Cyber Brief (February 2025)

March 3, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 433 open source reports for this Cyber Brief[1].
- **Policy, cooperation, and law enforcement**. The EU aims to strengthen the EU's response to large-scale cyber incidents, Sweden and the UK seek backdoor access to private companies, and a former Polish Justice Minister arrested in Pegasus spyware case. Moreover, the US stands down on cyber Russia planning, Japan approves Cyber Defence Bill to counter sophisticated threats, Australian government bans Kaspersky products from government systems, and several police operations result in the arrest of cybercriminals.
- **Cyberespionage**. China-linked threat actors compromised Belgian Secret Service e-mail exchanges, as well as telecommunications worldwide. Russia-linked threat actor Sandworm was active in targeting critical infrastructure in Europe. Multiple Russian threat actors targeted Microsoft device code authentication and Signal Messenger in multiple sectors, including defence. Pegasus software infected at least one EU government official, while another Israeli spyware targeted EU civil society, and North Korea continues targeting developers.
- **Cybercrime**. The Belgian Port of Ostend was a victim of a cyberattack, China-linked threat actors were active in cybercrime worldwide, as were North Korea-linked Lazarus group, who namely carried out what is considered the largest cryptocurrency theft in history.
- **Information operations**. China-linked Spamouflage operation targets the Spanish government, and a report analysed the impact of AI-driven disinformation in financial destabilisation. OpenAI removed accounts from China and North Korea that misused ChatGPT for malicious activities.
- **Data exposure and leaks**. Orange group was a victim of a hack-and-leak attack in Romania, as was the Bulgarian Supreme Administrative Court.

Europe

Cyber policy and law enforcement

EU Commission proposes new cybersecurity blueprint to enhance crisis coordination
On February 24, the European Commission unveiled a proposal to strengthen the EU's response to large-scale cyber incidents. The updated blueprint outlines roles for EU entities throughout the crisis lifecycle, emphasising preparedness, detection, response, and recovery. It also promotes collaboration between civilian and military sectors, including NATO, and aligns with initiatives like the Critical Infrastructure Blueprint. The proposal aims to bolster collective cyber resilience across member states. `legislation` link

Swedish government seeks backdoor access to encrypted messaging apps
On February 24, the Swedish government proposed legislation requiring messaging providers to grant law enforcement access to encrypted communications. The proposal, citing national security concerns, targets apps like Signal and WhatsApp. Signal opposed the measure, stating it would leave Sweden if passed. Sweden joins other European nations debating similar laws on law enforcement access to encrypted data. `backdoor` link

Apple removes Advanced Data Protection in the UK amid government demands
On February 21, Apple announced the discontinuation of its Advanced Data Protection (ADP) feature for new users in the UK, with plans to require existing users to disable it in the near future. This decision follows demands from UK security services for backdoor access to encrypted iCloud backups. Despite this change, services such as iMessage, FaceTime, health data, and iCloud Keychain will continue to have end-to-end encryption in the UK. `backdoor` link

UK government proposes ransomware legislation to curb payments and boost reporting
On February 19, the UK's home office reported the UK government's consultation on ransomware legislation aimed at reducing payments to cybercriminals and increasing incident reporting. Proposed measures seek to limit financial incentives for attackers, improve intelligence on ransomware transactions, and enhance government response capabilities. The consultation remains open until April 8, 2025, with responses invited from stakeholders. `legislation` `ransomware` link

Former Polish Justice Minister arrested in Pegasus spyware case
On January 31, the Polish Police arrested former Justice Minister Zbigniew Ziobro, accusing him of approving the use of government funds for Pegasus spyware to surveil opposition leaders. This follows the earlier arrest of the former Internal Security Agency chief, Piotr Pogonowski. `psoa` `arrest` link

Joint operation between The Netherlands and the United States to disrupt cybercrime group
On January 29, Dutch and US authorities launched "Operation Heart Blocker" against a Pakistan-based cybercrime group called Saim Raza, also known as "The Manipulaters". The group operated online marketplaces that sold hacking tools, including spam and phishing services, to thousands of customers, resulting in over 3 million US dollars in losses. Their tools were used by organised crime groups to conduct business e-mail compromise (BEC) schemes. `pakistan` link

Spanish police arrest suspect in cyberattacks against Spanish and international governmental organisations
On February 5, the Spanish police arrested an individual suspected of conducting 40 cyberattacks against public and private organisations, including the Spanish Guardia Civil and Ministry of Defence, the US Army, NATO, and the UN. `arrest` link

Cyberespionage

China-linked threat actors compromised Belgian Secret Service e-mail exchanges
On February 26, the newspaper Le Soir revealed that Chinese threat actors compromised the Belgian Secret Service (VSSE) e-mail exchanges between 2021 and 2023. The threat actors exploited a vulnerability in the e-mail system of a US software supplier, called Barracuda, that was previously reported in 2023 and was being used by Belgian intelligence as well as the Belgian Pipeline Organisation, which monitors pipelines in the North Sea. `china` link

Multiple Russian threat actors targeting Microsoft device code authentication
On February 13, Volexity reported that multiple Russian threat actors have targeted Microsoft 365 accounts using Device Code Authentication phishing. These campaigns involved spearphishing e-mails, impersonating various organisations such as the European Parliament, the US Department of State and the Ukrainian Ministry of Defence. Attackers aimed to deceive users into entering codes that allowed unauthorised access to accounts. Volexity tracks these campaigns under three threat actors, including CozyLarch. `diplomacy` `russia` link

Sandworm APT targets Ukrainian users with trojanised Microsoft KMS activation tools
On February 11, EclecticIQ reported that Sandworm (APT44), linked to Russia's GRU, is conducting cyberespionage against Ukrainian Windows users. Since late 2023, they have distributed pirated Microsoft Key Management Service activators and fake Windows updates to deploy the BACKORDER loader, which installs Dark Crystal RAT (DcRAT) malware. This campaign exploits Ukraine's reliance on unlicensed software, posing significant risks to national security and critical infrastructure. `russia` link

Microsoft uncovers BadPilot campaign by Russian Seashell Blizzard subgroup
On February 12, Microsoft revealed that a subgroup within the Russian state actor Seashell Blizzard (aka Sandworm) has been conducting a multiyear global access operation, termed the "BadPilot campaign." This subgroup exploited vulnerabilities in internet-facing infrastructure to persist on high-value targets across sectors like energy, telecommunications, and government, expanding their operations beyond Eastern Europe since at least 2021. `energy` `russia` `telecommunications` link

CERT-UA analysis complements Microsoft's findings on Sandworm’s BadPilot campaign
On February 23, CERT-UA reported that UAC-0212, a subcluster of the Russian GRU-linked Sandworm group, targeted supplier companies in Serbia, the Czech Republic, and Ukraine between July 2024 and February 2025. CERT-UA’s findings complement Microsoft’s assessment of BadPilot by detailing phishing-based initial access methods, where attackers posed as customers and delivered malicious PDFs exploiting CVE-2024-38213. CERT-UA reports that the campaign aimed to compromise critical infrastructure service providers. `russia` link

Multiple Russia-aligned threat actors actively targeting Signal Messenger
On February 20, Google's Threat Intelligence Group reported that Russian state-aligned threat actors are targeting Signal Messenger accounts of individuals of interest to Russia's intelligence services. These actors exploit Signal's "linked devices" feature by sending malicious QR codes that, when scanned, link the victim's account to a device controlled by the attacker, enabling real-time message interception. Signal has since updated its app to enhance security against such phishing attacks. `russia` link

Pegasus spyware infected private sector devices and at least on European government official
On February 19, iVerify, a US-based cybersecurity firm, reported new detections of Pegasus spyware on 11 out of 18.000 devices tested in December, including those of business executives in real estate, logistics, and finance, as well as a European government official. The findings suggest broader use of commercial spyware beyond civil society targets. Some victims were

monitored for years using multiple Pegasus variants. `finance` `psoa` `public administration` link

Cellebrite zero-day exploit used to target phone of Serbian student activist
On February 28, Amnesty International's Security Lab reported that Serbian authorities exploited a zero-day vulnerability in Cellebrite's software to access the phone of a student activist. This sophisticated attack targeted USB drivers in Android devices, allowing unauthorised access. Despite previous reports of misuse, Serbian security services continue to employ such tactics against civil society. In response, Cellebrite has suspended product use by certain Serbian customers. link

Cybercrime

Italian tycoons scammed by AI-generated minister's voice
On February 9, the Financial Times reported that Italian tycoons were targeted in an AI-driven scam where fraudsters used a deepfake voice of Defence Minister Guido Crosetto to request ransom payments for kidnapped journalists. Some business leaders were contacted, and at least one transferred 1 million Euros. Authorities suspect phone number spoofing, and the Bank of Italy denied involvement. The case echoes past high-profile scams. `artificial intelligence` link

Belgian Port of Ostend victim of cyberattack
On February 12, the Belgian port of Ostend announced having been the victim of a cyberattack on February 10 and filed a complaint with the federal government. The Centre for Cybersecurity Belgium (CCB) is leading a team of internal and external cybersecurity experts to resolve the issue. The attack targeted a system that logs ship movements and crew lists, called Ensor. `transport` link

Green Nailao ransomware campaign targets European healthcare sector
On February 18, Orange Cyberdefence CERT reported a ransomware campaign, "Green Nailao," targeting European organisations, notably healthcare, between June and October 2024. The attack exploited CVE-2024-24919 to deploy ShadowPad and PlugX backdoors, later delivering the previously undocumented NailaoLocker ransomware. Researchers assess with medium confidence that the activity aligns with Chinese threat actors but remains unattributed to a known group. `china` `health` `ransomware` link

Information operations

China-linked Spamouflage operation targets the Spanish government
On January 29, Graphika, a US social network analysis company, published a report outlining a China-linked social media operation dubbed Spamouflage, targeting the Spanish government. Masquerading as Safeguard Defenders, a Madrid-based NGO, the threat actors called for the overthrow of the Spanish government. Spamouflage has been operating since at least 2017, targeting countries and voters worldwide, including in Europe and the US. `china` `public administration` link

Report on the impact of AI-driven disinformation says financial destabilisation may be caused by disinformation campaigns.
On February 14, Say No to Disinfo and Fenimore Harper communications released a report on the impact of AI-driven disinformation in financial destabilisation. A simulated campaign targeting UK banks showed that 60.8% of exposed individuals considered moving their money, demonstrating the power of synthetic content to incite financial instability. The findings

highlight the potential for low-cost influence operations to trigger bank runs and the financial sector's lack of preparedness against such threats. `artificial intelligence` link

Data exposure and leaks

Threat actor leaks Orange Group information from Romania
On February 25, a threat actor alleged to have stolen almost 6.5 GB of data from Orange Group, specifically from Orange Romania. The leak mainly affects employees, partners, and contractors, as well as some customers. The data contains e-mail addresses, source code, invoices, contracts, customer and employee information. However, according to BleepingComputer who analysed some of the leaked information, most of it seems to be outdated or expired. `telecommunications` link

Bulgarian Supreme Administrative Court victim of ransomware
On February 25, Bulgarian media reported about a ransomware intrusion and data breach impacting a Bulgarian parliamentary committee of the Supreme Administrative Court. 3.5TB of data were allegedly exfiltrated containing documents and information related to judges, including personally identifiable information, and human resources documents. The Acting Chairman of Bulgaria's Supreme Administrative Court confirmed the ransomware intrusion and stated the court was investigating the possibility of the data leaked online. `justice` `ransomware` link

World

Cyber policy and law enforcement

Japan approves Cyber Defence Bill to counter sophisticated threats
On February 7, Japan's Cabinet approved the Cyber Response Capability Enhancement Bill to strengthen defences against sophisticated cyberattacks targeting critical infrastructure. This legislation aligns with the National Security Strategy (December 2022) and incorporates expert recommendations from November 29, 2024. The bill includes active cyber defence measures, such as proactively detecting threats and shutting down enemy servers during an incident to mitigate potential harm. `japan` `legislation` link

Australian government bans Kaspersky products from government systems
On February 17, the Australian government informed it would ban all Kaspersky products from government systems, citing national security risks. The decision follows concerns over potential access by Russian intelligence services to sensitive data. Australia joins other nations in restricting the use of Kaspersky software in critical infrastructure and public sector networks. `russia` `legislation` link

The Atlantic: Musk's DOGE poses cybersecurity risks to US federal systems
According to a report by The Atlantic on February 7, Elon Musk's Department of Government Efficiency (DOGE) has accessed critical US federal IT systems, including those of the Treasury Department and Office of Personnel Management. Cybersecurity experts warn that DOGE's untrained personnel could unintentionally or deliberately compromise these systems, posing national security risks. The full impact is unclear, but concerns grow over data breaches, system disruptions, and long-term cybersecurity threats. `united states` link

Hegseth orders Cyber Command to stand down on Russia planning
On February 28, The Record reported that Defense Secretary Pete Hegseth ordered US Cyber

Command to halt all planning against Russia, including offensive cyber operations. This directive, issued to Cyber Command Chief General Timothy Haugh, does not affect the National Security Agency's intelligence activities targeting Russia. The move aligns with the administration's efforts to normalise relations with Moscow. `russia` `united states` link

Trump administration retreats in fight against Russian cyber threats
On February 28, The Guardian reported that the Trump administration is downplaying Russia's cyber threat, diverging from longstanding intelligence assessments. This shift was evident when State Department official Liesyl Franz named China and Iran as cyber threats but omitted Russia. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) has reportedly been directed to deprioritise reporting on Russian cyber threats. `russia` `united states` link

Google Cloud introduces quantum-safe digital signatures in Cloud KMS
On February 21, Google announced the integration of quantum-safe digital signature algorithms into its Cloud Key Management Service (Cloud KMS). This enhancement offers software and hardware support for standardised quantum-safe algorithms, facilitating a seamless migration path for existing keys and protocols. The update aims to protect sensitive data from future quantum computing threats, aligning with NIST's post-quantum cryptography standards. `quantum computing` link

8Base ransomware site taken down as Thai authorities arrest four connected to operation
On February 10, authorities dismantled the 8Base ransomware group's leak site and arrested four European suspects in Phuket, Thailand. The suspects are accused of extorting 16 million US dollars from over 1.000 victims worldwide. This operation, dubbed PHOBOS AETOR, involved multiple international law enforcement agencies. `arrests` `ransomware` link

US sanctions LockBit ransomware's bulletproof hosting provider
On February 11, the US, Australia, and the UK imposed sanctions on Russia-based Zservers, a bulletproof hosting provider enabling LockBit ransomware operations. The action targets the infrastructure used for cyberattacks, aiming to disrupt ransomware ecosystems. This coordinated effort follows previous sanctions against LockBit actors, reinforcing international pressure on cybercriminal networks operating from Russia. `ransomware` `russia` `sanctions` `united states` link

Cyberespionage

Salt Typhoon continues targeting telecommunications and education sector worldwide
On February 13, Recorded Future reported about Salt Typhoon's continuing operations targeting the telecommunications sector, as well as education, despite the uncovering of their activities in recent months. Between December 2024 and January 2025, they were identified exploiting unpatched Cisco network devices worldwide. The targets included telecommunications providers in the US, the UK, and South Africa, universities in several countries, possibly to access research in telecommunications, engineering, and technology. `china` `education` `telecommunications` link

China-linked APT41 targets Japanese firms in RevivalStone cyberespionage campaign
On February 18, Japanese cybersecurity company LAC reported that China-linked APT41 targeted Japanese manufacturing, materials, and energy sectors in a campaign dubbed RevivalStone. Active since at least 2012, Winnti deployed new malware variants in 2024, exploiting an SQL injection vulnerability in an ERP system to drop web shells. The group used stolen certificates and rootkits for persistence and covert access. `china` `japan` link

Emerald Sleet uses PowerShell exploits to target international affairs professionals and NGOs
On February 11, Microsoft reported that North Korea-linked Kimsuky, also known as Emerald

Sleet, is using a tactic where victims are deceived into running PowerShell as an administrator and executing malicious code. This facilitates data exfiltration via a remote desktop tool. The group primarily targets individuals working in international affairs, particularly those focused on Northeast Asia, in America, Europe, and East Asia. `civil society` `north korea` link

Journalists and civil society members targeted on WhatsApp by Israeli spyware
On January 31, WhatsApp announced that 90 journalists and civil society members were targeted by Israeli spyware Paragon Solutions. The attack was a "zero-click", meaning the victims were possibly compromised by simply receiving the malicious PDF file that served as a vector. An Italian and a Swedish journalist were among the victims notified by WhatsApp. `civil society` `psoa` link

Cybercrime

Chinese espionage tools used in ransomware attack on Asian firm
On February 13, Symantec reported that tools typically linked to China-based espionage actors were used in a ransomware attack against an Asian software and services company. In late 2024, the attacker deployed a distinct toolset, including a PlugX variant, previously associated with Chinese espionage activities. This suggests potential crossover between state-sponsored espionage and cybercrime operations. `china` `ransomware` link

DeepSeek-themed malware campaign uses ClickFix technique to spread Vidar stealer
On February 25, Zscaler's ThreatLabz reported a malware campaign impersonating DeepSeek to distribute the Vidar stealer using the ClickFix technique. Attackers trick users with a fake CAPTCHA, which injects PowerShell commands via clipboard manipulation, leading to malware execution. The campaign exploits DeepSeek's popularity to deceive users and steal sensitive data. `artificial intelligence` link

Lazarus Group deploys Marstech1 JavaScript implant in targeted developer attacks
On February 14, SecurityScorecard linked the Lazarus Group to a new JavaScript implant, Marstech1, used in targeted attacks against developers. Delivered via a now-removed GitHub profile, the malware collects system data and manipulates browser settings, targeting cryptocurrency wallets like MetaMask. The implant has infected 233 confirmed victims across the US, Europe, and Asia, posing a supply chain risk through NPM packages. `north korea` link

Bybit crypto exchange suffers largest cryptocurrency theft in history
On February 21, Bybit, a Dubai-based cryptocurrency exchange, experienced a security breach resulting in the theft of approximately 1.46 billion US dollars in crypto assets. Initial reports suggest that malware was used to trick the exchange into approving unauthorised transactions. This incident surpasses previous records, marking it as the largest cryptocurrency theft to date. Blockchain analytics firm Elliptic attributed the attack to North Korea’s Lazarus group, citing transaction patterns linked to previous hacks. `north korea` link

Massive botnet exploits Basic Authentication to target Microsoft 365 accounts
On February 24, SecurityScorecard researchers reported on a massive botnet of over 130.000 compromised devices conducting password-spray attacks on Microsoft 365 accounts using Basic Authentication which will be deprecated in September. The attackers exploit credentials stolen by infostealer malware, targeting non-interactive sign-ins, which do not trigger MFA alerts, and exploiting environments where Basic Authentication remains enabled. `botnet` link

New macOS infostealer distributed via Fake Update campaign
On February 18, Proofpoint reported that a new macOS infostealer, FrigidStealer, had been deployed by threat actor TA2727 in collaboration with TA2726 and TA569. The malware is delivered via fake browser update pages and is part of a broader campaign which also targets

Windows and Android devices. According to Proofpoint, TA569, previously known for SocGholish malware, has shifted to working with other actors to distribute new payloads globally. `stealer` link

New Lumma stealer campaign use compromised educational infrastructure to target various sectors
On February 14, Cloudsek security researchers reported on a Lumma Stealer malware campaign exploiting compromised educational infrastructure to distribute malicious LNK files disguised as PDFs. This campaign targeted finance, healthcare, technology, and media sectors and reportedly steals passwords, browser data, and crypto wallets. These LNK files, when executed, initiate a multistage infection process leading to the deployment of Lumma stealer. `education` `finance` `health` link

Brute force attacks target VPN devices using 2.8 million IPs
On February 7, ShadowServer reported that a large-scale brute force attack was underway, utilising nearly 2.8 million IP addresses to target internet exposed networking devices from vendors such as Palo Alto Networks, Ivanti, and SonicWall. The attack aims to guess device credentials to gain initial access to network devices. Many of the attacking IPs are linked to compromised routers and IoT devices, indicating a widespread botnet operation. `brute-force` link

New XCSSET macOS variant targeting Xcode
On February 17, Microsoft reported on a new malware variant dubbed XCSSET which is targeting macOS by infecting Xcode projects. This variant introduces enhanced obfuscation, updated persistence mechanisms using zshrc and dock methods, and new infection techniques. The malware continues to target digital wallets, Notes app data, and system files. Limited attacks have been observed, but its capabilities highlight ongoing macOS security risks. `malware` link

Microsoft removes popular VSCode extensions over security concerns
On February 26, Microsoft removed two widely used Visual Studio Code extensions, 'Material Theme – Free' and 'Material Theme Icons – Free,' from the Visual Studio Marketplace due to alleged malicious code. Cybersecurity researchers Amit Assaraf and Itay Kruk identified suspicious code in these extensions, leading to their removal. The publisher, Mattia Astorino (aka equinusocio), claims the issue stems from an outdated dependency. Users now receive alerts in VSCode that the extensions have been automatically disabled. `technology` link

Information operations

OpenAI bans accounts misusing ChatGPT for surveillance and influence campaigns
On February 21, OpenAI announced the removal of accounts from China and North Korea that misused ChatGPT for malicious activities, including surveillance and opinion-influence operations. These actors generated anti-US news articles in Spanish and created fictitious job profiles to secure employment at Western firms. OpenAI continues to monitor and prevent such policy violations. `artificial intelligence` 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.