Cyber Brief (March 2025)

April 2, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 575 open source reports for this Cyber Brief[1].
- **Policy, cooperation, and law enforcement.** Europol, Finnish, German and US authorities seized servers linked to Garantex, a cryptocurrency exchange, which was reportedly being used to evade sanctions on Russia. Spanish authorities indicted NSO group executives over Pegasus spyware allegations. The US Defense Secretary reportedly ordered Cyber Command to stand down on Russia planning.
- **Cyberespionage.** Pro-Russia actors have reportedly recruited individuals through Telegram to conduct sabotage and espionage activities. China-linked Silk Typhoon reportedly targeted IT supply-chains to conduct cyberespionage on downstream customers and Ant Weaver reportedly infiltrated an Asian telecommunications company for four years.
- **Cybercrime.** Strela stealer was used in the targeting of European e-mail accounts in a widespread phishing campaign. North Korea-linked Lazarus group deployed six new fake npm packages that compromise developer environments to engage in cryptocurrency theft.
- **Data exposure and leaks.** Researchers at a company behind an open-source scanner reported nearly 12.000 API keys and passwords exposed in an AI training dataset, including AWS and MailChimp API keys.
- **Disruption.** Ukraine's state railway operator experienced a cyberattack disrupting access to online ticket sales and its mobile app.
- **Hacktivism.** Social media platform X experienced DDoS attacks claimed by pro-Palestine supposed hacktivist group Dark Storm.

Europe

Cyber policy and law enforcement

European Commission to invest 1.3 billion euro in artificial intelligence, cybersecurity and digital skills
On March 28, the European Commission announced 1,3 billion euro in funding on artificial intelligence (AI), cybersecurity, cloud technology, and digital skills through the Digital Europe Programme (DIGITAL) for 2025 to 2027. The initiative supports advanced cybersecurity measures for digital infrastructure, including hospitals and submarine cables, reinforcing Europe's technological sovereignty and digital resilience. link

Switzerland obliges critical infrastructure organisations to report cyberattacks within 24h
On March 10, Switzerland's National Cybersecurity Centre (NCSC) announced a new mandate through an amendment to the Information Security Act requiring critical infrastructure organisations in the country to report cyberattacks to NCSC within 24 hours of their discovery. The mandate will enter into force on April 1, 2025. link

Europol, Finnish, German and US authorities seize Russian cryptocurrency exchange's domain used to circumvent sanctions
On March 6, Garantex, a Russian cryptocurrency exchange, announced it was temporarily suspending operations after Europol, Finnish, German and US authorities seized its domain. The US Department of Justice accused the platform of processing at least 96 billion US dollars worth of cryptocurrency transactions to circumvent sanctions. The law enforcement entities seized servers that hosted Garantex's operations in their respective countries. link

Spain indicts NSO group executives over Pegasus spyware allegations
On March 3, a Spanish Provincial Court indicted three NSO Group executives for their alleged involvement in Pegasus spyware campaigns targeting a lawyer representing the Catalonia-based human rights group Irídia between 2019 and 2020. link

UK sets post-quantum cryptography migration timeline
On March 20, NCSC-UK outlined key milestones for the UK's migration to post-quantum cryptography. By 2028, organisations should define migration goals and assess cryptographic dependencies. By 2031, they must begin high-priority transitions and refine migration plans. Full migration should be completed by 2035, though some technologies may take longer. The guidance targets critical infrastructure, large enterprises, and bespoke IT systems. `quantum computing` link

Cyberespionage

Suspected data breach in the Finnish Foreign Ministry's remote access service
On March 27, the Finnish Ministry for Foreign Affairs detected suspicious activity in its remote access service, raising concerns about a possible data breach. In response, the Ministry swiftly disabled the service and launched an internal investigation. The incident was reported to the National Bureau of Investigation and cybersecurity authorities for further analysis. The Ministry emphasised its commitment to securing its systems and mitigating any potential risks. link

Two Serbian journalists targeted with Pegasus spyware in February 2025
On March 28, Amnesty International reported that two journalists from the Balkan Investigative Reporting Network (BIRN), an award-winning Serbian network of investigative journalists, were targeted with NSO Group's Pegasus spyware. According to Amnesty International investigation's investigation, the intrusion happened in February 2025. This is the third time in two years that

Amnesty International’s Security Lab has found NSO Group’s Pegasus spyware being used against civil society in Serbia. `psoa` link

Several state-sponsored threat actors exploit Windows zero-day vulnerability
On March 18, Trend Micro issued a report about a Windows zero-day vulnerability (ZDI-CAN-25373) which was reportedly exploited by as many as 11 state-sponsored APTs linked to North Korea, Russia, Iran, and China. `china` `iran` `north korea` `russia` 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. In response, Cellebrite has suspended product use by certain Serbian customers. `psoa` link

Russia reportedly recruits cyber saboteurs online for hybrid warfare in Europe
On March 12, Belgium-based VRT reported that pro-Russia actors recruited individuals online for sabotage and espionage activities in Europe, including in Belgium. These groups utilise platforms like Telegram to assign tasks such as collecting e-mail addresses of Belgian journalists or defacing vehicles, offering cryptocurrency as payment. Belgian State Security warns of increased use of disposable agents for intelligence gathering, propaganda, and sabotage, complicating attribution and enhancing Russia's hybrid warfare tactics. `russia` link

Cybercrime

Swiss company Ascom breached through Jira
On March 17, Swiss company Ascom reported to have experienced a cyberattack the day prior. The threat actors exploited compromised credentials to breach Ascom's Jira ticketing system, stealing approximately 44 GB of data, including source code, project details, and confidential documents. The incident did not impact Ascom's business operations. link

Strela Stealer targets European e-mail users with phishing campaign
On March 6, Trustwave reported that Strela Stealer, active since 2022, was used to collect Mozilla Thunderbird and Microsoft Outlook credentials in German-speaking regions. Delivered via phishing e-mails disguised as invoices, it verifies system locale before execution. link

Disruption

Cyberattack disrupted Ukrainian railway ticket sales
On March 24, a cyberattack on Ukraine's state railway operator, Ukrzaliznytsia, disrupted online ticket sales and its mobile app, causing long queues at Kyiv’s central station. Despite the attack, train schedules were unaffected. The company is investigating the incident with security services, but has not disclosed technical details. link

Hacktivism

DDoS attacks disrupt Dutch government login system DigiD, blocking access to critical services
On March 3, a series of DDoS attacks disrupted DigiD, the Dutch government's authentication system, blocking thousands from accessing vital services like tax filings, municipal resources, and medical portals. `public administration` link

World

Cyber policy and law enforcement

Microsoft disrupts global cybercrime network exploiting generative AI vulnerabilities
On February 27, Microsoft researchers identified a global cybercrime network, Storm-2139, exploiting vulnerabilities in generative AI services, including Azure OpenAI, to create and distribute illicit content. By filing a lawsuit and seizing key infrastructure, Microsoft disrupted the network's operations, named four defendants from Iran, the UK, Hong Kong, and Vietnam, and emphasised the need for robust AI safeguards and continued legal actions to combat the misuse of AI technologies. `artificial intelligence` link

LockBit ransomware developer extradited to US
On March 13, a dual Russian and Israeli national was extradited to the US for developing LockBit ransomware. Arrested in Israel in August, the individual allegedly helped build malware, disable antivirus software, and maintain LockBit's infrastructure. LockBit targeted over 2500 victims, extorting 500 million US dollars worth of cryptocurrency. The arrest follows a global law enforcement operation disrupting LockBit in February. `cat: cybercrime` link

US charges 12 Chinese nationals for state-sponsored cyberespionage
On March 5, the US Department of Justice charged 12 Chinese nationals, including officers of China's Ministry of Public Security and employees of Anxun Information Technology Co. Ltd. (i-Soon), for their roles in hacking campaigns aimed at stealing data and silencing dissent globally. The defendants allegedly infiltrated networks of US and foreign organisations, using stolen data for profit and state-sponsored espionage. `china` `united states` link

Canada launches cyber security certification program for defence contracts
On March 12, Canada launched the first phase of the Canadian Program for Cyber Security Certification (CPCSC) to strengthen defence sector security against supply-chain threats. This phase introduces a new cyber security standard, an accreditation process, and a self-assessment tool for level 1 certification. The CPCSC will be implemented gradually, ensuring companies meet security requirements at contract award to mitigate risks from cyber threats in the supply-chain. `defence` link

Turkey restricts access to social media amid political unrest
On March 19, NetBlocks confirmed that network data indicated Turkey had restricted access to multiple social media platforms, including X (formerly Twitter), YouTube, Instagram, and TikTok. This occurred amid unrest over the detention of the Istanbul mayor. `internet restriction` `Turkey` link

US Defense Secretary reportedly ordered Cyber Command to stand down on Russia planning
On February 28, The Record reported that the Defense Secretary ordered US Cyber Command to halt planning of operations such as offensive cyber operations against Russia. `russia` `united states` link

Cyberespionage

China-linked Weaver Ant long-term attack against Asian telecommunications services provider
On March 24, Sygnia, a cybersecurity company, reported on Ant Weaver, a China-linked threat actor. Ant Weaver reportedly conducted a campaign against a major Asian telecommunications company for more than four years, hiding traffic and infrastructure with the help of compromised Zyxel CPE routers. `china` link

Microsoft warns of Silk Typhoon's shift to IT supply-chain attacks
On March 5, Microsoft reported that the Chinese state-sponsored group Silk Typhoon targeted IT supply-chains, exploiting remote management tools and cloud services to access downstream customers. The group used stolen API keys and credentials, unpatched applications, and zero-day vulnerabilities to infiltrate networks across various sectors, including government, healthcare, and defence, leaving minimal traces by avoiding traditional malware and web shells. `china` link

China-linked cyberespionage actor UNC3886 targets Juniper routers
On March 12, Google Cloud reported that UNC3886, a China-nexus group, exploited Juniper Networks routers between mid-2023 and early 2024. The attackers deployed custom backdoors with active and passive capabilities, allowing long-term access while disabling logging mechanisms. This tactic enables persistent espionage and potential future disruptions to critical infrastructure. `china` link

China-linked FamousSparrow targets financial organisation in the US
On March 26, researchers from ESET published their findings about China-linked FamousSparrow targeting a US financial institution in July 2024. The threat actor was thought to be inactive since 2022, but in this targeting, researchers found two new versions of its custom backdoor SparrowDoor. `china` `finance` `united states` link

WhatsApp patched zero-click flaw exploited in Paragon spyware attacks
On March 19, WhatsApp disclosed that it had patched a zero-click, zero-day vulnerability exploited to install Paragons Graphite spyware. This flaw allowed attackers to infect devices without user interaction. Citizen Lab identified the exploit, leading to WhatsApp addressing the issue without requiring a client-side fix. Approximately 90 Android users, including journalists and activists, were notified of being targeted. `psoa` link

Russia-linked threat actor exploits zero-day in Microsoft's Management Console
On March 25, Trend Micro uncovered a campaign by the Russia-linked threat actor Water Gamayun exploiting a zero-day in Microsoft's Management Console to execute malicious code. By manipulating .MSc files and MUIPath, attackers stole sensitive data and maintain persistence. `russia` link

Cybercrime

Fake Cloudflare verification on vulnerable WordPress websites results in LummaStealer infections
On March 19, Sucuri reported a malware campaign where attackers exploit WordPress sites to display fake Cloudflare verification prompts. These prompts deceive Windows users into executing malicious PowerShell commands, leading to LummaStealer Trojan infections. The malware harvests sensitive data, including login credentials and cryptocurrency wallets. link

Black Basta and Cactus ransomware groups exploit Microsoft Teams to deploy BackConnect malware
On March 3, Trend Micro reported that Black Basta and Cactus ransomware groups have integrated BackConnect malware into their attacks, enabling persistent control over compromised systems. This malware, linked to QakBot, aids in exfiltrating sensitive data and expanding attackers' foothold, with incidents primarily occurring in North America and Europe since October 2024. These groups have evolved their tactics, using social engineering and legitimate tools like Microsoft Teams to gain unauthorised access. link

AI-generated fake GitHub repositories distribute Lumma Stealer malware
On March 11, Trend Micro reported that cybercrime actors are leveraging AI to create fake

GitHub repositories, distributing LummaStealer malware as its final payload. These repositories pose as legitimate tools, like employee time tracker Discord bot and cracks for software like IDA Pro, deceiving users into downloading malicious files. The campaign exploits GitHub's trusted reputation to evade detection. This story highlights the importance of downloading software only from official sources. link

Microsoft Trusted Signing service abused for malware campaigns
On March 22, Bleeping Computer reported that cybercrime actors are exploiting Microsoft's Trusted Signing service to codesign malware using short-lived three-day certificates. These certificates enhance malware credibility, bypassing security filters. Researchers identified campaigns like Crazy Evil Traffers and Lumma Stealer using this method. Microsoft is monitoring threats and revoking abused certificates, but the simplified verification process makes its service an attractive alternative to Extended Validation certificates. link

DollyWay campaign abused WordPress to redirect users to scam
On March 17, GoDaddy reported on a WordPress campaign dubbed DollyWay v3. It primarily targets visitors of infected WordPress sites via injected redirect scripts that employ a distributed network of Traffic Direction System nodes hosted on compromised websites. These scripts redirect site visitors to various scam pages through traffic broker networks associated with VexTrio, a cybercrime group. link

SocGholish aids RansomHub ransomware deployment
On March 14, Trend Micro highlighted SocGholish’s role in enabling RansomHub ransomware through the Water Scylla intrusion set. SocGholish spreads via compromised websites, tricking users into downloading malicious files. It employs an obfuscated JavaScript loader to evade detection, providing persistent access for data theft and malware deployment. link

DPRK-linked Lazarus group deploys six new fake npm packages
On March 10, Socket, a technology company, reported that North Korea-linked Lazarus group deployed six new fake npm packages, which have been downloaded over 300 times. The malicious packages compromise developer environments, steal credentials, deploy a backdoor, and extract cryptocurrency data. In some seemingly benign packages, researchers uncovered BeaverTail malware. `north korea` link

Data exposure and leaks

Nearly 12.000 API keys and passwords exposed in AI training dataset
On February 27, researchers at Truffle Security, the company behind the TruffleHog open-source scanner for sensitive data, discovered nearly 12.000 valid API keys and passwords in the Common Crawl dataset, which is used to train various AI models. The exposed secrets included AWS and MailChimp API keys, raising concerns about insecure coding practices influencing AI behaviour despite pre-processing efforts to remove sensitive information. `artificial intelligence` link

Hacktivism

DDoS attack disrupts X
On March 10, social media platform X suffered a DDoS attack that temporarily disrupted its services three times in a few hours. The DDoS was claimed by a pro-Palestine supposed hacktivist group. link

All CERT-EU's Security Advisories are available to the public on CERT-EU's website, `https://www.cert.europa.eu/publications/security-advisories/`

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.