Cyber Brief (July 2025)

August 4, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 287 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, the EU, UK, and US have imposed sanctions on Russian entities due to their involvement in cyberattacks and disinformation campaigns. Additionally, two more EU countries have banned DeepSeek AI citing security concerns.
- On the **cyberespionage** front, China-linked threat actors have been identified as being behind the ToolShell campaign, which exploits vulnerabilities in SharePoint. Meanwhile, the Russia-linked Turla threat actor has targeted diplomats in Moscow.
- Relating to **cybercrime**, researchers have discovered malware in trusted Chrome and Edge extensions that have been installed by approximately 2.3 million users while researchers identified a surge in Akira ransomware attacks exploiting SonicWall SSLVPN.
- There were **disruptive** incidents causing operational disruptions at two EU-based telecommunications companies. Furthermore, Russia's Aeroflot canceled flights after pro-Ukrainian hackers claimed responsibility for a cyberattack.
- As regards **data exposure and leaks** incidents, in Europe, an unsecured server exposed years' worth of data belonging to Swedish citizens. The Swiss healthcare giant AMEOS reported a data breach affecting patients, staff, and partners. Globally, Dell confirmed a breach by an extortion group, and leaked datasets revealed ties between Chinese cyber contractors and the government.
- Relating to **information operations**, at least four Russian operations targeting European countries have been identified, highlighting ongoing efforts in information manipulation and disinformation.

Europe

Cyber policy and law enforcement

EU targets Russian disinformation networks and electronic warfare operations in new sanctions
On July 15, the EU Council sanctioned nine individuals and six entities, including media groups, think tanks, and a GRU officer linked to Unit 74455, for spreading pro-Russia disinformation and conducting electronic warfare that disrupted civilian aviation. These sanctions reinforce the EU's commitment to counter Russian hybrid threats amid the ongoing Russia-Ukraine war. `russia` `sanctions` link

UK sanctions Russian GRU units and operatives for cyberattacks and disinformation
On July 18, the UK sanctioned three Russian GRU military units, 18 individuals, and a disinformation outlet for cyberespionage, information operations, and support for Russia's war in Ukraine, including targeting Yulia Skripal in 2013 and aiding strikes on Ukrainian civilians. `russia` `sanctions` link

Germany requests removal of DeepSeek AI from app stores
On June 27, Germany's data protection commissioner asked Apple and Google to remove DeepSeek AI from German app stores, citing unauthorised transfer of personal data to China without EU-standard safeguards. The move follows similar actions by Italy and the Netherlands. DeepSeek has not demonstrated compliance with GDPR or the Digital Services Act. Apple and Google are currently reviewing the request. `ban` `artificial intelligence` `china` link

Czech Republic bans DeepSeek AI over data security concerns
On July 9, the Czech government prohibited the use of Chinese AI startup DeepSeek in public administration, citing data security risks and concerns over Chinese government access to stored information. The move follows similar restrictions in Germany, Italy, and the Netherlands. `ban` `artificial intelligence` `china` link

Denmark introduces copyright law to combat Deepfake misuse
On June 26, the Danish government announced new copyright legislation to protect citizens from AI-generated deepfakes, allowing individuals to object to the unauthorised use of their bodies, faces, or voices and demand content removal from online platforms. This pioneering law in Europe comes amid a sharp rise in deepfake fraud, which increased by over 1.300% in 2024 and now drives nearly half of global fraud attempts. `regulation` `artificial intelligence` link

Chinese hacker tied to Silk Typhoon group arrested in Italy
On July 3, a Chinese national, Xu Zewei, was arrested in Milan on a US warrant for alleged ties to the state-backed Silk Typhoon group. He is accused of cyberattacks targeting US organisations, including 2020 campaigns aimed at stealing COVID-19 vaccine research and public health data. `china` `arrest` link

Europol and Eurojust coordinate takedown of NoName057(16) hacktivist group
On July 15, Europol and Eurojust coordinated a multinational operation that dismantled the pro-Russia hacktivist group NoName057(16), which conducted DDoS attacks against European infrastructure. Over 100 servers were seized, seven arrest warrants issued, and 4.000 supporters identified. The group's leaders are believed to reside in the Russian Federation. `russia` `takedown` link

Cyberespionage & prepositioning

In September 2024 Houken exploited three Ivanti zero-days to intrude French governmental and telecommunications entities
On July 1, ANSSI, the French National Cybersecurity Agency, publicly reported that in September 2024, a threat actor dubbed Houken sought to gain initial access through exploitation of zero-days on French entities. Houken specifically exploited three zero-day vulnerabilities on the Ivanti Cloud Service Appliance (CSA) devices of French entities in the governmental, telecommunications, media, finance, and transport sectors. `china` link

India-linked Patchwork uses Google Drive to target European foreign affairs ministry with spearphishing
On July 8, Trellix reported that India-linked Patchwork sent spearphishing e-mails impersonating defence officials to a southern European foreign affairs ministry. Victims clicked a Google Drive link delivering a malicious RAR archive that installed the "LoptikMod" backdoor via scheduled tasks, ensuring persistent access. While Patchwork typically targets government and defense entities in South Asia, this operation likely signals an expansion of interest toward European diplomatic entities. `diplomacy` `india` link

Cybercrime

North Korean IT experts infiltrate European tech firms under false identities
On July 10, Le Monde reported on North Korean IT experts, using fake identities and nationalities, are infiltrating Western companies — initially in the US, now in France — to earn salaries that are funnelled back to the regime or used for extortion. One example is US crypto firm Iqlusion, which unknowingly hired such developers, later alerted by the FBI to their ties to North Korea. `north korea` link

Disruption & destruction

Dutch Prosecution service disconnected after Citrix breach, operations severely disrupted
On July 18, the Dutch Public Prosecution Service (Openbaar Ministerie, OM) shut down all internet access after discovering that hackers likely exploited the Citrix Bleed 2 vulnerability, prompting a major operational disruption. The outage may last weeks, severely restricting remote access, e-mail, and digital file editing, raising concerns about the potential impact on ongoing legal proceedings and signalling a serious cybersecurity breach within a critical government institution. `justice` link

Orange Group suffered a cyberattack impacting some services at France-based enterprises
On July 25, Orange Group suffered a cyberattack causing service disruptions for some business and consumer clients, mainly located in France. No data breaches have been identified. Services are being progressively restored under enhanced monitoring. A formal complaint has been filed, and authorities are involved. `telecommunications` link

POST Luxembourg outage on July 23 traced to sophisticated cyberattack
On July 23, Luxembourg's POST suffered a nationwide four hour outage affecting mobile, fixed line and internet services—including emergency numbers—due to a targeted, exceptionally advanced and sophisticated cyberattack ground. According to POST and the government crisis unit, malicious actors exploited a software vulnerability to disrupt services. Internal systems weren't breached, no customer data was compromised, and services were restored by the evening—with investigations ongoing. `telecommunications` link

Information operations

Russia exploited no-confidence vote to undermine EU unity
On July 22, El País reported that Russia exploited the recent no-confidence vote against European Commission President Ursula von der Leyen to polarise the EU, using pro-Kremlin disinformation networks to frame the motion as a rebellion against corruption. Analysts identified over 20.000 coordinated posts across platforms, revealing a broader effort by Russian-linked actors to distort European democratic processes and amplify anti-EU narratives during politically sensitive moments. `russia` link

Russia-linked Storm-1516 impersonates journalists to spread disinformation across Europe
On July 7, the Gnida Project reported that Russia-linked network Storm-1516 has impersonated journalists since May to spread disinformation in Moldova, Armenia, France, and Germany. By hijacking real reporters' identities, the group seeks to boost the credibility of false narratives aligned with Russian interests—such as undermining Western alliances and discrediting leaders—while using fake media sites to amplify these messages. The Gnida Project tracks and analyses disinformation operations. `russia` link

Russia-linked "Matryoshka" disinformation campaign intensifies focus on Moldova with evolving tactics
On July 17, the Institute for Strategic Dialogue (ISD Global), a London-based non-profit countering disinformation, reported that Russia-linked operation "Matryoshka" intensified its focus on Moldova in Q2 2025. It impersonated media outlets and used AI personas to spread English content on TikTok and X. Despite evolving tactics and smear campaigns, the operation saw limited real engagement, as most content was removed by major platforms. `moldova` `russia` link

Russian disinformation campaign cloned British 999 call with AI
On July 31, BBC Verify revealed that the voice of a British 999 emergency call handler was cloned using AI for a Russian-linked disinformation campaign. The synthetic voice, lifted from an NHS training video, was used to spread fear ahead of Poland's May 2025 presidential election. The real call handler, Aaron, was shocked by its realism. `russia` link

China spread disinformation to undermine French Rafale jet sales
On July 6, French intelligence reported on China using its embassies to spread false claims about Rafale jet performance during India-Pakistan clashes, aiming to hurt French arms sales and promote Chinese alternatives, particularly targeting countries like Indonesia. `china` `defence` link

Data exposure and leaks

Unsecured server exposes years of Swedish citizens' data
On July 24, Cybernews reported that an unsecured Elasticsearch server exposed over 100 million detailed records on Swedish citizens and companies, including names, ID numbers, tax data, debt history, and address logs from 2019 to 2024. Believed to originate from a third-party client of Nordic firm Risika, the leak offers a comprehensive behavioural and financial profile that poses serious risks for identity theft, phishing, and corporate espionage. link

Swiss healthcare giant AMEOS reports data breach affecting patients, staff, and partners
On July 21, Swiss hospital group AMEOS announced a security breach affecting its IT systems, potentially exposing sensitive data of patients, employees, and partners across its network of over 100 healthcare facilities in Central Europe. While no evidence of data misuse has emerged yet, AMEOS has shut down systems, notified authorities, and launched a forensic investigation,

warning affected individuals to remain alert to possible phishing or fraud attempts. `health` link

Threat actor threatens to leak 106GB of data allegedly belonging to Telefónica
On July 4, BleepingComputer reported about a threat actor, affiliated with the Hellcat ransomware group, threatening to leak 106GB of data allegedly stolen from Telefónica Spanish telecommunications company. In fact, the threat actor alleges they breached the company through a Jira misconfiguration, similar to the January cyberattack. However, there are currently no indications that the leaked data is recent, and the company is denying the threat actor's claims. `telecommunications` link

World

Cyber policy and law enforcement

Microsoft used China-based engineers to support the US Department of Defense
On July 25, the non-profit investigative journalism organisation ProPublica revealed that Microsoft had relied on engineers based in China to support US Department of Defense and other federal systems, supervised by US-based "digital escorts," who reportedly, often lacked technical expertise. In response, Microsoft announced it will no longer use China-based engineering teams for support of US government cloud services—a practice now ceased amid mounting US national security scrutiny. `china` `united states` link

US sanctions Russian hosting company Aeza Group for aiding cybercrime and disinformation
On July 1, the US Department of the Treasury sanctioned Russian hosting company Aeza Group and four of its operators for providing bulletproof hosting services to cybercriminals, including ransomware gangs, infostealer platforms, and darknet drug markets. The sanctions target Aeza's involvement with groups like BianLian and RedLine, its role in Russian disinformation campaigns, and bar US entities from doing business with the group or its affiliates. `russia` `sanctions` `united states` link

Interpol's Operation Secure disrupts major infostealer networks across Asia-Pacific
On June 11, Interpol announced that Operation Secure, a coordinated effort with 26 Asia-Pacific nations, dismantled over 20.000 malicious assets and seized 41 servers used by infostealer networks, uncovering more than 200.000 victims. Despite these successes, including multiple arrests and the takedown of 79% of identified infrastructure, officials warn that cybercriminals are likely to rebuild operations using alternative platforms due to the continued profitability of corporate fraud and stolen data. `arrests` `seizure` `takedown` link

Cyberespionage & prepositioning

Microsoft links China-linked APTs to ToolShell campaign exploiting SharePoint vulnerabilities
On July 22, Microsoft confirmed that a portion of malicious activity exploiting SharePoint vulnerabilities in the ToolShell campaign has been attributed to China-linked groups APT27 (Linen Typhoon), APT31 (Violet Typhoon), and Storm-2603. APT27 and APT31 focused on espionage and data theft, while Storm-2603 deployed ransomware using the same vulnerabilities. `china` link

China-linked hackers escalate cyberattacks on Taiwan's semiconductor sector amid US-China tensions
On July 16, Proofpoint revealed that at least three China-linked hacking groups have intensified

cyberespionage campaigns targeting 15–20 Taiwanese semiconductor firms and financial analysts, including those at a US-headquartered bank, between March and June 2025. The campaigns, ranging from phishing e-mails to malware-laced PDFs, coincide with US-China tensions over chip exports and highlight China's persistent interest in disrupting and exploiting Taiwan's semiconductor supply chain and supporting industries. `china` `semiconductor industry` `taiwan` link

Chinese state-backed hackers breach US Nuclear Agency via Microsoft SharePoint zero-day
On July 23, the US National Nuclear Security Administration (NNSA) confirmed it was breached through a Microsoft SharePoint zero-day vulnerability chain, in a widespread cyberattack attributed to Chinese state-sponsored actors. While the Department of Energy reported minimal disruption and no classified data exposure, the incident is part of a broader campaign affecting over 400 servers and 148 global organisations. `china` `united states` link

China-linked campaign infiltrated US National Guard network for nine months
On July 15, US authorities confirmed that the cyberespionage group Salt Typhoon infiltrated a US state's Army National Guard network from March to December 2024. The campaign accessed network diagrams, geographic data, and personal data of service members, raising concerns about further compromise of state-level cybersecurity partners and law enforcement fusion centres. `china` `united states` link

Russia-linked threat actor Turla conducts adversary-in-the-middle campaign targeting diplomats in Moscow
On July 31, Microsoft Threat Intelligence reported on a cyberespionage campaign by the Russia-linked threat actor Secret Blizzard, also known as Turla. This campaign targets embassies located in Moscow using an adversary-in-the-middle (AiTM) position to deploy their custom ApolloShadow malware. ApolloShadow installs a trusted root certificate to trick devices into trusting malicious actor-controlled sites, enabling Turla to maintain persistence on diplomatic devices, likely for intelligence collection. `russia` link

North Korea-linked threat actor delivers XORIndex malware via 67 npm packages
On July 15, researchers revealed that North Korean actors uploaded 67 malicious packages to the npm repository, delivering the new XORIndex loader to developer systems. The campaign, linked to the Contagious Interview operation, used postinstall scripts to deploy payloads like BeaverTail and InvisibleFerret. Over 17.000 downloads were recorded before takedown reports were filed. `north korea` link

Cybercrime

Hackers exploit leaked Shellter Elite tool to spread infostealers as vendor responds with secured update
On July 3, Elastic Security Labs revealed that hackers have been abusing a leaked copy of Shellter Elite v11.0, a red team AV/EDR evasion tool, to deploy infostealers like Rhadamanthys and Lumma via phishing e-mails and YouTube comments. Shellter confirmed the misuse stemmed from a recently licensed customer, criticised Elastic for delayed disclosure, and released a secured v11.1 update, restricting future access to vetted clients only. link

Researchers uncover malware in trusted Chrome and Edge extensions installed by 2,3 million users
On July 8, KOI security researchers reported a widespread malware campaign named "RedDirection," involving 18 malicious extensions on Google Chrome and Microsoft Edge. Trusted by both companies and installed by over 2,3 million users, the extensions secretly hijacked browser traffic, harvested URLs, and redirected users via command-and-control servers —often long after installation and store verification. link

Cybercrime threat actor UNC3944 pivots to vSphere for stealthy ransomware deployment
On July 23, a Google report detailed a campaign conducted by cybercrime threat actor UNC3944 (a.k.a Scattered Spider) targeting retail, airline and transportation organisations in the US using social engineering to access VMware vSphere via compromised Active Directory accounts. The threat actor hijacked vCenter, exfiltrated data from domain controllers using hypervisor-level disk swaps, sabotaged backups, and deployed ransomware from ESXi hosts. link

Fake Cloudflare verification screen used to deliver undetected malware
On July 4, unknown threat actors launched a malware campaign using fake Cloudflare CAPTCHA screens to deceive users into running malicious PowerShell commands. The page injected code via the clipboard and contacted a Command and Control server using embedded webhooks. It fetched payloads from pastesio[.]com and axiomsniper[.]info, with evasion checks for virtual machines. The final BAT file showed zero detections on VirusTotal at the time of discovery. link

Akira ransomware exploits SonicWall SSL VPN in July 2025 surge
In July 2025, Arctic Wolf observed a surge in Akira ransomware attacks exploiting SonicWall SSL VPN connections for initial access, including on fully patched devices—suggesting a likely zero-day vulnerability. These breaches began around 15 July, often leading to rapid encryption following VPN logins, sometimes within hours. Credential-based attacks (e.g. brute force) remain possible vectors per Arctic Wolf's ongoing investigation. link

Data exposure and leaks

Dell confirms breach of demo platform by World Leaks extortion group, no sensitive data exposed
On July 21, Dell confirmed that the World Leaks extortion group, formerly Hunters International, breached its Customer Solution Centers, a test environment isolated from core systems, stealing mostly synthetic and non-sensitive data. Although 1.3 TB of data was leaked, Dell states no sensitive customer or corporate data was involved, while World Leaks continues its shift toward data extortion over ransomware, citing profitability and risk concerns. link

Leaked datasets expose Chinese cyber contractors' government ties
On July 1, SpyCloud reported that leaked data from VenusTech and Salt Typhoon, posted in May on DarkForums, expose their offensive cybersecurity work for Chinese state entities. The samples reveal intelligence targets across Asia and Europe, and link three Chinese companies to Salt Typhoon operations, highlighting China's expanding offensive cyber contractor ecosystem. `china` link

Disruption & destruction

Russia's Aeroflot cancels flights after pro-Ukrainian hackers claim cyberattack
On July 28, Russia's flag carrier Aeroflot had to cancel around 42–50 flights from Moscow's Sheremetyevo due to a massive cyberattack on its IT systems. The pro-Ukraine hacker groups "Silent Crow" and "Cyber Partisans BY" claimed responsibility, saying they infiltrated and destroyed about 7.000 servers, dumping flight databases and communications data. Russian prosecutors have since launched a criminal investigation into the breach. Flying and booking services remain disrupted while recovery efforts continue. `russia` `ukraine` link

Opportunistic

Patches available for critical vulnerabilities in SharePoint exploited in global ToolShell campaign
On July 20, Microsoft published guidance for CVE-2025-53770, a critical deserialisation

vulnerability in on-premise SharePoint Server rated 9.8/10. Eye Security reported large-scale exploitation beginning July 18 via a chain dubbed ToolShell, enabling remote code execution and cryptographic key theft. Proof-of-concept exploits and active campaign exploiting the ToolShell chain have been confirmed. Emergency patches for Subscription Edition, Server 2019, and Server 2016 are now available. link

CrushFTP vulnerability exploited to gain unauthorised administrative access
On July 18, CrushFTP observed exploitation of a previously patched vulnerability affecting versions below 10.8.5 and 11.3.4_23. Activity likely began on July 17, following possible reverse engineering of code changes. The flaw enabled unauthenticated administrative access via HTTP(S). Indicators include modified user.XML files and unauthorised admin accounts. Unpatched systems remain exposed to compromise. link

Cisco Identity Services Engine vulnerabilities exploited in the wild
On July 21, Cisco updated an advisory related to critical vulnerabilities affecting its Identity Services Engine, for which they have observed exploit attempts in the wild. The vulnerabilities (CVE-2025-20281, CVE-2025-20282, and CVE-2025-20337) allow for remote code execution by an unauthenticated attacker, issuing commands as root user. Patches have been released for the affected products (versions 3.3 and 3.4). link

Google fixes Chrome zero-day exploited for sandbox escape
On July 15, Google released a patch for CVE-2025-6558, a high-severity vulnerability actively exploited to escape Chrome's sandbox. The flaw, caused by insufficient input validation in ANGLE and GPU components, allowed remote code execution via crafted HTML pages. Users are urged to update Chrome to version 138.0.7204.157 or later. 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.