Cyber Brief (August 2025)

September 2, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 321 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, Ukraine, Romania, and Moldova joined forces and created a regional cyber alliance, and Romania created a CSIRT for the energy sector. Russia reportedly conducted tests to block WhatsApp and Telegram, and ordered state-backed MAX messenger app to be pre-installed on phones and tables.
- On the **cyberespionage** front, threat actors breached critical organisations in the Netherlands through a Citrix vulnerability, an Iran-linked threat actor targets Berlin Justice Senator, and several countries advise on Chinese threat actors targeting telecommunications.
- Relating to **cybercrime**, Salty 2FA phishing kit targets global industries, Akira ransomware was at the front of the news, and macOS was targeted in phishing and malvertisement campaign.
- There were **disruptive** attacks in Moldova and Norway, affecting government and water systems. Moreover, pro-Ukraine supposed hacktivists take over Russian TV on UA Independence Day.
- As regards **data exposure and leaks** incidents, Orange Belgium, Bouygues Telecom, Air France and KLM disclosed data breaches while the breach of Salesforce CRM service provider exposed customer data at scale. Ukraine conducted a cyber operation exposing secrets of Russia's new nuclear submarine. North Korea-linked Kimsuky suffer data breach.

Europe

Cyber policy and law enforcement

Regional Cyber Alliance formed by Ukraine, Romania and Moldova
On August 1, Ukraine's National Security and Defence Council announced the creation of a regional cyber alliance involving Ukraine, Romania and Moldova, following consultations on

July 30 in Chernivtsi. Its goals: enhancing cooperation against cyber and hybrid threats, AI-based threat detection, joint training, and strengthening infrastructure resilience and democratic institutions. The alliance is open to new democratic partners and aims to reinforce collective cyber defence, especially against threats from Russia. link

Romania sets up energy cybersecurity centre to support Ukraine and Moldova
On August 18, Romania's Ministry of Energy issued an ordinance to establish a CSIRT for the energy sector. It cites rising cyber threats fuelled by market liberalisation and Russia's war in Ukraine, underscoring Romania's role as a key electricity supplier to both Ukraine and Moldova and its duty to uphold regional energy security. Romania's National Cybersecurity Directorate has already stepped up coordination with Ukrainian and Moldovan counterparts. link

Cyberespionage & prepositioning

Iran-linked threat actor targets Berlin Justice Senator
On August 19, Tagesschau reported that Berlin's Justice Senator Felor Badenberg fell victim to a targeted cyberattack, likely by an Iran-linked group. Threat actors accessed her personal data, e-mails, and digital calendar, revealing her movements and home addresses. The attack originated from a malicious e-mail disguised as the Central Council of Jews. Authorities quickly isolated the affected computer, and investigations are ongoing. `iran` link

Dutch National Cyber Security Centre says threat actors successfully breached critical organisations through Citrix vulnerability
On August 11, the National Cyber Security Centre (NCSC) of the Netherlands updated a warning related to the exploitation of Citrix Netscaler vulnerability CVE-2025-6543. They mention that several critical organisations have fallen victim of successful attacks, and that threat actors have actively erased their tracks in order to hide compromise, showing a level of sophistication in these attacks. link

Russia-linked threat actor Curly COMrades targets Georgia and Moldova
On August 12, Bitdefender reported that Curly COMrades, a cyberespionage threat actor active since mid-2024, targeted Georgian government and judicial bodies and Moldovan energy firms with the custom three-stage MucorAgent backdoor. The group used COM hijacking, stealthy persistence, credential theft, and living-off-the-land tools to align operations with Russian interests while blending malicious traffic with legitimate activity. `russia` link

Cybercrime

Colt Technology Services targeted with Warlock ransomware
On August 12, Colt Technology Services suffered a cyberattack that disrupted hosting, porting, Colt Online, and Voice API platforms. The firm confirmed support systems, not its core network, were impacted and reported the incident to authorities. WarLock claimed responsibility, offering alleged stolen data for sale. Security researchers suggest a Microsoft SharePoint flaw (CVE-2025-53770) enabled access, with hundreds of gigabytes of files exfiltrated. `telecommunications` link

IT system supplier cyberattack impacts 200 municipalities in Sweden
On August 27, a cyberattack on Miljödata—an IT-system provider used by about 80 % of Sweden's municipal administrations—disrupted access in over 200 municipalities and raised concerns about stolen sensitive data, with attackers demanding a ransom of 1,5 BTC (approx. 146.000 Euro) to avoid data leaks. link

Salty 2FA phishing kit targets global industries

On August 19, ANY.RUN published a report on Salty 2FA, a new phishing framework hitting organisations across the US and Europe. It primarily targets Microsoft 365 users in finance, telecom, energy, logistics, healthcare, consulting, education, and government sectors. Victims span multiple regions, including the USA, the UK, Germany, Spain, Italy, Switzerland, Canada, and Greece, with lures themed around voicemail, payroll, invoices, and proposal requests. link

Disruption & destruction

Moldova's government systems targeted in coordinated cyberattack

On August 12, Moldova's Information Technology and Cyber Security Service (STISC) announced that its government systems were victims of a large organised cybersecurity attack. They assessed the threat actors were foreign, trying to damage key cyber systems that help run important state services. They also divulged that they suspect some government employees were involved. link

Pro-Russia supposed hacktivists linked to Norwegian dam sabotage

On August 13, Norwegian authorities officially linked a cyber-sabotage incident from April to pro-Russia supposed hacktivists. On April 7, attackers remotely opened a flood gate at the Bremanger dam—used for fish farming—releasing some 500 litres/sec for four hours before being stopped. No injuries occurred, but officials warned the act was intended to instil fear—not cause physical damage. link

Russia suspected of jamming GPS signal of European Commission President Ursula von der Leyen's plane

On August 31, European Commission President Ursula von der Leyen's plane was hit with GPS jamming the previous day while landing in Bulgaria. The European Commission suspects Russia of conducting the attack. Despite the interference, the plane landed successfully and there were no real consequences of the actions. The Commission's President was on a tour of European countries that are "frontline states" of Russia. link

Information operations

Moldovan authorities warn of Russian disinformation campaign targeting diaspora voters

On August 4, Politico published an article about Russia disinformation operations aimed at Moldovans living in Europe, ahead of the Presidential elections in September. In fact, according to National Security Adviser Stanislav Secrieru, the goal of the campaign is to encourage them not to vote or encouraging those who do to support a fake pro-EU force. They do so through imitating legitimate European news outlets. `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 Russia-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. `artificial intelligence` `russia` link

Data exposure and leaks

Orange Belgium discloses data breach impacting 850.000 customers

At the end of July, Orange Belgium detected a cyberattack impacting around 850.000 customer accounts. The breach exposed names, telephone numbers, SIM card numbers, PUK codes, and

tariff plans—but did not include passwords, e-mail addresses, financial data, or home addresses. Orange promptly blocked access. Affected users were notified via e-mail or SMS and urged to remain vigilant against phishing attempts. link

Bouygues Telecom confirms breach of 6,4 million customer records
On August 4, Bouygues Telecom disclosed a cyberattack that exposed personal and contractual data of 6,4 million clients, including IBANs. The operator reported the incident to CNIL and law enforcement, stating that it was resolved promptly. The breach raises the risk of phishing and banking scams. The company has not shared technical details, and the intrusion method remains unknown. link

Air France and KLM disclose data breach
On August 7, Air France and KLM disclosed that attackers breached a third-party customer service platform, exposing an undisclosed number of customer records. Affected data includes names, contact details, Flying Blue account information and subject lines of support tickets—but excludes sensitive personal or financial details like passwords, travel data, miles, passports or credit card information. The airlines cut off access, notified regulators, and informed customers to stay vigilant to phishing attempts. link

HUR cyber operation exposes secrets of Russia's new nuclear submarine
On August 4, Ukraine's military intelligence (HUR) published documents allegedly obtained via cyber operations, revealing detailed blueprints, crew lists, and vulnerabilities of Russia's new Borei-class nuclear submarine, the K-555 Prince Dmitry Pozharsky. The leak, exposing internal systems and personal data of the entire crew, is seen by analysts as a major intelligence coup with serious implications for Russian naval security. link

World

Cyber policy and law enforcement

Russia reportedly conducts tests to block WhatsApp and Telegram
On August 11, The Kyiv Independent published an article about Russia reportedly conducting tests to block WhatsApp and Telegram. In fact, the applications allegedly had their voice and video calls blocked. These actions come amid recurrent internet shutdowns, and the signing of a new law on June 24 to create a national digital platform. Their goal is to try to replace foreign services with domestic ones. `russia` link

Russia orders state-backed MAX messenger app, a WhatsApp rival, pre-installed on phones and tablets
On August 21, the Russian government announced that from September 1, 2025, all mobile phones and tablets sold in Russia must come pre-installed with MAX, a state-backed WhatsApp rival integrated with government services. The mandate also includes pre-installing the domestic app store RuStore on Apple devices and, from January 1, 2026, LIME HD TV on smart TVs. Critics warn of surveillance risks. `russia` link

FTC Chair warns tech firms against weakening data security or censoring Americans under foreign laws
On August 21, FTC Chair Andrew N. Ferguson sent letters to 13 major tech firms—including Apple, Amazon, Meta, Microsoft, and Alphabet—warning them not to weaken data security or censor American users under pressure from foreign laws such as the EU Digital Services Act or the UK's Online Safety and Investigatory Powers Acts. He cautioned that doing so could breach US law. `united states` link

Microsoft scales back Chinese access to cyber early warning system
On August 21, Reuters reported that Microsoft has reduced access for certain Chinese firms to its cybersecurity early-warning system following suspicions that Beijing-linked actors exploited the Microsoft Active Protections Program (MAPP) to facilitate a hacking campaign targeting SharePoint servers in late June and early July. As a precaution, Microsoft is withholding proof-of-concept code from those firms and reaffirmed its commitment to reviewing and removing partners who breach their contracts. `china` link

Massive INTERPOL operation arrests 1.209 cybercriminals across Africa
Between June and August 2025, INTERPOL-led Operation Serengeti 2.0 resulted in 1.209 cybercriminal arrests across 18 African nations and the UK. Targeting ransomware, online scams, and business e-mail compromise, the operation seized 97.4 million US dollars and dismantled 11.432 malicious infrastructures, impacting nearly 88.000 victims globally. link

Cyberespionage & prepositioning

Several countries advise on Chinese threat actors targeting telecommunications
On August 27, 13 countries, namely seven European Union countries, the Five Eyes, and Japan, issued an advisory warning about China-linked cyberespionage threat actors. They focus on those targeting networks worldwide, especially in telecommunications and government, and mention Salt Typhoon specifically. The threat actor's main focus are routers of major telecommunications providers, as well as edge routers, compromised devices, and trusted connections. `china` link

China-linked threat actor conducts 10-month-long campaign infiltrating telecommunications in South-west Asia
On July 29, Unit42 published their findings about a 10-month-long campaign conducted by a China-linked threat actor targeting telecommunications in South-west Asia. From February to November 2024, they found indicators of compromise in telecommunication companies in several countries, leveraging interconnected mobile roaming networks. However, they did not find clear evidence of data collection or exfiltration. The campaign, dubbed CL-STA-0969, was highly sophisticated and heavily overlaps with Liminal Panda. `china` 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 Turla, also known as Secret Blizzard. 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

Static Tundra exploiting Cisco devices in long-running cyberespionage campaign
On August 20, Cisco reported that the Russian state-sponsored cyberespionage group Static Tundra has been exploiting CVE-2018-0171 in Cisco IOS Smart Install to compromise unpatched, end-of-life network devices. The group is linked to the FSB's Centre 16 unit and operates as a sub-cluster of the broader Energetic Bear group. Their primary goal is intelligence gathering, targeting sectors such as telecommunications, higher education, and manufacturing across multiple continents. Related CERT-EU product: TA 25-134. `russia` link

Surge in Fortinet brute-force activity may signal zero-day risk
On August 3, GreyNoise observed a sharp rise in brute-force attempts against Fortinet SSL VPNs, followed by August 5 activity targeting FortiManager. Such spikes precede new vulnerability disclosures in 80% of cases. The malicious actor's adaptive campaign uses specific IPs for testing

and intrusion. The top targeted regions are Brazil and Hong Kong. Defenders should block listed IPs, tighten login controls, and restrict external access. link

Tracking Candiru's DevilsTongue spyware in multiple countries
On August 5, Recorded Future published a report on Candiru's spyware infrastructure. They uncovered eight operational clusters linked to Candiru's DevilsTongue spyware. The infrastructure varies in design, with some using intermediaries or Tor. Five clusters are likely still active—among them, Hungary and Saudi Arabia. One Indonesia-linked cluster was active until November 2024, while two Azerbaijani clusters remain of uncertain status. `psoa` link

Canadian House of Commons breach likely tied to Microsoft SharePoint ToolShell flaw
In mid-August, Canada's House of Commons reportedly began investigating a cyberattack that occurred on August 8. Attackers exploited Microsoft SharePoint Toolshell (CVE-2025-53770) to access a database of employee details used for managing computers and mobile devices. Stolen data includes staff names, e-mail addresses, job titles, office locations, and device information. link

Belarus-linked DSLRoot proxy network deploys hardware in US residences, including military homes
On August 8, Infrawatch and KrebsOnSecurity uncovered DSLRoot, a Belarusian-run residential proxy network operating across 20+ US states. The network exploits consumer modems and Android devices—without authentication—to provide rotating SOCKS5 proxies. The investigation revealed compromised homes, including one linked to the military, highlighting the risks of foreign-operated proxy infrastructure inside the US. link

Apple issues emergency patches for zero-day CVE-2025-43300 actively exploited in targeted attacks
On August 20, Apple released emergency updates to fix CVE-2025-43300, an out-of-bounds write flaw in Image I/O actively exploited in sophisticated attacks. The patch applies to iOS 18.6.2, iPadOS 18.6.2, 17.7.10, and macOS Sequoia 15.6.1, Sonoma 14.7.8, Ventura 13.7.8. This is the sixth zero-day exploited in 2025, making immediate installation of these updates critical. link

Cybercrime

Russia-linked RomCom exploits WinRAR CVE-2025-8088 exploited as a zero-day in phishing attacks
On August 8, ESET researchers reported that Russia-linked threat actor RomCom exploited WinRAR CVE-2025-8088 as a zero-day in spearphishing attacks to deploy various backdoors. The directory traversal flaw, fixed in version 7.13, allowed crafted archives to place executables in autorun paths for remote code execution. Users must manually update WinRAR, which lacks auto-update. `russia` link

Akira affiliates abuse drivers for evasion tactics
On August 5, GuidePoint reported that Akira ransomware activity involved repeated abuse of two Windows drivers— `rwdrv.sys` and `hlpdrv.sys`. The group likely used `rwdrv.sys` to gain kernel-level access and enable `hlpdrv.sys`, which disables Windows Defender via registry changes. This Bring Your Own Vulnerable Driver (BYOVD) technique has appeared in multiple cases and serves as a strong detection indicator for defenders. link

ClickFix phishing campaign targets macOS with AppleScript-based credential theft
On August 7, Forcepoint reported a ClickFix phishing campaign targeting macOS users with a fake CAPTCHA page that delivers the Odyssey Stealer malware. The malicious AppleScript steals credentials, crypto wallet data, cookies, and files, then exfiltrates them via a ZIP archive. The

threat actor uses OS-specific instructions and obfuscation to avoid detection and erases traces post-exfiltration. link

Cookie Spider malvertising campaign delivering Shamos malware for macOS
On August 20, CrowdStrike reported on Cookie Spider's Shamos malware campaign targeting over 300 macOS environments between June and August 2025. The cybercrime group used malvertising and fake help sites to trick users into running a malicious one-line command that bypassed Gatekeeper security checks and installed Shamos, which stole credentials, cryptocurrency data, and enabled persistence. CrowdStrike observed spoofed ads, GitHub repositories, and botnet modules in this activity. link

Storm-2460 leverages Windows zero-day and fake ChatGPT app to deliver malware
On August 18, Microsoft reported on a malware campaign leveraging a trojanized version of the open-source ChatGPT Desktop app to distribute a new modular backdoor called PipeMagic delivering a framework for running ransomware operations. Storm-2460, the financially motivated group behind PipeMagic, leveraged a Windows zero-day vulnerability (CVE-2025-29824) in the Common Log File System (CLFS). `finance` `technology` link

SpyVPN Chrome extension secretly screenshots users' activity and exfiltrates data
On
August 19, Koi Security revealed that a Chrome-featured VPN extension named FreeVPN.One—also known as SpyVPN —with over 100.000 installs was covertly taking screenshots of everything users visited (banking, Google Sheets, personal photos) and sending them off to a remote server without consent or any visible indication. link

Data exposure and leaks

Google confirms Salesforce CRM data breach
On August 5, Google updated a June report confirming its Salesforce CRM was breached via a vishing attack linked to UNC6040 (ShinyHunters), a financially motivated threat actor. Attackers accessed limited business contact data before access was cut. The incident is part of a broader campaign using malicious OAuth apps and social engineering, targeting major firms. Salesforce maintains that its core platform remains secure. link

Widespread data theft targets Salesforce instances via Salesloft Drift
On August 26, Google reported that an unknown threat actor named UNC6395 abused OAuth tokens from Salesloft's Drift app to exfiltrate data from Salesforce instances of technology, finance, and healthcare firms. Between August 8 and 18, attackers automated theft of AWS keys, passwords, and Snowflake tokens. Salesforce and Salesloft revoked tokens on August 20 and removed Drift from AppExchange. Affected organisations were notified. link

North Korea-linked Kimsuky suffer data breach
On August 11, two unaffiliated threat actors named Saber and cyb0rg, publicly leaked data reportedly from North Korea-linked Kimsuky group. They mention moral reasons for the leak, namely saying that Kimsuky are morally perverted because they steal to enrich their leaders and fulfil their political agenda. The dump amounts to 8.9GB of data, and includes phishing logs from targeted South Korean governmental entities and websites, malware, among others. `north korea` link

Information operations

China's GoLaxy uses AI-driven propaganda system GoPro to influence public opinion
On August 6, a New York Times article reported that leaked internal documents, obtained by

Vanderbilt University researchers, reveal how Chinese firm GoLaxy uses its AI-powered Smart Propaganda System GoPro to monitor and shape public opinion in Hong Kong, Taiwan, and China, and collect data on US politicians. While no US election targeting is confirmed, GoPro can mass-produce tailored propaganda, bolstering China's influence as US countermeasures wane. `china` link

Disruption & destruction

Malicious npm packages targeting WhatsApp developers contain remote kill-switch
On August 6, Socket's Threat Research Team revealed two malicious npm packages—naya-flore and nvlore-hsc—masquerading as WhatsApp integration libraries. These packages feature a remote kill-switch that fetches a base-64–encoded whitelist of phone numbers; if a developer's number isn't listed, the code executes a destructive rm –rf * to wipe their system. Despite having over 1110 downloads, both packages remain active on npm. link

Pro-Ukraine supposed hacktivists take over Russian TV on UA Independence Day
On August 24, Ukraine's Independence Day, pro-Ukraine supposed hacktivists—likely Belarusian Cyber Partisans—hijacked Russia's third-largest TV provider, airing messages on war losses and shortages for three hours across 116 channels, reaching 50.000 households. Ukrainian intelligence called them "local cyber partisans"; no group claimed responsibility. `russia` link

Opportunistic

N-able N-central vulnerabilities exploited in the wild
On August 13, CISA warned that threat actors are exploiting two N-able N-central vulnerabilities - CVE-2025-8875 and CVE-2025-8876 - enabling command execution and injection. N-able patched them in version 2025.3.1 and urged immediate updates. According to Shodan, there are around 2000 instances exposed online with the majority being in the US, Australia, Germany and the Netherlands. link

Threat actors leveraging AI to replicate official government websites
On August 5, cybersecurity company Zscaler ThreatLabz published their findings on a campaign that uses generative AI tools to create malicious replicas of Brazilian governmental websites. In fact, researchers have observed threat actors using AI tools like DeepSite AI and BlackBox AI to produce phishing templates mimicking the official websites. This is symptomatic of how AI tools are being increasingly leveraged by threat actors. `artificial intelligence` link

Trend Micro enterprise products face active exploitation (CVE-2025-54948 and CVE-2025-54987)
On August 6, Trend Micro disclosed command injection flaws (CVE-2025-54948, CVE-2025-54987) in its enterprise endpoint security management console. A threat actor has already exploited CVE-2025-54948. Trend Micro mitigated the issues in cloud-based products on July 31. On-premise users should apply the Fixtool immediately and await a critical patch expected mid-August. 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.