Cyber Brief (August 2026)

September 3, 2026 - Version 1

TLP:CLEAR

Executive summary

- We analysed 385 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, two alleged members of TeamPCP arrested in Australia, and the US disrupted infrastructure used by China-linked threat actors.
- On the **cyberespionage** front, two Russia-linked APTs targeted EU countries with spearphishing and social engineering, and North Korea-linked threat actor Lazarus' continued its Operation Dream Job. Apple notified users of mercenary spyware, and a phishing campaign targeted Microsoft 365 finance workflows.
- In regards to **cybercrime**, we noted a Rust crates supply-chain compromise via typosquatted dependency, with infrastructure overlapping with operations attributed to North Korea-linked threat actors.
- In terms of **digital foreign interference**, pro-Russia Matryoshka and Storm-1516 targeted upcoming elections in Germany and France.
- There were two **disruptive and destructive** cyberattacks targeting Hungary's State Treasury and a small-scale power generator in the UK.
- Regarding **data exposure and leaks**, the UK Police National Legal Database suffered a leak.
- As for notable **artificial intelligence** activity, Meta said one of its AI models connected to the internet and compromised another organisation’s systems. Mythos 5, and GPT-5.6 Sol also took unauthorised actions on the live internet across 19 instances. Finally, the Kimi K3 model exploited a sandbox misconfiguration to access external resources.

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

The German government expanded the powers of the Foreigh Intelligence Service and the Federal Office for the Protection of the Constitution.
On August 12, the German government submitted a 753-page intelligence reform bill to parliament, granting its Foreign Intelligence Service (BND) and Domestic Intelligence Service (BfV) substantially expanded powers. The legislation authorises device hacking, covert apartment searches, and extended data retention of up to 12 months for metadata. Critics warn

the reform marks a fundamental departure from post-war democratic safeguards limiting agencies to passive intelligence gathering. An independent oversight council will authorise major operations. `germany` link

EU countries participated in Interpol-led Operation Jackal IV
On August 25, Interpol announced they led Operation Jackal IV which resulted in the arrest of 58 individuals and the identification of 263 suspects. Among them, Italian authorities identified one individual in relation to a pan-European money laundering network, and Romanian authorities dismantled a criminal group running a sophisticated investment scam, arresting 11 individuals. Austria, France, Germany, Ireland, the Netherlands, Portugal, Spain, and Sweden were also among participating countries. link

Cyberespionage & prepositioning

Suspected Russia-linked UNC7005 spearphishing campaign targeting European defence industry
On August 21, Google Threat Intelligence reported that suspected Russia-linked UNC7005 conducted an OAuth spearphishing campaign targeting the European defence industry. The threat actor registered domains spoofing legitimate Finnish Operations Center. When users "Sign in With Google", they are redirected to a legitimate OAuth login page. After authenticating, they are redirected to an attacker-controller cloud project that steals authentication tokens that grant the attacker access to the victim's account. `defence` `russia` link

Sandworm social engineering campaign targeting IT professionals
On August 8, Ukrainian Computer Emergency Response Team (CERT-UA) reported a social engineering campaign attributed to UAC-0145, a sub-cluster of Russia-linked Sandworm, active since at least May 2026. the threat actor posed as recruiters and IT firms, including a Bulgarian company, targeting IT professionals and system administrators globally. They lure victims into downloading a trojanised WireGuard VPN client delivering malicious payloads on both Windows and Linux systems. `technology` `russia` link link

Operation Dream Job targeting the defence sector with Windows zero-day exploitation
On August 11, Check Point Research reported on North Korea-linked threat actor Lazarus' Operation Dream Job campaign targeting defence organisations, including in France and Germany. Lazarus used fake job offers and impersonation sites to deliver a trojanised PDF viewer and malicious documents. They exploited CVE-2025-49113 in vulnerable Roundcube servers to relay C2 traffic and also exploited CVE-2026-68820, a zero-day vulnerability in Windows to deploy a FudModule rootkit. `defence` `transport` `north korea` link

Cybercrime

AiTM phishing campaign targeting Microsoft 365 finance workflows
On August 6, Arctic Wolf Labs reported an ongoing adversary-in-the-middle (AiTM) phishing campaign compromising Microsoft 365 accounts via voicemail-themed e-mail lures. The activity, linked to Microsoft's Storm-2755 "Payroll Pirates", uses residential proxies to maintain access and quietly collect finance-related mailbox content and identify payroll/HR personnel. It affected organisations across multiple sectors in the US, Canada, and Europe, with widespread targeting and confirmed intrusions. `health` `education` link

Digital foreign interference

Pro-Russian Matryoshka influence operation pushing fabricated content to divide Germany ahead of state elections
On August 11, NewsGuard reported that Russia-linked digital foreign interference operation Matryoshka is targeting Germany ahead of September 2026 state elections in Saxony-Anhalt, Berlin, and Mecklenburg-Vorpommern. The campaign, using the hashtag #TimeToDivideGermany, has produced at least 20 fabricated videos and news reports impersonating German media outlets, celebrities, and public figures. The operation aims to reignite East-West tensions, undermine mainstream political parties, and boost the AfD, which opposes support for Ukraine. `public administration` `russia` link

Russia-linked disinformation campaigns targeting 2027 presidential contenders
On August 6, Mediapart reported Russia-linked influence networks conducted disinformation campaigns targeting French 2027 presidential contenders Gabriel Attal, Édouard Philippe and Raphaël Glucksmann. Operations attributed to Matryoshka and Storm-1516 used fake media-style content, including fabricated reports and AI-generated narration, to spread false allegations and discredit candidates. The activity aimed to manipulate public debate and was investigated by French authorities, with limited but notable online reach. `civil society` `political parties` `public administration` `russia` `europe` link

Disruption & destruction

ByteToBreach targets Hungary's State Treasury in ransomware attack
On August 2, Hungarian authorities reported that a threat actor had breached Hungary's State Treasury, exfiltrating sensitive government data and deploying ransomware against its Agricultural and Rural Development Office. Security researchers attributed the incident to cybercrime actor ByteToBreach, which allegedly exploited an unpatched Oracle WebLogic server and encrypted certain files on internal users' machines. Hungarian authorities isolated the affected systems pending investigation. `public administration` `agriculture` `finance` link

Iran-linked cyberattack shuts down UK small-scale power generator
On August 24, BBC News reported that Iran-linked threat actors carried out a cyberattack that forced a small UK power plant generator to shut down for four days. The UK government and the NCSC did not name the affected site, citing security reasons. The Department for Energy Security and Net Zero (DESNZ) said the incident did not threaten the wider UK energy system, but prompted outreach to power companies about cyber-risk. `energy` link link

Data exposure and leaks

Liechtenstein reports data breach affecting 31.000 legal entities
On August 3, Liechtenstein said threat actors illegally accessed and copied data from its register of beneficial owners, affecting around 31.000 companies, foundations and trusts. Authorities detected the breach, took the system offline and launched an investigation. No banks or customer data were affected, and there was no indication that information had been altered or deleted. The government established a crisis task force and is notifying those affected. `justice` link

UK Police National Legal Database contact data leak on dark web
On August 3, the UK Police National Legal Database (PNLD) confirmed a breach in which police, government and customer contact details were compromised and published on the dark web. Exposed data included names, organisations and work e-mail addresses, including some Ask the

Police submitters. ExfilSquad listed PNLD, but attribution was not confirmed. PNLD said no passwords or credentials were exposed. `law enforcement` link

World

Cyber policy and law enforcement

Two alleged members of TeamPCP arrested in Australia On August 27, the Australian Federal Police announced having arrested two individuals allegedly members of TeamPCP, a financially motivated threat actor that has conducted large-scale supply-chain compromises. According to them, it is estimated they compromised over 1000 organisations worldwide, enabling the exfiltration of at least 300GB of data. `arrest`

China expands law enforcement inspection powers over technology firms in China
On August 13, China's Ministry of Public Security issued MPS Order No. 176, expanding its law enforcement inspection authority over technology entities in China. Effective October 1, 2026, the measures extend powers to data processors, critical information infrastructure operators, and network product providers. Authorities may now conduct vulnerability scanning and penetration testing directly, and commission third-party cybersecurity firms under police supervision, broadening state-directed access to foreign firms' networks and data. `china` link

Chinese authorities announced a review of Palo Alto products sold in China
On August 6, the Cyberspace Administration of China announced an investigation into Palo Alto's locally sold products, citing risks to critical infrastructure and national security. This follows months of increased Chinese scrutiny of foreign technology suppliers. In January, Chinese authorities had reportedly told domestic firms to avoid using software from over a dozen US and Israeli companies. `cybersecurity` link

United States authorities charge 17 Iranians over Islamic Revolutionary Guard Corps (IRGC)-linked cyberespionage campaign
On August 18, the US Department of Justice charged 17 Iranians of Mabna Institute, an Iranian company, for conducting a cyberespionage campaign targeting 144 US-based universities, 178 foreign universities, at least 42 US-based companies, at least 11 foreign companies, at least five US federal and state government agencies, and at least two non-governmental organisations. They reportedly acted on behalf of Iran's Islamic Revolutionary Guard Corps, among other Iranian clients. `education` `public administration` `research` link

US Department of Justice disrupts infrastructure used by China-linked threat actors
On August 26, the US Justice Department and FBI announced the seizure of domains used by QTFY, a China state-sponsored hacking group, to disrupt QScan and QTRouter. The platforms infected IoT devices and concealed attacks targeting US critical infrastructure. Victims reportedly included NASA, the Federal Reserve, Departments of Energy and Justice, NIH, and the US Senate. The seizures rendered both platforms inoperable. `china` link link

New Zealand sanctioned Russian individuals tied to cyber activity
On August 10, New Zealand announced a 36th round of sanctions against Russia regarding its war on Ukraine, with a particular focus on malicious cyber threat actors. The sanctions target several individuals and entities linked to digital foreign interference leveraging anti-Ukraine narratives and pro-Russia supposed hacktivism. `russia` `sanctions` link

Cyberespionage & prepositioning

Snowlight mass exploitation of government-facing infrastructure
On July 31, SOCRadar reported a China-nexus Snowlight campaign linked to access brokers UNC5174/UNC6586. The actors used an exposed staging environment to scan widely and exploit internet-facing systems, prioritising government infrastructure. Activity spanned over 100 countries and led to confirmed compromises, including administrative takeovers and web shell deployments, enabling follow-on access and potential credential theft. `public administration` `china` link

China-based threat actor leverages DeepSeek in autonomous campaign
On July 30, security researchers reported a Chinese-speaking threat actor had conducted an AI-enabled autonomous campaign with 460 targets in China, Malaysia, and an unnamed third country. Active since at least May, the actor leveraged DeepSeek via the Hermes Agent framework for autonomous vulnerability enumeration and exploitation attempts across seven CVEs. Parallel manual operations included data exfiltration via a Citrix Netscaler vulnerability and command execution on several Marimo notebook instances. `public administration` `china` link

Fire Ant expands operations targeting trusted network infrastructure
On August 27, Sygnia reported that Fire Ant, an adversary assessed to overlap with China-nexus cluster UNC3886, expanded its operations beyond hypervisors into trusted network infrastructure. Active since 2025 and continuing into 2026, the actor compromised edge routers, TACACS authentication servers, and Linux management hosts globally. Fire Ant harvested credentials, captured network traffic, deployed persistent backdoors, and manipulated telemetry to obscure activity, positioning itself to reach connected high-value environments, including critical infrastructure. `china` link

Midnight Blizzard's captive portal traffic manipulation and device code phishing campaign
On July 31, Microsoft reported Storm-2945, a sub-cluster of Midnight Blizzard, conducting CaptiveCrunch attacks by manipulating traffic on hospitality captive portal networks worldwide. The activity redirected travellers to lookalike Microsoft sign-in pages for credential theft and enabled follow-on access to Microsoft 365 accounts. Microsoft also observed malware delivery via fake update prompts, leading to compromised devices and broader data exposure across affected venues. `russia` link link

Apple notifies users of mercenary spyware
On August 13, Apple sent a notification to certain users warning them of mercenary spyware attack targeting their iPhones. According to TechCrunch, Apple told them that it notified users in 110 countries. The threat actor was not identified and the notifications do not confirm successful compromise. Apple advised recipients via push alerts, e-mail, and account logins to take protective actions. link

Fake CCleaner delivers GhostDesk Chrome spyware
On August 11, Sav Wheeler reported a campaign using a fake CCleaner download site to infect Windows users with a malicious Chrome extension dubbed GhostDesk. The installer alters Chrome to enable browser-based spying, including credential theft, keystroke logging, cookie theft, and screen capture, with data sent to attacker-controlled infrastructure. No threat actor was identified. The activity appears globally scoped and may also spread via other fake software installers. link link

Cybercrime

Rust crates supply-chain compromise via typosquatted dependency On August 20, Wiz Research reported malicious releases of the Rust crates arrayref, internment and append-only-vec on crates[.]io that introduced a typosquatted dependency to execute a remote payload during builds. Any developer or CI environment compiling affected projects could be compromised, with follow-on credential and browser data exposure and persistence. Infrastructure overlaps with operations attributed to North Korea-linked threat actors. `north korea` link

Fake Zoom installer delivers Overlord RAT on macOS
On August 6, Jamf Threat Labs reported a campaign using a fake Zoom installer to trick users into installing a malicious downloader that deploys the Overlord remote access tool on macOS, while also installing the legitimate Zoom app to reduce suspicion. The activity targets macOS systems globally and enables remote surveillance and control. No specific threat actor was attributed. link

Fake Cloudflare Captcha pages hosted via npm mirrors
On August 25, OX Security reported a campaign abusing the npm registry to host fake Cloudflare Captcha pages across 24 malicious packages. The activity appears aimed at phishing and redirecting users to attacker-controlled destinations, with potential to deliver ClickFix malware. Impact is primarily exposure of users who browse package files via trusted npm mirror domains, which can lend legitimacy and extend reach even after takedowns. link link

Exploitation of macOS Screen Sharing bypass (CVE-2026-65400) to deploy Monero miner
On August 12, NCSC-NL reported threat actors actively exploiting CVE-2026-65400, a macOS Screen Sharing authentication bypass, to gain unauthorised access to internet-exposed systems. A PoC exploit for CVE-2026-65400 was released on GitHub. In observed cases, attackers obtained root access and deployed a Monero cryptocurrency miner. The activity affected multiple macOS hosts with Screen Sharing reachable from the internet, indicating opportunistic compromise and potential for broader system misuse. link link

Data exposure and leaks

ShinyHunters vishing-led SSO phishing against ReliaQuest
On August 22, ReliaQuest employees were reportedly targeted in a ShinyHunters social engineering campaign involving phone-based impersonation and a fake SSO login page on a lookalike domain. One employee entered credentials and approved MFA, giving the actor temporary view-only access to an identity dashboard. ReliaQuest said no applications or customer data were accessed and no persistence was established. `technology` link link link

Mozilla updates GPG signing key for Firefox releases after exposure
On August 10, 2026, Mozilla replaced the GPG signing subkey for certain Firefox and Thunderbird releases after an unencrypted copy was inadvertently committed to a private GitHub repository. Mozilla found no evidence of unauthorized access, revoked the old key, and added safeguards. Most users need no action; manual signature verifiers and some Firefox RPM users must update their keys. `technology` link

Enumeration campaign targeting Salesforce and ServiceNow guest interfaces
On August 12, security researchers reported a campaign, dubbed 'City-Forum', in which an unknown threat actor had been systematically enumerating publicly exposed Salesforce Experience Cloud and ServiceNow Service Portal instances worldwide. Operating from a single Contabo-hosted IP, the actor exploits over-permissioned guest user configurations across telecoms, financial services, enterprise software vendors, and public-sector organisations to

extract records at scale. `telecommunications` `finance` `technology` `public administration` link

Artificial intelligence

Meta AI model hacked another organisation during testing
On August 6, Meta said one of its AI models connected to the internet and compromised another organisation's systems during an independent security evaluation by Irregular. Meta attributed the incident to a tester misconfiguration and said it is investigating. The affected organisation was not named, but the activity involved unauthorised access beyond the test scope, echoing similar recent AI-agent incidents. `technology` link

Mythos 5 and GPT-5.6 Sol agentic AI unauthorised intrusions during UK AISI cyber evaluation
On August 4, the UK's AI Security Institute reported that during cyber capability evaluations conducted between 25–28 July 2026, AI agents, primarily Mythos 5, and GPT-5.6 Sol took unauthorised actions on the live internet across 19 instances. Activity included supply-chain attacks, creation of fake GitHub accounts, sockpuppeting, spearphishing, prompt injection, and deceptive social engineering targeting real, uninvolved individuals. No real-world harm was reported. `technology` link

Kimi K3 cheating via sandbox egress leak in cybersecurity benchmarks
On August 6, UK AI Safety Institute reported that the Kimi K3 model exploited a sandbox misconfiguration to access external resources and obtain benchmark solutions, rather than completing defensive tasks as intended. Unlike previous AI hacking incidents, this case involves a model already widely available to the public, with only the standard safeguards an average user would encounter. `technology` link

Opportunistic

Chaindrop Shai-Hulud npm supply-chain worm compromises keyv ecosystem
On August 4, Aikido reported that the ChainDrop (Shai-Hulud-based) self-propagating malware was distributed via compromised npm packages after a Keyv maintainer's GitHub account was taken over. The campaign steals credentials from developer and CI/CD environments and uses them to spread to additional maintainers. At least hundreds of packages and over 2 billion monthly installs were exposed, impacting organisations globally. `technology` link link link

BdThemes WordPress plugins supply-chain compromise via poisoned promotional API
On August 8, Wordfence reported a supply-chain compromise affecting multiple BdThemes WordPress plugins, where attackers poisoned a trusted promotional API feed to trigger malicious activity in administrators' sessions. The campaign enabled creation of rogue admin accounts, installation of webshells, and persistence mechanisms, leading to full site takeover. The threat actor was not named, but infrastructure was linked to recent similar WordPress supply-chain attacks. ` link link

Zero-day exploitation of PaperCut NG/MF servers
On August 27, PaperCut Software reported active zero-day exploitation of a vulnerability affecting all versions of PaperCut NG and PaperCut MF. Attacks targeted organisations with internet-exposed Application Servers, with confirmed customer incidents. PaperCut urged immediate restriction of web access to trusted IP addresses and released emergency patches for some versions. The threat actor and follow-on objectives were not disclosed. link link

Gitea critical RCE vulnerability CVE-2026-60004 exploited in the wild
On August 25, CISA added Gitea's critical RCE vulnerability CVE-2026-60004 to its Known

Exploited Vulnerabilities catalogue. The vulnerability allows a malicious actor with ordinary write access to a repository to execute arbitrary shell commands as the Gitea OS user. With default open registration, an unauthenticated visitor can obtain the required write access by registering an account and creating a repository. Gitea disclosed and patched the vulnerability in July. link

Exploitation of critical MLflow SSRF vulnerability enabling cloud credential theft
On August 19, CISA reported that threat actors are actively exploiting CVE-2026-64849, a critical server-side request forgery vulnerability in MLflow, an open-source AI engineering platform. The flaw allows unauthenticated attackers to access internal services and steal cloud credentials, including AWS IAM credentials. link link

Windows IKE RCE vulnerability CVE-2026-33824 exploited in the wild
On August 19, CISA reported that threat actors are exploiting CVE-2026-33824, a critical Windows Internet Key Exchange (IKE) Service Extensions flaw, to gain remote code execution on unpatched Windows 10, Windows 11, and Windows Server systems. Malicious actors can exploit this vulnerability by sending maliciously crafted packets through UDP ports 500 or 4500. The vulnerability was patched in April. link

Active exploitation of critical SAP Commerce Cloud RCE vulnerability
On August 14, Defused, a cybersecurity company, reported that a maximum-severity remote code execution vulnerability in SAP Commerce Cloud (CVE-2026-58231) is being actively exploited. Unauthenticated attackers are targeting the flaw, which carries a CVSS score of 10.0, with exploitation attempts observed on honeypots. The vulnerability was patched three days earlier. Over 4.200 internet-facing SAP Commerce Cloud instances have been identified globally, primarily across Europe and North America. link 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.