CERT-EU

Cyber Brief (September 2025)

October 1, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 285 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, Russia-linked bulletproof host Stark Industries has evaded EU sanctions, and Italy approved the first artificial intelligence law in line with the EU's AI act. Czechia's cyber agency warns critical infrastructure entities against Chinese technology and updates its assessment of China-linked disruption to 'high'.
- In regards to **cybercrime**, Cloudflare and Microsoft jointly take down RaccoonO365 PhaaS domains, and ESET discloses PromptLock, the first alleged AI-powered ransomware. Acronis identified a spearphishing campaign using FileFix to harvest credentials.
- On the **cyberespionage** front, Iran-linked UNC1549 conducted a multi-sector spearphishing campaign in Europe, and two Dutch teenagers were arrested for Russia-linked espionage against Europol and Eurojust. Russia-linked APTs Turla and Gamaredon reportedly collaborated to target Ukraine.
- There were **disruptive** attacks that impacted several European airports, and Moldova's electoral commission suffered a denial-of-service attack days before its elections. Ukraine's HUR cyber units attacked Russian fuel and telecommunications networks.
- Regarding **data exposure and leaks** incidents, Polish Bank PKO Polski, allegedly experienced a breach of its employee contact data, and London North Eastern Railway reported a breach of its customer data.
- On the **hacktivism** front, Russia-linked hacktivists NoName057 claimed DDoS attacks against Romanian websites to oppose joint Romanian-Ukraine drone development, and claimed DDoS attacks against French websites citing their solidarity with the French 'Block Everything' protest.

Europe

Cyber policy and law enforcement

Bulletproof host Stark Industries evades EU sanctions
On September 11, KrebsOnSecurity reported that EU sanctions imposed on May 20, 2025, against Stark Industries Solutions, a bulletproof host tied to Russia-linked threat actors, had limited effect. Within weeks, Stark rebranded as 'the[.]hosting' under Dutch entity WorkTitans BV. By June 24, 2025, they shifted infrastructure to Moldova's PQ Hosting Plus. Both remain linked to the original operators. `russia` link

Italy approves new AI law
On September 17, Italy's Parliament approved a law on the safe use of artificial intelligence. The law covers several sectors, including public administration, health, labour, justice, and education, requiring traceability and human oversight of AI decisions. This makes Italy the first European Union country with comprehensive AI regulations aligned with the EU's AI Act. `artificial intelligence` link

Czech cyber agency warns critical sectors against using technology that transfers data to China
On September 3, the Czech Republic's National Cyber and Information Security Agency (NUKIB) warned critical infrastructure operators to avoid using Chinese technology citing a newly assessed 'High' risk of disruption. The agency stressed that Chinese suppliers can access sensitive data and already conduct hostile cyber activity, urging sectors like energy, healthcare, transport, and finance to include these threats in risk analyses and adopt strong mitigation measures. `china` link

Poland increases cybersecurity budget amid daily Russia-linked attacks disrupting hospitals and water supply plants
On September 16, Poland announced an increase in its cybersecurity budget from 600 million euros to one billion euros after ongoing reported Russia-linked sabotage attacks. Several incidents reportedly caused temporary outages at healthcare facilities, in addition to a major attempt against a water supply plant in a major city. `russia` link

Cyberespionage & prepositioning

Iran-linked UNC1549 deploys malware in campaign targeting defence, telco and aerospace sectors in Europe
On September 22, CheckPoint research reported on Iran-aligned UNC1549 conducting a long-running cyberespionage campaign targeting the defence, telecommunications, and aviation sectors in Europe. The campaign involved spearphishing attacks luring victims to fake career portals. These portals were used to deliver malware through a multi-stage DLL side-loading technique, which involved the use of previously undocumented low-level APIs. `Iran` link

Dutch teenagers arrested for Russia-linked spying on Europol and Eurojust
On September 27, Dutch authorities arrested two 17-year-old boys accused of using Wi-Fi sniffer devices to surveil Europol, Eurojust and the Canadian embassy after recruitment via Telegram to spy for Russia. A Europol spokesperson confirmed the incident, reporting no signs of a compromise on the agency's systems. `russia` link

Targeted cyberattack on Austrian Interior Ministry IT systems
On August 30, an Austrian media outlet reported a cyberattack affecting the IT infrastructure of Austria's Ministry of Interior, which led to unauthorised access of 100 out of 60.000 e-mail accounts. No sensitive or personal data were reportedly affected. link

Russia-linked Gamaredon and Turla collaborate
On September 19, ESET revealed the first known collaboration between the Russian FSB-linked groups Gamaredon and Turla. Gamaredon used tools like PteroGraphin, PteroOdd, and PteroPaste to restart Turla's Kazuar v3 backdoor and to deploy Kazuar v2 implants on select machines in Ukraine. Turla appears to be operating only on high-value targets in Ukraine, while Gamaredon handles broader initial access operations. `russia` link

Disruption & destruction

European airports disrupted by cyberattack
On September 20, a cyberattack on Collins Aerospace's MUSE system disabled electronic check-in and baggage drop at Brussels, Heathrow, Berlin, and other European airports, forcing a switch to manual operations. In Brussels, several flights were cancelled or diverted, and authorities advised that half of the departing flights scheduled for September 21 be cancelled to ease the backlog. `transport` link

Moldova's electoral commission experienced cyberattack ahead of elections
On September 26, Moldova's Central Election Commission experienced an alleged Russia-linked cyberattack days before its parliamentary elections. Wi-Fi routers were allegedly hijacked for denial-of-service against its servers. The European Commission deployed its new cyber reserve to assist Moldova, marking the first activation of the EU capability under the Cyber Solidarity Act. `russia` link

Ukraine's HUR cyber units attack Russian fuel and telecom networks, causing millions in losses
On September 7, Ukraine's Defense Intelligence (HUR) cyber units launched cyberattacks against Russian infrastructure, reportedly disrupting fuel payment systems, telecom networks, and online platforms. The attacks also included the defacement of Russian websites with pro-Ukraine messages marking Military Intelligence Day. The attacks allegedly caused an estimated 1–3 million US dollars in losses. `russia` link

Information operations

Russia-linked information operations targeting Moldovan elections
On September 3, Recorded Future reported on Russia-linked information operations targeting Moldovan elections. These campaigns included Operation Overload, Foundation to Battle Injustice, Operation Undercut, Portal Kombat, and Russia-based social media pages. The campaigns pushed unfavourable narratives of Moldova's President and advocated for a closer relationship between Moldova and Russia. `russia` link

Russia-linked Storm-1516 targets European and North American countries leveraging AI-generated deepfakes
On September 18, Recorded Future reported on CopyCop (Storm-1516), a Russian GRU-linked influence campaign that launched over 200 fake media sites targeting the US, France, Canada, Germany, Armenia and Moldova. It now also publishes in Turkish, Ukrainian and Swahili, pushing AI-generated deepfakes and dossiers to undermine support for Ukraine. Its reach and organic engagement remain high. `russia` link

ISD uncovers Czech X network spreading pro-Russia propaganda ahead of elections
On September 4, the Institute for Strategic Dialogue (ISD) published an investigation exposing a Czech-language X community of around 70 pseudonymous accounts spreading pro-Russia propaganda and anti-Ukraine narratives ahead of the Czech elections in October. The accounts

repackage Russia state media articles promoting conspiracies for Czech audiences. Its current reach remains limited. `russia` link

Russia-linked disinformation targets Poland after drone incident
On September 12, Poland reported that a Russian disinformation campaign followed drone incursions into its airspace. Poland's National Research Institute NASK detected anti-Ukraine disinformation campaigns portraying Poland as weak and suggesting military escalation with Belarus. Poland's cybersecurity leadership held emergency meetings and pledged to provide verified updates to counter the campaign's wide online reach. `russia` link

Data exposure and leaks

PKO Bank Polski allegedly breached with data of employees contact information for sale
On September 9, an unnamed threat actor on a cybercrime forum claimed to sell data pertaining to the details of 32.815 employees and 17.135 devices obtained from Polish Bank PKO Polski. The bank confirmed that an actor had contacted them over allegedly obtained employee contact information, but reported that no sensitive or private data of bank employees or its customers were exposed. `finance` link

LNER reports third-party data breach affecting customer contact details
On September 10, London North Eastern Railway (LNER) reported that files held by a third-party supplier had been accessed without authorisation, exposing customer contact details and partial past journey information but did not include payment, bank or password data. Train services and ticketing were reportedly unaffected. `transport` link

Hacktivism

Pro-Russia hacktivists NoName057 target Romanian government and transport sites
On September 29, pro-Russia hacktivist group NoName057 claimed responsibility for unverified distributed denial-of-service (DDoS) campaigns targeting at least five Romanian websites, including government, transportation and airport entities. The group framed the activity as part of their #OpRomania campaign, citing media reports of joint Romanian-Ukrainian drone development. `Russia` link

NoName057 targets French organisations amid Block Everything protests
On September 10 and 11, Russia-linked hacktivist group NoName057 made unverified claims of DDoS attacks against at least 15 French organisations, including government agencies, an insurance firm, an airport and manufacturing entities, citing support for France's 'Block Everything' protests. `russia` link

World

Cyber policy and law enforcement

US Secret Service dismantle network of electronic devices in New York City
On September 23, the US Secret Service reportedly dismantled a network of electronic devices located within 55km of the United Nations. They seized over 300 SIM servers and 100.000 SIM cards. These could have been used to carry out anonymous threats towards US officials and could have been used to conduct telecommunications attacks, including DDoS. They reportedly

found evidence of communications between nation-state threat actors and individuals known to law enforcement. `telecommunications` link

Cyberespionage & prepositioning

WhatsApp patches zero-click flaw exploited in targeted attacks
On August 29, WhatsApp released patches for a critical zero-click vulnerability (CVE-2025-55177) affecting iOS, WhatsApp Business on iOS, and macOS clients, which was exploited in sophisticated targeted attacks. The flaw allowed unauthorised users to trigger content processing from arbitrary URLs on a victim's device, potentially combined with an Apple OS-level vulnerability (CVE-2025-43300). Affected users were urged to update promptly and consider a factory reset if notified of compromise. `telecommunications` link

North Korea-linked Famous Chollima monitors their infrastructure using public threat intelligence sources
On September 4, SentinelLabs reported that North Korea-linked threat actor Famous Chollima is leveraging public threat intelligence sources to actively monitor their infrastructure. The threat actor used Gmail addresses with Astrill VPN IPs to create Validin accounts. They also monitor the Maltrail project on GitHub to check for indicators linked to Lazarus and used Slack to coordinate their activities. `north korea` link

APT29 watering hole campaign mimicking Cloudflare verification pages
On August 29, Amazon disrupted a watering hole campaign by Russia-linked threat actor APT29. The group compromised websites to redirect users to domains mimicking Cloudflare, luring them into Microsoft's device code authentication flow for credential harvesting. Amazon isolated affected infrastructure, partnered with providers to block domains, and shared intelligence with Microsoft. `russia` link

Cybercrime

Cloudflare and Microsoft joint takedown of RaccoonO365 PhaaS domains
On September 10, Cloudflare and Microsoft announced that they dismantled RaccoonO365, a Phishing-as-a-Service enterprise that sold phishing kits via telegram designed to steal Microsoft 365 credentials. They conducted a joint takedown of hundreds of Cloudflare domains and Worker accounts in coordination with Microsoft's broader efforts through a civil lawsuit filed in August. link

Global spearphishing campaign leverages FileFix to harvest credentials
On September 16, Acronis reported a spearphishing campaign leveraging a variant of the FileFix technique to harvest credentials. The campaign uses multilingual phishing pages and leveraged steganography to hide an obfuscated PowerShell and payloads inside JPG images. The multi-stage payloads fetched a Go-based loader that drops the StealC infostealer that harvests browsers, wallets and cloud credentials. Worldwide detections suggest an accelerating global campaign. link

Malicious npm packages used to conduct supply-chain attack
On September 8, Aikido's intelligence feed reported an incident affecting 18 popular npm packages with over 2.6 billion weekly downloads. Unknown threat actors injected malicious code that acts as a browser-based interceptor, capable of hijacking network traffic and application APIs. It reportedly monitors for cryptocurrency addresses and transactions, which they then redirect to attacker-controlled wallet addresses. The threat actors were able to modify the packages after delivering phishing e-mails to maintainers. link

ESET reveals first alleged case of AI-powered ransomware PromptLock
On August 27, ESET disclosed PromptLock, a proof-of-concept ransomware they claim is the first known AI-powered variant. It reportedly leverages a local OpenAI gpt-oss:20 b model via the Ollama API to dynamically generate and execute malicious Lua scripts to enumerate files, exfiltrate data and encrypt systems across Windows, macOS and Linux. While not yet observed in the wild, PromptLock highlights that AI-driven adaptability will likely continue to enhance threat actor operations. `artificial intelligence` link

Opportunistic

Cisco ASA vulnerabilities CVE-2025-20333 and CVE-2025-20362 actively exploited as zero-days
On September 25, Cisco reported that a threat actor is chaining exploitation of two zero-days affecting Cisco ASA devices, namely CVE-2025-20333 and CVE-2025-20362. The exploitation allows for unauthenticated, remote code execution and full device control on affected devices. Cisco observed the exploitation on legacy Cisco ASA 5500-X firewalls running ASA Software with VPN web services enabled. Related CERT-EU product: TA 25-153. link

Cisco IOS and IOS XE zero-day vulnerability CVE-2025-20352 exploited in the wild
On September 24, Cisco issued a security advisory for Cisco IOS and IOS XE for CVE-2025-20352. Attackers exploiting this vulnerability can perform Denial-of-Service with low privileges and remote code execution with root privileges. A threat actor exploited this vulnerability in the wild as a zero-day after compromising local administrator credentials. Affected organisations should patch as there are no known workarounds for this vulnerability. link

GreyNoise warns of massive scans targeting Cisco ASA devices ahead of possible exploits
On September 4, GreyNoise reported a sharp surge in scans against Cisco ASA devices, logging up to 25.000 unique IPs, mostly from a Brazilian botnet, probing ASA login portals and Cisco IOS Telnet/SSH. Researchers warn such reconnaissance often precedes vulnerability disclosures and urge administrators to patch ASA devices, enable MFA, restrict external access to interfaces, and use shared indicators to block or limit suspicious traffic before exploitation attempts occur. link

Over 3.300 secrets stolen in GhostAction supply chain campaign via GitHub workflows
On 5 September, GitGuardian disclosed GhostAction, a supply chain campaign in which threat actors injected malicious GitHub Actions workflows into 817 repositories across 327 users. These workflows exfiltrated 3.325 secrets, including PyPI, npm and Docker Hub tokens, to an attacker-controlled endpoint via HTTP POST requests. The breach underscores the significant risks of compromised CI/CD pipelines and workflows within the software supply chain. link

Microsoft Entra ID flaw allowed hijacking any company's tenant
On September 21, serious vulnerability CVE-2025-55241 was revealed in Microsoft Entra ID (formerly Azure AD) that let attackers hijack any company's tenant. By exploiting 'actor tokens' (undocumented, unsigned tokens) via the deprecated Azure AD Graph API, a threat actor could impersonate any user, including global administrators, accessing sensitive data without triggering tenant logs. Microsoft patched the issue on September 4. 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.