota, and even Fortinet itself. According to the published records, the incident also impacted a number of Czech organizations. The theft of sensitive technical data from the Turkish defense contractor ASELSAN has also been documented.

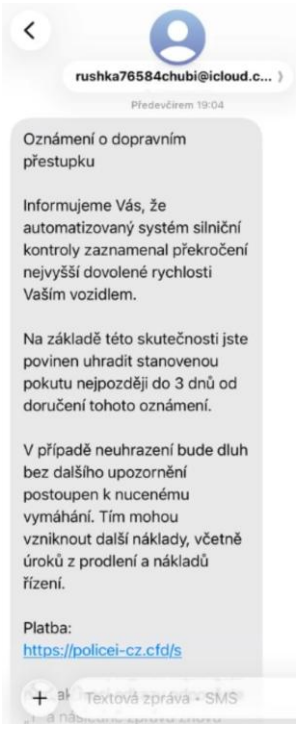
Analysis of the attackers' infrastructure indicates that no specific vulnerability was exploited to obtain the credentials. Instead, the credentials were acquired through brute-force attacks that had likely been ongoing since mid-May 2026. After gaining initial access, the attackers exfiltrated additional credentials from within the compromised networks. Guidance on mitigation measures has been published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Warning about a smishing campaign in which attackers impersonate the Czech Police

In May, NÚKIB issued a warning through its Portal about a smishing campaign in which attackers impersonated the Police of the Czech Republic via SMS messages in an attempt to obtain victims' payment card information.

In this campaign, victims typically receive an SMS message informing them of an alleged traffic violation, such as speeding, and urging them to pay a fine within a specified deadline, for example within three days. The message contains a link to a fraudulent website impersonating an official government portal. The attackers use various combinations of terms such as "police," "gov," "portal," "euprava," or "listek" in the malicious URLs, often paired with less common top-level domains such as .cfd, .bond, or .xyz. The exact domains used may change over time. If victims enter their payment card details, the information may subsequently be misused for unauthorized financial transactions or other fraudulent activities.

Example of an SMS used in the smishing campaign



In connection with this campaign, it is important to note that the Police of the Czech Republic does not request payment of fines in this manner and does not send payment links via SMS messages. More broadly, in relation to fraudulent campaigns of this kind, NÚKIB recommends:

- Do not click on links contained in unsolicited SMS messages, especially if they include a request to pay a fine.
- If you do open such a link, do not enter any personal or payment information.

- If in doubt, verify the authenticity of such messages exclusively through the official channels of the Police of the Czech Republic or other relevant institutions.
- If you have entered any information, contact your bank immediately and take appropriate measures, such as blocking your payment card and reviewing recent transactions.

European Values think tank targeted by the Chinese cyber espionage actor SparkyCarp

The Czech think tank European Values (Evropské hodnoty, EH) became the target of the Chinese state-sponsored cyber espionage actor SparkyCarp (also known as UNK_SparkyCarp). EH Director Jakub Janda was contacted via email by an individual impersonating Didi Tang, a real journalist from the Associated Press (AP). After moving the conversation to the Signal messaging application, the attacker urged him to provide information through a Google Form. However, the link led to a fraudulent Google login page. The objective of the attack was to obtain the victim's account credentials and, most likely, gain further access to the organization's internal communications, contacts, and analytical materials.

NÚKIB, which was informed of the incident, was able to link the email to a broader campaign targeting Taiwan that had previously been reported by the private cybersecurity company Proofpoint. The identified infrastructure may also have been used in operations targeting Chinese dissidents and human rights organizations around the world. This campaign highlights the fact that non-governmental organizations are also among the targets of interest for certain state-sponsored or state-backed threat actors.

The e-mail used to initiate contact with EH Director Jakub Janda

Dear Director Janda,

My name is Didi Tang, and I'm part of the Asia coverage team at the AP Washington bureau, working on a story about U.S.-China relations.

We're currently preparing a piece on recent shifts in U.S.-China policy, and we'd greatly value your insights on the topic. Would you be available for a brief interview (15–20 minutes) sometime this week or next? We're happy to accommodate your schedule and preferred format.

Thank you very much for your time and consideration. I look forward to your response.

Best regards,

Didi Tang

Asian Affairs Reporter

--

AP
Didi Tang
Asian Affairs Reporter
The Associated Press

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.

The new AI Frontier models significantly enhance the ability to autonomously detect and exploit vulnerabilities. It is only a matter of time before malicious actors exploit them

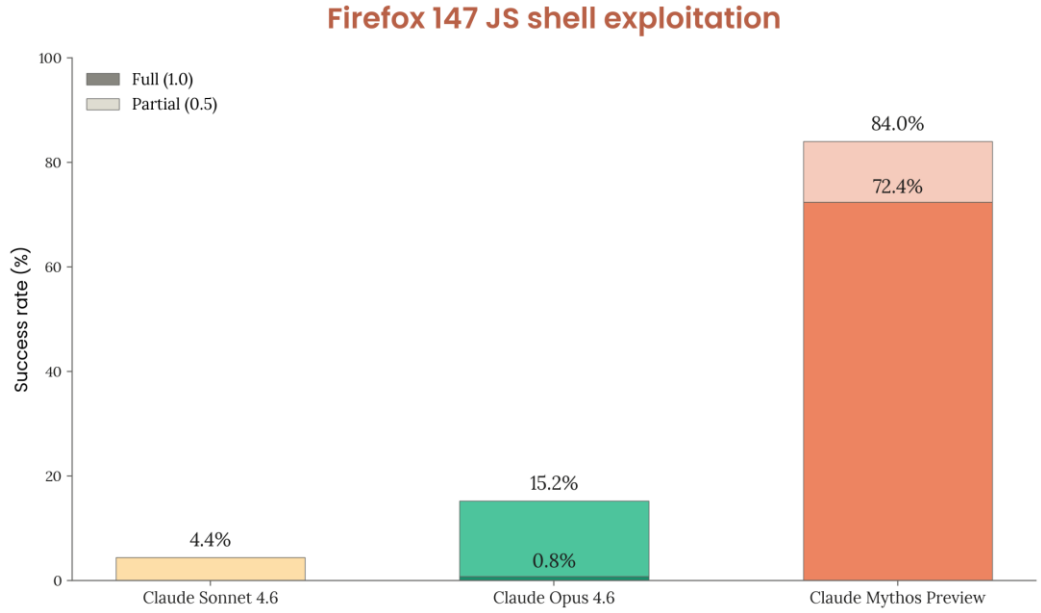
In April 2026, Anthropic unveiled Mythos, an artificial intelligence (AI) model that, thanks to advanced automation, is capable of identifying, validating, and exploiting even previously unknown vulnerabilities at scale far more effectively than older large language models. This capability constitutes a real and serious risk to cybersecurity. It represents a shift across the entire AI industry, in with other companies are also achieving similar capabilities in vulnerability discovery and exploitation. These capabilities will almost certainly become available to both state-sponsored and non-state threat actors, if they are not already in their possession.

These advanced Frontier AI models, when applied to cybersecurity, are very likely to significantly reduce the time between the discovery of a vulnerability and its exploitation, as they automate the search for, validation of, and chaining of vulnerabilities on a large scale. However, the pace of patching will continue to be limited by human and technical capacities.

In the short term, new AI models may increase the number of cyber incidents in the Czech Republic as well, both through direct attacks on Czech entities and indirectly through global compromises of major service providers via supply chains.

NÚKIB has published an analytical report that looks into the new advanced AI models in greater detail.

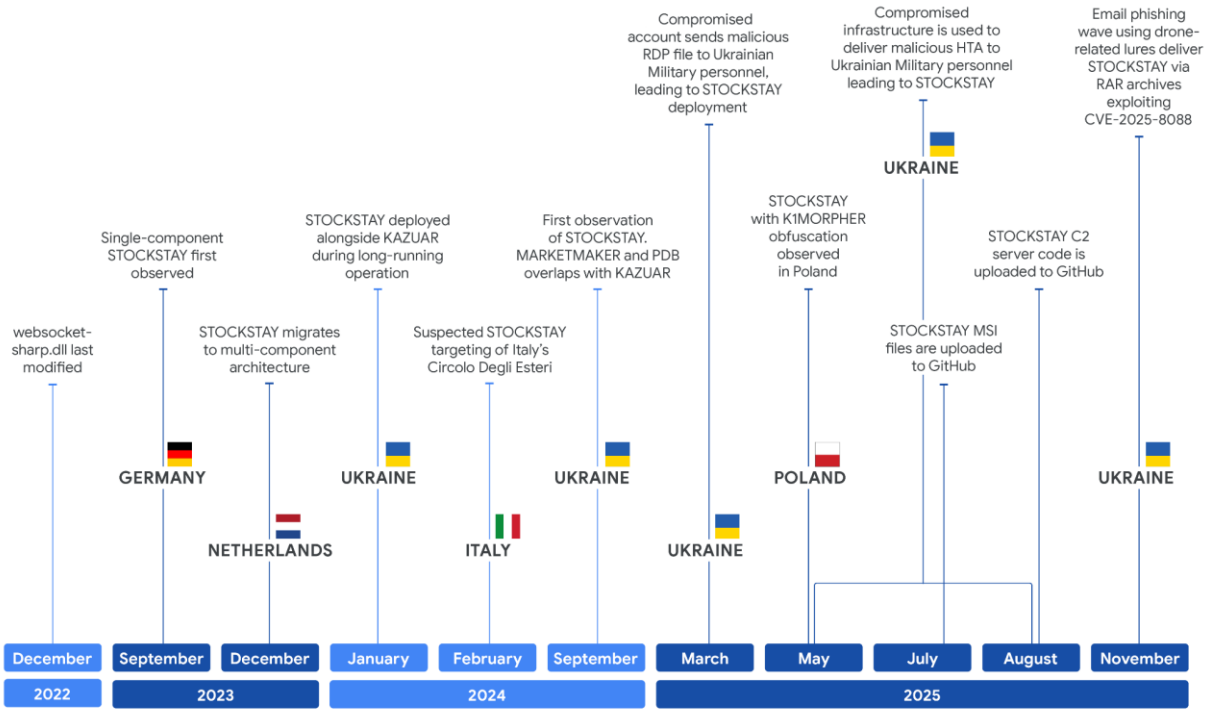
Success rate of the Mythos model in identifying a Firefox browser vulnerability compared with previous Anthropic models (vellum.ai)



Google attributed the STOCKSTAY backdoor to the Russian state-sponsored threat actor Turla

Cybersecurity researchers from Google Threat Intelligence Group (GTIG) attributed the previously undocumented STOCKSTAY backdoor to the Russian state-sponsored threat actor Turla (also known as Venomous Bear or Secret Blizzard), which has been linked to Russia's Federal Security Service (FSB). This cyber espionage malware was first observed in 2022 and has been identified in several European countries, including Germany, Poland, and Italy. Over the past year, however, it has been deployed repeatedly against targets in Ukraine. There, it was distributed through phishing campaigns targeting government and military institutions, disguised as diplomatic or academic correspondence. STOCKSTAY consists of several components that communicate with each other through a custom inter-process communication (IPC) channel. These components were designed to masquerade as benign applications, such as a purported stock market data lookup tool.

STOCKSTAY backdoor activity timeline



Last year's telecommunications outage in Luxembourg was caused by a zero-day vulnerability in Huawei routers

The widespread telecommunications outage in Luxembourg in July 2025 was caused by the exploitation of a zero-day vulnerability in Huawei routers. The incident disrupted telecommunications infrastructure, including fixed-line, 4G, 5G, and emergency communications services, for more than three hours. The attackers used specially crafted network traffic that repeatedly triggered Huawei routers to reboot, thereby disabling critical components of Post Luxembourg's telecommunications infrastructure. Luxembourg initially described the incident as a highly sophisticated cyberattack and later clarified that it was not a typical DDoS attack. The available evidence also did not indicate a specific intent to target either Post Luxembourg or Luxembourg itself. Huawei did not publicly disclose the vulnerability but stated that it had not been exploited again.

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, as part of the Polish-Czech team, placed fourth in Locked Shields 2026, the world's largest cyber defence exercise

The National Cyber and Information Security Agency (NÚKIB) participated in the prestigious international cyber exercise Locked Shields 2026 from 21 to 24 April 2026. Organized annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Locked Shields is widely regarded as the largest and most comprehensive cyber defence exercise in the world. Competing against fifteen other teams, the Polish-Czech team secured an impressive fourth-place finish.

The primary objective of Locked Shields 2026 was to strengthen and further develop the cyber defence capabilities of participating nations, foster international partnerships and cooperation between the public and private sectors, and promote innovation in the field of cybersecurity.

The exercise simulated a large-scale, realistic cyber conflict in real time and tested participants' technical, operational, and strategic capabilities. The fictional scenario incorporated elements of geopolitical tension, including violations of international borders and state sovereignty, the construction of artificial islands, and coordinated cyberattacks designed to disrupt government functions and undermine public trust. This year, the exercise designers also included issues related to election security in the scenario.

NÚKIB Director Lukáš Kintr held talks in Estonia on strengthening cybersecurity cooperation

As part of the presidential delegation, NÚKIB Director Lukáš Kintr visited Estonia during the state visit in June. Over the course of a two-day program in Tallinn and Tartu, a series of meetings were held with strategic partners from the public, private, and academic sectors. These discussions reaffirmed the strong and long-standing partnership between the two countries in the field of cybersecurity and opened up opportunities for further deepening this cooperation.

One of the key points of the program was a meeting with the e-Governance Academy (eGA), a long-standing partner of the Czech Republic in digital transformation and cybersecurity. The discussions focused primarily on the further development of projects aimed at building cyber capacity, including the Cyber Balkans 2 initiative and projects of the NATO Cyber Defence Capacity Building program.

Additional bilateral meetings in Tallinn were held with representatives of the Estonian Information System Authority (RIA), where discussions focused on national priorities, current cybersecurity challenges, and the growing threat posed by online fraud. The delegation also took part in an expert meeting of cybersecurity professionals at the University of Tartu. Discussions covered cooperation in research and development, strengthening links between industry and academia, and sharing experiences from student exchange programs.

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.