CERT-EU

Cyber Brief (October 2025)

November 3, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 281 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, the European Commission published a landmark report on the resilience of European data cable infrastructure. A joint law enforcement operation with Europol dismantled a fraudulent SIM box operation, and 65 countries signed the first United Nations treaty to combat cybercrime.
- On the **cyberespionage** front, China-linked Salt Typhoon and Flax Typhoon were observed collaborating in a Premier Pass-as-a-Service scheme. Graphite spyware targeted an Italian businessman and journalists using zero-click attacks, and China-linked UTA0388 engaged in a global e-mail spearphishing campaign that likely leveraged LLMs.
- There were **disruptive** attacks on Latvian state websites, causing a significant disruption in service, and an attack on the Dutch Public Health Institute RIVM caused a temporary shutdown. Pro-Russia hacktivists breached a decoy water-treatment plant HMI.
- Regarding **data exposure and leaks** incidents, Stormous cybercrime group reportedly breached France Travail using an automated credential stuffing attack, and a Swedish national electric grid operator was breached via an external file transfer system. US company F5 disclosed a nation-state intrusion that stole undisclosed vulnerabilities and source code.
- As for **opportunistic** attacks, Broadcom disclosed a zero-day being exploited by China-linked threat actors, while Getsafety uncovered a fake npm package posing as Anthropic’s Claude tool. Koi researchers observed a supply chain attack in which a self-propagating worm, GlassWorm, compromised Microsoft's VSCode marketplace.

Europe

Cyber policy and law enforcement

Security of Cables: Commission publishes landmark report and funding for Cable Hubs

On October 23, the European Commission published a landmark report assessing the resilience of Europe’s submarine data-cable infrastructure, identifying seven main risk scenarios, guidance for stress-testing and launching a 10 million euros call under the Digital Europe Programme to establish regional “cable hubs” to monitor threats and reinforce resilience. `guidance` link

Joint operation SIMCARTEL dismantles fraudulent SIM box operation
On October 10, Europol officials alongside Eurojust, Austria, Estonia and Latvia, collaborated to dismantle a criminal network engaged in fraudulent SIM box operations. They arrest five Latvian cybercriminals, took down five servers and seized 1.200 SIM box devices alongside 40.000 active SIM cards. Investigators attributed over 1.700 cyber fraud cases in Austria and Latvia to the criminal network. `takedown` link

Spain dismantles GXC Team cybercrime network
On October 9, Spain’s Guardia Civil announced they dismantled the GXC Team cybercrime group, led by a 25-year-old Brazilian known as “GoogleXcoder.” The gang sold AI-powered phishing kits, Android malware, and voice-scam tools via Telegram, targeting banks and companies worldwide. Coordinated raids across Spain seized electronic devices, stolen cryptocurrency, and shut down scam channels. `takedown` link

Azerbaijan–Slovakia cybersecurity cooperation talks
On October 8, Azerbaijan and Slovakia met to discuss cybersecurity cooperation, focusing on critical infrastructure, with options for experience-sharing and joint public–private projects. On October 9, military officials also met to explore technical and training exchanges, including cybersecurity for weapons systems and IT, with mention of AI-enabled cybersecurity tools. `cooperation` link

Cyberespionage & prepositioning

China-linked Salt Typhoon and Flax Typhoon collaborating in Premier Pass-as-a-Service scheme
On October 22, Trend Micro revealed a “Premier Pass-as-a-Service” collaborative scheme between China-aligned groups Salt Typhoon and Flax Typhoon, with one providing access, the other exploiting it. Victims include government agencies, aerospace and defence contractors, and technology firms across Asia and Europe. This partnership-as-a-service model complicates attribution and detection, prompting Trend Micro to propose a four-tier framework to analyse such operations. `china` link

China-linked Salt Typhoon targets European telecom organisation
On October 20, Darktrace reported that the China-linked cyberespionage group Salt Typhoon targeted a European telecommunications organisation in July 2025, beginning with a compromise of a Citrix NetScaler appliance. They used DLL sideloading via legitimate antivirus software and multi-channel C2 infrastructure to execute the backdoor SNAPPYBEE and conduct stealthy exfiltration. `china` link

North Korea-linked Lazarus Group targets the UAV sector
On October 23, ESET revealed that the North Korea-aligned APT group Lazarus Group resumed its “Operation DreamJob” campaign targeting European defence firms, especially in the unmanned aerial vehicle (UAV) sector. Their goal was likely to steal proprietary UAV-related technology and know-how using job-offer lures and trojanised open-source tools. `north korea` link

Graphite spyware targets Italian businessman and journalists
On October 9, Irpi Media revealed that Israeli-made Graphite spyware, developed by Paragon Solutions, was used in highly targeted zero-click attacks against at least seven Italian individuals, including businessman Francesco Gaetano Caltagirone, journalists, and activists.

The campaign's origin remains unclear, with the possible involvement of state actors. `psoa` link

Disruption & destruction

Latvian state websites hit by cyberattack
On October 2, several Latvian state websites, including those on the gov.lv platform and eParaksts.lv, experienced a cyberattack that caused a significant service outage. The Latvian State Radio and Television Centre (LVRTC) confirmed that the affected websites were fully restored after approximately one hour and 20 minutes. `public administration` link

Dutch Public Health Institute RIVM shuts website following cyberattack
On October 14, the Dutch Public Health Institute (RIVM) shut down its website around 11:15 a.m. after detecting a cyberattack exploiting a vulnerability in an outdated web-form plugin. The site later came back online, though data submission forms remained temporarily disabled while security gaps were addressed. `health` link

Hacktivists tamper with decoy water plant after rapid web-layer breach
On October 9, Forescout reported that pro-Russia hacktivists "TwoNet" breached a decoy water-treatment HMI with default credentials. Within 26 hours of initial access, they used an old XSS vulnerability (CVE-2021-26829) to broadcast "Hacked by Barlati," disabled logs, alarms, and removed PLCs from data sources and changed their setpoints. `water` link

Data exposure and leaks

Stormous cybercrime group breached France Travail with an automated credential stuffing attack
On October 27, Stormous cybercrime group reportedly breached France Travail with an automated credential stuffing attack. The group allegedly leveraged stolen credentials and exploited a vulnerability in France Travail's backend PDF generation API to download victim documents. They also claimed to have automatically exfiltrated the data of 30.257 user accounts which included identification, bank information, work history, and salary records. `labour` link

Data breach affecting Swedish national electric grid operator Svenska kraftnät
On October 25, Svenska kraftnät identified a data breach involving an external file transfer system but stated that mission-critical systems or the transmission of electricity were unaffected. The threat actor "Everest" claimed responsibility for the breach, alleging they stole 280GB of data. `energy` link

World

Cyber policy and law enforcement

65 countries sign first UN Cybercrime Treaty, marking global milestone
On October 25, 65 countries signed the first United Nations treaty to combat cybercrime, marking a milestone for global digital cooperation. The Convention against Cybercrime establishes a universal framework for investigating and prosecuting online offences, from ransomware to image-based abuse, enhancing cross-border evidence sharing and law enforcement collaboration, while safeguarding privacy and human rights. `cooperation` link

Russia reportedly actively managing cybercriminal groups
On October 23, Recorded Future reported that the Russian government has moved from tolerating cybercriminal groups to actively managing them. Since 2023, Russian authorities have coordinated arrests, leveraged hackers as geopolitical tools, and selectively enforced laws to balance foreign pressure and domestic interests, turning cybercrime into both a strategic asset and a controlled liability within Russia's evolving state-cybercriminal ecosystem. `russia` link

Russia enforces 24-hour block on foreign SIMs
On October 6, Russian mobile users reported that foreign SIMs went dark for 24 hours as authorities enforced a policy blocking non-Russian SIM cards that register inside Russia, reportedly to disrupt drone operators. Blocks trigger on network registration and can reapply after inactivity; carriers were instructed to implement the measure. The disruption also affected neighbouring CIS countries' users. `russia` link

Revelations on Group 78, a secret US Cybercrime Unit
On October 16, Le Monde revealed that a secret US unit called Group 78 operates with the mission to combat cybercrime. The unit was introduced in November 2024 to European police and judicial authorities, proposing strategies including covert action in Russia to force cybercriminal actors to relocate and be apprehended. `united states` link

Project Nimbus included secret 'wink' mechanism to alert Israel on data disclosures to foreign authorities
On October 29, several newspapers jointly reported that under Project Nimbus, a cloud contract established in 2021, Israel required Google and Amazon Web Services to send "coded" payments, a so-called "winking" mechanism, to alert Israel when either firm disclosed Israeli data to foreign authorities under a gag order. They were also allegedly barred from suspending Israel's access to their cloud services, even if terms of service were breached. `israel` link

Cyberespionage & prepositioning

China-linked threat actor UTA0388 leveraging LLMs in global spearphishing operations
On October 8, Volexity reported on spearphishing campaigns from China-linked threat actor UTA0388. The threat actor sent e-mails in several languages, including English, Chinese, Japanese, French, and German. The e-mails contained a link to a malicious ZIP file containing Govershell malware. Volexity assessed that UTA0388 is very likely leveraging Large Language Models in their operations. `china` link

ArcGIS turned into a web shell in an incident attributed to China-linked Flax Typhoon
On October 14, ReliaQuest reported that the China-linked APT Flax Typhoon compromised an ArcGIS system, a geographic information system used to manage and analyse spatial data. They converted a trusted Java server object extension into a persistent web shell. They used a hardcoded key and embedded it in backups, maintaining over a year of covert access, enabling command execution, lateral movement, and credential harvesting across multiple hosts. `china` link

Chinese MSS accuses the US NSA of targeting its National Time Service Center
On October 19, the Chinese Ministry of State Security reported that the US National Security Agency targeted its National Time Service Center. They reportedly found evidence dating back to at least March 2022 in which the NSA allegedly exploited a vulnerability in the messaging service of a foreign smartphone brand to access staff members' phones. `china` `united states` link

Russia-linked Coldriver delivers new malware using ClickFlix and Captcha lure
On October 20, Google Threat Intelligence reported on the Russia-linked group Coldriver

deploying a new malware chain that combines the ClickFix technique with a Captcha lure. Throughout 2025, multiple threat actors, some state-sponsored, have adopted ClickFix. `russia` link

Callisto's new multi-stage ClickFix campaign targeting members of Russian civil society
On September 24, Zscaler ThreatLabz reported a multi-stage ClickFix phishing campaign attributed with moderate confidence to Russia-linked COLDRIVER (Callisto). The operation targeted Russian civil society, deploying the BAITSWITCH downloader and SIMPLEFIX backdoor to enable persistence, reconnaissance, and data exfiltration. `russia` link

Cybercrime

LockBit ransomware returns with new 5.0 variant, targeting global organisations
On October 23, Check Point reported that the LockBit ransomware group has reemerged after its early 2024 disruption, launching new attacks across Europe, America, and Asia. A dozen organisations were targeted in September, half by the new LockBit 5.0 “ChuongDong” variant, which features faster encryption, stronger evasion, and cross-platform capability. `russia` link

Clop ransomware targets Oracle E-Business Suite users with extortion e-mails
On October 1 and 3, Bleeping Computer reported that a Clop ransomware campaign sent extortion e-mails to executives and IT staff at multiple companies, claiming theft of Oracle E-Business Suite (EBS) data and threatening leaks unless paid. Oracle linked the campaign to vulnerabilities patched in its July 2025 Critical Patch Update, advising customers to apply updates to prevent potential exploitation. No confirmed breaches were reported. `russia` link

Microsoft disrupts ransomware attacks targeting Teams users
In early October 2025, Microsoft disrupted a ransomware campaign enacted by cybercriminal group Vanilla Tempest (aka Vice Spider). Microsoft revoked over 200 certificates that the threat actor had fraudulently signed and used in fake Teams setup files to deliver Oyster backdoor and Rhysida ransomware. link

Data exposure and leaks

F5 breach exposes BIG-IP source code and undisclosed flaws
On October 15, F5 disclosed a nation-state intrusion first detected on August 9 that maintained long-term access to its BIG-IP product development and engineering knowledge platforms. F5 reported no supply-chain impact or malicious code changes and no evidence of exploitation to date. The disclosure was delayed at the US government's request. link

Crimson Collective claims Red Hat breach and data theft
On October 2, threat group Crimson Collective claimed to have breached Red Hat’s private repositories, stealing 570GB of internal data including sensitive customer reports. Red Hat confirmed a consulting-related security incident but did not verify the group’s claims. The alleged stolen data reportedly covers major global organisations across multiple sectors. link

ShinyHunters launches Salesforce data leak site to extort 39 victims
On October 3, cybercrime group ShinyHunters reportedly launched a data leak site to publicly extort 39 companies impacted by Salesforce breaches. The site includes data samples from victims, warning them to act before an October 10 deadline to prevent full disclosure. The group claimed to have stolen approximately 1.5 billion Salesforce records using compromised Salesloft Drift OAuth tokens. link

Opportunistic

VMware zero-day CVE-2025-41244 exploited by China-linked UNC5174

On September 29, 2025, Broadcom disclosed CVE-2025-41244, a local privilege escalation vulnerability in VMware's guest service discovery features. NVISO identified zero-day exploitation of this flaw by the Chinese state-sponsored group UNC5174 since mid-October 2024. The vulnerability affects both VMware Tools and VMware Aria Operations, enabling unprivileged users to execute code in privileged contexts. `china` link

Zimbra zero-day vulnerability exploited via malicious iCalendar files

On September 30, Strikeready reported that attackers exploited a Zimbra XSS (CVE-2025-27915) zero-day via oversized .ICS iCalendar files containing obfuscated JavaScript, launching strikes from early January and spoofing the Libyan Navy to target a Brazilian military organisation. The payload harvested credentials, e-mails, contacts, added mail-forwarding filters, exfiltrated data periodically. Zimbra patched the flaw on January 27 while stating exploitation does not appear to be widespread. link

GlassWorm supply chain worm compromises IDE marketplaces

On October 18, Koi researchers uncovered GlassWorm compromising OpenVSX and VSCode extensions using invisible Unicode to hide code and Solana blockchain C2 with Google Calendar fallback. The threat actor steals GitHub, npm, Git and OpenVSX credentials, deploys RAT features (SOCKS proxy, HVNC), targets crypto wallets, and self-propagates via stolen accounts. At least seven extensions and roughly 35.800 installs were affected; several remained active. link

PhantomRaven: malicious npm packages execute credential-stealing malware via hidden dependencies

On October 29, Koi Security reported the PhantomRaven campaign, in which an unknown threat actor distributed 126 malicious Node Package Manager (npm) packages globally. The malware concealed itself in remote dynamic dependencies to evade detection, harvesting developer credentials and CI/CD secrets. Over 86.000 downloads were recorded, impacting corporate networks, cloud environments, and individual developers through automated execution during package installation. link

Typosquatted npm packages execute credential stealer on install

Socket.dev reported 10 malicious typosquatted npm packages imitating popular libraries. The packages run automatically during npm install via postinstall, show a fake Captcha, fingerprint the system, and fetch a 24 MB cross-platform binary called data_extracter. The binary steals browser passwords, SSH keys, tokens and other secrets from developer machines on Windows, Linux and macOS, then exfiltrates the data to attacker infrastructure. link

Malicious npm package impersonates Claude Code to exfiltrate data via C2

On October 27, Getsafety uncovered a fake npm package posing as Anthropic’s Claude tool. Published since August with 19 versions, it installs a look-alike “claude” command that steals keys, profiles the device, and plants files. It then taps into real Claude traffic, capturing prompts and account data and sending them to a rogue server. 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.