CERT-EU

Cyber Brief (February 2026)

March 2, 2026 – Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 303 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, the European Commission preliminarily found TikTok to be in breach of the Digital Services Act for its addictive design, while French authorities raided social media platform X Paris headquarters in an ongoing cybercrime investigation. Additionally, the United States sanctioned entities linked to an exploit broker network for the theft and sale of US government cyber tools.
- On the **cyberespionage** front, a Signal messaging app phishing campaign reportedly targeted high-profile figures across Europe, while Russia-linked APT28 weaponised CVE-2026-21509 in a campaign targeting users in Central and Eastern Europe. We noted several global China-linked campaigns, such as APT group Lotus Blossom's Notepad++ supply-chain compromise and UNC2814's campaign targeting telecoms and government entities worldwide.
- In regards to **cybercrime**, we observed a trend in threat actors targeting common AI assistant ecosystems. In early February, a large-scale supply-chain attack reportedly abused the OpenClaw AI assistant ecosystem, while a coordinated campaign by unknown threat actors leveraged fake AI assistant extensions in Chrome.
- In terms of **digital foreign interference**, a pro-Russia Storm-1516 disinformation campaign reportedly falsely associated French President Emmanuel Macron with Jeffrey Epstein.
- There were **disruptive** DDoS attacks that targeted Deutsche Bahn in Germany, and Romanian oil pipeline operator Conpet suffered a cyberattack claimed by the Qilin ransomware group.
- Regarding **data exposure and leaks** incidents, Dutch telecom provider Odido experienced a major data breach involving millions of customer records, while an unknown threat actor accessed France's national banking accounts database via stolen credentials. Further, Microsoft reported a 365 Copilot bug that allowed it access to e-mails marked as confidential.
- On the **hacktivism** front, pro-Ukraine hacktivists Fenix Cyber Analytical Center reportedly breached Russian Drone Systems to support Ukrainian military operations.

- As for **opportunistic** attacks, Ivanti Endpoint Manager Mobile (EPMM) critical zero-day vulnerabilities CVE-2026-1281 and CVE-2026-1340 were exploited in the wild, Microsoft addressed six actively exploited zero-days, and unknown threat actors actively exploited SolarWinds Web Help Desk vulnerabilities (CVE-2025-26399 and CVE-2025-40551).

For more information regarding CERT-EU's analytical and operational standards to classify, assess, and prioritise malicious cyber activities, please review our Cyber Threat Intelligence Framework here.

Europe

Cyber policy and law enforcement

European Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act
On February 6, the European Commission preliminarily found TikTok in breach of the Digital Services Act for its addictive design. The features like infinite scroll, autoplay, push alerts and personalised recommendations breach the EU's Digital Services Act and harm users, including minors and vulnerable adults. `policy` link

Sweden and Ukraine sign Memorandum of Understanding on cybersecurity cooperation
On February 12 Sweden and Ukraine signed a Memorandum of Understanding valid for five years on cybersecurity cooperation, aiming to strengthen both countries' resilience to cyberattacks. `cooperation` link

French headquarters of Elon Musk's X raided by Paris cybercrime unit
On February 3, French prosecutors' cybercrime unit raided the Paris headquarters of Elon Musk's social media platform X as part of a long-running investigation into alleged algorithm manipulation and other offences, including spreading child abuse imagery and explicit deepfakes. `artificial intelligence` `law enforcement` link

Suspected China-linked espionage case involving four individuals in France
On February 5, French authorities placed four people, including two Chinese nationals, under formal investigation on suspicion of spying for China. They are accused of trying to capture and transmit sensitive data, including satellite and military information, to China. `china` link

Greek court convicts Intellexa executives in Predator spyware wiretapping scandal
On February 26, a Greek court found Intellexa founder Tal Dilian and three others guilty of breaching personal data linked to the country's wiretapping scandal, sentencing them to prison terms capped at eight years for illegal surveillance conducted between 2020 and 2021. The ruling, connected to the Predator spyware case affecting journalists and politicians, also prompted prosecutors to pursue further investigations into potential serious offences, including espionage. `psoa` link

Cyberespionage & prepositioning

Signal Messenger phishing campaign targeting high-profile figures in Europe
On February 6, German authorities reported a sophisticated phishing campaign impersonating Signal's support bot, urging users to re-enter PINs or re-register devices. The attack, suspected

to be state-sponsored, targeted politicians, military personnel, and journalists across Europe. Victims were urged to contact Bundesverfassungsschutz or BSI. `public administration` Link

Russia-linked APT28 Operation Neusploit via CVE-2026-21509
On February 3, Zscaler ThreatLabz reported that Russia-linked APT28 conducted Operation Neusploit, exploiting CVE-2026-21509 in malicious RTF files to target Ukraine, Slovakia, and Romania. The campaign delivered e-mail-stealing and backdoor malware, enabling data theft and remote access. This activity demonstrates APT28's continued focus on Central and Eastern Europe and its rapid adoption of newly disclosed Microsoft Office vulnerabilities. `public administration` `russia` link

Russian spacecraft intercept European satellites
On February 4, EU officials warned that for several years, two Russian satellites, Luch-1 and Luch-2, have carried out repeated suspicious manoeuvres in orbit. Since 2023, Luch-2 has crept beside at least 17 European civilian-and-government satellites, harvesting unencrypted command links; the data could let Moscow spoof orbital instructions, misalign or crash craft, and map users for future jamming. `space` `telecommunications` `russia` link

Russia-linked Mercenary Akula (aka UAC-0050) spearphishing targeting Ukraine-supporting bank advisor
On February 24, BlueVoyant reported a spearphishing campaign by Russia-linked Mercenary Akula (UAC-0050) against a European financial institution supporting Ukraine. The attack spoofed Ukrainian judicial domains to target a senior legal advisor, aiming to gain remote access for intelligence gathering or financial theft. This incident suggests the group may be expanding operations beyond Ukraine to Western Europe-based, Ukraine-supporting entities. `finance` `russia` link

China-linked cyberespionage on Italian government ministry
On February 23, the Italian media La Repubblica reported a suspected China-linked espionage campaign targeting an Italian government ministry between 2024 and 2025. The operation allegedly stole sensitive data on around 5.000 law enforcement agents, including those investigating Chinese dissidents and organised crime. The breach likely served counterintelligence purposes, though attribution remains unconfirmed due to a lack of technical indicators. `public administration` `defence` `china` link

Cybercrime

Diesel Vortex freight phishing campaign
On February 24, Have I Been Squatted reported that the Diesel Vortex threat group conducted a phishing campaign targeting freight and logistics organisations in the US, Germany, France, and Lithuania. Active since September 2025, the group stole over 1.600 unique credentials from major industry platforms, enabling fraud and cargo diversion, and causing significant disruption to supply chain operations. `transport` link

Digital foreign interference

Pro-Russia Storm-1516 Macron-Epstein disinformation campaign
On February 6, French authorities reported a pro-Russia Storm-1516 disinformation campaign falsely associating President Emmanuel Macron with Jeffrey Epstein. The operation used a fake France-Soir website and fabricated e-mails, amplified via X, to damage Macron's reputation. French authorities removed the counterfeit site, but videos persisted online. `public administration` `russia` link

Disruption & destruction

Deutsche Bahn targeted DDoS disruption
On February 18, Deutsche Bahn reported a targeted distributed denial of service attack that disrupted its ticketing and travel information systems. The attack occurred in waves, causing outages on its website and Navigator app. Defensive measures restored partial service, with customer data protection and system availability prioritised. `transport` link

Conpet ransomware attack by Qilin group
On February 5, BleepingComputer reported that Romanian oil pipeline operator Conpet suffered a cyberattack claimed by the Qilin ransomware group. The incident disrupted corporate IT systems and took down the company's website, though operational technologies remained unaffected. Qilin alleges theft of nearly 1TB of sensitive data, including financial records and passport scans. `energy` link

Data exposure and leaks

Netherlands-based telecom provider Odido customer data breach
On February 16, NU.nl reported that telecom provider Odido suffered a major data breach by an unknown threat actor involving millions of customer records, including names, addresses, phone numbers and bank account details. Passwords were not compromised. The breach was disclosed to the Dutch Data Protection Authority, and customers were urged to remain vigilant against potential fraud. `telecommunications` link

French national banking accounts database breach via credential theft
On February 19, the French Ministry of Economics, Finance and Industrial and Digital Sovereignty reported that a malicious actor accessed the national banking accounts database (FOCOBA) by using stolen credentials of a government official. The breach exposed personal and banking details of approximately 1.2 million accounts in France, prompting alerts to affected users and coordination with banks to mitigate potential fraud. `finance` link

Hacktivism

Pro-Ukraine hacktivists breach Russian Drone Systems to support Ukrainian military operations
On February 21, Militarnyi reported that pro-Ukraine Fenix Cyber Analytical Center, working with the InformNapalm intelligence community, breached Russian military accounts and monitored drone-operator systems, revealing how Russia uses Belarusian civilian infrastructure to guide UAV attacks against Ukraine and test routes near NATO territory. `ukraine` link

World

Cyber policy and law enforcement

United States Treasury sanctions exploit broker network for theft and sale of US government cyber tools
On February 24, the United States Treasury's Office of Foreign Assets Control sanctioned a Russia-based company known as Operation Zero, along with five associated individuals and entities, for trafficking in stolen cyber 'exploits' that target software vulnerabilities and threaten US national security. The action, the first under the Protecting American Intellectual Property

Act, follows a related case involving the theft and sale of proprietary cyber tools to illicit overseas buyers. `russia` `sanctions` link

Cyberespionage & prepositioning

China-linked TGR-STA-1030 "Shadow Campaigns" target government ministries across 37 countries
On February 5, Unit 42 reported on TGR-STA-1030, a state-aligned cyberespionage group operating from Asia conducting Shadow Campaigns. Over the past year, the group compromised government and critical infrastructure organisations across 37 countries, including five national law enforcement entities and three finance ministries. Reconnaissance activities targeted 155 countries between November and December 2025, focusing on economic partnerships and natural resources. `china` link

Disruption of China-linked GRIDTIDE global cyberespionage operation targeting telcos and government
On February 25, Google Threat Intelligence reported the disruption of UNC2814's global cyberespionage campaign leveraging the GRIDTIDE backdoor. The suspected China-linked group targeted telecommunications and government entities across 42 confirmed and 20 suspected countries, using cloud-based API abuse for covert command-and-control. The coordinated takedown severed attacker access, dismantled infrastructure, and mitigated the threat's extensive surveillance capabilities. `china` link

Notepad++ supply-chain compromise by China-linked Lotus Blossom
On February 11, Palo Alto reported that between June and December 2025, the official hosting infrastructure for the text editor Notepad++ had been compromised by a China-linked APT group Lotus Blossom. The campaign selectively targeted administrators and developers in multiple global sectors, including government, energy and finance, delivering backdoors for likely long-term intelligence gathering without disrupting operations. `public administration` `technology` `telecommunications` `finance` `energy` `china` link

Dell RecoverPoint zero-day exploitation by China-linked UNC6201
On February 17, Google Threat Intelligence Group (GTIG) reported that China-linked UNC6201 was exploiting CVE-2026-22769 in Dell RecoverPoint for Virtual Machines since mid-2024, allowing lateral movement, persistent access, and the deployment of malware including SLAYSTYLE, BRICKSTORM, as well as a novel backdoor tracked as GRIMBOLT. `china` link

GitLab disrupts North Korean IT workers campaigns
On February 19, GitLab Threat Intelligence Team reported disrupting North Korea-linked campaigns involving Contagious Interview malware distribution and fraudulent IT worker operations. These actors targeted global software developers, stealing credentials and enabling remote control of devices. GitLab banned 131 accounts in 2025 linked to these activities, exposing infrastructure and tradecraft to aid industry-wide defence against evolving threats. `north korea` link

Cybercrime

Malicious Chrome AI extensions campaigns
On February 12, cybersecurity firm LayerX reported a campaign distributing malicious Chrome extensions posing as popular AI assistants. The operation, impacting over 260,000 users, leveraged remote-controlled iframes to harvest sensitive data and evade takedowns through extension spraying. While the threat actor remains unidentified, the campaign exploited trusted

AI branding to gain widespread installation and facilitate persistent surveillance across user environments. `artificial intelligence` link

ClawHavoc malicious skills campaign steals crypto keys and credentials
On February 2, Koi researchers reported a large-scale supply-chain attack abusing the OpenClaw AI assistant (formerly Clawdbot/Moltbot) ecosystem, with at least 341 malicious "skills" published to ClawHub and GitHub that deliver info-stealing malware targeting cryptocurrency API keys, wallet private keys, SSH credentials and browser passwords. Many skills mimic legitimate utilities to trick users into execution. `artificial intelligence` `technologies` `finance` link

OpenClaw AI personal assistant identity theft via infostealer
On February 17, Hudson Rock reported a live infostealer infection targeting personal AI assistant OpenClaw software, resulting in theft of configuration files, cryptographic keys, and personal AI context. The attack enabled potential impersonation and access to sensitive data, marking a shift towards AI-focused data theft. No specific threat actor was identified, but the incident highlights growing risks to AI-integrated workflows. `artificial intelligence` link

Shai-Hulud-style npm worm targets CI and AI toolchains
On February 20, Socket Research Team reported an active Shai-Hulud-style npm supply chain worm campaign spreading via typosquatting, stealing CI secrets, and compromising AI coding assistants. Linked to two npm aliases, the threat targets developers globally, enabling lateral movement and persistence across repositories. The campaign poses high risk to software supply chains, with destructive capabilities and broad propagation potential. `technology` `artificial intelligence` link

LummaStealer malware resurgence via CastleLoader
On February 11, Bitdefender reported a global resurgence of LummaStealer, coordinated with CastleLoader infrastructure, despite a major 2025 law-enforcement takedown. The infostealer, linked to the GrayBravo threat actor, is spreading through social engineering lures such as fake CAPTCHAs. The campaign enables large-scale credential theft, financial fraud, and identity compromise, affecting victims worldwide across multiple sectors. link

Malicious Next.js repositories targeting developers
On February 24, Microsoft Defender Experts and Microsoft Defender Security Research Team reported a coordinated campaign using malicious Next.js repositories to target software developers. The operation disguised projects as legitimate technical assessments, leading to remote code execution and potential theft of source code, credentials, and cloud access. `technology` link

Data exposure and leaks

Microsoft 365 Copilot confidential e-mail summarisation bug
On February 18, Microsoft reported a bug in Microsoft 365 Copilot Chat, active since late January, that summarised confidential e-mails from Sent Items and Drafts, bypassing Data Loss Prevention policies. Microsoft attributed the issue to a code error, began deploying a fix in early February, and is monitoring remediation across affected enterprise customers globally. link

Substack user data breach exposes e-mails and phone numbers
On February 5, Substack confirmed a data breach in which an unauthorised third party accessed user e-mail addresses, phone numbers, and internal metadata. The incident, occurring in October 2025, was detected five months later. No financial data was compromised. The number of affected users remains undisclosed, though Substack hosts over 50 million subscriptions globally. link

Opportunistic

Ivanti EPMM vulnerability CVE-2026-1281 exploited in the wild
On February 10, Greynoise Research observed active exploitation of two critical zero-day vulnerabilities for Ivanti Endpoint Manager Mobile (CVE-2026-1281 and CVE-2026-134), first reported in late January. Greynoise's report indicated 83% of attacks came from a single bulletproof-hosting IP address not widely circulated on IOC lists. Many widely shared indicators actually targeted unrelated software, highlighting a detection gap. `zero-day` link

AI-assisted AWS intrusion achieves administrative access in eight minutes via credential theft
On February 3, Sysdig disclosed an AI-assisted intrusion targeting an AWS environment where threat actors achieved administrative privileges in under 10 minutes. Initial access was gained through credentials discovered in public S3 buckets. Multiple indicators suggest large language models were leveraged throughout the operation to automate reconnaissance and generate malicious code. link

Microsoft February 2026 Patch Tuesday addresses six actively exploited zero-days
On February 10, Microsoft's February 2026 Patch Tuesday addressed 58 vulnerabilities, including six actively exploited zero-days. Threat actors reportedly exploited these vulnerabilities to bypass security warnings and escalate privileges to system level. `zero-day` link

SolarWinds WHD Exploitation with RMM and Velociraptor C2
On February 9, Huntress reported active exploitation of SolarWinds Web Help Desk vulnerabilities (CVE-2025-26399 and CVE-2025-40551) by unidentified threat actors, deploying remote management tools and Velociraptor for command and control. The campaign affected multiple organisations globally, enabling persistence, reconnaissance, and disabling of security controls. 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.