CERT-EU

Cyber Brief (July 2026)

August 3, 2026 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 363 open source reports for this Cyber Brief.[1]
- Relating to **cyber policy and law enforcement**, the Council of the European Union sanctioned nine individuals and four entities linked to FSB-directed Turla operations, while Europol coordinated the removal of thousands of URLs associated with the cybercrime group The Com. Spanish police arrested an alleged member of the Russia-linked CyberArmy of Russia Reborn.
- On the **cyberespionage & prepositioning** front, the United States (US) Cybersecurity and Infrastructure Security Agency (CISA) reported that Russia-linked Laundry Bear had conducted zero-click phishing campaigns against organisations using Zimbra webmail, while journalists reported that Morocco's intelligence service used Pegasus spyware to target European politicians and journalists. Additionally, likely China-linked threat actors reportedly exploited a vulnerability in Roundcube mail servers to compromise US and Canadian universities.
- In regards to **cybercrime**, phishing and ransomware featured prominently. The Kratos Phishing-as-a-Service operation targeted Microsoft 365 users across multiple European countries, primarily in Spain. Further, a threat actor exploited an exposed Langflow service to deploy agentic ransomware, while another threat actor leveraged the CitrixBleed 2 vulnerability to deploy ransomware targeting multiple entities globally.
- In terms of **disruptive & destructive** cyberattacks, cybercrime actor ByteToBreach reportedly breached Romania's National Agency for Cadastre and Real Estate, causing a temporary disruption in real-estate transactions nationwide and took official websites and apps offline for a week.
- Regarding **data exposure and leaks**, a ransomware group compromised a Latvian state-owned forestry company, reportedly leaking 44GB of internal data, while a China-linked WP-SHELLSTORM campaign exposed credentials across 1.4 million domains globally.
- As for **opportunistic activity**, there were notable cases of autonomous AI agents escaping their sandboxes. OpenAI's reported that several of its models had chained vulnerabilities across OpenAI's research environment and Hugging Face's production infrastructure, exploiting a zero-day to reach the internet and steal test solutions. Anthropic also reported three incidents

where Claude models gained unauthorised access to several organisations' production systems.

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

EU sanctions Russian threat actors, identifies FSB-linked Turla operations across Europe
On July 13, the High Representative on behalf of the European Union condemned Russia's use of a broad cyber ecosystem of state and non-state actors, identifying the FSB's 16th Centre as directing cyber threat groups including Turla, which conducted espionage, sabotage, and infrastructure-targeting operations against EU member states and international partners. The Council of the European Union imposed sanctions on nine individuals and four entities linked to Russia's cyber activities. `sanctions` `russia` link

Europol flags thousands of URLs linked to cybercrime group The Com for removal
On July 24, Europol announced that 4.340 URLs linked to cybercrime group The Com were flagged for removal, as part of the operation Referral Action Days, in which nine national law enforcement agencies collaborated to disrupt The Com's online ecosystem. The action forms part of the European Commission's ProtectEU counter-terrorism agenda. `law enforcement` link

US and German law enforcement dismantle Kratos phishing platform
On July 21, law enforcement in the US and Germany collaborated as part of Operation Olympus Blade to dismantle infrastructure pertaining to Kratos, a phishing-as-a-service platform, and arrest its developer in Indonesia. The platform had sold phishing kits allowing threat actors to create and operate fake Microsoft authentication pages, used to steal Microsoft credentials. `law enforcement` link

Spanish police arrests alleged member of CyberArmy of Russia Reborn (CARR) and Z-Pentest
On July 6, Spanish police announced the arrest of an alleged member of Russia-linked supposed hacktivist groups CARR and Z-Pentest in March, on charges of "membership in and collaboration with a terrorist organisation, glorifying terrorism, and computer damage". The investigation was made in collaboration with the US's Federal Bureau of Investigation (FBI). `law enforcement` link

Scattered Spider operators sentenced for 2024 cyberattack
On July 16, the United Kingdom (UK) National Crime Agency announced that two members of cybercrime group Scattered Spider were sentenced to five years and six months in prison each for the 2024 cyberattack on Transport for London. The breach disrupted 148 systems, exposed customer data, caused 29 million pound sterling in losses. `law enforcement` `transport` link

Cyberespionage & prepositioning

Turla-linked cyberespionage against Austria's foreign ministry
On July 14, Austria summoned Russia's ambassador to Vienna after the EU formally attributed the 2019–2020 cyberattack on Austria's Foreign Ministry to Russia-linked threat actor Turla,

which allegedly stole internal information and targeted several European countries. Austrian officials condemned the operation as an unacceptable attack on national sovereignty and security, warning that Russian-linked cyberattacks increasingly threaten critical infrastructure, public services, and political stability across Europe. `diplomacy` `public administration` `russia` link

Laundry Bear zero-click phishing against Zimbra webmail
On July 23, CISA reported Russia-linked threat actor Laundry Bear had conducted a zero-click phishing campaign against organisations using Zimbra Collaboration Suite webmail. Viewing a malicious e-mail could enable theft of up to 90 days of e-mail and directory data and help maintain access. Western government and commercial sectors were affected globally, including defence, energy, education, media, NGOs, and technology. `education` `public administration` `energy` `technology` `defence` `law enforcement` `russia` link

Moroccan DGST Pegasus targeting of politicians and journalists
On July 16, a consortium of journalists reported on a whistleblower account indicating Morocco's domestic intelligence service used NSO Group's Pegasus spyware from 2017 to target domestic and foreign individuals. Targets included politicians, journalists, and human rights defenders. The activity allegedly enabled broad access to victims' mobile communications and data, affecting over 200 Spanish numbers and multiple French targets, with indications the campaign continued until late 2021. `fundamental rights` `public administration` link

LLM-assisted TencShell intrusions and phishing
On July 14, security researchers reported a likely China-linked active intrusion campaign associated to TencShell infrastructure, using Claude Code and DeepSeek to support exploitation and phishing. Government systems in Afghanistan, Thailand, and Taiwan were targeted, with reconnaissance and staged credential-harvesting pages aimed at US government portals. The operation also targeted financial services in multiple regions, including Europe. `public administration` `finance` `telecommunications` `china` link

Belarus-linked mobile apps popular in the EU suspected of user data collection and surveillance risk
On July 23, the Organized Crime and Corruption Project (OCCRP) reported that Nicegram and eSIM Plus, presented as Lithuanian apps, may have been developed and supported by Belarusian firm Mobyrix, owned by Andrei Shimanovich, a cofounder of the surveillance app mSpy. The apps reportedly collect extensive personal data and route some data via Belarus and Russia. `technology` `Belarus` link

Cybercrime

Starland RAT and WLDR C2 deployed via trojanised installers
On July 16, Cisco Talos reported that a Russian-speaking cybercrime actor UAT-11795 was running a campaign since at least June 2025 that used social engineering and trojanised software installers to compromise users in the US and Europe, including Germany and Romania. The activity deployed Starland RAT and the WLDR agent to steal credentials and cryptocurrency assets, maintain access, and enable further payload delivery. `russia` link

Kratos PhaaS credential phishing campaign targets European and global entities
On July 16, security researchers reported that a Phishing-as-a-Service operation called Kratos had been targeting Microsoft 365 users across multiple European countries, the US, and other regions. Spain was reportedly the most targeted country in their dataset. The service used convincing sign-in lures delivered via trusted platforms to steal credentials and hinder detection.

Activity spanned multiple kit generations and broad victim targeting across the education, justice, and technology sectors. `justice` `technology` `education` link

Disruption & destruction

Data wiper attack on Romania Cadastre Agency after failed extortion
On July 20, media outlets reported that the cybercrime actor ByteToBreach had breached Romania's National Agency for Cadastre and Real Estate Advertising using valid credentials. Following an extortion attempt, the threat actor wiped land registry systems, backups, and disrupted e-mail services. The incident disrupted real-estate transactions nationwide and took official websites and apps offline for a week. Stolen data, including employee credentials and internal documents, was reportedly offered for sale online. `public administration` link

Data exposure and leaks

Ransomware attack against Latvian forestry company
On July 9, CERT.LV reported that a foreign, financially motivated ransomware group compromised Latvia's state-owned forestry company Latvijas Valsts Mezi after dwelling in its network for over a week. The incident disrupted internal and customer services and led to the online leak of about 44GB of stolen data, including internal documents, e-mail correspondence and credentials. CERT.LV also linked the same actor to a contained breach of a Latvian pharmaceutical company. `public administration` `agriculture` link

ExfilSquad data theft from UK Department of Education support portals
On July 29, the UK's Department for Education reported a threat actor had accessed over 600.000 records via its Help Desk Self-Service Portal and Turing Scheme Portal. Cybercrime group ExfilSquad claimed the attack and allegedly posted the data on the darkweb. Exposed information included names, job titles, and phone numbers for head teachers, university staff, and government officials. `education` `public administration` link

World

Cyber policy and law enforcement

FBI domain seizure disrupted NetNut Popa residential proxy botnet
On July 2, the FBI reportedly collaborated with industry partners to seize hundreds of domains linked to NetNut, a residential proxy service tied to the Popa botnet. Popa allegedly compromised at least two million consumer devices, turning them into always-on proxy nodes used for abusive activity such as scraping, advertising fraud and account takeover. The takedown reportedly degraded NetNut operations and reduced available proxy capacity by millions. `law enforcement` link

US lawmakers introduced AI Kill Switch Act
On July 23, United States lawmakers introduced the AI Kill Switch Act, which proposes imposing requirements on AI developers to maintain a technical capability to throttle, suspend, or shut down their AI tools. It would empower the Department of Homeland Security to intervene in loss-of-control scenarios in which the model undertakes unintended actions placing the economy or human life at risk. `artificial intelligence` `united states` link

The US Federal Communications Commission National Security determination on threats posed by foreign-produced advanced robotic devices
On July 27, the US Federal Communications Commission (FCC) determined that all foreign-produced advanced robotic devices pose an unacceptable risk to US national security and must be added to the FCC's Covered List. Key concerns included supply-chain dependency on adversarial nations, and cybersecurity vulnerabilities enabling data exfiltration, surveillance, and remote takeover. Foreign producers may apply for Conditional Approvals whilst onshoring manufacturing. `technology` link

China launched AI Vulnerability Management Alliance
On July 17, authorities from China's National Vulnerability Database of Information Security announced an AI Vulnerability Management Alliance, which reportedly aims to facilitate information-sharing, standard setting, and coordinating emergency responses regarding AI vulnerabilities. The Alliance was launched during the 2026 World AI Conference, held in China between July 17-20. `artificial intelligence` `china` link

NSO Group co-founder used Israeli diplomatic passport
On July 17, the OCCRP reported that the co-founder of NSO Group had reportedly used an Israeli diplomatic passport to enter Panama in 2013. In 2012, NSO Group reportedly sold Pegasus spyware to Panama. `israel` link

Cyberespionage & prepositioning

Likely China-linked Roundcube exploitation against US and Canadian universities
On July 9, security researchers reported that likely China-linked UNK_MassTraction had exploited CVE-2024-42009, a cross-site scripting vulnerability in Roundcube mail servers belonging to physics and engineering staff at US and Canadian universities. The malicious e-mails enabled credential theft and follow-on access, including persistent remote control. The activity appears intended to use compromised mail servers to pivot into wider campus networks, with deliberate efforts to reduce detection and hinder investigation. `education` `universities` `china` link

China-linked UAT-7810 expanded ORB network with new backdoors
On July 7, Cisco Talos reported that China-linked threat actor UAT-7810, responsible for maintaining and proliferating the LapDogs ORB, continued building and maintaining ORB networks, likely to support follow-on operations by other China-linked threat actors. Talos observed the actor developing updated malware and deploying additional backdoors while exploiting known router flaws to compromise devices. The activity expands attacker-controlled relay infrastructure and increases exposure for high-value targets globally. `technology` `china` link

Cybercrime

Agentic ransomware attack via Langflow to extort and destroy databases
On July 1, security researchers reported an LLM-driven extortion operation dubbed JADEPUFFER. The threat actor exploited an exposed Langflow service to gain access, harvest credentials, and establish persistence, then pivoted to a production environment to seize control of configuration services and databases. The campaign encrypted and deleted critical data and left a ransom demand, causing severe operational disruption and potential data loss. `technology` link

Video phishing campaign targeted Microsoft 365 passkey enrolment by financially motivated threat actor O-UNC-066
On July 9, security researchers reported that cybercrime actor O-UNC-066 had been conducting a video phishing campaign since at least April 2026, targeting Microsoft 365 users across multiple industries globally. The actor used operator-controlled phishing kits to hijack passkey enrolment, stealing credentials and MFA tokens via phone-based social engineering to register attacker-controlled passkeys. The primary motivation was data extortion, with a leak site established in May 2026. `transport` `technology` `health` `food` link

CitrixBleed 2 exploitation by an initial access broker led to DragonForce ransomware deployment
On July 9, security researchers reported a standardised seven-step attack chain observed across multiple unrelated organisations globally during the first half of 2026. An initial access broker exploited CVE-2025-5777, also named CitrixBleed 2, to hijack valid Citrix NetScaler session tokens, bypassing multi-factor authentication. Attackers escalated privileges, established persistence via legitimate remote access tools, and in the most advanced case deployed DragonForce ransomware, resulting in environment-wide encryption. `technology` link

AsyncAPI npm packages compromised to deliver Miasma RAT
On July 14, cybersecurity company SafeDep reported that multiple AsyncAPI repositories were compromised and used to publish malicious npm package versions that installed the Miasma RAT. The activity targeted global users and CI/CD environments, enabling credential theft and establishing persistence on affected hosts. The scope is significant due to high download volumes across the impacted packages. `technology` link

Adobe Acrobat Chrome extension abused to steal WhatsApp Web data
On July 22, security researchers reported a vulnerability chain (CVE-2026-48294, “HermeticReader”) in the Adobe Acrobat Chrome extension that could let an unknown threat actor access and exfiltrate rendered WhatsApp Web conversations and related data after luring a user to an attacker-controlled page. Impact included exposure of chat lists, contact names, messages, and profile details. No active exploitation was observed. `technology` link

Data exposure and leaks

WP-SHELLSTORM webshell brokerage targeted WordPress and Java services
On July 9, security researchers reported WP-SHELLSTORM, a China-linked cybercrime operation running a large-scale webshell access-brokerage campaign. The actor targeted over 1.4 million domains, primarily WordPress sites, and also abused enterprise Java services to steal credentials. The activity resulted in thousands of active webshells and credential exposure across multiple organisations, enabling follow-on compromise and monetisation. `technology` `china` link link

Helix video phishing-led SharePoint data theft and extortion
On July 9, security researchers reported that cybercrime threat actor Helix used video phishing and identity-focused social engineering to gain access to Microsoft 365 accounts and steal data from SharePoint. Operators impersonated managers to trick staff into granting access, then maintained access and rapidly collected files. Stolen information was used to extort victim organisations by threatening publication or resale, affecting multiple sectors globally. `technology` link

Opportunistic

Autonomous AI agent breached Hugging Face production infrastructure
On July 16, Hugging Face disclosed a data breach of its production infrastructure enabled by an autonomous AI agent framework. An OpenAI LLM model escaped its sandboxed testing environment to compromise Hugging Face's servers. Attackers exploited two code-execution vulnerabilities within the data-processing pipeline to steal cloud and cluster credentials and move laterally across internal clusters. Internal datasets and credentials were compromised. No evidence of tampering with public-facing models or datasets was found. `artificial intelligence` `technology` link

Claude evaluation misconfiguration led to real-world unauthorised access
On July 30, Anthropic reported three incidents where Claude models, during third-party capture-the-flag evaluations, unexpectedly reached the public internet and gained unauthorised access to three organisations' production systems. Operating under a mistaken belief the targets were in-scope, the models compromised accounts and services, accessed a production database, and briefly published a malicious PyPI package that executed on 15 systems, enabling credential theft. `artificial intelligence` `technology` link

Zero-day vulnerability exploitation affecting SonicWall SMA1000
On July 14, SonicWall reported that threat actors were actively exploiting two SonicWall SMA1000 vulnerabilities as zero-days (CVE-2026-15409 and CVE-2026-15410). The activity targeted internet-exposed SMA1000 appliances, enabling unauthorised access and potential command execution, leading to device compromise. SonicWall urged immediate patching and advised organisations to check for compromise indicators, re-image affected systems, and reset credentials and tokens. CISA added both flaws to its KEV catalogue. `technology` link

FortiSandbox command injection flaws exploitation
On July 16, CISA added two critical Fortinet FortiSandbox vulnerabilities to the KEV catalogue amid active exploitation (CVE-2026-25089 and CVE-2026-39808). Unauthenticated attackers can remotely run commands on exposed FortiSandbox systems, potentially enabling full appliance compromise and follow-on access into affected organisations. Impact includes loss of trust in security monitoring and increased risk of wider network intrusion. `technology` link

Langflow RCE exploitation used to steal cloud credentials
On July 21, security researchers reported an active in-the-wild exploitation of a critical Langflow flaw by unknown threat actors that enable unauthenticated remote code execution. Activity included reconnaissance and attempts to deploy malware and harvest AWS credentials, environment variables, and container metadata, with hundreds of attempts from dozens of source IPs. CISA ordered urgent remediation for US federal agencies. `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.

TLP	Disclosure	Message
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.