CERT-EU

# Cyber Brief (May 2025)

***June 3, 2025 - Version: 1***

## TLP:CLEAR

*Disclosure is not limited.*

*TLP:CLEAR information may be distributed freely.*

## Executive summary

- We analysed 328 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, in Europe, seven EU Member States called out Russian GRU activity, while the Council of the EU sanctioned entities responsible for Russia's destabilising actions abroad. The Council of the EU and the Czech Republic condemned China-linked malicious cyber activity. Elsewhere, Iran intensified its collaboration with China on AI, Vietnam banned Telegram, in Moscow foreign visitors will reportedly soon be obliged to install a smartphone app which tracks them and NSO Group was ordered to pay over 167 million US dollars to WhatsApp over Pegasus hacking.
- On the **cyberespionage** front, in Europe, a Russia-linked actor targeted entities and individuals linked to Ukraine and linked to the European defence sector, and Iran-linked actors imitated a German private entity. Elsewhere, Chinese cyberespionage intruded the Guatemalan Foreign Ministry and hidden communication devices were found in Chinese-made solar inverters, while a Pakistani actor spoofed India's Ministry of Defence.
- Relating to **cybercrime**, in Europe, AutoIt-compiled droppers were sighted targeting the Netherlands and Hungary, while a wave of Clickfix abuse targeted a range of Portuguese sectors.
- There were **disruptive and destructive** attacks in the form of DDoS attacks in response to military support from EU Member States to Ukraine and the Romanian government during its election. Researchers uncovered a destructive supply-chain attack involving three malicious Go modules hid destructive code within seemingly legitimate packages.
- As regards **data exposure and leaks** incidents, xAI Dev leaked an API Key for Private SpaceX and Tesla LLMs, meanwhile a South Korean telecom breach led to unauthorised access to the data of 26.5 million users.
- Relating to **information operations**, in Europe, influence operations targeted social media to influence narratives around elections in Poland and Portugal and to discredit European leaders ahead of Ukraine peace talks in Turkey.

- In this Cyber Brief we have included notable vulnerabilities exploited opportunistically in May 2025.

# Europe

## Cyber policy and law enforcement

**Several EU countries participate in joint advisory related to Russia-linked APT28**
On May 21, the governments of seven EU Member States and allied countries issued a joint advisory related to activity from the Russian General Staff Main Intelligence Directorate (GRU) which targeted Western logistics entities and technology companies. The activity included APT28 conducting cyberespionage activity repeatedly towards logistics entities and IT companies since 2022. `russia` link

**The Council of the EU imposes sanctions towards Stark Industries web hosting service**
On May 20, the Council of the European Union imposed additional restrictive measures against 21 individuals and six entities responsible for Russia's destabilising actions abroad. These include Stark Industries, a web hosting service that has been affiliated with several Russia-linked threat actors. `russia` `sanctions` link

**Czechia attributes cyberespionage to China-linked APT31**
On May 28, the Czech government publicly attributed a prolonged cyberespionage campaign targeting its Ministry of Foreign Affairs to the China-linked group APT31. The attacks, ongoing since 2022, affected an unclassified network designated as critical infrastructure. The High Representative on behalf of the European Union strongly condemned the malicious cyber activities. `china` `diplomacy` link

**Dutch government passes law aimed at cyberespionage**
On May 15, the Dutch government approved legislation that extends existing espionage laws to include cyberespionage. The Dutch government took the measure to protect national security, the security of people, critical infrastructure and technology. link

**Ireland fined TikTok over unlawful data transfer to China**
On May 2, the Irish Data Protection Commission (DPC) fined TikTok 530 million euro for breaching GDPR by transferring user data to China without ensuring adequate protection and by failing to inform users transparently. The DPC ordered TikTok to comply within six months or face suspension of transfers, following inaccurate disclosures and violations between July 2020 and December 2022. link

**Moldovan and Dutch authorities arrest suspect cybercriminal related to DopperPaymer ransomware**
On May 12, Moldovan authorities announced the arrest of an individual suspected to be linked to DopperPaymer ransomware attacks that targeted Dutch organisations in 2021. The operation was led jointly with Dutch law enforcement. link

## Cyberespionage & prepositioning

**Google exposes ColdRiver's new cyberespionage malware strain**
On May 7, Google Cloud reported that Russia-linked Coldriver deployed a new malware named Lostkeys. The malware is designed to steal files and system data from government advisors, NGOs, journalists, and individuals linked to Ukraine. Delivered via fake CAPTCHA pages

prompting users to run PowerShell scripts, Lostkeys represents an evolution in Coldriver's espionage tactics. `russia` link

**Laundry Bear, a new Russia-linked threat actor, conducts cyberespionage activity towards governmental entities in the EU**
On May 27, Microsoft and the Dutch government reported on Russia-linked Laundry Bear who reportedly has conducted cyberespionage operations since at least April 2024. In September 2024, Laundry Bear breached the Dutch police, exfiltrating contact data using stolen session cookies. In an April 2025 spearphishing campaign, Laundry Bear targeted individuals involved in the European defence sector. `russia` link

**Iranian APT group poses as German modeling agency**
On May 7, Palo Alto reported that Iranian cyber actors, linked with low confidence to APT35, created a fake website mimicking a German modeling agency. The site collected visitor data via obfuscated JavaScript and featured a fictitious model profile. `iran` link

**Apple warns users of spyware targeting**
On April 29, Apple notified users in 100 countries that they may have been targeted with government spyware, including an Italian journalist and a Dutch activist. link

## Cybercrime

**Threat actor used AutoIt-based DarkCloud Stealer in targeted phishing attack**
On May 14, Palo Alto Networks reported about campaigns using phishing e-mails and AutoIt-compiled droppers to target government and tech sectors. The malware steals credentials and browser data, with samples seen in the US, Brazil, the Netherlands, and Hungary. link

**ClickFix campaign for data theft**
On May 6, Unit 42 reported that Lampion malware operators targeted the Portuguese governmental, finance, and transport sectors using a new ClickFix technique. Victims were tricked into executing malicious PowerShell commands under the guise of fixing issues. The attack chain involved obfuscated scripts and staged loaders. link

## Disruption & destruction

**Pro-Russia supposed hacktivists target Dutch public organisations with DDoS attacks**
On April 30, NoName057(16), a pro-Russia supposed hacktivist claimed disruptions of Dutch public and private services with DDoS attacks, targeting websites across several provinces and municipalities. The group claimed retribution for military aid to Ukraine. Despite service disruptions, Dutch officials confirmed no internal systems were compromised. `russia` link

**Pro-Russia supposed hacktivists targeted Romanian websites during Presidential election**
On May 4, NoName057(16), a pro-Russia supposed hacktivist claimed responsibility for DDoS attacks against Romanian websites. These attacks coincided with the first round of Romania's Presidential election rerun. The attacks hit the website of the Romanian Constitutional Court, the main government portal, the Romanian Foreign Ministry site and the websites of four Presidential candidates. `russia` link

## Information operations

**Disinformation campaign targeted Portuguese May elections**
On May 19, Cyabra, a company analysing disinformation online, reported on a disinformation

campaign targeting the May 18 Portuguese elections. 58% of the accounts commenting on the far-right party Chega's X and threads were fake. Almost half of the accounts commenting on the other two main political parties (PS and PSD) were also fake. The main narratives were to amplify Chega's positions and discredit its opponents. link

**Russian cyber interference targets Polish elections, warns Minister**
On May 6, the Polish Minister of Digital Affairs reported unprecedented Russian interference in the Presidential elections, involving cyberattacks and disinformation campaigns targeting all political committees. In 2024, over 600.000 incidents were reported, with more than 100.000 addressed by Polish services, marking a 60% year-over-year increase. `election` `russia` link

**Warnings of potential foreign interference in Polish Presidential campaign**
On May 14, NASK, a Polish research institute, reported identifying political advertisements on Facebook that may have been financed from abroad. These ads, displayed within Poland, appeared to support one candidate while discrediting others. The involved advertising accounts were reported to Meta, and the Internal Security Agency was notified. link

**Pro-Russia actor deployed AI-generated media to discredit European leaders ahead of Istanbul peace talks**
On May 14, EclecticIQ reported that Storm-1516, a pro-Russia actor, orchestrated a campaign using AI-generated media to falsely accuse European leaders of drug use during a diplomatic visit to Kyiv. The operation aimed to erode public trust and undermine European unity before the Istanbul peace talks scheduled for May 15. `artificial intelligence` `russia` link

# World

## Cyber policy and law enforcement

**Moscow to track foreigners via smartphone app**
On May 21, Roskomsvoboda, a Russian digital rights advocacy group, reported that starting September 1, 2025, Moscow and the Moscow region will implement a digital surveillance pilot targeting foreign nationals. Foreigners will be required to submit biometric data, undergo fingerprinting, register their residence, and install a mobile app enabling authorities to track their location. Non-compliance may lead to inclusion in a monitored registry and deportation. `russia` link

**Azerbaijan links February 2025 cyberattack on media to Russia**
On May 2, the Chairman of Azerbaijan's Parliamentary Commission on Countering Foreign Interference, revealed that the February 2025 cyberattack on Azerbaijani media was linked to Russia, specifically APT29. He suggested the attack was retaliation for Azerbaijan's closure of the Russian Information and Cultural Center and Sputnik's operations. `russia`

**Iran seeks Chinese AI expertise through technology diplomacy**
On May 14, Teheran Tines reported that Iran conducted a series of artificial intelligence–related diplomatic meetings with China, seeking to expand Tehran’s technological relationship with Beijing. `artificial intelligence` `china` `iran` link

**Vietnam bans Telegram over illegal content concerns**
On May 21, Vietnam ordered telecom firms to block Telegram, citing police reports that 68% of its 9600 local channels were used for fraud, drugs, and suspected terrorism. The government accused Telegram of failing to remove illegal content. Telegram said it had responded to legal requests and was surprised by the move. `ban` `vietnam` link

**NSO Group ordered to pay over 167 million US dollars to WhatsApp for spyware attack**
On May 6, a US federal jury ordered Israeli spyware firm NSO Group to pay over 167 million US dollars in damages to WhatsApp for a 2019 hacking campaign that targeted more than 1.400 users with Pegasus spyware. `psoa` link

**US sanctions disrupt ICC Prosecutor’s work, with Microsoft canceling Khan’s e-mail address**
On May 16, AP News reported that US sanctions on ICC Prosecutor Karim Khan disrupted court operations, including freezing assets and stalling investigations. Microsoft, for example, canceled Khan’s e-mail address, forcing the prosecutor to move to Proton Mail. `united states` link

## Cyberespionage & prepositioning

**US and Guatemala expose Chinese cyberespionage targeting Foreign Ministry**
On April 29, the US Embassy in Guatemala announced that a joint cybersecurity review with the Guatemalan government uncovered that the Ministry of Foreign Affairs' systems had been infiltrated by China-linked APT15. The Guatemalan Foreign Ministry clarified that this breach occurred between September 2022 and February 2025. `china` link

**Hidden communication devices in Chinese solar inverters spark US cybersecurity concerns**
On May 14, Reuters reported that US officials found hidden communication devices in Chinese-made solar inverters and batteries, raising fears of potential cyber threats. These components, essential to managing renewable energy flow into power grids, could allow unauthorised remote access. `china` `energy` `united states` link

**Marbled Dust exploits Output Messenger zero-day to target Kurdish entities**
On May 12, Microsoft Threat Intelligence reported that Marbled Dust, a supposed Turkey-linked actor, exploited a zero-day vulnerability in Output Messenger to gain authenticated access, deploy malware, and exfiltrate data, targeting Kurdish military entities in Iraq. Microsoft disclosed the issue to the developer, who released a patch to address the threat. `defence` `turkey` link

**APT36-linked campaign spoofs India's Ministry of Defence portal using ClickFix method**
On May 5, Hunt[.]io reported that Pakistan-linked APT36 mimicked India's Ministry of Defence press release portal to deliver cross-platform malware in March. The fake site used a ClickFix-style method to copy malicious commands to users’ clipboards. The campaign showed hallmarks of APT36, including cloned content, clipboard tactics, and spoofed government subdomains hosted on compromised infrastructure. `india` `pakistan` link

## Data exposure and leaks

**Data broker LexisNexis discloses data breach affecting 364.000 people**
On May 29, LexisNexis Risk Solutions, a US-based data broker, disclosed a breach affecting 364.000 people. The December 2024 breach, detected in April, involved unauthorised access via a compromised GitHub account. Exposed data included names, contact details, social security and driver’s license numbers, and birth dates. link

**xAI Dev Leaks API Key for Private SpaceX, Tesla LLMs**
On May 1, KrebsOnSecurity reported that an xAI developer inadvertently exposed an API key on GitHub, granting access to over 60 private and unreleased large language models fine-tuned with proprietary data from SpaceX, Tesla, and Twitter/X. Despite GitGuardian's alert on March 2, the key remained active until April 30, raising concerns over xAI Dev's internal security practices and the potential misuse of sensitive AI models. `artificial intelligence` link

### 26.5 million users affected by South Korean SK Telecoms breach

On May 20, SK Telecoms, a leading South Korean mobile network operator, gave additional details about the breach they disclosed in April. The company said that it had been ongoing since at least 2022, and 26.5 million users are affected by the attack, exposing their sensitive data. `south korea` link

## Disruption & destruction

### Malicious Go modules deliver disk-wiping payload

In April, Socket uncovered a destructive supply-chain attack involving three malicious Go modules that used obfuscation to download and run a Linux-targeted disk-wiping script. Exploiting Go's decentralised ecosystem and namespace ambiguity, the threat actor hid destructive code within seemingly legitimate packages, leading to irreversible data loss and system failure if executed. link

## Opportunistic

### SonicWall flags two VPN vulnerabilities as potentially exploited in active attacks

On April 30, SonicWall updated advisories for CVE-2023-44221 and CVE-2024-38475, warning that both VPN-related vulnerabilities were potentially being exploited in the wild. CVE-2023-44221 affects the SMA100 SSL-VPN management interface and permits command injection by authenticated users. CVE-2024-38475, impacting Apache mod_rewrite, may enable unauthenticated code execution. Both flaws affect multiple SMA models and are patched in firmware version 10.2.1.14-75sv and later. link

### Hackers exploit OttoKit Wordpress plugin flaw as most sites auto-patched by April 24

On April 11, a security researcher disclosed a critical vulnerability, CVE-2025-27007, in the OttoKit WordPress plugin that allowed unauthenticated attackers to create rogue admin accounts via its API. Although hackers began exploiting the flaw within 90 minutes of public disclosure, by April 24, most plugin users had been force-updated to a patched version, mitigating the risk for over 100.000 affected sites. link

### Google patches Chrome zero-day enabling OAuth token theft

On May 15, Google released a security update addressing CVE-2025-4664, a high-severity vulnerability in Chrome's Loader component. The flaw allows attackers to leak cross-origin data via crafted HTML pages, potentially leading to account takeover by capturing sensitive information like OAuth tokens. Google is aware of reports of exploits existing in the wild. link

### Malicious NPM packages target Cursor AI on macOS

On May 7, researchers at Socket, a cybersecurity company, reported that threat actors used three NPM packages aimed at the macOS version of Cursor AI code editor. The packages have been downloaded over 3200 times and are still available online. Once installed, it can be used to steal user credentials, fetch an encrypted payload, overwrite Cursor's main.js file, and they can maintain persistence by disabling auto-updates. link

### Critical Langflow flaw exploited to hack AI app servers

On May 5, CISA warned of active exploitation of a critical remote code execution flaw (CVE-2025-3248) in Langflow, an open-source tool for building AI workflows using LangChain. Attackers can execute code on servers running vulnerable versions. Widely used in experimental and production AI apps, Langflow is affected before version 1.3.0. Users should update immediately to secure their systems. `artificial intelligence` link

**Chinese threat group linked to SAP NetWeaver exploitation**
On May 8, cybersecurity firm Forescout revealed that a previously known exploitation of a critical SAP NetWeaver vulnerability (CVE-2025-31324) has now been attributed to the Chinese threat group Chaya_004. The group used web shells and backdoors like Supershell in targeted attacks. `china` 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. |