CERT-EU

Cyber Brief (April 2026)

May 4, 2026 – Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 366 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, the Council of the European Union sanctioned several Russian entities and individuals for supporting Russian hybrid activities, while Austrian and Albanian law enforcement, supported by Europol and Eurojust, arrested individuals involved in crypto fraud worth 50 million euros. Europol supported a global operation involving 21 countries against DDoS-for-hire users.
- On the **cyberespionage & prepositioning** front, Russia-linked threat actors reportedly conducted reconnaissance against France's nuclear deterrent communications ecosystem. Two China-linked threat actors engaged in phishing campaigns targeting diaspora activists and journalists globally.
- In regards to **cybercrime**, cyberattacks continued to target the software development ecosystem globally: a threat actor pushed a malicious version of a popular elementary-data package Python Package Index (PyPI) to load an infostealer, while North Korea-linked Contagious Interview reportedly engaged in a supply-chain operation deploying malicious packages across npm, PyPI, Go Modules, crates.io, and Packagist.
- As for **disruptive & destructive** cyberattacks, a supposed hacktivist group claimed control of Venice San Marco flood defence pumps in Italy. The US Cybersecurity and Infrastructure Security Agency (CISA) reported that Iranian state-sponsored threat actors had been targeting internet-exposed programmable logic controllers across US critical infrastructure, while Iran-linked 313 Team claimed responsibility for a DDoS attack against social media platform Bluesky.
- Regarding **data exposure and leaks**, France's National Agency of Secure Titles (ANTS) disclosed a security incident potentially exposing users' personal data, for which a minor was taken into custody over suspected involvement. Additionally, researchers alleged that hundreds of Hungarian government e-mail addresses and associated passwords were found across online breach databases, affecting most government ministries.

- In terms of **opportunistic** attacks observed globally, a fake website impersonating Anthropic's Claude reportedly distributed a trojanised Windows installer, while an npm supply-chain worm reportedly stole tokens and self-propagated via compromised packages.
- As for notable **Common Vulnerabilties and Exposures (CVEs)**, Fortinet released an update for an Improper Access Control vulnerability in FortiClient EMS (CVE-2026-35616), while CISA reported active exploitation of a Microsoft SharePoint spoofing vulnerability CVE-2026-32201.

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

Europe

Cyber policy and law enforcement

The Council of the European Union sanctioned two entities tied to Russia's digital foreign interference operations
On April 21, the Council of the EU imposed restrictive measures on Euromore and Pravfond for supporting Russian hybrid activities. The entities spread disinformation, legitimised Kremlin narratives, and undermined EU institutions and Ukraine. The measures include asset freezes and funding bans, bringing totals to 69 individuals and 19 entities under the EU's sanctions regime against destabilising actions. `russia` `sanctions` link

Europol-supported operation targeted over 75.000 DDoS-for-hire users in 21 countries
On April 13, Europol supported a global operation involving 21 countries against DDoS-for-hire users, leading to four arrests, 25 search warrants, 53 domain takedowns and more than 75.000 warning messages sent to identified criminal users. The action also disrupted booter infrastructure and used seized data to identify millions of criminal user accounts, supporting Operation PowerOFF's wider enforcement and prevention efforts. `law enforcement` link

CERT-EU's response to AI vulnerability discovery developments
On April 21, CERT-EU shared its analysis related to AI-powered tools discovering and exploiting vulnerabilities faster than traditional patch cycles, with exploitation occurring before patches exist. In response, CERT-EU has developed an AI-powered penetration testing pipeline and recommended eight defensive actions, ranging from reducing the attack surface, adopting AI security testing responsibly, and building cross-functional teams. `artificial intelligence` link

The chair of the European Securities and Markets Authority warned cyber threats are growing as AI speeds up risks
On April 24, the chair of the European Securities and Markets Authority warned cyber threats are rising as AI accelerates attacks' speed and complexity, urging stronger oversight, improved cybersecurity in finance, and tighter regulation, including action against unlicensed crypto firms. `artificial intelligence` link

Alleged Silk Typhoon member extradited from Italy to the United States
On April 27, the US Department of Justice announced the extradition of a Chinese national from Italy to face charges related to cyberespionage. He allegedly worked as a contracted hacker for China's Ministry of State Security, operating under the Silk Typhoon group. Between February 2020 and June 2021, he allegedly exploited Microsoft Exchange zero-days to breach thousands of organisations and steal sensitive data. `law enforcement` `china` link

Austrian and Albanian authorities dismantled crypto investment fraud ring worth 50 million euro

On April 17, Austrian and Albanian authorities, supported by Europol and Eurojust, arrested ten suspects and searched three call centres and nine residences in Tirana, dismantling a criminal network responsible for at least 50 million euros in fraud losses. Victims across Italy, Germany, Greece, Spain, Canada, and the United Kingdom (UK) were lured to fake cryptocurrency investment platforms via social media. `law enforcement` link

Cyberespionage & prepositioning

Russian reconnaissance targeted French nuclear deterrent communications

On April 16, Russia-linked cyber operatives reportedly conducted reconnaissance against France's nuclear deterrent communications ecosystem. Campaigns since early March reportedly focused on mapping low/very low frequency transmission sites, continuity and redundancy mechanisms, and associated personnel. Targeting also extended to staff linked to the Joint Directorate of Infrastructure Networks and Information Systems (DIRISI) and key contractors, aiming to profile dependencies across military communications supporting SSBN and strategic forces, potentially enabling future disruption. `defence` `russia` link

APT28 router compromise enabled DNS hijacking and credential theft

On April 8, the UK's National Cyber Security Centre and Microsoft reported that APT28 has been compromising SOHO routers since at least 2024 to redirect DNS traffic through actor-controlled servers. This enables Adversary-in-the-Middle attacks targeting Microsoft Outlook and government services, harvesting credentials and OAuth tokens. Over 200 organisations and 5.000 consumer devices have been impacted globally, spanning government, IT, telecommunications, and energy sectors. `telecommunications` `public administration` `energy` `russia` link

Disruption & destruction

Threat actors claimed control of Venice San Marco flood defence pumps

On April 12, a researcher reported that threat actors using the names Infrastructure Destruction Squad and Dark Engine claimed to have breached Venice's San Marco flood defence pump system. The group said it gained administrative control, could disable protections and flood coastal areas, and published alleged evidence via Telegram. They also offered to sell root access for 600 US dollars, raising public safety concerns. `environment` link

Data exposure and leaks

Suspected cyberespionage in data breach of Finnish government mobile device management service

On April 21, Finnish police expanded an investigation on a January data breach affecting Finnish State Information and Communication Technology Centre Valtori's mobile device management service for government agencies. The investigation expanded to include suspicion of cyberespionage. An unknown attacker exploited a zero-day in a commercial product to access operational and personal data. About 50.000 users were impacted. No device-stored data was confirmed compromised. `public administration` link

France's National Agency of Secure Titles user data leak allegedly sold on cybercrime forum

On April 20, France's National Agency of Secure Titles (ANTS), disclosed a security incident potentially exposing users' personal data, including names, e-mail addresses, and dates of birth.

A cybercrime forum claimed to be selling data allegedly affecting 19 million people, though the figure was unverified. The Paris prosecutor was notified and investigations were assigned to the Anti-cybercrime Office. On April 25, a minor using the persona breach3d was taken into custody over suspected involvement. `public administration` link

French Ministry of Education targeted in data leak
On April 14, France's Ministry of Education reported a targeted cyberattack involving impersonation of an authorised staff account and exploitation of a vulnerability in an EduConnect-related student account management service. An unknown threat actor downloaded pupils' personal data, including names, EduConnect identifiers, school/class details, and optional e-mail addresses; some activation codes for inactivated accounts were exposed. The number of affected pupils remains under assessment. `public administration` `education` link

Alleged Hungarian government credential exposure via breach databases
On April 10, Bellingcat reported that approximately 795 Hungarian government e-mail addresses and associated passwords were circulating in online breach databases, affecting 12 of 13 ministries. The exposed data allegedly impacts sensitive personnel including military officers, diplomats, and counter-terrorism staff. Additionally, 97 machines were reportedly identified as compromised by credential stealers, with stealer logs dating as recently as early 2026. Exposure was attributed primarily to weak password reuse on non-work platforms. `public administration` `defence` link

World

Cyberespionage & prepositioning

China-linked phishing campaigns targeted diaspora activists and journalists
On April 27, Citizen Lab reported two distinct China-linked threat actors, tracked as Glitter Carp and Sequin Carp, conducted targeted phishing campaigns against Uyghur, Tibetan, Taiwanese, and Hong Kong diaspora activists, as well as international journalists covering Chinese transnational repression. Glitter Carp harvested credentials via impersonation and fake security alerts, whilst Sequin Carp abused OAuth consent flows to gain persistent e-mail account access, bypassing multi-factor authentication. `fundamental rights` `china` link

LinkedIn covert browser fingerprinting and extension surveillance campaign
On April 3, Fairlinked e.V., an association of commercial LinkedIn users, reported that Microsoft's LinkedIn was covertly scanning users' browsers for over 6.000 installed extensions via hidden JavaScript, collecting device data without disclosure or consent. The activity, independently partially confirmed by BleepingComputer, affects LinkedIn's one billion global users. LinkedIn acknowledged the scanning but stated it is used to protect platform integrity and detect terms-of-service violations, disputing allegations of misuse or third-party data sharing. `social media` link

Threat actor Bitter linked to hack-for-hire campaign targeting MENA civil society
On April 8, researchers reported that a hack-for-hire espionage campaign, which they associate to threat actor Bitter, was active since at least 2022 and had targeted civil society members, journalists, and opposition politicians across the Middle East and North Africa region. The operation reportedly combined spearphishing via fake social media personas with ProSpy Android spyware, delivered through fraudulent messaging app lures. The threat actor also conducted credential theft and account compromise against iOS users. `civil society` link

China-linked threat actors breached FBI surveillance system in major cyber incident
On April 1, the FBI declared a China-linked intrusion into a sensitive internal surveillance

system a major incident under the Federal Information Security Modernization Act, indicating significant risk to US national security. Threat actors accessed a system containing law enforcement surveillance returns and personal data relating to FBI investigation subjects, likely providing China with a significant counterintelligence advantage. The breach was reportedly facilitated via a commercial internet service provider's vendor infrastructure. `law enforcement` link

UAT-4356 exploitation of Cisco Firepower FXOS with Firestarter backdoor
On April 23, Cisco Talos reported on threat actor UAT-4356's continued targeting of Cisco Firepower devices running FXOS. The actor exploited known vulnerabilities to gain unauthorised access and deploy the custom Firestarter backdoor, enabling remote control and code execution. The activity impacts network perimeter security appliances globally and may support espionage operations, following earlier reporting linking UAT-4356 to the ArcaneDoor campaign. link

Surge in device code phishing campaigns abusing OAuth 2.0 for account takeover
On April 4, researchers reported a surge in device code phishing activity globally across the month of March. Multiple threat actors are exploiting OAuth 2.0 Device Authorisation Grant flows to steal access tokens, bypassing MFA and passkeys. Previous major campaigns were attributed to Russia-linked Storm-2372 and criminal group Scattered Lapsus$ Hunters. At least 10 distinct phishing kits are in circulation, with EvilTokens the most prevalent, targeting platforms including Microsoft 365 and GitHub. `russia` link

Cybercrime

Trojanised Claude Code leak lure distributing Vidar and GhostSocks malware
On April 3, researchers reported a campaign exploiting public interest in the accidental Anthropic Claude Code source code leak to distribute malware via trojanised GitHub repositories. Attributed to threat actor idbzoomh, the campaign used a malicious archive masquerading as leaked source code to deliver Vidar v18.7, an information stealer, and GhostSocks, a SOCKS proxy trojan. The campaign targeted developers globally, with repositories appearing prominently in search engine results. `technology` link

UAT-10608 large-scale automated credential harvesting via React2Shell
On April 7, threat actor UAT-10608 reportedly engaged in a large-scale automated credential harvesting campaign. The group exploited CVE-2025-55182 (React2Shell), a pre-authentication remote code execution vulnerability in Next.js applications, to compromise at least 766 hosts globally. Targeting appears indiscriminate, consistent with automated internet-wide scanning. link

North Korea's Contagious Interview cross-ecosystem supply chain campaign
On April 7, North Korea-linked Contagious Interview reportedly engaged in a supply-chain operation deploying malicious packages across npm, PyPI, Go Modules, crates.io, and Packagist under different aliases. The campaign impersonated legitimate developer tooling to deliver RAT-enabled infostealers targeting credentials, browser data, password managers, and cryptocurrency wallets. One variant included full post-compromise capabilities. Over 1.700 malicious packages have been linked to the broader operation. `technology` `north korea` link

AMOS Stealer delivered via Cursor AI agent session
On April 24, researchers reported an incident where Amos stealer was delivered through a Cursor AI coding agent session after the operator was socially engineered into running malicious content. The malware stole credentials and other sensitive data, rapidly exfiltrated it, and then installed a persistent implant on a macOS endpoint. `technology` link

Forged elementary-data release delivers credential stealer via PyPI and GitHub Container Registry
On April 25, a supply-chain compromise reportedly targeted the elementary-data project, where a forged release was published to PyPI and a matching trojanised container image was pushed to the GitHub Container Registry. The activity aimed to steal developer secrets and cryptocurrency wallets. Users who installed version 0.23.3 or pulled the affected images may be exposed and should rotate credentials. `technology` link

Disruption & destruction

DDoS disruption of Bluesky platform and API
On April 20, Bluesky disclosed a DDoS attack that caused intermittent outages from April 15 and disrupted core features including feeds, notifications, threads and search. The Iran-linked 313 Team claimed responsibility, stating it targeted Bluesky's API, though Bluesky did not attribute the incident. Service stability was restored by April 16 despite continued attacks, and no unauthorised access to private user data was found. `social media` `iran` link

Iranian APT exploitation of internet-exposed PLCs across US critical infrastructure
On April 7, CISA reported that threat actors, linked to Iran's Islamic Revolutionary Guard Corps Cyber Electronic Command, had been targeting internet-exposed Rockwell Automation/Allen-Bradley programmable logic controllers across US critical infrastructure since at least March 2026. Sectors affected include public administration, water management systems, and energy. The activity resulted in manipulation of HMI and SCADA displays, project file extraction, and in some cases operational disruption and financial loss. `public administration` `energy` `iran` link

Lotus Wiper destructive campaign against Venezuelan energy and utilities
On April 21, researchers reported that an unknown threat actor had reportedly targeted Venezuela's energy and utilities sector deploying the Lotus Wiper in late December 2025 and January 2026. The operation used staged scripts and tools to coordinate execution across a domain, disrupt access, and permanently erase data. Impact included widespread system disruption and unrecoverable loss of files and drive contents across affected hosts. The incident coincided with the US military operation in Venezuela in January 2026. `energy` link

Data exposure and leaks

Vercel breach via third-party OAuth compromise
On April 19, Vercel, a US cloud application company, confirmed a security incident involving unauthorised access to internal systems, reportedly originating from a compromised third-party AI tool OAuth app tied to a breached employee Google Workspace account. A threat actor claiming to be ShinyHunters alleged theft and sale of data and access, including employee records and customer environment variables. Vercel said only a limited subset of customers was affected. `technology` link

Opportunistic

Fake website impersonating Anthropic's Claude delivers PlugX
On April 10, researchers reported a fake website impersonating Anthropic's Claude that distributed a trojanised Windows installer. Victims received a working Claude app while malware was installed in the background, enabling remote access and potential credential theft

via the PlugX malware family. The campaign lure users globally through deceptive “Pro” Claude downloads. link

Unauthenticated nginx-ui MCP endpoint exploitation for nginx takeover
On April 15, researchers reported active exploitation of a critical nginx-ui flaw by unknown threat actors that allowed unauthenticated network attackers to take over nginx management functions. Adversaries could alter configurations to hijack traffic, exfiltrate sensitive data, or disrupt services, affecting exposed and internally reachable deployments globally. link

Npm supply-chain worm stealing tokens and self-propagating via compromised packages
On April 22, researchers observed a malicious npm supply-chain worm, in which compromised package releases stole authentication tokens and other secrets, then attempted to self-propagate by republishing additional packages from hijacked publisher accounts. The activity affected multiple npm packages, including pgserve and Namastex-related tooling, risking widespread credential exposure across developer and CI/CD environments. No threat actor attribution was confirmed. `technology` link

Notable CVEs

Active exploitation of critical FortiClient EMS authentication bypass vulnerability CVE-2026-35616
On April 5, Fortinet released an emergency weekend security update following active exploitation of a critical improper access control vulnerability in Fortinet's FortiClient Enterprise Management Server. The flaw, tracked as CVE-2026-35616, allows unauthenticated attackers to bypass authentication and authorisation controls entirely, enabling remote code or command execution. Affecting versions 7.4.5 and 7.4.6, over 2.000 exposed instances were identified globally, predominantly in the US and Germany. link

Exploitation of critical Flowise RCE vulnerability CVE-2025-59528
On April 7, researchers reported active exploitation of CVE-2025-59528, a maximum-severity arbitrary code execution vulnerability in Flowise, an open-source AI development platform. Exploitation was detected via VulnCheck's Canary network, with activity originating from a single Starlink IP address. Between 12.000 and 15.000 Flowise instances are currently exposed online. Users are urged to upgrade to version 3.1.1 immediately. Two additional Flowise vulnerabilities were also being actively exploited. `artificial intelligence` link

SharePoint spoofing flaw CVE-2026-32201 exploited in the wild
On April 15, CISA reported active exploitation of a Microsoft SharePoint spoofing vulnerability CVE-2026-32201, alongside coordinated reconnaissance activity targeting SharePoint deployments. The threat actor was not identified. The activity may enable unauthorised access leading to viewing and altering confidential information, with global exposure for organisations running affected SharePoint versions. 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.