CERT-EU

Cyber Brief (June 2026)

July 1, 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 approved Ukraine's inclusion into the EU's Cybersecurity reserve, while Europol and law enforcement from several countries coordinated under Operation Endgame to dismantle the SocGholish malware network. The United States' (US) authorities seized domains allegedly used for China-linked intelligence collection, and placed a bounty on operators of Russia-linked threat actors UNC5792 and UNC4221.
- On the **cyberespionage** front, suspected Belarus-linked threat actor Ghostwriter reportedly engaged in a spearphishing campaign targeting Polish Gmail users, and the Belgian intelligence services were targeted by an unknown threat actor through Ivanti EPMM exploitation.
- Regarding **cybercrime**, an unknown threat actor reportedly uploaded malicious plugins on the JetBrains Marketplace posing as AI coding assistants for credential theft, while unknown threat actors reportedly abused Instagram's Meta AI account recovery tool for account takeovers.
- In terms of **digital foreign interference**, French authorities tied Israel-based firm Blackcore to an information manipulation operation targeting France during the March 2026 municipal elections.
- Regarding **disruptive and destructive** cyberattacks, the US Cybersecurity and Infrastructure Security Agency (CISA) reported unknown threat actors actively exploited a SolarWinds Serv-U vulnerability, creating a risk of disruption for organisations running Serv-U.
- We observed numerous **data exposure and leaks** incidents. ShinyHunters claimed a data breach affecting the Council of Europe and Oracle PeopleSoft customer instances globally. Unknown threat actors compromised the French State's encrypted messaging service Tchap, and other unknown threat actors breached the World Food Programme's Gaza self-registration portal, exposing beneficiary data.

- As for notable **Common Vulnerabilties and Exposures (CVEs)**, Google issued an emergency update for Chrome to address CVE-2026-11645, a high-severity zero-day vulnerability actively exploited in the wild, while Microsoft announced a patch for an actively exploited Exchange Server zero-day CVE-2026-42897 enabling cross-site scripting against Outlook Web Access users.

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 Council of the EU approved Ukraine's inclusion in the EU Cybersecurity Reserve
On June 15, the European Commission announced that Ukraine can activate emergency EU cyber support to respond to large-scale cybersecurity incidents, after the Council of the EU approved its inclusion in the EU Cybersecurity Reserve. The decision forms part of the EU's strategic digital partnership agenda. `cybersecurity` link

Operation Endgame dismantled SocGholish malware network
On June 18, the Dutch, US, Canadian, and German authorities, backed by Europol and Eurojust, disrupted a key infection chain used by cybercrime groups, remediating 14.971 websites infected with SocGholish malware, tied to Russian-speaking threat actor Evil Corp. Worldwide, they took down 106 servers and domains. `law enforcement` link

France's cybersecurity agency announced it will stop certifying products without quantum-safe encryption
On June 16, France's cybersecurity agency, ANSSI, announced it would halt the certification of security products that lack quantum-resistant encryption from 2027, and stated businesses should acquire only quantum-safe products by 2030. ANSSI approval of products is required for use in French government agencies and critical infrastructure. `technology` link

Polish authorities arrested four accused of SIM-swapping and cryptocurrency theft
On June 25, Polish authorities arrested four members of a cybercrime group accused of stealing millions in cryptocurrency through SIM-swapping attacks. The suspects allegedly compromised telecom partners and employee accounts to hijack phone numbers, bypass SMS-based authentication, and access victims' crypto accounts. The operation involved Polish authorities, the FBI, and Homeland Security Investigations. `law enforcement` link

Cyberespionage & prepositioning

Belarus-linked threat actor Ghostwriter Gmail credential and 2FA phishing campaign
On June 12, CERT Polska reported that likely Belarus-linked threat actor Ghostwriter has been running high-intensity phishing campaigns targeting Gmail users in Poland. The actor used fraudulent e-mails impersonating Gmail security alerts to harvest login credentials and two-factor authentication codes, enabling account takeovers. Victims included people in political and public life, journalists, researchers, and public administration, with repeated targeting and broad spillover to unrelated recipients due to address guessing. `public administration` `belarus` `russia` link

Fortinet FortiGate and MSSQL targeted in Fortibleed campaign against organisations worldwide
On June 15, a security researcher reported a credential harvesting campaign that targeted exposed Fortinet FortiGate SSL VPNs, with data used in global follow-on attacks. At least four organisations across Japan, Taiwan, Vietnam, Iraq, and Turkey were compromised, including a Turkish NATO defence contractor suffering classified document exfiltration. The operation processed 1.16 billion credential attempts against 320.777 FortiGate targets and 2.1 billion against 163.650 MSSQL servers. `transport` `technology` `defence` link

Belgian intelligence services targeted by an unknown threat actor through Ivanti EPMM exploitation
On June 19, journalistic outlets reported that Belgium's civilian intelligence service was breached between May 2025 and spring 2026 after unknown threat actors exploited Ivanti Endpoint Manager Mobile flaws to access and potentially exfiltrate work mobile telephony and e-mail data. Exposed information included names, phone numbers, e-mail addresses, phone ID, and GPS positions. Details of people contacted through the phones were also potentially exposed. `public administration` `defence` link

Possible Mustang Panda phishing campaign targeting the Greek representation to NATO
On June 23, a security researcher shared indicators from a submission on AnyRun's online sandbox, which indicated a possible China-linked Mustang Panda phishing campaign targeting the Greek representation to NATO. The threat actor spoofed a Montenegro diplomatic e-mail address to deliver a lure regarding the Ankara Summit. The phishing link redirects through a fake Cloudflare check to a Google Drive clone, dropping a malicious ZIP. `diplomacy` `defence` `china` link

Digital foreign interference

Rokh Solis influence operation targeted French municipal elections
On June 11, France's service for monitoring and protection against foreign digital interference, Viginum, reported on Rokh Solis, an information manipulation operation targeting France during the March 2026 municipal elections. The campaign used coordinated online personas and websites to smear La France Insoumise, specific candidates, and to polarise debate by exploiting narratives about the Muslim community. Viginum assessed foreign involvement, linked to the Israeli influence firm Blackcore. Overall online reach appeared limited. `political parties` `public administration` `civil society` `israel` link

Data exposure and leaks

ShinyHunters claimed data breach against Council of Europe
On June 14, cybercrime actor ShinyHunters claimed a data breach belonging to the Council of Europe. ShinyHunters claimed to have exfiltrated more than 297GB of data, including personal data impacting up to 10.000 staff, and has threatened to leak the data on June 16 unless demands were met. The Council of Europe reports it is investigating the breach. `justice` `fundamental rights` link

Compromise of the French State's encrypted messaging service Tchap
On June 8, France's Interministerial Directorate for Digital Affairs, DINUM, reported a compromise of the French State's encrypted messaging service Tchap, detected by ANSSI after account impersonation. Authorities identified and blocked the malicious account, and investigations continue to determine accessed conversations and any data exfiltration. Private encrypted chats were not accessible; potential exposure is limited to unencrypted public rooms. DINUM notified CNIL and warned users. `public administration` link

Breach of State Accreditation Service system via Apache Superset
On June 10, Lithuanian Health Minister Marija Jakubauskienė reported a cyber incident affecting a system run by the State Accreditation Service for Health Care Activities. An unknown threat actor gained unauthorised access and may have accessed over 62.000 records, including specialists' professional and contact details, administrators' data, competency records, and technical metadata. The central e-health system was not affected. `public administration` `health` link

Clinical trial and healthcare provider data theft at Novo Nordisk
On June 11, Novo Nordisk disclosed a cyber incident in which unknown threat actors accessed a limited number of internal IT systems and personal data. Stolen information included pseudonymised clinical trial participant details and identifiable healthcare provider contact data such as names and e-mail addresses. Novo Nordisk engaged external experts, notified authorities, and temporarily took some systems offline. `pharmaceuticals` `health` link

World

Cyber policy and law enforcement

US authorities seized 13 website domains reportedly tied to Chinese intelligence collection
On June 10, US federal authorities seized 13 domains tied to China-linked fabricated consulting firms reportedly designed to lure former US government and military staff to provide intelligence to Chinese agents. The seizure follows the publication of a Five Eyes notice warning that China's military intelligence services are increasingly using online job platforms and intensive recruitment strategies to gather non-public information. `defence` `public administration` `china` link

US government directive suspended global access to Claude Fable and Mythos
On June 12, a US export-control directive citing national security ordered Anthropic to block all foreign-national access, forcing it to disable both models for all customers worldwide, while other Claude models remain unaffected. Anthropic says the cited jailbreak is narrow, already known, and comparable to other models' capabilities, and is working to restore access. The export ban was lifted on June 30. `artificial intelligence` link

US Department of State offered 10 million US dollars for information on Russia-linked threat actors
On June 29, the US Department of State published an announcement offering 10 million US dollars for information helping identify or locate members of the Russia-linked threat actors UNC5792 and UNC4221. These include names, locations, affiliations, links to Russian intelligence services, contractors and third-party providers, operational infrastructure, funding sources, financial accounts, banking relationships, and financial networks supporting operations. Both of these threat actors are known for targeting victims through Signal. `russia` `united states` link

Chinese firm Qihoo 360 claimed it developed an AI model matching Mythos capabilities
On June 24, Chinese cybersecurity firm 360 Security Technology (Qihoo 360) claimed it developed AI tools that rival US-based Anthropic's Mythos models. It developed two tools, one called Tulongfeng, for automated vulnerability discovery, and Yitianzhen, a tool to automate cyber defence and incident response. Qihoo 360's founder described such AI tools as national strategic assets used for defending critical infrastructure and to gain offensive advantages. `artificial intelligence` `cybersecurity` `china` link

China-based Z.ai's GLM-5.2 matched leading US models for vulnerability discovery
On June 13, Chinese technology company Z.ai released its latest open-weight model, GLM-5.2. Security researchers widely assessed its vulnerability discovery capabilities match those of models from leading US companies such as Anthropic and OpenAI. `artificial intelligence` `china` link

Russia revised AI model legislation to support domestic development
On June 25, a trusted partner reported that Russia approved revised AI legislation regulating large-scale fundamental models and defining national and sovereign AI models. The draft narrows earlier broad AI-governance proposals to frontier models, removes restrictions on foreign data and components, enables federal support and government use, and may permit Federal Security Service-approved access to federal systems. `artificial intelligence` `russia` link

Russia abused Cellebrite to extract information from a human rights activist's phone
On June 25, Citizen Lab reported that Russia abused forensic acquisition tool Cellebrite to extract information from the iPhone of human rights activist Andrey Pivovarov. Russian authorities arrested him in May 2021 and confiscated his iPhone and MacBook. Analysis from the Citizen Lab found that the device was accessed with Cellebrite in June 2021. Russian authorities continued to use Cellebrite despite Cellebrite's cancellation of Russian contracts. `civil society` `europe` `russia` link

Cyberespionage & prepositioning

China-linked Warp Panda compromised edge appliances to access M365
On June 4, China-linked threat actor Warp Panda reportedly compromised a victim and their managed services provider, abusing edge appliances to maintain covert access. The actor used stolen credentials to regain entry, pivot internally, and leverage the foothold to access Microsoft 365 while blending with legitimate traffic. Multiple appliances were affected over an extended period, increasing exposure and complicating detection and remediation. `china` link

Alleged Alibaba-linked distillation campaign against Anthropic Claude
On June 22, Anthropic accused operators linked to Alibaba of illicitly extracting Claude AI model capabilities via large-scale distillation attacks. Anthropic said the activity used thousands of fraudulent accounts and nearly 29 million exchanges to harvest high-value model behaviours for training competing systems. The reported scope suggests an industrial-scale effort to repackage US AI capabilities, prompting calls for stronger penalties and protections. `artificial intelligence` `china` link

Alleged attempted Israeli interception of US–Iran talks via wiretapping
On June 8, journalistic outlets reported US intelligence concerns that Israeli intelligence agencies attempted to intercept communications of senior US officials involved in Iran negotiations. Reports cited suspected surreptitious installation of software to tap communications on US defence personnel's phones and other eavesdropping attempts. The Pentagon reportedly raised Israel's counterintelligence threat level to critical, potentially affecting information-sharing and operational coordination. `defence` `public administration` `israel` link

NSO-linked spearphishing attempt via WhatsApp lures
On June 8, WhatsApp reported it caught and disrupted Israel-based NSO Group-linked spearphishing and social engineering attempts targeting users globally. The activity sought to trick recipients into clicking malicious links that redirected them to external websites, and included the creation of test accounts and groups that were removed. WhatsApp shared

indicators to help potential victims identify targeting across platforms such as text message, e-mail, and WhatsApp. `social media` `israel` link

Russia-linked UNC5792 and UNC4221 target Signal users' backup recovery keys in phishing campaign
On June 26, the US Federal Bureau of Investigation published a public service announcement regarding Russia-linked threat actors UNC5792 and UNC4221 targeting Signal users' backup recovery keys in phishing campaigns. The threat actors continue to masquerade as Signal support but are also attempting to elicit victims' backup recovery key. This allows the attacker to view the account's backup messages, private and group messages, and take over the victim's account. `russia` link

Cybercrime

Instagram Meta AI account recovery abused for account takeovers
On June 2, threat actors reportedly abused Instagram's Meta AI account recovery tool to obtain password reset codes and hijack accounts without proper verification. They targeted high-value short-handle accounts and rapidly resold them via Telegram channels. Meta stated no backend breach occurred and patched the issue after public reporting. The activity enabled unauthorised account takeovers affecting premium Instagram usernames globally. `social media` link

JetBrains Marketplace malicious plugins campaign stole AI API keys
On June 16, researchers reported a coordinated malware campaign by an unknown threat actor on the JetBrains Marketplace. At least 15 IDE plugins posing as AI coding assistants secretly stole users' AI provider API keys. The activity affected multiple vendor accounts and may have reached nearly 70.000 installs. Stolen keys could enable unauthorised AI usage, account abuse, and unexpected costs for victims. `technology` link

Disruption & destruction

Active exploitation of SolarWinds Serv-U DoS flaw CVE-2026-28318 to crash servers
On June 5, CISA reported unknown threat actors were actively exploiting a recently patched SolarWinds Serv-U vulnerability, tracked as CVE-2026-28318, to crash exposed file transfer servers. The activity is global and requires no authentication, creating disruption risks for organisations running Serv-U. CISA added the issue to its Known Exploited Vulnerabilities Catalog and urged rapid patching and mitigation. `technology` link

Data exposure and leaks

Unauthorised access to World Food Programme Gaza self-registration portal exposed beneficiary data
On June 2, journalistic outlets reported unknown threat actors accessed the World Food Programme (WPF)'s Palestine self-registration application (People Portal), exposing personal data of around 600.000 Gazan households. Compromised information reportedly included names, IDs, mobile numbers, and location data. WFP said the intrusion occurred on May 14, and shut down the platform to contain the incident. `public administration` link

ShinyHunters data theft targeted Oracle PeopleSoft instances
On June 10, researchers reported data theft attacks targeting Oracle PeopleSoft customer instances, linked to the ShinyHunters cybercrime group. The threat actor claimed to have stolen data from 300 instances across more than 100 organisations, with many victims in the

education sector. Victims reportedly received extortion demands. Nottingham University was named as impacted, with data allegedly published on the group's leak site. `technology` link

Notable CVEs

One-click github.dev token theft via VS Code zero-day
On June 3, a security researcher reported a VS Code zero-day that can be abused to steal GitHub authentication tokens after a victim clicks a crafted github.dev link. The exploit enables installation of a malicious extension that exfiltrates the token and can be used to access and modify repositories, including private ones, and enumerate accessible repositories. `technology` link

Chrome zero-day CVE-2026-11645 exploited in the wild
On June 8, Google issued an emergency update for Chrome to address CVE-2026-11645, a high-severity zero-day vulnerability actively exploited in the wild. The flaw, residing in the V8 JavaScript engine, allows remote attackers to execute arbitrary code via crafted HTML pages. This marks the fifth Chrome zero-day patched in 2026. The threat actor remains unknown. Patched versions are available for Windows, Mac, and Linux. `technology` link

Exchange Server XSS zero-day exploited via Outlook Web Access
On June 10, Microsoft announced a patch for an actively exploited Exchange Server zero-day (CVE-2026-42897) enabling cross-site scripting against Outlook Web Access users. Remote attackers could send specially crafted e-mails that, when opened under certain conditions, execute malicious scripts in the user's browser context. The activity affected Exchange Server 2016, 2019 and Subscription Edition globally, prompting urgent patching and continued mitigation. `technology` link

Exploitation of Cisco Unified CM SSRF flaw for device probing
On June 23, a researcher reported active exploitation of CVE-2026-20230 in Cisco Unified Communications Manager (CUCM). The researcher observed attacks from a single IP address attempting to identify vulnerable systems by writing a test file, with potential follow-on abuse to gain elevated access. No specific threat actor was attributed. The activity indicates global scanning and early-stage compromise risk for exposed CUCM servers. `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.

TLP	Disclosure	Message
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.