# Cyber Brief (May 2026)

***June 2, 2026 - Version: 1***

**TLP:CLEAR**

*Disclosure is not limited.*

*TLP:CLEAR information may be distributed freely.*

## Executive summary

- We analysed 325 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, Europol supported international efforts to disrupt pro-Iranian digital foreign interference content. Additionally, France and Poland announced a joint military satellite programme featuring encryption and cybersecurity defences.
- On the **cyberespionage** front, Austria expelled three Russian diplomats over suspected signals espionage linked to satellite installations on diplomatic buildings in Vienna. A China-linked threat actor exploited unpatched Microsoft Exchange servers to target government and defence organisations in Asia and Poland, while another China-linked threat actor enacted a global supply-chain compromise leveraging Daemon Tools installers distributed from the software's legitimate site.
- In regards to **cybercrime**, we continued to see sustained supply-chain attacks targeting the open-source software development ecosystem. TeamPCP's Mini Shai-Hulud worm compromised over 160 npm and PyPI packages. Shortly after TeamPCP published their malware source code, it was adopted by copycat actors. In late May, cybercrime groups began engaging in ticket spearphishing and fraud campaigns targeting the 2026 FIFA World Cup.
- As for **disruptive** cyberattacks, a compromised mistralai PyPI package delivered a Linux credential stealer containing a geo-fenced destructive payload targeting systems in Israel and Iran.
- Regarding **data exposure and leaks**, Lithuanian authorities reported a likely state-actor breach exposing over 600.000 entries from national registers. Globally, cybercrime group ShinyHunters claimed to have stolen data from Instructure's e-learning platform Canvas, affecting educational institutions globally.
- As for notable **Common Vulnerabilties and Exposures (CVEs)**, the Linux zero-day Dirty Frag (CVE-2026-43284), which enables local root privilege escalation, was publicly disclosed with a proof-of-concept following a broken embargo, affecting most major distributions. Threat actors exploited CVE-2026-35616 in FortiClient EMS to distribute an infostealer disguised as a legitimate Fortinet patch.

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

**Europol removed pro-Iranian regime digital foreign interference**
On May 18, Europol announced that 19 countries collaborated to disrupt digital foreign interference content linked to Iran's Islamic Revolutionary Guards Corps. Between February 13 and April 28, authorities carried out joint referrals to online platforms. This forms part of the ongoing Europol support to EU Member States in line with the EU's ProtectEU Internal Security Strategy. `law enforcement` `iran` link

**VPN used by ransomware actors dismantled in global crackdown**
On May 21, Europol announced the dismantling of First VPN, as part of Operation SaffRon. First VPN is a VPN service reportedly widely used by ransomware groups and other cybercrime actors to hide attacks and fraud. Authorities in multiple countries seized 33 servers and shut down key domains, while investigators identified thousands of users linked to cybercrime. `law enforcement` link

**ANSSI director general reported encryption does not protect against US Cloud Act**
On April 30, the French Cybersecurity Agency's (ANSSI) director general Vincent Strubel warned that encryption does not protect against the United States (US)' Cloud Act's extraterritorial data access via US-based service providers. Strubel also stated it did not prevent kill switch risks, quoting the case of the International Criminal Court, whose access to Microsoft services was allegedly disrupted following US sanctions. link

**France and Poland launched secure military satellite partnership**
On April 30, France and Poland announced a joint military satellite program with Airbus Defence and Space, Thales Alenia Space, and Polish supplier RADMOR, to provide Poland's armed forces with secure geostationary satellite communications. The system will feature encryption, anti-jamming protections, and cybersecurity defences against electronic warfare and cyberattacks, while giving Poland sovereign control over military communications infrastructure as part of broader European defence-readiness efforts. `defence` link

**Poland urged officials to ditch Signal for state-run messaging apps**
On May 18, Poland urged government officials and cybersecurity agencies to stop using Signal for official communications and switch to state-developed encrypted messaging platforms instead. Authorities cited phishing and social-engineering attacks targeting public officials, including campaigns impersonating Signal support staff to hijack accounts, amid growing concerns over foreign-linked cyber threats and digital sovereignty. link

## Cyberespionage & prepositioning

**Austria expelled Russian diplomats over suspected espionage through satellite dishes on diplomatic buildings**
On May 4, Austria reportedly expelled three Russian diplomats over suspected signals espionage linked to numerous satellite dishes on Russian diplomatic buildings in Vienna. Austrian services

assessed threat actors could use the installations to intercept other states' satellite communications. `europe` `russia` link

**Breach of Sistemi Informativi an IBM Italy subsidiary**
On May 3, newspapers reported that Sistemi Informativi, an IBM Italy subsidiary, suffered a breach. Sistemi Informativi provides IT infrastructure supporting public and private institutions. IBM stated they contained the incident and restored services. `technology` link

**Shadow-Earth-053 reportedly exploited unpatched Exchange servers**
On May 4, researchers reported that cyberespionage actor Shadow-Earth-053 had exploited unpatched Microsoft Exchange and Internet Information Services servers to gain persistent access and steal sensitive information. The activity reportedly targeted government and defence-related organisations across Asia and also reportedly affected Poland. `technology` `public administration` `defence` link

## Data exposure and leaks

**Lithuanian national register's data leaked by suspected state-actor via compromised institutional credentials**
On May 26, Lithuanian authorities reported a leak of over 600.000 entries from national registers, mainly real estate and legal entities, accessed using credentials from authorised institutions. `public administration` link

**Cyberattack on Moldova medical payments database**
On April 27, a large-scale cyberattack reportedly targeted a Moldovan medical database platform aggregating hospital data, including personal information and healthcare payment records. The Cybersecurity Agency said around 30% of data was affected and that they did not receive a ransom demand. `health` link

**Alleged Nowa Nadzieja member database advertised on cybercrime forum**
On May 19, researchers reported a threat actor advertising an alleged database linked to Poland's Nowa Nadzieja political party on a cybercrime forum. The unverified listing claimed it contains members' and supporters' personal and political-affiliation data, including national identification numbers, dates of birth, phone numbers, e-mail and home addresses. `civil society` `political parties` link

## World

## Cyber policy and law enforcement

**US sanctioned two US nationals for facilitating North Korea-linked IT Workers campaign**
On May 6, two US nationals were sentenced to 18 months' imprisonment for enabling North Korea-linked remote IT worker fraud schemes. They hosted company laptops in the US, installed remote access tools, and helped overseas operatives pose as US-based employees, generating over 1.2 million US dollars for North Korea and affecting nearly 70 US firms. `north korea` link

**Project Glasswing initial update**
On May 22, Anthropic released an update on Project Glasswing, revealing that its Claude Mythos Preview model and approximately 50 partners found over 10.000 high or critical severity software vulnerabilities across major systems and open-source projects. Anthropic said AI has shifted cybersecurity's bottleneck from finding bugs to verifying, disclosing, and patching

them, while delaying public release of Mythos-class models over misuse concerns. `artificial intelligence` link

**Glassworm botnet disrupted after C2 infrastructure takedown**
On May 26, CrowdStrike, Google, and the Shadowserver Foundation disrupted the Glassworm botnet by simultaneously taking down its C2 infrastructure. Glassworm played a major role in software supply-chain compromises, infecting developer tools, VSCode extensions, npm/PyPI packages, and GitHub repositories to spread malware and steal credentials. `technology` link

**Internet started to return in Iran after 3-month blackout**
On May 26, Iran's First Vice President Mohammad Reza Aref announced moves to lift internet outages, guided by President Pezeshkian and a new cyberspace headquarters. Following an 88-day blackout, Netblocks reported partial restoration, with content creators allegedly regaining access. `iran` link

**Microsoft Israel chief to step down after inquiry into military surveillance use of Azure**
On May 12, the Guardian reported that the head of Microsoft's Israel branch, Alon Haimovich, will step down after an inquiry into the company's ties with the Israeli military. The investigation followed revelations that Unit 8200 used Microsoft Azure to store and analyse millions of intercepted Palestinian phone calls, prompting concerns over possible ethics violations and leading Microsoft to revoke the unit's access to certain cloud and AI services. `telecommunications` `defence` link

## Cyberespionage & prepositioning

**Daemon Tools supply-chain compromise delivered multi-stage malware**
On May 5, researchers reported a supply-chain compromise affecting Daemon Tools installers distributed from the vendor's legitimate site. Trojanised, validly signed components enabled remote command execution and staged deployment of additional malware, including profiling and backdoor capabilities. The campaign has been active since April 8 and remains ongoing, with thousands of infection attempts globally and targeted follow-on activity against a small subset of organisations. `public administration` `education` `china` link

**UAT-8616 exploited Cisco Catalyst SD-WAN vulnerabilities to gain admin access and deploy web shells**
On May 14, Cisco Talos reported ongoing exploitation of Cisco Catalyst SD-WAN Controller and Manager vulnerabilities. The actor tracked as UAT-8616 exploited an authentication bypass to obtain high privileges and attempt deeper access. Separately, multiple other clusters abused earlier flaws to compromise unpatched systems and deploy malicious tooling. Activity was observed globally and could enable unauthorised access and follow-on compromise. `technology` link

**Identity-driven cloud data exfiltration via Microsoft 365 and Azure abuse**
On May 20, Microsoft reported Storm-2949 conducted a sustained, identity-driven campaign to steal sensitive data from a victim's cloud environment. The actor used social engineering to take over accounts, then accessed Microsoft 365 and Azure resources to collect and exfiltrate large volumes of files and production data. `technology` link

## Cybercrime

**OpenClaw skill supply-chain compromise delivered Remcos RAT and GhostLoader**
On May 6, researchers reported a campaign abusing a deceptive OpenClaw "DeepSeek-Claw" skill to trick developers and AI agents into running malicious installation steps. Impact includes

compromised developer environments and potential downstream access to connected services and repositories. `technology` `artificial intelligence` link

**TeamPCP Mini Shai-Hulud supply-chain worm targeted npm and PyPI ecosystems**
On May 11, TeamPCP engaged in a supply-chain attack dubbed Shai-Hulud that compromised over 160 npm and PyPI packages by abusing GitHub Actions cache poisoning and stolen OIDC tokens to publish malicious updates. The malware targeted CI/CD secrets, cloud credentials, and developer tokens. It impacted ecosystems tied to TanStack, Mistral AI, UiPath, and OpenSearch before the packages were pulled and credentials rotated. `technology` link

**Copycat actor deploys Shai-Hulud following TeamPCP release of malware source code**
On May 17, researchers reported four malicious npm packages uploaded by an unknown threat actor, targeting developers via typosquatting. The packages deploy infostealer malware, including a non-obfuscated clone of the leaked Shai-Hulud source code and a DDoS botnet. TeamPCP, the threat actor behind the Shai-Hulud campaigns, had published their own malware code to GitHub, and independent threat actors have already begun modifying it and expanding its reach. link

**GitHub internal repositories breached via malicious VS Code extension**
On May 19, GitHub began investigating unauthorised access to internal repositories, with TeamPCP claiming theft of roughly 4.000 private code repositories and seeking to sell the data. GitHub confirmed about 3.800 repositories were breached after an employee installed a malicious VS Code extension. GitHub said there was no evidence customer data outside internal repositories was affected. `technology` link

**SEO-poisoned Gemini and Claude Code installers delivered fileless infostealer**
On May 21, researchers reported an SEO poisoning campaign impersonating Gemini CLI and Anthropic Claude Code installation pages to trick developers into running malicious commands. The financially motivated actor used typosquatted domains to deliver a memory-resident infostealer on Windows. Targeting primarily affected users in the US and UK. `technology` `artificial intelligence` link

**FIFA World Cup 2026 ticket phishing and fraud ecosystem**
On May 27, Group-IB reported a large-scale fraud ecosystem abusing the 2026 FIFA World Cup, including the Chinese-speaking threat actor GHOST STADIUM running a coordinated phishing and fake ticket operation. The activity used thousands of FIFA-impersonating domains to steal credentials, personal data and payments, amplified via social media advertising and other channels. Group-IB assessed potential losses could reach hundreds of millions, with broader impact potentially in the billions. `sports` link

## Disruption & destruction

**Compromised mistralai PyPI package delivered credential stealer with destructive option**
On May 12, Microsoft reported a compromise of the mistralai PyPI package (v2.4.6) used to deliver a Linux credential stealer via malicious code that runs when the package is imported. The activity includes environment-aware checks: it avoids Russian-language environments and contains a geo-fenced destructive option affecting systems in Israel or Iran. The scope is global for users who installed the tainted version. `technology` link

## Data exposure and leaks

**Unauthorised access to Trellix source code repository**
On May 1, cybersecurity company Trellix disclosed a breach in which unattributed threat actors

gained unauthorised access to a portion of its source code repository. Trellix reported no evidence that the accessed source code was exploited or altered, or that its release and distribution process were affected. Cybercrime actor RansomHouse claimed responsibility. `cybersecurity` link

**ShinyHunters data theft from educational tech company Instructure**
On May 1, Instructure, a US-based educational technology company, confirmed data was stolen in a cyberattack affecting Canvas, its e-learning system. Exposed data included user names, e-mail addresses, student ID numbers and private messages. Cybercrime group ShinyHunters claimed responsibility, alleging the breach impacted 280 million records tied to students and staff from 8.809 institutions globally. After reaching an agreement with the threat actor, the group reportedly returned the data to Instructure, and received digital confirmation of data destruction. `education` link

**Unauthorised Grafana's GitHub token access and codebase extortion attempt**
On May 17, Grafana Labs reported that an unauthorised party obtained a token granting access to its GitHub environment and downloaded the company codebase. The threat actor then attempted to blackmail Grafana Labs, demanding payment to prevent release of the code. Grafana Labs stated no customer data or personal information was accessed and found no evidence of impact to customer systems or operations. `technology` link

## Notable CVEs

**Palo Alto published a security advisory on a critical vulnerability in PAN-OS**
On May 6, Palo Alto published a security advisory addressing a critical vulnerability affecting PAN-OS. This vulnerability, tracked as CVE-2026-0300, allows an unauthenticated attacker to execute arbitrary code with root privileges. Palo Alto observed limited exploitation of this vulnerability. The risk can be mitigated if User-ID Authentication Portal access is restricted to only trusted zones, or disabled if not required. `technology` link

**Dirty Frag Linux zero-day enables root privilege escalation**
On May 8, a researcher reported a new Linux zero-day, Dirty Frag (CVE-2026-43284), with a public proof-of-concept enabling local attackers to gain root privileges. The disclosure followed a broken embargo after a third party published exploit code. Most major Linux distributions are affected and remain unpatched, increasing risk of rapid opportunistic exploitation and widespread compromise of vulnerable systems. `technology` link

**PoC exploits leaked for BitLocker bypass and Windows privilege escalation**
On May 13, a cybersecurity researcher published PoC exploits for two unpatched Microsoft Windows vulnerabilities named YellowKey and GreenPlasma, which are a BitLocker bypass and a privilege-escalation flaw. The latest exploits follow the researcher's previous disclosure of the BlueHammer (CVE-2026-33825) and RedSun. On May 19, Microsoft reported that it tracks the flaw under CVE-2026-45585 and shared mitigation measures to defend against potential attacks exploiting it in the wild. `technology` link

**FortiClient EMS exploit used to push EKZ infostealer as fake patch**
On May 27, researchers reported an unknown threat actor exploiting CVE-2026-35616 in FortiClient EMS to abuse trusted management workflows and distribute EKZ Infostealer disguised as a Fortinet patch. The activity enabled malware execution across EMS-managed endpoints and theft of browser credentials and session data, with subsequent exfiltration to attacker infrastructure. `technology` 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. |