CERT-EU

Cyber Brief (December 2025)

January 5, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 368 open source reports for this Cyber Security Brief[^1].
- Relating to **cyber policy and law enforcement**, the EU fined X and sanctioned Russian individuals and entities. The UK and Poland took legal actions against the GRU and individuals. Germany and Denmark attributed cyberattacks to Russia.
- On the **cyberespionage** front, China-linked Ink Dragon expanded operations to target European government entities. Russia-linked Callisto targeted a French NGO and France probes foreign interference of passenger ship. Intellexa was accused of accessing government spyware data. Iran-linked MuddyWater targeted critical infrastructure in Israel and Egypt.
- As regards to **cybercrime**, a sophisticated phishing kit enables the impersonation of major European banks, initial access broker Storm-0249 exploits EDR tool for ransomware, and malicious Firefox extension campaign affected over 50.000 globally.
- There were **disruptive** attacks in France and Romania, affecting postal services and water systems. Venezuela's state-owned oil company was also hit by a cyberattack.
- Regarding **data exposure and leaks** incidents, justice (namely France's Ministry of Interior), personal information, and telecommunications were targeted in France, the health sector in the UK, and Docker Hub all disclose data breaches.
- As for **opportunistic** attacks, China-linked threat actors exploit React2Shell vulnerability and vulnerabilities in Cisco products. SonicWAll reported threat actors exploiting a zero-day vulnerability. Fortinet also reported the exploitation of several vulnerabilities.

Europe

Cyber policy and law enforcement

EU fines X 120 million euros for Digital Services Act violations
On December 5, the European Commission fined X 120 million euros for violating the Digital Services Act (DSA), accusing the platform of deceiving users through paid verification without

proper identity checks and failing to ensure transparency in its advertising repository. X has 60–90 days to propose corrective measures or face additional penalties, marking the first major enforcement action under the DSA amid growing EU scrutiny of large social media platforms. `fine` link

EU Council sanctions 12 individuals and two entities over Russian hybrid threats against Europe
On December 15, the EU Council sanctioned 12 individuals and two entities for supporting Russian hybrid threats against Europe. The list includes three individuals linked to GRU Unit 29155 threat actor Cadet Blizzard, who targeted EU member states, NATO allies and Ukraine. The list also includes individuals involved in spreading pro-Russia propaganda as well as the 142nd Separate Electronic Warfare Battalion involved in GPS jamming in the EU airspace. `sanctions` link

UK and Poland intensify legal actions against Russian intelligence operations
On December 4, the UK and Poland announced major legal actions against Russian intelligence operatives, with the UK sanctioning the GRU and 11 officers for hybrid warfare and cyber operations across Europe, while Poland indicted an FSB-linked Russian national for leading a sabotage and espionage network. Despite these measures, Russian intelligence services are highly likely to continue cyber and physical operations targeting European governments and critical infrastructure through at least mid-2026. `sanctions` `russia` link

UK sanctions two China-based tech firms for their role in global cyberattacks
On December 9, the UK's Foreign, Commonwealth and Development Office sanctioned China-based companies I-Soon and Integrity Tech for their alleged role in malicious activity targeting the IT systems of over 80 government, public, and private-sector entities. The UK's National Cyber Security Centre highlighted these companies exemplify an ecosystem of private sector actors that very likely support China's state-sponsored operations. A Chinese Foreign Ministry spokesperson denied the claims and denounced the sanctions as "political manipulation." `sanctions` `china` link

Germany officially attributes cyber activities to Russia-linked threat actors
On December 12, Germany's Foreign Ministry publicly attributed several cyber incidents to Russia-linked threat actors. These include an August 2024 cyberattack impacting German Air Traffic Control attributed to APT28, and an information operations campaign targeting Germany's February 2025 elections attributed to Storm-1516. They also mentioned acts of sabotage, without specifying them or the threat actor conducting them. These attributions likely serve as diplomatic pressure towards Russia. `attribution` `russia` link

Denmark says Russia was behind two 'destructive and disruptive' cyberattacks
On December 18, the Danish Defence Intelligence Service accused Russia of orchestrating two major cyberattacks: the first by the pro-Russian group Z-Pentest in 2024, targeting a Danish water utility, and the second by NoName057(16) in November 2025, disrupting websites during local elections. Both groups are linked to the Russian state and are part of Moscow's hybrid warfare strategy to destabilise Western support for Ukraine. `attribution` `russia` link

Belgium bans DeepSeek for federal government employees
On December 1, 2025 the Belgian federal government banned the use of DeepSeek by its employees. All DeepSeek apps must be removed from government-issued devices by that date. The decision follows a security review by the Centre for Cybersecurity Belgium, which identified privacy and data-protection risks linked to DeepSeek. `policy` `china` link

Portugal creates a safe harbour for good-faith security researchers
On December 4, Portugal updated its cybercrime law to create a safe harbour for good-faith security research, exempting certain hacking activities when done solely to identify vulnerabilities and improve cybersecurity. The law requires no financial gain, immediate

reporting to owners and the national security centre, minimal and non-harmful actions, confidentiality, timely data deletion, and bans risky techniques. Similar protections have recently emerged in Germany and the United States, strengthening responsible vulnerability disclosure. `policy` link

Bulgaria announces centralised National Cybersecurity System
On December 5, Bulgaria announced it is developing a centralised national cybersecurity system to strengthen security, protect data sovereignty, and support EU initiatives discussed at the Transport, Telecommunications, and Energy Council meeting, including the upcoming EU Digital Identity Wallet planned for 2026. Minister Valentin Mundrov also emphasised Bulgaria's growing tech potential, ongoing NIS2 transposition, and broader European efforts to build technological sovereignty and coordinated cybersecurity capabilities. `policy` link

Finnish police seize ship suspected of sabotaging undersea cable
On December 31, 2025, Finnish authorities seized the cargo ship Fitburg in the Gulf of Finland on suspicion it damaged an undersea telecommunications cable linking Finland and Estonia, disrupting critical infrastructure. Fourteen crew members were detained and investigators opened a criminal probe into aggravated interference and damage, amid rising concerns about sabotage of Baltic Sea infrastructure. `arrest` link

Israel and Germany launch cybersecurity partnership
On December 9, Israel National Cyber Directorate announced a new cybersecurity partnership with Germany aimed at strengthening shared capabilities through best-practice exchanges, a joint AI-focused Cyber Center of Excellence, collaborative exercises, and enhanced regulation and risk management efforts. `cooperation` link

Cyberespionage & prepositioning

Russia-linked Callisto targets French NGO Reporters Without Borders with spearphishing
On December 3, Sekoia reported that the Russia-linked group Callisto targeted the French NGO Reporters Without Borders with spearphishing for credential harvesting in March. Callisto sent the phishing e-mail from a ProtonMail address disguised as a trusted contact and containing a non-working link. After the recipient requested the missing file, the attacker sent a document that led to a compromised page mimicking the ProtonMail login page. `russia` link

France probes 'foreign interference' after passenger ship hit by remote-control malware
On December 17, France launched an investigation into possible foreign interference after malware capable of remotely controlling systems was found on the Italian-operated passenger ferry Fantastic docked in Sète. French counterespionage authorities, alerted by Italian intelligence, arrested a Latvian crew member charged with acting for an unnamed foreign power; a Bulgarian was released. Officials have not ruled out any responsible actors. `transport` link

Ink Dragon expands relay network targeting European governments
On December 16, Check Point Research reported that China-linked threat actor Ink Dragon had expanded its operations to target European government entities. The group repurposes compromised servers into a covert relay network, enabling stealthy command-and-control and persistent multi-organisational access. This campaign reflects a strategic shift from data theft to infrastructure control, increasing operational reach and complicating defensive efforts across affected regions. `telecommunications` `public administration` link

Intellexa accused of accessing government spyware targets' data
On December 4, Amnesty International and media partners reported that Intellexa, known for selling the highly invasive spyware Predator, had remote access to government customers' surveillance systems and data belonging to individuals targeted with Predator. The leaked

material suggested Predator stores victim data and that Intellexa employees could view it, raising concerns about widespread exposure of sensitive information, though Intellexa denies wrongdoing. `spyware` link

Cybercrime

New Spiderman phishing kit enables scalable attacks on European financial institutions
On December 9, Varonis reported that a sophisticated phishing kit called Spiderman enables cybercriminals to impersonate dozens of major European banks and crypto platforms, launching highly convincing attacks with just a few clicks. The kit provides real-time credential and OTP theft, advanced filtering to evade detection, and a full-control panel for managing victim sessions, making large-scale, cross-country financial fraud far easier for attackers. `finance` link

GhostPairing WhatsApp account hijacking campaign
On December 15, Gen Digital reported a campaign dubbed GhostPairing, in which threat actors hijack WhatsApp accounts by tricking victims in Czechia into linking the attackers' devices via legitimate pairing features. Compromised accounts are used to spread lures to contacts, enabling further compromises. The attack grants persistent access to messages and media, facilitating impersonation, fraud, and broader social engineering operations. link link

Disruption & destruction

Coordinated DDoS disruption of French postal and banking services
On December 22, French postal service La Poste disclosed it was the victim of a DDoS attack that impacted postal services and the company's banking provider, La Banque Postale. The incident caused disruptions to some services, including postal operations and online banking access; however, payments, interbank transfers, cash withdrawals, in-store purchases, transfers, and online payments were unimpacted. On December 23, pro-Russia supposed hacktivist group NoName claimed responsibility for the attacks. `DDoS` `russia` link

BitLocker ransomware attack on Romanian national water agency
On December 22, Romania's National Directorate of Cyber Security reported a ransomware attack on their national water management agency, locking staff out of around 1.000 systems. Attackers misused Microsoft's BitLocker tool to encrypt devices, disrupting e-mail communications but leaving operational infrastructure unaffected. A ransom note demanded contact within seven days; authorities advised against engaging with the cyber extortionists. `ransomware` link

Data exposure and leaks

French authorities arrest suspect linked to Interior Ministry cyberattack
On December 12, French Ministry of the Interior reported a cyberattack compromising its e-mail servers, granting attackers access to certain files. The breach, claimed by BreachForums actors, allegedly compromised police records of over 16 million individuals. Officials have not confirmed data theft, and investigations continue into possible links between the suspect and the forum's revenge-motivated intrusion. On December 17, French authorities arrested a 22-year-old suspect. `justice` link

Pass'Sport-linked data leak exposes millions of households in France
On December 18, Les Numériques reported a criminal forum publication of a 15GB file containing personal data from approximately 3.5 million French households. The leak, allegedly linked to the Pass'Sport programme, aggregate information from multiple public bodies. Threat

actors claim the release is retaliation against the French state, posing risks of identity theft and targeted phishing for affected individuals. `personal data` link

SFR customer data breach via technician tool compromise
On December 18, Les Echos reported that French telecom operator SFR suffered a cyberattack involving unauthorised access to a technician network management tool, leading to theft of customer data including names, addresses, phone numbers, and e-mails. No banking details were exposed. The identity of the attackers remains unknown, and the incident follows a series of recent breaches in France's telecommunications sector. `telecommunications` link

Barts Health NHS discloses data breach after Oracle zero-day hack
On December 5, Barts Health NHS Trust, a major healthcare provider in England, disclosed that Clop ransomware actors exploited an Oracle E-Business Suite zero-day to steal years' worth of invoices containing names and addresses of patients, former staff, and suppliers. Although clinical systems were not affected, the Trust has notified authorities, is seeking a High Court order to restrict dissemination, and advises affected individuals to remain alert for suspicious communications. `health` link

World

Cyber policy and law enforcement

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 now be allowed on IDF-issued lines. The decision follows an internal security review after the October 7 attacks, motivated by fears of cyber-espionage, "honeypot" malware schemes, and social-engineering exploitation of soldiers' Android devices — vulnerabilities the IDF believes are reduced with iPhones. `israel` link

US indicts Ukrainian national for supporting two Russian state-sponsored cyberattack groups
On December 9, the US Department of Justice announced indictments against Ukrainian national Victoria Dubranova for allegedly supporting two Russian state-sponsored groups, CyberArmyofRussia_Reborn and NoName057(16), in destructive cyberattacks targeting US critical infrastructure. The DOJ, FBI, and federal partners emphasised that these state-backed hacktivist operations pose a major national security threat, and the State Department issued rewards of up to 10 million dollars for information leading to co-conspirators. `indictment` link

FCC may bar Chinese telecom companies from connecting to US networks
On December 8, 2025, the US FCC threatened to bar China Mobile, China Telecom, and China Unicom from US networks over robocall concerns and national security risks. The companies have two weeks to prove their presence in the US robocall mitigation database is safe. This follows previous bans and ongoing scrutiny of Chinese telecom firms, including HKT and Huawei, as Washington tightens restrictions on Beijing-linked entities. `ban` `china` link

Cyberespionage & prepositioning

China-linked actors compromise VMware servers globally with Brickstorm malware
On December 4, the US CISA reported Chinese state-sponsored actors deploying Brickstorm malware to compromise VMware vSphere servers globally. Victims are primarily in the government and IT sectors. Brickstorm is a sophisticated backdoor for VMware vSphere

(specifically VMware vCenter servers and VMware ESXI) and Windows environments. The same day, Crowdstrike linked multiple Brickstorm intrusions targeting VMware vCenter environments at US-based entities, to the newly identified China-nexus adversary Warp Panda. `china` link

ShadyPanda seven-year malicious browser extension campaign
On December 1, Koi Security reported that China-linked ShadyPanda conducted a seven-year campaign weaponising trusted Chrome and Edge extensions. The operation infected over 4.3 million browsers globally, enabling large-scale surveillance and remote control. By exploiting marketplace trust and auto-update mechanisms, ShadyPanda amassed millions of users before deploying malicious updates, posing significant risks to individuals and enterprises worldwide. `china` link

Iran-linked MuddyWater critical infrastructure campaign in Israel and Egypt
On December 2, ESET reported that Iran-aligned group MuddyWater targeted critical infrastructure and other sectors in Israel and Egypt. The campaign employed custom malware and refined tactics to improve persistence and evade detection. Victims included government, manufacturing, engineering, and utilities organisations, indicating a focused espionage operation with potential operational overlap with fellow Iran-aligned group Lyceum. `iran` link

Apple WebKit zero-days exploited in targeted attacks
On December 12, Apple reported two Apple WebKit zero-day vulnerabilities, CVE-2025-43529 and CVE-2025-14174, discovered by Apple and Google Threat Analysis Group, and exploited in an extremely sophisticated campaign against specific individuals. Affected devices include recent iPhone, iPad, Mac, and other Apple platforms. `sophisticated` link

Cybercrime

Ransomware broker exploits EDR tools for stealthy malware delivery
On December 9, ReliaQuest reported that initial access broker Storm-0249 is abusing trusted endpoint detection and response components and Windows utilities to stealthily load malware, maintain persistence, and support ransomware operators. In one analysed attack, the actor used ClickFix social engineering, curl-delivered MSI payloads, and DLL sideloading through SentinelOne components to execute malicious code inside a trusted EDR process, evading detection and profiling systems for ransomware affiliates. `ransomware` link

Amos Stealer via AI-poisoned search results
On December 9, Huntress reported a global Amos stealer campaign exploiting AI trust by poisoning search results to legitimate ChatGPT and Grok conversations. Victims were tricked into executing malicious macOS Terminal commands, leading to credential theft, persistent malware, and data exfiltration. This represents a significant evolution in social engineering, bypassing traditional defences through trusted platforms and familiar user interactions. `stealer` link

New ConsentFix OAuth phishing technique
On December 11, Push Security reported a global phishing campaign using a novel "ConsentFix" technique to hijack Microsoft accounts via Azure CLI OAuth abuse. The browser-native attack bypassed passwords and MFA, enabling account compromise without direct credential theft. The campaign leveraged compromised high-reputation sites and advanced evasion, posing significant risks to enterprise cloud environments worldwide. `phishing` link

China-linked DarkSpectre multi-campaign browser extension operation
On December 30, Guardio Labs reported that China-linked threat actor DarkSpectre conducted coordinated malicious browser extension campaigns, including ShadyPanda, GhostPoster, and

The Zoom Stealer. Over 8.8 million users worldwide were affected through long-term surveillance, fraud, and corporate espionage operations, demonstrating strategic, well-funded, and large-scale activity across Chrome, Edge, Firefox, and Opera platforms over more than seven years. `browser extension` link

Information operations

Russia increasingly targeting Armenia with disinformation campaigns ahead of June 2026 parliamentary election
On November 30, DW published an article about Russia increasingly targeting Armenia with disinformation campaigns ahead of the upcoming parliamentary election in June 2026. Although the country is often the target of information operations by Russia-linked threat actors, they have intensified recently and innovated with AI-generated photos, audio, and deepfakes. There are likely several campaigns operating in Armenia, and one of them is Matryoshka, previously observed in EU countries. `public administration` `civil society` link

Disruption & destruction

Cyberattack disrupts Venezuelan oil giant PDVSA's operations
On December 15, Petróleos de Venezuela (PDVSA), Venezuela's state-owned oil company, reported that it was hit by a disruptive cyberattack over the weekend that disrupted its export operations. The specific nature of the attack was not disclosed. In its Monday statement, PDVSA alleged that the United States and domestic conspirators were responsible, attempting "to undermine national stability." This cyberattack comes amid escalating tensions between Venezuela and the US. `energy` link

Data exposure and leaks

Docker Hub container images exposed credentials
On December 10, cybersecurity company Flare revealed that they found over 10.000 Docker Hub container images exposing credentials that should have been protected. These exposures included credentials for production systems, CI/CD pipelines, and keys for large language models (LLMs). link

Opportunistic

China-linked cyber threat groups rapidly exploit React2Shell vulnerability (CVE-2025-55182)
On December 4, Amazon published a report on the rapid exploitation of CVE-2025-55182 (React2Shell) by China-linked threat actors. Observed groups, including Jackpot Panda and Earth Lamia, targeted React and Next.js Server Functions to achieve remote code execution and deploy web shells. Exploitation attempts were also seen originating from an anonymisation network node. CERT-EU linked this node to China-linked GhostVPN ORB. `china` link

UAT-9686 actively targets Cisco Secure Email Gateway and Secure Email and Web Manager
On December 17, Cisco reported about UAT-9686, an active campaign by a China-linked advanced persistent threat targeting Cisco AsyncOS Software used in Cisco Secure Email Gateway and Cisco Secure Email and Web Manager appliances. The threat actor deploys tools including a Python backdoor called AquaShell, enabling system-level access on devices with non-standard configurations, and Cisco advises following security guidance to mitigate the campaign. `china` link

SonicWall SMA1000 zero-day attack chain
On December 17, SonicWall PSIRT reported on threat actors exploiting a chained zero-day attack against SonicWall SMA1000 appliances, enabling remote code execution with root privileges. The campaign targeted exposed devices globally, posing significant risks to enterprises, government, and critical infrastructure. SonicWall urged immediate patching to mitigate ongoing exploitation and prevent further compromise of sensitive systems. `zero-day` link

VS Code extensions hide trojan in fake PNG
On December 10, ReversingLabs reported a global malicious campaign involving 19 Visual Studio Code extensions embedding trojan malware within modified dependencies, disguised as a PNG image. The threat actors leveraged trusted npm packages to evade detection, potentially compromising developer systems worldwide. The campaign highlights evolving supply-chain attacks targeting the VS Code Marketplace, with all identified extensions now reported to Microsoft. `vs code` link

FortiGate SSO Exploitation via CVE-2025-59718 and CVE-2025-59719
On December 15, Arctic Wolf reported malicious single sign-on logins targeting FortiGate devices, exploiting recently disclosed CVE-2025-59718 and CVE-2025-59719. The activity involved unauthorised administrative access and configuration exfiltration from multiple hosting provider IPs. Impacted Fortinet products include FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager, with potential credential compromise. No specific threat actor attribution was made, but exploitation appears opportunistic and widespread. `fortinet` link

Five-year-old Fortinet 2FA bypass (CVE-2020-12812) still exploited in the wild
On January 2, Shadowserver identified over 10.000 Fortinet firewalls exposed to active exploitation of a critical five-year-old 2FA bypass vulnerability (CVE-2020-12812). On December 24, 2025, Fortinet had reported that the vulnerability was still being exploited in the wild. `fortinet` link

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.