Cyber Brief (December 2024)

January 3, 2025 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 258 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, the UN General Assembly adopted its first international cybercrime treaty, enhancing global collaboration against cyber threats. Meanwhile, the US imposed sanctions on a Chinese firm for exploiting firewall vulnerabilities and delayed a TikTok ban, balancing national security concerns with legal challenges. The US also sanctioned Russian and Iranian entities over election interference.
- On the **cyberespionage** front, the US disclosed that a ninth US telecommunications company was breached by the Chinese-linked cyberespionage group Salt Typhoon. The US also accused Chinese hackers of breaching the US Treasury in a supply-chain attack compromising the cybersecurity company BeyondTrust. Meanwhile, Russian state-sponsored groups like Turla and BlueAlpha/Gamaredon escalate their campaigns using advanced tools and tactics, targeting Ukraine and exploiting other threat actors' infrastructure.
- Relating to **cybercrime**, a ransomware attack on Romania's Electrica Group disrupted services, exposing risks to critical energy infrastructure. Additionally, ESA merchandise store was compromised with malicious scripts to steal payment details, highlighting vulnerabilities in third party hosting.
- Relating to **disruption**, Finnish authorities detained a tanker suspected of damaging undersea cables, emphasising risks to energy and internet stability. Additionally, vulnerabilities in solar installations pose significant threats to Europe's power grid amidst rising renewable energy adoption.
- On the **information operations** front, Russian influence operations on TikTok disrupted the Romanian presidential election, revealing sophisticated disinformation tactics. Concurrently, according to a report by Japanese media, China's increasing adoption of Russian-style online manipulation showcases collaborative geopolitical influence strategies.
- As regards **data exposure and leaks** incidents, a breach at UK-based AI technology company Builder.ai exposed 3 million records, including sensitive company documents, raising concerns over database security.

Europe

Cyber policy and law enforcement

Operation PowerOFF: Law enforcement shuts down DDoS-for-hire platforms
On December 11, law enforcement agencies disrupted 27 major DDoS-for-hire platforms as part of Operation PowerOFF. Europol coordinated the effort involving 15 countries, arresting three administrators and identifying over 300 users. The operation targeted cybercriminals behind holiday season DDoS attacks, which cause severe disruptions. Authorities also launched an online deterrence campaign to prevent further offences, using targeted ads and educational outreach. `takedown` link

Law enforcement operation against phone phishing gang in Belgium and the Netherlands
On December 6, Europol reported that Belgian and Dutch authorities dismantled a phone-phishing gang, arresting eight suspects and conducting 17 searches. The gang targeted older victims across Europe, posing as police or banking staff, stealing millions to fund lavish lifestyles. Authorities seized luxury items, cash, and a firearm. Europol and Eurojust coordinated investigations and urged vigilance against phishing schemes. `arrests` link

Albanian authorities dismantle Rydox cybercrime marketplace with international collaboration
On December 12, the special prosecution of Albania (SPAK) concluded Rydox a major operation targeting an illegal cybercrime marketplace, with international collaboration. Authorities arrested three administrators, seized assets, and shut down the platform offering stolen personal data and hacking tools to 18.000 users. Active since 2016, Rydox generated 230.000 US dollars from 7600 sales. Investigations continue to trace the network's full criminal scope. `arrests` `seizure` `takedown` link

BSI warns about pre-installed malware on IoT devices
On December 12, Germany's BSI disrupted malware communication on 30.000 IoT devices with outdated Android versions. The pre-installed malware, BadBox, enables fake-news distribution, ad fraud, and proxy misuse, linking users' IPs to crimes. The BSI advises disconnecting vulnerable devices, scrutinising cybersecurity before purchase, and reviewing networked devices. Consumers with infected devices may be informed by providers. `takedown` link

Cyberespionage

Russia-linked Turla escalates cyberespionage operations in Ukraine
On December 11, Microsoft reported that Turla used spearphishing and Amadey bots to deploy Tavdig and KazuarV2 backdoors on Ukrainian military devices. The group employed RC4-encrypted reconnaissance tools, DLL-sideloading, and PowerShell droppers for persistence and data exfiltration. Turla also repurposed third-party malware infrastructure and utilised strategic web compromises to expand access and target systems effectively. `defence` `russia` link

Russia-linked BlueAlpha abuses Cloudflare tunnels in recent activities
On December 5, Recorded Future reported on Russian state-sponsored cyber threat group BlueAlpha's latest tactics. The group has been targeting Ukrainian organisations since 2014 with custom malware, including GammaLoad and GammaDrop. BlueAlpha recently started using Cloudflare Tunnels to conceal its staging infrastructure, making it harder to detect. `russia` link

Chinese APT campaign targeting IT providers in Southern Europe
On December 10, SentinelLabs and Tinexta Cyber reported "Operation Digital Eye," a Chinese APT campaign targeting Southern Europe's B2B IT providers in mid-2024. The attackers

exploited Visual Studio Code Remote Tunnels and Azure infrastructure for covert C2 operations, aiming to infiltrate supply chains. Early intervention disrupted their activities. Evidence highlights a shared vendor maintaining espionage tools within China's APT ecosystem, demonstrating advanced persistence and evasion. `china` link

Effective phishing campaign targeting European companies and institutions
On December 18, Palo Alto Networks reported a phishing campaign targeting European companies, particularly in Germany and the UK. The campaign, active from June to September 2024, aimed to harvest account credentials and compromise Microsoft Azure cloud infrastructure. Approximately 20.000 users in the automotive, chemical, and industrial compound manufacturing sectors were affected. Attackers used fake forms created with HubSpot's Free Form Builder and malicious PDFs mimicking DocuSign documents. `automotive` `chemical` link

Serbian authorities deploy NoviSpy spyware to target journalists, activists, and dissidents in Serbia
On December 16, Amnesty International reported that Serbian authorities deployed a new spyware, NoviSpy, targeting Android devices. Researchers shared exploit artefacts with Google's Threat Analysis Group, revealing vulnerabilities in Qualcomm's DSP, likely exploited to deploy NoviSpy. The spyware targeted journalists, activists, and dissidents in Serbia. Google identified additional compromised devices, removed the spyware, and sent "government-backed attack" notifications to all affected users to protect them. link

Cybercrime

Romanian energy supplier Electrica hit by ransomware attack
On December 9, Romanian electricity supplier Electrica Group reported a ransomware attack impacting its operations. While critical systems like SCADA remain unaffected, protective measures have caused temporary service disruptions. Serving over 3.8 million users, Electrica collaborates with national cybersecurity authorities to address the issue. This attack follows a surge in cyber threats tied to election interference, underscoring Romania's growing cybersecurity challenges. `energy` link

ESA online store targeted with malicious payment script
On December 24, Sansec identified malicious JavaScript on the European Space Agency's merchandise store, redirecting users to a fake Stripe payment page to steal card details. Source Defense Research confirmed the findings and captured evidence of the script. ESA stated the store is third party hosted. The site is offline, but the script remains visible in the source code. link

Disruption

Finland boards oil tanker suspected of causing internet, power cable outages
On December 26, Finnish authorities detained the oil tanker Eagle S in the Baltic Sea, suspecting it of damaging the Estlink 2 undersea power cable and four internet cables between Finland, Estonia, and Germany a day earlier. The vessel, allegedly part of Russia's shadow fleet evading oil sanctions, is believed to have severed the cables with its anchor. The crew is under investigation for serious sabotage. `energy` `russia` `telecommunications` link

Europe's power grid risks solar-driven cyber threats
On December 12, Bloomberg highlighted Europe's vulnerable power grid, exacerbated by rising solar panel installations. Cybersecurity experts warned that flaws in solar inverters could allow threat actors to disrupt grid operations, risking widespread outages. Despite EU efforts to

bolster defences, fast growth and cost pressures undermine security. NATO drills and regulations aim to address the risk as renewables become critical infrastructure, but challenges persist. `energy` link

Information operations

Russian information operation on TikTok related to the Romanian presidential election
On December 4, Romanian authorities informed that ultranationalist presidential candidate Cătălin Georgescu benefited from a TikTok campaign similar to Kremlin-run operations in Ukraine and Moldova. Declassified Romanian intelligence documents revealed the operation. The European Commission ordered TikTok to "freeze and preserve data" amid the election, citing concerns of Russian interference. An investigation is underway, leading to the Constitutional Court's annulment of the presidential election on December 6. `election` `russia` link

France's foreign minister accuses Russia of interference
On December 18, French Foreign Minister Jean-Noël Barrot revealed that Kremlin-linked actors contacted over 2.000 European influencers, including 20 in France. At least nine French influencers from fields like lifestyle and history allegedly accepted deals to spread pro-Russian narratives. Barrot urged vigilance, highlighting evolving interference methods and reinforced French tools to counter such threats as investigations continue into their awareness or manipulation. `russia` link

Data exposure and leaks

UK-based AI company Builder.ai suffered a data breach exposing 3 million records
On December 19, the cybersecurity researcher Jeremiah Fowler discovered an unprotected Builder.ai database containing over 3 million records (1,29 TB), including invoices, NDAs, and cloud storage access keys. Despite responsible disclosure, the database remained exposed for nearly a month. Builder.ai is a London-based company offering AI software and app development solutions. `artificial intelligence` link

World

Cyber policy and law enforcement

UN General Assembly adopts milestone cybercrime treaty
On December 24, the UN General Assembly adopted its first legally binding cybercrime convention, the first international anti-crime treaty in 20 years. It strengthens international cooperation and helps developing nations counter cybercrime trends like unauthorised data access, online abuse, and money laundering. Adopted after five years of negotiations, it opens for signatures in Vietnam in 2025 and takes effect 90 days after 40 ratifications. `cooperation` link

Saudi Arabia leads inaugural Arab Cybersecurity ministers' council
On December 25, Saudi Arabia, chaired by Majid Al-Mazid, hosted the first Arab Cybersecurity Ministers' Council in Riyadh. Officials, including Arab League ministers and Secretary-General Ahmed Aboul Gheit, discussed regional cybersecurity cooperation. Al-Mazid highlighted the importance of a unified strategy to bolster Arab security. Key outcomes included plans for joint exercises and developing an Arab Cybersecurity Strategy to address shared challenges. `cooperation` link

Trump appeals to Supreme Court to delay TikTok ban
On December 27, Donald Trump asked the US Supreme Court to delay a law threatening to ban TikTok or force its sale by January 2025. The president-elect cited concerns over national security and First Amendment rights, proposing more time for his administration to address the issue. This marks a reversal from his 2020 stance supporting TikTok's ban, as the app faces scrutiny from lawmakers and state attorneys general. `ban` `united states` link

US CISA releases best practice guidance for mobile communications
On December 18, the US CISA released Mobile Communications Best Practice Guidance. The guidance was crafted in response to identified cyber espionage activity by China's government-affiliated threat actors targeting commercial telecommunications infrastructure, specifically addressing "highly targeted" individuals who are in senior government or senior political positions and likely to possess information of interest to these threat actors. `guidance` `china` `telecommunications` `united states` link

US sanctions Chinese company involved in compromise of firewall products and attempted ransomware attacks
On December 10, the US Treasury sanctioned Sichuan Silence, a Chinese cybersecurity firm, and employee Guan Tianfeng for exploiting a firewall vulnerability in April 2020, compromising 81.000 devices globally, including critical US infrastructure. The attack aimed to steal data and deploy ransomware. Sanctions block their US-related assets and warn against transactions with them. The DOJ indicted Guan, and a reward was offered for further information. `china` `sanctions` `united states` link

US sanctions entities in Iran and Russia over AI-generated election disinformation
On December 31, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned entities in Iran and Russia for attempting to interfere in the 2024 US election. Designated groups include Iran's Cognitive Design Production Center, linked to the Islamic Revolutionary Guard Corps, and Russia's Center for Geopolitical Expertise, associated with the Main Intelligence Directorate. These actions aim to counter foreign malign influence undermining US democratic processes. `russia` `iran` `united states` `sanctions` `election` link

Fourteen North Korean nationals indicted for multi-year fraudulent IT worker scheme and related extortions
On December 12, a US federal court in St. Louis, Missouri, indicted 14 North Korean nationals for conspiring to violate US sanctions, commit wire fraud, money laundering, and identity theft. Operating through DPRK-controlled companies in China and Russia, they used stolen identities to secure remote IT jobs with US firms, generating at least 88 million US dollars over six years to fund North Korea's weapons programs. `indictment` `north korea` link

Cyberespionage

Moonshine exploit kit and DarkNimbus backdoor enabling Earth Minotaur's multi-platform attacks
On December 5, Trend Micro reported about the China-linked Earth Minotaur threat actor using Moonshine exploit kit in the wild. Moonshine, which has over 55 servers identified as of 2024, has been updated with more exploits and functions compared to its previous version reported in 2019. Moonshine exploit kit targets vulnerabilities in instant messaging apps on Android devices, primarily affecting Tibetan and Uyghur communities and WeChat instant messenger. `china` link

White House links ninth telecom breach to Salt Typhoon
On December 27, White House's deputy national security adviser for cyber and emerging technologies, Anne Neuberger, disclosed that a ninth US telecommunications company was breached by the Chinese-linked cyberespionage group Salt Typhoon. This group has infiltrated telecom networks in dozens of countries, enabling them to geolocate individuals and record phone calls. `china` `telecommunications` `united states` link

Chinese hackers breached US Treasury sanctions office in a supply-chain attack
On December 8, the US Treasury was notified by a third-party software service provider, BeyondTrust, that a threat actor had gained access to a key used by the vendor to secure a cloud-based service used to remotely provide technical support for end users. Hackers compromised the Office of Foreign Assets Control and the Office of Financial Research, that administers economic sanctions. China denies involvement, criticising US accusations. `china` `united states` link

Espionage cluster Paper Werewolf engages in destructive behaviour
On December 26, BI.ZONE, a Russia IT company, reported increased activity from the Paper Werewolf (aka GOFFEE) cyberespionage group, active since 2022, targeting Russian government, energy, financial, and media sectors. They use phishing e-mails with malicious Word macros to deploy PowerShell scripts and custom malware, compromising systems and, in some cases, disrupting operations after achieving espionage objectives. `energy` `finance` `russia` link

Lookout identifies Russian surveillance tools targeting Central Asia
On December 11, Lookout disclosed BoneSpy and PlainGnome, Android surveillance tools tied to Russia-linked threat actor Gamaredon. These tools, targeting Russian speakers in former Soviet states, collect sensitive data via trojanised apps like Telegram. BoneSpy, active since 2021, is rooted in open-source DroidWatcher, while PlainGnome, debuting in 2024, uses a unique code for staged deployments. Both exploit dynamic DNS infrastructure. `mobile phone` `malware` `russia` link

Russia-linked Turla exploits infrastructure of another threat actor, Storm-0156, for cyberespionage
On December 4, Microsoft revealed that Turla, linked to Russia's FSB, has exploited infrastructure from other actors, notably the Pakistani group Storm-0156, for intelligence operations. This includes backdoors like TwoDash and TinyTurla to access sensitive data in Afghanistan and India. Turla's tactics leverage compromised systems and tools for prolonged surveillance, highlighting risks of multi-actor compromises in targeted networks. `russia` link

Citizen Lab uncovers Monokle-type spyware in FSB-compromised device
On December 5, Citizen Lab reported on spyware resembling the Monokle family covertly installed on a Russian programmer's phone after its confiscation by authorities. The spyware allows extensive surveillance, including tracking, call recording, and keylogging. Linked to Russia's FSB, the malware showcases updates or code reuse from earlier Monokle samples. Citizen Lab highlights the risks of device confiscation and urges expert analysis upon return. `russia` link

Cybercrime

North Korean hackers stole 1,3 billion US dollars of crypto in 2024
On December 20, the BBC reported that North Korean hackers have stolen 1,3 billion US dollars in cryptocurrencies this year, accounting for over half of the 2,2 billion US dollars in total digital assets stolen globally. This marks a significant increase from the previous year. The hackers

infiltrated crypto and technology firms, often posing as remote IT workers, to compromise private keys and access user funds. `north korea` link

Cyberhaven employee targeted in Chrome extension compromise
On December 25, an unknown threat actor compromised Cyberhaven's administrative account to distribute a malicious Chrome extension update. Cyberhaven is a data security firm specialising in insider threat prevention and data leak protection for organisations. The update exposed users to data exfiltration risks for 30 hours. Cyberhaven removed the package within an hour and is investigating with Mandiant. Customers were advised to update the extension and review logs. link

Cloudflare's developer domains increasingly abused by threat actors
On December 2, security company Forta reported that Cloudflare's 'pages.dev' and 'workers.dev' domains, used for deploying web pages and facilitating serverless computing, are being increasingly abused by cybercriminals for phishing. The researchers believe the use of these domains is aimed at improving the legitimacy and effectiveness of these malicious campaigns, taking advantage of Cloudflare's trusted branding, service reliability, low usage costs, and reverse proxying options that complicate detection. link

A new phishing-as-a-service 'Rockstar 2FA' facilitating attacks to steal Microsoft 365 credentials.
On December 2, Trustwave highlighted Rockstar 2FA, a phishing-as-a-service platform enabling large-scale adversary-in-the-middle attacks targeting Microsoft 365 accounts. It intercepts login credentials and session cookies, bypassing multifactor authentication. Active since August 2024, the service offers features like randomized source code and Cloudflare Turnstile Captcha to evade detection, making it a growing tool among cybercriminals. link

Bypassing browser isolation through QR Code-based C2 technique
On December 4, Mandiant reported on a novel method for bypassing browser isolation — a security measure separating user activity from local devices. The technique uses QR codes to establish command-and-control (C2) communication, allowing attackers to exploit remote, on-premises, or local isolation setups. While effective, this method highlights browser isolation's vulnerabilities, underscoring the need for layered security strategies like monitoring network anomalies and automation-mode browser use. `techniques` link

Information operations

China is taking a page from Russia's disinformation playbook
On December 25, The Japan Times reported that China is adopting Russian disinformation tactics to promote its global narrative. Both nations utilise troll farms and social media manipulation to sway public opinion. Russia's extensive experience in propaganda has influenced China's strategies, leading to overlapping narratives and coordinated influence operations. This collaboration aims to advance their shared geopolitical interests and challenge Western perspectives. `china` `russia` link

Disruption

Japan Airlines was hit by a cyberattack which caused flights delays during the year-end holidays
On December 26, Japan Airlines (JAL) experienced a cyberattack that disrupted internal and external systems, leading to delays for over 20 domestic flights. The attack began at 7:24 a.m., causing malfunctions and temporarily halting same-day ticket sales. By the evening, systems

were restored, and ticket sales resumed. No customer data was compromised, and there was no damage from computer viruses. `transport` 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	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.
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
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.