CERT-EU

Cyber Brief (January 2026)

February 2, 2026 – Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 268 open source reports for this Cyber Security Brief.[1]
- Relating to **cyber policy**, The European Commission proposed an EU Cybersecurity package to strengthen ICT supply chains, and the EU and India signed a security & defence partnership covering cooperation on cyber issues.
- On the **cyberespionage** front, China-linked Salt Typhoon allegedly infiltrated United Kingdom (UK) telecom networks in a long-running campaign, and in the US they were attributed to the compromise of congressional committee staff e-mail systems. The North Korea-linked Contagious Interview campaign was observed exploiting Visual Studio Code tasks for malware delivery.
- In regards to **cybercrime**, a new Russia-linked ClickFix campaign targeted European hospitality organisations, while the global Kimwolf botnet reportedly expanded, exploiting residential proxy networks.
- There were **disruptive** attacks in Poland, with Russia-linked Sandworm targeting renewable energy entities with a data wiper, though the national energy supply was not disrupted. In Iran, nationwide protests led to an internet blackout, with authorities likely blocking signals from Starlink satellites. Further, internet outages were reported in parts of Caracas, Venezuela, corresponding to power cuts during the US military operation that captured President Nicolás Maduro.
- Regarding **data exposure and leaks** incidents, cybercrime actor Scattered Lapsus Hunters reportedly exfiltrated 500GB of data from the European Space Agency, and Eurail B.V. reported a security breach exposing customer data.
- As for **opportunistic** attacks, Ivanti released a security advisory to inform customers of two critical vulnerabilities in one of its products. Microsoft reported a high-severity zero-day vulnerability affecting multiple office versions, and Cisco disclosed and patched a remote code execution zero-day.

Europe

Cyber policy and law enforcement

The European Commission proposes EU Cybersecurity Package to strengthen ICT supply chains and ENISA
On January 20, the European Commission proposed a cybersecurity package to strengthen EU resilience, tighten IT supply-chain security via a revised Cybersecurity Act, and simplify certification. It also proposed targeted NIS2 amendments to ease compliance and expand ENISA's role in threat alerts, incident response, and the single-entry reporting point. Once approved by the Parliament and Council, Member States would have one year to implement. link

The EU and India sign security & defence partnership covering cooperation on cyber issues
On January 27, the EU and India signed a partnership on a range of security and defence issues, including cyber. The document outlines that the EU and India will deepen the existing Cyber Dialogue by enhancing regular exchanges on the threat landscape, as well as the coordination of diplomatic responses to malicious cyber activities and capacity-building efforts. The partnership also highlights continued collaboration on the UN framework for responsible state behaviour in cyberspace. link

Microsoft, Europol, and national authorities take down global cybercrime subscription service
On January 14, Microsoft announced disrupting RedVSD along with Europol, Germany and UK authorities. RedVDS is a global cybercrime subscription service, providing criminals with access to disposable virtual computers. It has caused losses of millions of dollars worldwide. The operation seized key malicious infrastructure and took RedVDS marketplace offline. link

Ireland proposes legislation allowing spyware use by law enforcement
On January 20, Ireland's Minister for Justice, Home Affairs and Migration secured government approval to strengthen legislation on the lawful interception of communications, providing a new legal basis for police to use spyware in cases of serious crime and threats to national security. If passed, this would update the Communications (Interception and Lawful Access) Bill and replace the Interception of Postal Packets and Telecommunications Messages (Regulation) Act of 1993. link

France announces its National Cybersecurity Strategy for 2026-2030
On January 29, France's General Secretariat of Defence and National Security presented its new National Cybersecurity Strategy spanning 2026-2030. As part of France's National Strategic Review initiative, the strategy sets out a structured framework covering five key areas, which include strengthening the country's pool of cyber talent, national cyber resilience, deterring cyber threats, digital sovereignty, as well as international cooperation on global cyberspace norms. Link

Spanish law enforcement operation disrupts Black Axe–linked BEC network
On January 9, Spanish National Police announced a multi-year operation that arrested 34 suspects, including alleged senior Black Axe members, for adversary-in-the-middle fraud and business e-mail compromise. Authorities seized cash, froze bank accounts, and linked roughly 3.2 million euros in losses to the case. The disruption is likely short-lived given Black Axe's scale and ability to regenerate. link

Cyberespionage & prepositioning

Salt Typhoon Downing Street telecom compromise
On January 27, The Telegraph reported that China-linked Salt Typhoon allegedly infiltrated UK telecom networks, compromising phones of senior Downing Street aides since 2021. The activity reportedly exposed sensitive communications and metadata involving figures around former prime ministers, with breaches discovered in 2024. Intelligence sources warned the intrusion reached the heart of government, raising concerns over persistent state-backed espionage. `telecommunications` `public administration` `china` link

State and criminal actors exploit WinRAR CVE-2025-8088
On January 27, Google Threat Intelligence Group reported ongoing exploitation of WinRAR vulnerability CVE-2025-8088 by Russia- and China-linked state actors and financially motivated groups. Campaigns target Ukrainian government and military entities, among others, using malicious archives for persistence and malware delivery. `finance` `defence` `russia` link

Cybercrime

A new ClickFix campaign uses fake Windows BSOD screens to launch malware
On January 5, Securonix Threat Research reported a Russia-linked PHALT#BLYX campaign targeting European hospitality organisations. The attackers used fake Booking.com reservation cancellations, social engineering with simulated blue screens of death (BSODs), and trusted MSBuild.exe abuse to deploy DCRat for remote access and secondary payload delivery. The campaign aimed to bypass defences, maintain persistence, and harvest sensitive data during the busy holiday season. link

Slovenia-based gas supplier Geoplin targeted in likely ransomware attack
On January 29, Slovenia-based gas supplier Geoplin was targeted in a likely ransomware attack, with reportedly limited impact on Geoplin's IT environment. The attackers allegedly demanded 6.8 million euros in exchange for stolen data, which reportedly includes employee data, confidential internal documents and financial data. `energy` link

Disruption & destruction

Poland renewable energy operators targeted in Russia-linked Sandworm data wiper attack
On December 29, 2025, renewable energy operators in Poland experienced an attempted cyberattack using data-wiping malware, dubbed DynoWiper by ESET. While the national energy supply was not impacted, the wiper had targeted two combined heat and power plants in addition to a management system used for electricity generated from renewable sources. The attack was attributed to Russia-linked threat actor Sandworm, which 10 years ago had conducted a destructive data-wiping attack on Ukraine's energy grid. `energy` `russia` link

La Poste and La Banque Postale DDoS disruption
On January 1, Agence France-Presse reported a renewed cyberattack against La Poste and La Banque Postale in France, disrupting multiple online services including parcel tracking and Digiposte. The pro-Russia group NoName057(16) had previously claimed responsibility for a similar December DDoS attack. While service access was severely impacted, physical deliveries continued and no data breach was reported. `finance` link

Data exposure and leaks

Cybercrime actor Scattered Lapsus Hunters exfiltrate 500GB of data from the European Space Agency
On January 8, CyberInsider reported that attackers claiming to be Scattered Lapsus$ Hunters exfiltrated 500GB of sensitive ESA technical data after gaining access in September 2025 via an unpatched public vulnerability, then moving laterally to a compromised internal data-sharing platform. The dataset reportedly includes partner data linked to SpaceX, Airbus Group, Thales Alenia Space, OHB System AG and Teledyne. This is separate from the 888-linked December 30, 2025 breach. `defence` `space` link

Eurail customer data breach
On January 10, Eurail B.V. reported a security breach involving unauthorised access to customer data, potentially including identity, contact, order, reservation, and passport details. The incident affects Eurail customers and DiscoverEU participants. No threat actor has been identified, with no evidence of misuse or public disclosure. `transport` link

Unsecured database exposes personal data of over 45 million French citizens
On January 14, a massive leak containing over 45 million French citizens' records was published online, likely compiled by malicious data collectors from multiple breaches. It included demographic, healthcare, financial and insurance information, posing severe privacy and fraud risks. The repository was hosted on an unsecured cloud server and has since been taken offline after researchers alerted the host. `civil society` link

World

Cyber policy and law enforcement

The United States weighs expanding private companies' role in cyberwarfare
On January 14, The New York Times revealed the Trump administration is weighing a plan to expand private companies' role in offensive cyberwarfare within its upcoming National Cybersecurity Strategy. Proposals include embedding military cyberoperators in private firms or having companies develop attack code under Cyber Command's oversight. The shift aims to scale US cyber capabilities but requires congressional approval. `united states` link

China updates its cybersecurity law with expanded extraterritorial reach
On January 1, China's revised Cybersecurity Law entered into force. The new framework significantly expands its extraterritorial reach, granting Chinese authorities the power to penalise foreign entities whose activities abroad threaten China's national security. International organisations must now navigate complex compliance obligations and potential audits to avoid substantial financial penalties and legal repercussions within the region. `china` link

China's Ministry of Education announces the establishment of the College of Cybersecurity
On January 4, China's Ministry of Education announced the future establishment of the College of Cybersecurity, focused on developing talent in cybersecurity roles. It will consist of four Schools: Cybersecurity Technology, Artificial Intelligence Security, Cybersecurity Governance, and General Education. Students will receive hands-on training in an approach centred on real-world scenarios. The private industry will have an integral role, underscoring the close relationship between cybersecurity companies and the Chinese state. `china` link

Cyberespionage & prepositioning

China-linked HoneyMyte (Mustang Panda) expands CoolClient with credential theft tools
On January 27, Kaspersky reported that HoneyMyte (Mustang Panda), conducted cyberespionage campaigns in Myanmar, Mongolia, Malaysia, Russia, Pakistan and Thailand. The group deployed an enhanced CoolClient backdoor alongside browser credential stealers and data exfiltration scripts, targeting government entities. These operations indicate a broadened focus on persistent surveillance, credential harvesting and large-scale data theft across multiple regions. `public administration` `china` link

Salt Typhoon e-mail compromise of US congressional staff
On January 8, Financial Times reported on China-linked threat actors, operating under the Salt Typhoon campaign, compromising e-mail systems of US congressional committee staff. The activity, attributed to China's Ministry of State Security, enabled access to sensitive communications, including calls and messages, affecting senior officials and legislative bodies. `public administration` `telecommunications` `china` link

China-linked PDFSIDER DLL sideloading espionage campaign
On January 18, Resecurity reported the discovery of PDFSIDER, an advanced persistent threat leveraging DLL sideloading to deploy a covert backdoor with encrypted communications. The campaign, potentially linked to Mustang Panda tradecraft, targeted global entities via spearphishing. Its stealth and evasion capabilities suggest a focus on long-term espionage operations rather than mass-scale attacks, posing significant risks to high-value organisations worldwide. `public administration` `technologies` `china` link

China-linked UAT-8837 targets critical infrastructure in North America via zero-day and n-day exploitation
On January 15, Cisco Talos reported that China-nexus APT group UAT-8837 has been targeting critical infrastructure sectors in the US and Canada since at least 2025. The group gains initial access through zero-day and n-day exploits, then conducts reconnaissance and credential harvesting. Recently, the threat actor likely exploited CVE-2025-53690, a ViewState deserialisation zero-day vulnerability in SiteCore products. `china` link

North Korea-linked Contagious Interview campaign uses Visual Studio Code tasks for malware delivery
On January 20, Abstract Security Threat Research Organization (ASTRO) reported on the North Korea-linked Contagious Interview campaign exploiting Visual Studio Code task files to deliver malware during fake recruitment exercises. The campaign targets developers globally, enabling silent code execution once a project is opened and trusted. `technologies` `north korea` link

Cybercrime

Kimwolf botnet exploiting residential proxy networks
On January 2, Synthient reported the rapid expansion of the Kimwolf botnet, believed to be operated by cybercrime threat actors abusing unsecured residential proxy networks. The campaign has infected over two million devices globally, including Android TV boxes and digital photo frames, enabling large-scale DDoS attacks, ad fraud, and network intrusions. Impacted regions include Vietnam, Brazil, India, Saudi Arabia, Russia, and the US. link

MacSync Stealer via SEO poisoning and fake GitHub repositories
On January 16, Daylight Security MDR Team reported an active global campaign distributing the MacSync information stealer through SEO poisoning and fraudulent GitHub repositories impersonating legitimate software. The operation targets macOS and Windows users, harvesting

credentials, system data, and other sensitive assets. Over 20 malicious repositories remain active, indicating a sustained and evolving threat with significant cross-platform impact. link

Real-time vishing-adapted phishing kits target identity solutions, including Okta SSO or Microsoft Entra
On January 22, Okta Threat Intelligence reported that threat actors are using custom phishing kits with real-time session orchestration to support voice-based social engineering. These kits enable attackers to synchronise phishing pages with live calls, bypassing non-phishing-resistant MFA. Targets include identity solutions, including Google, Microsoft, and Okta, increasing the effectiveness and scale of vishing campaigns. link

Disruption & destruction

Caracas internet outages during US military operation
On January 4, NetBlocks reported significant internet outages in parts of Caracas, Venezuela, corresponding to power cuts during a US military operation that captured President Nicolás Maduro. President Trump suggested US cyber capabilities may have been used to disable power. The disruption coincided with a surge in Tor usage, indicating heightened public concern over surveillance and censorship amid political upheaval. `telecommunications` link

Starlink signals continue to be blocked in Iran
On January 8, Iran was plunged into a nationwide internet blackout as mass protests over worsening economic conditions spread across all 31 provinces, driven by soaring prices and a collapsing currency. On January 12, several media outlets reported that Iran continued to block signals from Starlink satellites, likely through sophisticated military jamming equipment. Uplink and downlink traffic has been affected to up to 80%. It is currently unconfirmed if Iran is receiving outside help to carry out these operations, although some have theorised about China and or Russia helping with the signal jamming due to previous known capacities to do so. `iran` link

Cloudflare IPv6 BGP route leak disruption
On January 26, Cloudflare reported a 25-minute IPv6 Border Gateway Protocol route leak caused by a misconfiguration, inadvertently affecting external networks globally. The incident led to congestion, packet loss, and dropped traffic, with potential security risks from unintended routing. No malicious actor was involved, and Cloudflare implemented safeguards to prevent similar disruptions in the future. `cybersecurity` link

Opportunistic

Ivanti EPMM vulnerability CVE-2026-1281 exploited in the wild
On January 29, Ivanti released a security advisory to inform customers of two critical vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM). These vulnerabilities do not affect Ivanti Neurons for MDM (our cloud mobile product), Ivanti Sentry (a standalone add-on to EPMM) or Ivanti Endpoint Manager. Link

PackageGate exposes zero-day gaps in JavaScript package managers, npm declines to fix
On January 26, Koi Security disclosed “PackageGate,” six zero-day flaws in JavaScript package managers that bypass lifecycle script disablement and lockfile integrity protections widely adopted after prior supply-chain attacks. Researchers found bypass techniques in npm, pnpm, vlt and Bun, but while others patched the issues, the npm project declined to address its vulnerabilities, stating users must vet packages manually. `zero-day` link

Microsoft Office CVE-2026-21509 zero-day exploited
On January 26, Microsoft reported a high-severity zero-day vulnerability, CVE-2026-21509, affecting multiple Microsoft Office versions and actively exploited in attacks. The flaw allows local attackers to bypass security features via malicious files requiring user interaction. No threat actor attribution was provided. The issue impacts global users, with partial mitigations available while patches for Office 2016 and 2019 remain pending. `zero-day` link

Fortinet FortiSIEM CVE-2025-64155 exploit release
On January 13, Horizon3.ai reported the discovery and public release of exploit code for CVE-2025-64155, a critical unauthenticated command injection vulnerability in Fortinet FortiSIEM. The flaw enables remote code execution and potential full system compromise. While no active exploitation has been confirmed, the release significantly increases the risk of global targeting by threat actors, given Fortinet's history of being a frequent attack vector. `Fortinet` link

Active exploitation of a critical RCE vulnerability in Cisco Unified Communications products
On January 21, Cisco disclosed and patched a critical Unified Communications and Webex Calling remote code execution zero-day, CVE-2026-20045, actively exploited to gain root access via crafted HTTP requests against management interfaces. The flaw affects Unified CM, IM & Presence, SME, Unity Connection, and Webex Calling Instance. Cisco urges upgrades, notes no workarounds, confirms in-the-wild exploitation, and says CISA added it to the Known Exploited Vulnerabilities Catalog with a February 11, 2026 deadline. `zero-day` link

Coordinated LLM SSRF and enumeration campaigns
On January 8, GreyNoise reported two coordinated campaigns targeting global LLM infrastructure. One exploited SSRF vulnerabilities to trigger outbound connections, likely by grey-hat actors, while another conducted large-scale endpoint enumeration linked to a professional threat actor. Over 91.000 sessions were recorded, indicating systematic reconnaissance and potential preparation for exploitation against exposed AI services worldwide. 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.

TLP	Disclosure	Message
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.