CERT-EU

Cyber Brief (November 2025)

December 2, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 277 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, Operation Endgame coordinated by Europol and Eurojust seized servers from malware-as-a-service infrastructure, while Dutch police seized servers from a Dutch bulletproof hosting provider. China issued draft regulations with stricter localisation measures.
- On the **cyberespionage** front, an Italian political consultant was reportedly targeted with Paragon spyware, a China-linked cyberespionage campaign leveraged AI agentic capabilities to target thirty global organisations, while several newspapers analysed potential suspects of the leaked Witkoff-Ushakov Ukraine peace call. Additionally, Russia-linked Killnet claimed stealing sensitive drone industry data in Ukraine, and a spearphishing campaign targeted Special Operations Command personnel specialising in Drone operations.
- In regards to **cybercrime**, a German-based hosting provider was identified as a key transit for global malicious hosting networks. New GlassWorm malware activity was identified on OpenVSX, and Danabot malware resurges six months after law enforcement's Operation Endgame disrupted its infrastructure.
- There were **disruptive** Russia-linked Sandworm attacks using data wipers to disrupt Ukraine's grain sector, while Dutch broadcaster RTV Noord suffered a suspected ransomware attack that limited news updates and impacted its role as an emergency broadcaster. Cloudflare reported worldwide disruptions to its Global Network.
- Regarding **data exposure and leaks** incidents, a ticketing platform used by Eurofiber France was allegedly breached by threat actor ByteToBreach, while the company Logitech reported a data breach linked to the Clop cybercrime group. Hungary's opposition party TISZA Party reported a personal data leak affecting users of its app.
- On the **hacktivism** front, Pro-Russia NoName057(16) claimed DDoS attacks against Danish entities ahead of local elections, and also claimed DDoS attacks against several Belgian telecommunications websites.

- As for **opportunistic** attacks, North Korea-linked FlexibleFerret macOS malware is being used in fake job opportunities, and Cisco reported that firewall flaws were being actively abused for DoS attacks. Fortiweb reported attackers were actively exploiting an unpatched vulnerability to gain unauthorised administrative access on exposed appliances.

Europe

Cyber policy and law enforcement

European media outlets identified and tracked EU officials through geolocated advertisement data
On November 4, French newspaper Le Monde among other media outlets jointly obtained geolocation data derived from advertising platforms, which made it possible to identify and track several European Union officials, and in some cases identify home addresses. They obtained a free sample dataset from a data broker, spanning a few days in October focusing on Belgium. The report highlighted the limitations of the General Data Protection Regulation. link

Police disrupt Rhadamanthys, VenomRAT, and Elysium malware operations
On November 13, authorities from nine countries, coordinated by Europol and Eurojust, expanded Operation Endgame to dismantle the Rhadamanthys infostealer, VenomRAT, and Elysium botnet networks. The operation targeted malware-as-a-service infrastructures, seizing over 1.000 servers worldwide and included the arrest of a key suspect in Greece. link

Dutch police seized 250 servers used by bulletproof hosting provider
On September 25, Dutch police seized about 250 servers and thousands of virtual machines from a Dutch bulletproof hosting provider used in ransomware, botnet, phishing, and child abuse cases since 2022, disrupting ongoing cybercrime operations. Investigators will analyse the seized infrastructure to identify operators and clients; no arrests are reported yet. link

New UK laws to strengthen critical infrastructure cyber defences
On November 12, the United Kingdom announced the Cyber Security and Resilience Bill, expanding the NIS Regulations 2018 to strengthen cyber defences for critical infrastructure sectors such as energy, water, transport, and healthcare. The bill requires major IT service providers to meet strict security standards, report serious incidents quickly, and grants regulators new powers to enforce compliance and resilience. `regulation` link

Cyberespionage & prepositioning

Paragon spyware targeting Italian political consultant
On November 6, TechCrunch reported that Italian political consultant Francesco Nicodemo was targeted with Paragon spyware, in a case allegedly linked to Italian intelligence agencies. The case expands Italy's ongoing spyware scandal, affecting journalists, activists, executives, and political figures. `civil society` `political parties` `telecommunications` link

Alleged Russia-linked Killnet cyberattack on Brave1 cluster
On November 12, Intelligence Online reported that Russian-linked threat actors Killnet claimed responsibility for a cyberattack on Ukraine's Brave1 defence cluster. They allegedly stole sensitive drone industry data, including technical details and GPS coordinates of facilities. While the breach's authenticity remains unconfirmed, it reportedly alarmed Ukraine's defence sector, highlighting an ongoing strategy to disrupt and intimidate Ukraine's military innovation network. `defence` `russia` link

Belarusian military lure targeting Special Operations Command personnel specialising in Drone operations
On October 31, Cyble reported that a threat actor distributed malware utilising a Belarusian military lure targeting Special Operations Command personnel specialising in UAV/drone operations. The threat actor used nested ZIPs and LNK-triggered PowerShell to deploy Tor binaries on compromised Windows hosts. Cyble assessed with moderate confidence that the techniques used aligned with those of the Russia-linked Sandworm. `defence` link

Cybercrime

German-based hosting provider serves as a key transit for global malicious hosting networks
On November 6, Recorded Future reported that German hosting provider aurologic GmbH serves as a key upstream transit for multiple threat activity enablers, including sanctioned Aeza International Ltd. The company's connectivity supports high concentrations of malicious infrastructure linked to cybercrime, disinformation, and malware distribution worldwide, highlighting how permissive upstream relationships sustain global threat operations despite sanctions and abuse reports. `internet service provider` link

Major Italian gas firm SIAD confirms data breach by Russia-linked ransomware group
On November 11, Russia-linked Everest ransomware group claimed to have stolen 159GB from SIAD Group, a leading Italian chemical and industrial gas company, listing the firm on its darkweb leak site with an eight-day countdown. The leak site included screenshots of internal project files. SIAD confirmed an intrusion on a perimeter IT component, and that operations remain uninterrupted with no current evidence of personal data compromise. `chemicals` `energy` link

Information operations

Russian intelligence escalates Baltic disinformation operations
On November 19, Lithuanian National Radio and Television reported that Russian intelligence services are intensifying disinformation and propaganda campaigns in Latvia, Lithuania, and Estonia. Recruitment targets include low-income individuals and youth, often via Telegram or travel to Russia. Activities involved coordinated narratives, pro-Russia media production, and ideological groundwork, aiming to influence public opinion and destabilise Baltic societies. link

Disruption & destruction

Russia-linked Sandworm uses data wipers to disrupt Ukraine's grain sector
On November 5, ESET released a reported that Russia-linked threat actor Sandworm deployed ZEROLOT and Sting wipers against a Ukrainian university in April 2025. In June and September 2025, they also deployed wipers to government, energy, logistics, and grain sectors, exploiting Active Directory Group Policy. Another group tracked as UAC-0099 was confirmed to provide initial access and transfer validated targets to Sandworm for follow-up destructive activities. `education` `universities` `food` `public administration` `russia` link

RTV Noord suspected ransomware disruption
On November 10, Dutch broadcaster RTV Noord suffered a suspected ransomware attack. The incident blocked access to systems, forcing manual music playback and limiting news updates. Internal communications were disrupted, with the newsroom reachable only via WhatsApp. The attack impacted RTV Noord's role as an emergency broadcaster, highlighting risks to critical public information services. `media` link

Data exposure and leaks

Eurofiber France ticketing system breach claimed by ByteToBreach threat actor
On November 16, Eurofiber announced that a cybersecurity incident was detected on November 13, affecting the ticket management platform used by Eurofiber France. A threat actor called ByteToBreach claimed the breach on a data leak forum, and mentioned exfiltrating data allegedly from 10.000 businesses and government clients. The breach affected the French division and sub-brands, with no critical data confirmed stolen. `telecommunications` `public administration` link

French social security agency Pajemploi personal data breach and exposure of 1.2 million individuals
On November 14, French social security agency Pajemploi detected a data breach that exposed the personal data of up to 1.2 million individuals, with exfiltrated data including full names, place of birth, postal address, social security number, names of used banking institutions, Pajemploi number, and accreditation number. The agency said they would notify persons affected individually. No threat actor has yet claimed the data breach. `labour` link

Hungarian TISZA opposition party hit by major data breach
On November 3, the opposition party TISZA Party reported that personal data of around 200.000 users of its app “TISZA Világ” had been leaked online. The party leader, Péter Magyar, blamed Russian-backed threat actors and accused the government of intimidation, while the government alleged Ukrainian involvement and launched a national-security investigation. `civil society` `political parties` `russia` link

Hacktivism

Pro-Russia hacktivists NoName057(16) claims DDoS attacks against Danish entities ahead of local elections
On November 17, pro-Russia supposed hacktivist group NoName057(16) claimed DDoS attacks against Danish entities ahead of Denmark's 2025 local elections on November 18. The attacks did not disrupt the voting process. Several party websites were targeted, including the Conservatives, the Red-Green Alliance, the Moderates and Social Democrats, temporarily disrupting access. Another confirmed target was The Copenhagen Post. Denmark’s intelligence service announced the likelihood of attacks in early November. `political parties` `civil society` `russia` link

Pro-Russia hacktivists NoName057(16) targeted several Belgian telecommunications websites with DDoS
On November 5, Belgian newspaper RTBF relayed that Russia-linked supposed hacktivists NoName057(16) targeted several Belgian telecommunications websites with DDoS attacks. The threat actors claimed on Telegram to have targeted Scarlet, Proximus, and Telenet, all telecommunications operators. Scarlet's website remained unavailable for over three hours. However, the impact for all three remained very limited. `telecommunications` `technologies` `russia` link

World

Cyber policy and law enforcement

Russian national arrested in Thailand confirmed former FSB employee
On November 15, Russian state-controlled outlet RT identified the Russian national arrested on November 6 in Thailand as Denis Obrezko, a cybersecurity specialist who was a former Federal Security Service (FSB) Cryptography Academy employee. He also held positions at Kaspersky Lab and within the Russian government. Thai police and US authorities allege Obrezko was previously linked to Laundry Bear, a recent Russia-linked threat actor. Obrezko was arrested following a tip to Thai police by the US government. `russia` link

United States, Australia, and the United Kingdom joint sanctions against Russia-based bulletproof hosting providers
On November 19, the United States, Australia, and the United Kingdom announced sanctions against Russia-based bulletproof hosting company Media Land and its network as well as Aeza Group for enabling online criminal marketplaces and ransomware groups such as Lockbit, BlackSuit, and Play. Additionally, Five Eyes cybersecurity agencies released a joint guidance to mitigate risks from bulletproof hosting providers. `russia` `united states` link

Israel Defense Force bans Android phones for senior officers, iPhones now mandatory
On November 26 the Israel Defense Forces (IDF) issued a directive banning Android phones for officers of rank lieutenant colonel and above. Only Apple iPhones will be allowed on IDF-issued lines. The decision follows an internal security review after the October 7 attacks, motivated by fears of cyberespionage, “honeypot” malware schemes, and social-engineering exploitation of soldiers’ Android devices, vulnerabilities the IDF believes are reduced with iPhones. `israel` link

China issues draft data privacy regulations with stricter localisation measures
On November 22, China’s Cyberspace Administration and Ministry of Public Security issued a draft rule, "regulations on personal information protection for large online platforms" aimed at entities that process large volumes of personal data, and which builds upon the 2021 Personal Information Protection Law. It also mandates that personal data be stored in data centres located in China that must meet national security standards. The draft stems from China's cyber sovereignty objective, seeking to improve government oversight and control of domestic data processing. `china` link

Cyberespionage & prepositioning

Leak of Witkoff-Ushakov Ukraine peace call
On November 26, several newspapers analysed potential suspects of the leaked of Witkoff-Ushakov Ukraine peace call. US intelligence operatives, a NATO ally, and Russia or its proxies are considered potential sources of the leak. Some suspect an insider in US spy agencies, while a European ally may have leaked it to block pro-Russian negotiations. Although Russia denies involvement, suspicions persist due to a second intercepted call. `diplomacy` link

China-linked AI-agentic cyberespionage campaign targeted multiple global organisations
On November 13, Anthropic reported a China-linked cyberespionage campaign leveraging AI agentic capabilities to target around thirty global organisations, successfully breaching a small number of them. The operation, largely executed autonomously via a jailbroken AI tool to bypass its guardrails, targeted technology, finance, manufacturing, and government sectors. `chemicals` `technologies` `public administration` `finance` `china` link

Landfall Android spyware campaign via Samsung zero-day

On November 7, Palo Alto Networks reported the discovery of Landfall, a commercial-grade Android spyware targeting Samsung Galaxy devices in Iraq, Iran, Turkey and Morocco. Delivered through malicious image files exploiting a Samsung zero-day, the campaign enabled extensive surveillance and data exfiltration. Infrastructure and tradecraft suggest links to private-sector offensive actors operating in the Middle East, though direct attribution remains unconfirmed. `cybersecurity` link

PlushDaemon EdgeStepper update hijacking campaign

On November 19, ESET reported that China-linked threat actor PlushDaemon has been conducting a global cyberespionage campaign by hijacking software update traffic using its EdgeStepper implant. Since 2018, the group has targeted organisations and individuals across Asia, North America, and Oceania, compromising manufacturers, universities, and other sectors. The activity enables widespread network infiltration and data theft through malicious update redirection. `technologies` `transport` `education` `china` link

Cybercrime

Glassworm malware returns to OpenVSX with new Visual Studio Code extensions

On November 6, Koi Security reported on a new GlassWorm malware activity on OpenVSX with three new VSCode extensions downloaded more than 10.000 times. It uses Solana transactions, invisible Unicode to deploy JS payloads stealing GitHub, NPM, OpenVSX credentials and cryptocurrency wallet data. Koi Security accessed attacker infrastructure confirming global victims and Russian-speaking operators. `russia` link

DanaBot malware resurgence targeting Windows systems

On November 12, Zscaler reported the resurgence of DanaBot malware, six months after law enforcement's Operation Endgame disrupted its infrastructure. The new variant is actively targeting Windows users globally, leveraging rebuilt command-and-control systems. Operating under a malware-as-a-service model, DanaBot enables credential and cryptocurrency theft, posing renewed risks to organisations and individuals through malicious e-mails, SEO poisoning, and malvertising campaigns. `finance` link

Disruption & destruction

Cloudflare Global Network Outage

On November 18, Cloudflare reported a worldwide disruption to its Global Network, causing widespread website errors and service unavailability. The outage impacted numerous online platforms, including those relying on Cloudflare's security and performance services. No threat actor has been identified, and the incident appears linked to ongoing maintenance. The disruption affected global connectivity, leaving many businesses and users unable to access critical online resources. `technologies` `cybersecurity` link

Russia-based port operator reports DDoS attacks

On November 13, Russia-based port operator Port Alliance reported that unknown actors had attempted DDoS attacks and other network intrusions against its systems since November 10, aiming to disrupt coal and fertiliser exports across multiple Russian seaports. The activity did not impact port operations. The reported cyberattacks were followed by a November 14 Ukrainian drone attack against Russia's Black Sea Port in Novorossiysk. `transport` `maritime` `transport` link

Data exposure and leaks

Clop Oracle E-Business Suite breach affects Logitech
On November 14, Logitech International S.A. reported a data breach linked to the Clop cybercrime group, involving theft of approximately 1.8TB of data via a third-party zero-day vulnerability in Oracle E-Business Suite. The incident exposed limited employee, consumer, customer, and supplier information, though no sensitive identifiers or payment data were compromised. Operations and products remained unaffected. `technologies` link

Research study revealed WhatsApp security flaw exposing billions of accounts
On November 18, researchers at the University of Vienna reported on a vulnerability in WhatsApp's contact-discovery system, allowing them to query over 100 million phone numbers per hour and enumerate 3.5 billion active accounts. They extracted metadata, such as public keys, profile pictures, OS type, account age, and number of linked devices, but never accessed message content. link

Chinese security firm Knownsec data leaked on GitHub
On November 2, Chinese security firm Knownsec had more than 12.000 documents leaked on GitHub. According to security researchers, the documents reveal that the data is from a 2023 breach. The documents describe surveillance tools such as remote access trojans (RATs), and a power bank designed for data theft. A Chinese Foreign Ministry spokesperson stated unfamiliarity with the breach but asserted that China opposes all cyberattacks. `china` link

Opportunistic

FlexibleFerret malware continues to strike with fake jobs assessment
On November 25, 2025, Jamf Threat Labs reported that the North Korea-linked FlexibleFerret macOS malware is being used in targeted social-engineering campaigns against individuals approached with fake job opportunities. The goal is to trick victims into granting attackers remote access, enabling theft of personal data, credentials, and other sensitive information. The campaign suggests financially motivated actors seeking high-value personal and corporate access. `north korea` link

Cisco: Actively exploited firewall flaws now abused for DoS attacks
On November 5, Cisco warned that two vulnerabilities (CVE-2025-20362 and CVE-2025-20333) which have been used in zero-day attacks, are now being exploited to force ASA and FTD firewalls into reboot loops. CISA and Cisco linked the attacks to the ArcaneDoor campaign, which exploited two other Cisco firewall zero-days (CVE-2024-20353 and CVE-2024-20359) in November 2023. `china` link

FortiWeb flaw with public PoC exploited to create admin users
On November 13, researchers reported that attackers were actively exploiting an unpatched FortiWeb vulnerability to gain unauthorised administrative access on exposed appliances, using publicly circulating proof-of-concept code to automate compromise. Intrusion attempts included creation of rogue admin accounts. Fortinet advised customers to apply the latest fixes and review systems, stating there is no indication patched versions remain affected. link

1. Conclusions or attributions made in this document merely reflect what publicly available sources report. They do not reflect our stance.

TLP definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
AMBER	Limited disclosure, restricted to participants' organisations and their clients.	Recipients may share TLP:AMBER information only with members of their own organisation and its clients.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
CLEAR	Disclosure is not limited.	TLP:CLEAR information may be distributed freely.