Cyber Brief (January 2025)

February 3, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 262 open source reports for this Cyber Brief[1].
- **Policy, cooperation, and law enforcement**. Lithuania inaugurates its Cyber Defence Command, Turkey establishes a new Cybersecurity Directorate, while the US hits back at cyber threats with offensive operations. The EU and US impose sanctions on Russian, Iranian, Chinese, and North Korean entities for cyberattacks, election interference, and espionage, targeting individuals, companies, and state-linked groups. Russia and Iran as well as Japan and Cambodia strengthen cybersecurity cooperation. The UN Security Council discussed commercial spyware threats for the first time.
- **Cyberespionage**. Hackers from China, Iran, and North Korea use AI tools as a research assistant to enhance cyberattacks. Chinese threat actors exploit new zero-days and target US infrastructure & global telecoms in cyber warfare operations. Russian hackers target WhatsApp accounts of high-profile officials while North Korean attempt to infiltrate the technology sector.
- **Cybercrime**. Cybercriminals use AI tool GhostGPT to assist in creating malware, developing exploits, and crafting convincing phishing e-mails. They also develop and share new tools to bypass multi-factor authentication.
- **Information operations**. New pro-Kremlin disinformation campaigns target elections in Croatia, Germany, and Poland, spreading false narratives to sway public opinion. Russian-linked actors used AI-generated fake news to discredit politicians.
- **Data exposure and breaches**. Data breach incidents affect several sectors including transportation (car makers), telecommunications, a government database, and cybersecurity vendors.
- **Disruption & destruction**. Several incidents of various origins (cybercriminal or likely state-sponsored) cause disruptions in the education, financial, and telecommunication sectors.
- **Telecommunications**. Telecom providers remain prime targets for espionage and disruption, with attacks ranging from Chinese state-backed breaches of US and European networks to Ukraine-linked cyberattacks on Russian ISPs and sabotage of undersea cables.

- **Artificial intelligence**. In January, AI-related events focus on security risks and geopolitical tensions, including cybercriminals using AI tools like GhostGPT for phishing and malware, state-backed hackers from China, Iran, and North Korea leveraging AI for cyberattacks, regulatory scrutiny over DeepSeek's data practices, and the US imposing sanctions on AI-driven election interference from Russia and Iran.

Europe

Cyber policy and law enforcement

EU imposes sanctions on Russian individuals for cyberattacks on Estonia
On January 27, the EU sanctioned three Russian individuals linked to GRU Unit 29155 for 2020 cyberattacks on Estonia, targeting ministries and stealing sensitive data. The sanctions include asset freezes and travel bans. This action reflects the EU's commitment to countering cybercrime and promoting cybersecurity, with 17 individuals now under its cyber sanctions regime. Relevant acts are published in the EU's Official Journal. `sanctions` link

Lithuania launches its own cyber defence command
On January 1, Lithuania inaugurated its Cyber Defence Command (LTCYBERCOM), a new unit within the Armed Forces responsible for planning and executing cyber operations, as well as managing strategic and operational communications and information systems. This initiative aims to enhance interoperability with NATO and other institutions, strengthening Lithuania's cyber defence capabilities. `capacity` link

Spain approves cybersecurity law
On January 14, Spain's Council of Ministers approved a draft Law on Coordination and Governance of Cybersecurity to strengthen protection against cyber threats, creating the National Cybersecurity Center and incorporating EU's NIS-2 directive into law, enhancing critical network security. `legislation` link

DeepSeek AI app blocked in Italy and investigated in Ireland
On January 29, DeepSeek's AI Assistant app was removed from Apple and Google stores in Italy due to data privacy concerns. Italy's data protection authority requested more details, while Ireland's Data Protection Commission launched a GDPR investigation. Meanwhile, the US National Security Council announced a national security review of the app, raising further scrutiny over its data collection and privacy practices. `artificial intelligence` `china` `privacy` link

TikTok, AliExpress, SHEIN & Co surrender Europeans' data to authoritarian China
On January 16, the Austrian advocacy group noyb filed GDPR complaints against six Chinese companies—TikTok, AliExpress, SHEIN, Temu, WeChat, and Xiaomi—for unlawfully transferring EU user data to China. These actions violate EU regulations, as China lacks adequate data protection standards. Noyb urges immediate suspension of these data transfers and potential fines up to 4% of global revenue. `china` `privacy` link

Europol dismantles major cybercrime forums
Between January 28 and January 30, a Europol-backed operation led by Germany shut down Cracked and Nulled, the world's largest cybercrime forums, with over 10 million users. Authorities arrested two suspects, seized 17 servers, 50 devices, and 300.000 euros in cash and cryptocurrency. The platforms enabled cybercrime-as-a-service, including stolen data and malware. Europol coordinated cross-border efforts involving eight countries. `takedown` link

Cyberespionage

Cybercrime

Financially motivated threat actor delivering new TorNet backdoor
On January 28, Cisco Talos published a report about a malicious ongoing campaign targeting users in Poland and Germany since at least July 2024, delivering payloads including Agent Tesla and a new backdoor called TorNet. The threat actor is financially motivated and uses techniques such as scheduled tasks and network disconnections to evade detection and maintain persistence on victim machines, also using the TOR network for stealthy communication. `backdoor` link

Ransomware attack on EuroCert compromises personal data
On January 15, EuroCert, a Poland-based provider of qualified electronic signature services, announced that on January 12, 2025, a ransomware attack compromised personal data, including identification details, contact information, PESEL numbers, and ID card numbers of clients, contractors, and employees. The company has notified law enforcement and cybersecurity authorities and is working to restore its IT systems. `ransomware` link

Slovakia's Land Registry hit by major ransomware attack
On January 9, The Slovak Spectator reported that Slovakia's Office of Geodesy, Cartography, and Land Registry (UGKK) suffered a large-scale ransomware attack, rendering its systems and services unavailable. Hackers are reportedly demanding millions of euros for decryption. The UGKK has disconnected from external networks and is working to restore services. The Security Council is scheduled to convene on January 10 to address the incident. `ransomware` link

Disruption

Eindhoven University of Technology suspends classes following cyberattack disruption
On January 12, Eindhoven University of Technology (TU/e) revealed it had identified a cyberattack on January 11, by unknown actors. In response, the university took its network offline, causing class disruptions and exam delays. Although the campus remains open, e-mail and various educational and collaboration systems became unavailable. `education` link

Ukraine’s Intel disrupts Lukoil and sparks payment failures and holiday chaos in Russia
On January 1, Kyiv Post reported that Ukraine's Main Intelligence Directorate (HUR) conducted a cyberattack on Russia's Lukoil, targeting its digital payment systems. The operation disrupted payment platforms, rendering mobile app purchases impossible and causing significant financial losses for Lukoil during the busy holiday period. `energy` `russia` `ukraine` link

Russian ISP confirms Ukrainian hackers "destroyed" its network
On January 8, the Russian internet provider Nodex confirmed its network was "destroyed" following a cyberattack claimed by Ukrainian hackers. The attack disrupted Nodex's services, and the company said it was working to restore systems from backups. The Ukrainian Cyber Alliance group claimed responsibility for the attack, stating they had "completely looted and wiped" Nodex's data. `russia` `telecommunications` link

Sweden opens sabotage probe into Baltic undersea cable damage
On January 26, a vessel was seized on suspicion of damaging an undersea internet cable between Latvia and Sweden. Swedish authorities have initiated a sabotage investigation, with suspicions targeting a vessel. The damaged cable belongs to the Latvian State Radio and Television Centre (LVRTC) and was cut near the Swedish island of Gotland. Latvia has also

started a criminal investigation, attributing the damage to external influences. `telecommunications` link

Information operations

Poland identifies GRU-linked threat group targeting upcoming presidential election in May 2025
On January 10, the Polish government announced the identification of a threat group linked to the Russian military intelligence agency (GRU), which reportedly aims to influence Poland's upcoming presidential elections scheduled for May 18 through disinformation and recruitment campaigns to disrupt political cohesion. In response Poland intends to release a comprehensive election protection plan later in January 2025. `election` `russia` link

Pro-Kremlin disinformation campaign targets Croatian presidential run-off
On January 8, the Centre for Information Resilience (CIR) - an independent organisation dedicated to exposing human rights abuses, countering disinformation - reported that researchers uncovered a pro-Kremlin disinformation campaign ahead of Croatia's presidential run-off. A bot network spread pro-Russian, anti-EU, and anti-NATO narratives, amplifying support for incumbent President Zoran Milanović. The campaign escalated following Milanović's first-round lead and his statements opposing Croatian involvement in the Ukraine conflict. `election` `russia` link

Russian disinformation campaign targeting German election exposed
On January 24, German nonprofit investigative Correctiv exposed a Russian disinformation campaign, attributed to the Russia-linked Storm-1516 threat actor, targeting Germany's February general election. Over 100 fake websites spread AI-generated false claims against politicians, including Green party candidate Robert Habeck and Foreign Minister Annalena Baerbock. `election` `russia` link

Think-tank warns of Russian meddling in German election
On January 20, Reuters reported that the German think-tank CeMAS found that Russia is conducting a disinformation campaign on social media to influence Germany's upcoming election, aiming to boost the far-right Alternative for Germany (AfD) party and undermine mainstream parties. The campaign, which has typical patterns of Russia's Doppelgaenger and has reached over 2.8 million views, spreads false information and has been amplified by fake accounts. `election` `russia` link

Data exposure and leaks

Entire Georgian country population exposed in a massive data leak
On January 27, cybersecurity researcher Bob Dyachenko and the Cybernews team discovered an unprotected Elasticsearch index hosted by a Germany-based cloud service provider, containing nearly five million personal data records of Georgian citizens, including ID numbers, full names, birth dates, genders, and phone numbers. The database was taken offline shortly after the discovery, but the exposure poses significant risks for the affected individuals. link

Spanish Telecommunications company Telefónica confirms ticketing system breach
On January 10, Telefónica, Spain's largest telecom company, confirmed a breach of its internal ticketing system after stolen data appeared on a hacking forum. The company, operating in 12 countries, is investigating the incident and has taken steps to block further unauthorised access. `telecommunications` link

Customer data from 800.000 electric cars and owners exposed online
On December 27, 2024, Der Spiegel reported that Cariad, Volkswagen's software subsidiary,

exposed terabytes of data from around 800.000 electric cars due to IT misconfigurations. The data, linked to drivers and vehicle locations, included Volkswagen, Audi, Seat, and Skoda models. A whistleblower alerted the Chaos Computer Club, which informed Cariad in November. Access was closed on the same day, and Cariad found no evidence of misuse beyond ethical hacking by the CCC. `transport` link

Hacktivism

NoName057(16) claims DDoS attacks against Italy- and Germany-based entities
On January 13, pro-Russia hacktivist group NoName057(16) claimed responsibility for DDoS attacks targeting 14 Italy-based and 4 Germany-based defence, energy, financial, government, technology, and transportation entities. The group cited Ukraine's ongoing military support from Italy and Germany as motivation. Italy's cyber agency is assisting affected entities, with several Italian websites still inaccessible. Germany's recent blocked military aid proposal for Ukraine also featured as a justification for the attacks. link

World

Cyber policy and law enforcement

UN Security Council members meet on spyware for first time
On January 14, the UN Security Council discussed commercial spyware threats for the first time. US Ambassador Dorothy Camille Shea urged stricter export controls and justice for victims. Google's Shane Huntley tracked 40 surveillance vendors, noting misuse by authoritarian regimes. Citizen Lab's John Scott-Railton emphasised Europe's role in spyware abuses. China and Russia opposed the meeting, prioritising other cybersecurity issues. `cooperation` `psoa` link

Japan and Cambodia sign agreement for election equipment and cybersecurity
On January 23, Japan and Cambodia signed an agreement in Phnom Penh for a grant aid project worth 750 million yen. This initiative aims to provide Cambodia with updated election-related equipment, including servers and cybersecurity tools, to enhance fair election processes and strengthen cybersecurity measures. This cooperation aligns with Japan's commitment to developing social infrastructure and supports Cambodia's digital economy and societal advancement. `cooperation` `japan` `election` link

Iran and Russia strengthen cybersecurity cooperation with new agreement
On January 17, Iran and Russia signed an agreement to deepen military, security, and technological ties, with a focus on cybersecurity and internet regulation. The deal formalises existing cooperation between the two countries, including expertise-sharing on national internet control and cybercrime prevention, reflecting their broader efforts to assert greater control over digital spaces. `cooperation` `iran` `russia` link

Leaked documents reveal Microsoft's deepened ties with Israeli military during Gaza war
On January 23, the Guardian revealed that Microsoft expanded its collaboration with Israel's military after October 2023, providing cloud computing, AI tools, and technical support worth at least 10 million US dollars to aid the country's war effort in Gaza. The investigation highlights the increasing reliance of the Israel Defense Forces (IDF) on US tech giants, including Microsoft, Amazon, and Google, for data processing, intelligence analysis, and combat-related digital infrastructure. `cooperation` `defence` `israel` `technology` link

Turkey establishes cybersecurity directorate to boost national defence
On January 8, Turkey established a new Cybersecurity Directorate, which will report directly to President Recep Tayyip Erdoğan and be responsible for protecting the country's IT infrastructure and developing national cybersecurity policies. On January 15, the Turkish Parliament also passed a new cybersecurity bill that outlines the directorate's powers and aims to reduce Turkey's reliance on foreign products and increase its technological sovereignty. `capacities` `turkey` link

US sanctions entities in Iran and Russia over AI-generated election disinformation
On December 31, 2024, 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. `artificial intelligence` `election` `iran` `russia` `sanctions` `united states` link

US sanctions Chinese company aiding Flax Typhoon threat actor
On January 3, the US Department of the Treasury sanctioned Beijing-based Integrity Technology Group, Incorporated (Integrity Tech) for supporting the Chinese state-sponsored cyber group Flax Typhoon. Active since at least 2021, Flax Typhoon has targeted US critical infrastructure sectors. `china` `sanctions` `united states` link

US imposes sanctions on China-based hacker and firm linked to telecom and treasury breaches
On January 17, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Yin Kecheng, a Shanghai-based hacker, and Sichuan Juxinhe Network Technology Co., a Chinese cybersecurity firm, for cyberattacks on the US Treasury and telecom companies. The sanctions block US assets, holding accountable those responsible for breaches attributed to Chinese state-backed hackers, with a 10 million US dollars reward offered for information on similar threats. `sanctions` `china` `telecommunications` `united states` link

US Treasury Department sanctions North Korea for using remote IT workers to fund weapons programs
On January 16, the US Treasury Department imposed sanctions on two individuals and four entities allegedly involved in North Korea's illicit remote IT workforce operations, which funnel money back into the country's weapons programs. The scheme involves sending thousands of skilled IT professionals abroad to secure freelance jobs under false pretences, with the government taking up to 90%. `north korea` `sanctions` `united states` link

Trump repeals Biden's AI safety order, citing innovation concerns
On January 20, US President Donald Trump revoked a 2023 executive order signed by his predecessor Joe Biden, which aimed to reduce the risks associated with artificial intelligence (AI). The revoked order required developers to share safety test results with the government before releasing AI systems, but Trump's administration has argued that such regulations hinder AI innovation and instead supports AI development rooted in free speech and human flourishing. `artificial intelligence` `united states` link

US Justice Department and FBI conduct international operation to delete malware used by China-backed hackers
On January 14, the US Department of Justice and FBI announced the successful removal of PlugX malware from over 4 200 computers worldwide. This malware, allegedly deployed by China-backed hackers Mustang Panda and Twill Typhoon, was used for cyberespionage since at least 2014. The operation involved collaboration with French law enforcement and private cybersecurity firm Sekoia.io. `china` `united states` link

TikTok returned online after Trump vowed to reinstate it
On January 20, TikTok was back online in the US just hours after shutting down, following president-elect Donald Trump's pledge to delay the enforcement of a law banning the app and work on a long-term solution. While this move provided temporary relief, TikTok's long-term future remains uncertain amid legal and political challenges, with potential solutions including a forced sale or legislative reversal. `social media` `united states` link

US hits back at cyber threats with offensive operations
On January 17, Politico reported on statements by Anne Neuberger, a senior Biden administration cyber official, who disclosed that the US had carried out secret offensive cyber operations against foreign adversaries targeting critical infrastructure. These classified measures aim to disrupt malicious networks and strengthen cybersecurity. Neuberger also emphasised the administration's initiatives to address vulnerabilities, including a recent executive order requiring secure software for federal agencies. `united states` link

US FTC sues GoDaddy for years of poor hosting security practices
On January 15, the US Federal Trade Commission sued GoDaddy for years of poor hosting security practices, alleging failure to protect customer data and implement adequate security measures. The lawsuit seeks penalties and requires GoDaddy to improve its cybersecurity protocols to safeguard user information. `prosecution` link

The US launches cybersecurity safety labels for smart devices
On January 7, the US government introduced the US Cyber Trust Mark, a cybersecurity labelling program for smart devices. This voluntary initiative allows manufacturers to display a shield logo on IoT (Internet of Things) devices that meet federal cybersecurity standards. The label includes a QR code providing detailed security information. The program aims to help consumers identify secure internet-connected devices and encourage manufacturers to enhance cybersecurity measures. `united states` link

Cyberespionage

Hackers from China, Iran, and North Korea use AI tools to enhance cyberattacks
On January 29, The Wall Street Journal reported that hackers from China, Iran, and North Korea are using US AI products, including Google's Gemini, to enhance their cyberattacks. They appear to treat the platform more as a research assistant than a strategic asset, relying on it for tasks that boost productivity rather than developing new, advanced hacking techniques. These tools assist in tasks like reconnaissance and anomaly detection evasion. `artificial intelligence` `china` `iran` `north korea` link

Ivanti Connect Secure VPN targeted in new zero-day exploitation
On January 8, Google detailed active exploitation of CVE-2025-0282, a zero-day in Ivanti Connect Secure VPNs. Attackers used reconnaissance, buffer overflow exploitation, and malware like PHASEJAM for persistence and remote access. Post-exploitation, they modified logs and disabled defences to maintain control. Linked to UNC5337, part of suspected China-nexus UNC5221, the attackers demonstrated advanced tactics, targeting ICS appliances with customised malware for espionage and prolonged network compromise. `china` link

China targets US infrastructure and telecoms in cyber warfare operations
On January 4, The Wall Street Journal reported on China's advanced cyberattacks on US infrastructure and telecom networks, signalling a shift from corporate espionage to military strategy. Hackers infiltrated ports, utilities, and telecom systems, collecting intelligence and preparing to disrupt operations during potential conflicts, such as over Taiwan. The attacks highlighted vulnerabilities in US cybersecurity and raised concerns about China's growing cyber capabilities. `china` `critical infrastructure` `telecommunications` `united states` link

China-linked MirrorFace threat actor target Japanese government and politicians since 2019
On January 9, the Japanese National Police Agency (NPA) reported that the Chinese state-backed hacking group MirrorFace has been conducting cyberespionage campaigns against the Japanese government and politicians since 2019. The group employs spearphishing e-mails to deploy malware such MirrorStealer, aiming to steal sensitive information related to national security and advanced technology. `china` `japan` link

APT32 poisoning GitHub, targeting Chinese cybersecurity professionals and specific large enterprises
On January 9, ThreatBook CTI reported that the Vietnam-linked APT group OceanLotus (APT32) had targeted Chinese cybersecurity professionals and specific large enterprises by poisoning a GitHub repository with a Cobalt Strike exploit plugin containing a trojan. The attack used a novel method of embedding malicious code in a Visual Studio .suo file. `china` `technology` link

New backdoor targets governments and ISPs in the Middle East
On January 6, Kaspersky reported on updated backdoor dubbed EAGERBEE, which was deployed at ISPs and government entities in the Middle East. The researchers link with a moderate confidence to the Chinese threat actor they call CaughingDown, based on code similarities and IP address overlaps. This news highlights the global reach of Chinese operations in the telecommunications sector. `china` `telecommunications` link

Salt Typhoon also breached 3 more telecommunications provider networks in recent wave of attacks
On January 6, the Wall Street Journal revealed new victims of the Chinese state-backed Salt Typhoon telecom hacks: Charter Communications, Consolidated Communications, and Windstream, The hackers gained access to sensitive customer data and communications. In response, the US government is considering banning China Telecom's operations and TP-Link routers. `china` `telecommunications` `united states` link

US Treasury breach attributed to China-aligned Silk Typhoon
According to a report by Bloomberg from January 8, the US Treasury breach disclosed in December has been linked to the Chinese state-backed group Silk Typhoon (aka Hafnium). The group exploited a compromised BeyondTrust API key to access the network, focusing on the Office of Foreign Assets Control. Investigations suggest the breach aimed to gather intelligence on potential US sanctions. Treasury officials, CISA, and the FBI continue their inquiry, with BeyondTrust supporting mitigation efforts. `china` `united states` link

US CISA warns of backdoor in Contec patient monitors sending data to China
On January 30, the US Cybersecurity and Infrastructure Security Agency (CISA) warned that the Contec CMS8000, a multi-parameter patient monitor used in healthcare, contains a backdoor transmitting patient data to a hard-coded IP address linked to a Chinese university. This backdoor enables remote code execution, allowing full device takeover. The activity is unlogged, leaving administrators unaware. Contec has not responded to CISA's requests to address these vulnerabilities. `china` `health` link

Russia-nexus APT possibly related to APT28 conducts cyberespionage on Central Asia and Kazakhstan diplomatic relations
On January 13, Sekoia reported that a Russia-linked group, UAC-0063, possibly associated with APT28, conducted cyberespionage against Central Asian diplomatic entities, notably in Kazakhstan. The attackers used legitimate documents from Kazakhstan's Ministry of Foreign Affairs, embedding malware like HATVIBE and CHERRYSPY to gather intelligence on Kazakhstan's diplomatic and economic relations. `diplomacy` `russia` link

New Star Blizzard spearphishing campaign targets WhatsApp accounts
On January 16, Microsoft reported that the Russian-linked hacking group Star Blizzard launched a spearphishing campaign targeting WhatsApp accounts of government officials, diplomats, defence policy experts, and individuals assisting Ukraine. The attackers sent e-mails impersonating US government officials, containing QR codes that, when scanned, granted unauthorised access to victims' WhatsApp messages. `russia` link

FBI warns of North Korean IT workers stealing source code for extortion
On January 23, the FBI warned that North Korean IT workers are infiltrating US companies, stealing source code, and extorting employers by threatening to leak sensitive data. To mitigate these threats, organisations are urged to enforce strict access controls, monitor remote connections for suspicious activity, and strengthen hiring practices to detect fraudulent applicants using AI and identity-masking techniques. `north korea` `united states` link

Cybercrime

Sneaky 2FA: exposing a new AiTM Phishing-as-a-Service
On January 16, cybersecurity company Sekoia exposed "Sneaky 2FA," an Adversary-in-the-Middle phishing kit sold as Phishing-as-a-Service via a Telegram bot. Active since at least October 2024, it bypasses multi-factor authentication to compromise Microsoft 365 accounts. The kit employs obfuscated code, anti-analysis techniques, and pre-fills phishing pages with victims' e-mail addresses to enhance credibility. link

Ransomware groups employ e-mail bombing and Teams vishing in attacks
On January 21, Sophos reported that they responded to two ransomware campaigns utilising "e-mail bombing" and Microsoft Teams "vishing" tactics. The threat clusters, identified as STAC5143 and STAC5777, exploit Office 365 functionalities to overwhelm targets with spam and impersonate tech support via Teams. These methods aim to deploy malware and facilitate data theft. link

Unknown threat actor attempts to brute force Microsoft 365 accounts globally using FastHTTP
On January 13, US-based cybersecurity company SpearTip revealed a global campaign using the fasthttp Go library to launch high-speed brute-force attacks on Azure Active Directory via the Graph API. Adversaries targeted Microsoft 365 accounts, with 9.7% of attempts achieving unauthorised access. Most traffic originated from Brazil. Attacks included MFA spamming to exploit MFA fatigue. link

Malicious VS Code extension impersonates Zoom to target Chrome cookies
On January 21, researchers at Hunt.io identified a malicious Visual Studio Code extension impersonating Zoom to steal Google Chrome cookies. Active since November 30, 2024, it exploited the VS Code Marketplace and used obfuscated JavaScript to access cookie data via SQLite queries. The extension linked to legitimate repositories to build trust, exposing critical security risks in development environments. link

Threat actors exploit .gov domains for phishing campaigns
On January 29, Cofense reported that threat actors have exploited vulnerabilities in government (.gov) domains for phishing campaigns from November 2022 to November 2024. They mainly used open redirects to bypass secure e-mail gateways (SEGs), often leveraging CVE-2024-25608. US government domains ranked third in abuse, mostly redirecting victims to credential phishing pages disguised as Microsoft login portals. link

Over 4000 backdoors hijacked by registering expired domains
On January 8, WatchTowr reported that over 4000 abandoned but active web backdoors were hijacked by registering expired domains used for commanding them. The researchers found

backdoors on government and university systems, and sinkholed the traffic to prevent malicious actors from taking control. link

Cyberattackers use GhostGPT to write malicious code
On January 27, reports highlighted the emergence of GhostGPT, an uncensored AI chatbot marketed to cybercriminals for 50 US dollars per week. Unlike mainstream AI models with ethical safeguards, GhostGPT assists in creating malware, developing exploits, and crafting convincing phishing e-mails, thereby lowering the barrier for malicious activities. Its availability via Telegram and absence of user activity logs make it particularly appealing to attackers. `artificial intelligence` link

Operation 99: Lazarus group's targeting of Web3 and cryptocurrency developers
On January 9, SecurityScorecard revealed Operation 99, a Lazarus Group campaign exploiting Web3 and cryptocurrency developers through fake recruiters. Malicious GitLab repositories inject modular malware, like Main99 and MCLIP, to steal credentials, cryptocurrency, and intellectual property. Enhanced obfuscation and persistence highlight North Korea's financial motives. Developers must verify recruiters, scrutinise repositories, and adopt robust endpoint security to mitigate such advanced threats. `north korea` link

Malicious Chrome extensions: a new supply chain attack uncovered
On January 22, Sekoia reported about a targeted supply chain attack on Chrome browser extensions, where attackers used phishing e-mails to compromise developers and upload malicious versions of their extensions. The attack, which began in December 2024, affected dozens of extensions and potentially hundreds of thousands of users, enabling the theft of sensitive data such as API keys and authentication tokens from platforms like ChatGPT and Facebook for Business. `technology` link

Data exposure and leaks

Threat actor leaks sensitive data of 15.000 FortiGate devices worldwide on BreachForum
On January 14, a threat actor called Belsen Groups leaked sensitive data of approximately 15.000 FortiGate devices worldwide on BreachForum underground forum. The leaked data, which includes IP addresses, passwords, and configurations, has been released for free on the underground forum as a way to enhance their reputation during their first official operation. link

Exposed DeepSeek database leaking sensitive information, including chat history
On January 29, Wiz Research uncovered a publicly accessible ClickHouse database linked to DeepSeek, exposing over a million log entries containing sensitive data like chat history, API keys, and backend details. This unsecured database allowed full control over operations and posed significant security risks. Wiz promptly notified DeepSeek, who secured the exposure. The incident highlights the critical need for robust security in rapidly adopted AI services. `artificial intelligence` link

Thousands of security vendor credentials found on Dark Web
On January 22, Cyble reported that credentials from major cybersecurity vendors, including internal and customer accounts, were found on the dark web. These credentials, likely extracted by infostealer malware, were available for as little as 10 US dollars and encompassed access to platforms like Okta, Jira, GitHub, AWS, and Microsoft Online. The affected vendors include CrowdStrike, Palo Alto Networks, Fortinet, and others. `technology` link

HPE investigates potential security breach following source code theft claim
On January 16, Hewlett Packard Enterprise (HPE) became aware of claims being made by a group called IntelBroker, saying that they had stolen documents from the company's developer

environments. HPE is investigating these breach claims, which include accessing API, GitHub, and source code, but has found no evidence of a breach so far. `technology` link

Subaru STARLINK flaw exposed vehicles to remote control and data access
On November 20, 2024, researchers Sam Curry and Shubham Shah found a flaw in Subaru's STARLINK admin panel allowing unauthorised access to vehicles and customer data across the US, Canada, and Japan. Exploitation required minimal details and enabled remote control, PII access, and location tracking. Subaru patched the issue within 24 hours following the disclosure. The detailed report was published on January 23, 2025, highlighting systemic challenges in connected vehicle platforms. `transport` link

UN ICAO investigates potential recruitment data breach
On January 7, the International Civil Aviation Organization (ICAO) reported a potential breach of 42.000 recruitment records from 2016–2024, claimed by threat actor Natohub. Exposed data includes names, e-mail addresses, dates of birth, and employment histories. ICAO stated no financial, passwords, or aviation systems were impacted. The organisation is investigating, enhancing security measures, and notifying affected individuals. `transport` link

Disruption

DeepSeek reports cyberattack amid surge in AI model demand
On January 27, Chinese AI startup DeepSeek reported large-scale malicious attacks on its servers, disrupting new registrations and website access amid high demand for its DeepSeek-R1 model. Media speculated a DDoS attack on its API and web-chat platform. On January 28, China Central Television (CCTV) cited Qi An Xin researchers, who claimed the attacks originated solely from US IP addresses. `artificial intelligence` `china` `united states` link

Taiwan-Matsu undersea cables cut, suspected Chinese involvement raises concerns
On January 22, two undersea cables connecting Taiwan and the Matsu Islands were reported broken, with initial faults occurring on January 15. Chunghwa Telecom, Taiwan's largest integrated telecommunications operator, announced that communication between Taiwan and the Matsu Islands was restored on January 24. Authorities suspect that Chinese vessels may have been involved in damaging these cables, raising concerns about potential "gray zone operations" by China to disrupt Taiwan's communications. `china` `telecommunications` link

Conduent confirms cybersecurity incident behind widespread service outage
On January 22, Conduent, a major American business services provider and government contractor, confirmed that a recent outage affecting multiple US agencies was caused by a cybersecurity incident. While the company stated that the issue was contained and systems were restored, it has not disclosed details on the scope of the attack, potential data theft, or whether a ransom demand was made. `united states` 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.