Cyber Brief (November 2024)

December 3, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 232 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, Germany announced plans to legislate responsible vulnerability disclosure, while global operations dismantled cybercriminal infrastructures. Interpol's Serengeti operation led to 1.006 arrests in Africa, and China took measures to expand data oversight.
- On the **cyberespionage** front, in Europe, the Russia-linked threat actor APT28 compromised Ukrainian Wi-Fi networks near their targets for covert access. China-linked threat actors leveraged exploits and targeted telecommunications globally.
- Relating to **cybercrime**, in Europe, the most active ransomware operations were Ransomhub, KillSecurity, and Play while the most targeted sectors were technology, manufacturing, and healthcare.
- Relating to **disruption**, DDoS attacks spurred financial institutions to issue preparedness advisories. These incidents underscore heightened security risks amid geopolitical tensions.
- As regards **data exposure and leaks** incidents, several significant breaches exposed sensitive data, with pro-Russia actors targeting German institutions and healthcare sectors. Financial and telecom firms like Finastra also reported significant incidents.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in November 2024.

Europe

Cyber policy and law enforcement

Germany to legislate responsible disclosure of vulnerabilities

On November 4, the German Ministry of Justice declared that they are drafting a legal

framework for responsible disclosure of vulnerabilities. The idea is that those who report IT security flaws should get recognition rather than a sanction.

Cyberespionage

APT28 exploited Ukrainian Wi-Fi networks near their targets
On November 22, Volexity revealed that Russia-linked threat actor APT28 used a novel "Nearest Neighbour Attack" against Ukraine in February 2022 to exploit nearby Wi-Fi networks for covert access. By targeting dual-homed systems and leveraging compromised credentials, they bypassed MFA-secured systems to infiltrate Ukraine-related projects, demonstrating the unprecedented risks posed by proximity-based Wi-Fi exploitation. `russia`

New Windows zero-day vulnerability exploited in attacks against Ukrainian entities
On November 13, ClearSky Cyber Security uncovered CVE-2024-43451, a zero-day vulnerability affecting Windows systems, actively exploited against Ukrainian entities via phishing e-mails containing malicious URL files disguised as academic certificates. The flaw, triggered through actions like right-clicking or moving the file, allows attackers to deploy SparkRAT malware for remote access, with CERT-UA attributing the campaign to suspected Russian threat actor UAC-0194. Microsoft has issued a patch to address the issue. `russia`

Information stealers malware campaign targets Swiss civilians via fake MeteoSwiss letters
On November 14, the Switzerland's NCSC reported on fraudulent letters claiming to be from MeteoSwiss and urging recipients to download a fake severe weather app via a QR code, installing the Android malware "Coper." The fake app mimics the Alertswiss app to steal sensitive data from over 383 apps, including e-banking. The real Alertswiss app, used for official alerts, has a distinct round logo. Only Android devices are affected. `android malware`

Cybercrime

Hungary confirms cyberattack on Defence Procurement Agency
On November 14, Hungary's government confirmed that the Defence Procurement Agency's IT systems were breached by a foreign threat actor, though no sensitive military structure data was compromised. While an investigation is ongoing, reports suggest the INC Ransomware group may have been involved, accessing procurement plans and encrypting files, but officials stated national security remains unaffected. `defence`

PXA stealer targets sensitive data in government and education sectors
On November 14, Cisco researchers uncovered PXA Stealer, a python-based malware targeting sensitive information in education sector in India and government organisations in European countries, including Sweden and Denmark. Operated by a Vietnamese-speaking threat actor, the malware extracts credentials, browser data, financial information, and gaming accounts, employing obfuscated scripts and Telegram bots for data exfiltration, highlighting sophisticated cybercriminal tactics. `education` `public administration`

Likely financially motivated cyberecurity incident disrupts UK hospital
On November 25, Wirral University Teaching Hospital (WUTH) in the UK disclosed a cybersecurity incident causing operational disruptions, including the cancellation of outpatient appointments and restricted access to test results and medical records at Arrowe Park Hospital. No threat actor has claimed responsibility. Similar incidents have targeted UK healthcare providers in 2024, with ransomware intrusions being the primary cause of disruptions. `health`

Nokia investigates potential source code leak through third party provider

On November 4, Nokia confirmed to Bleeping Computer that they opened an investigation into a potential compromise of a third party provider because a cybercrime actor Grep publicly claimed to have exfiltrated Nokia source code.

Disruption

Bank of Finland advises preparedness for cyberattacks on financial institutions

On November 13, the Bank of Finland advised households to keep enough cash on hand to cover three days of expenses in case of banking disruptions caused by cyberattacks, such as recent DDoS attacks that have impacted Finnish financial institutions. It also recommended maintaining accounts with multiple banks, using alternative online payment platforms, and having a backup electronic ID verification system to prepare for potential service outages. `finance`

Data exposure and leaks

Pro-Russia threat actor breaches German Federal Statistical Office and sells company data on darknet

On November 14, NZZ newspaper reported that pro-Russia threat actor Indohaxsec breached Germany's Federal Statistical Office (Destatis), stealing and listing for sale 3.8 GB of company data, including sensitive contact and login details, on the darknet. Although Destatis recently updated its Idev reporting system in August 2024, it remains unclear how the hackers accessed the system to acquire data on German firms. `public administration`

French hospital suffered a data breach exposing 750.000 records

On November 19, a French hospital suffered a data breach, exposing 750.000 patient records through stolen credentials used to access MediBoard, an EPR system by Softway Medical Group. The company stated that the data was hosted by the hospital. The hacker, using the nickname "nears," claims to have breached multiple facilities, affecting over 1,5 million patients. `health`

Financial software company Finastra suffered a data breach

On November 19, Finastra, a London-based global financial software firm, reported a cybersecurity incident that occurred on November 7. An attacker accessed its Secure File Transfer Platform (SFTP) using compromised credentials. No evidence suggests the breach spread beyond SFTP. Finastra's services include lending, payments, cloud banking, and trading risk management. `finance`

World

Cyber policy and law enforcement

China expands data security oversight with new regulations impacting foreign businesses

On September 30, China’s State Council released the Network Data Security Management Regulations, expanding national security oversight over foreign and domestic entities handling data related to Chinese individuals or organisations, effective January 1, 2025. These regulations, which require compliance with strict data localisation and transfer controls, are expected to pose operational challenges for multinational companies by necessitating dual compliance with China’s data security standards and other global frameworks like the EU-GDPR. `china`

Chinese national indicted for trade secret theft

On October 31, the US government released an indictment of a Chinese national accused of trade secret theft. The individual reportedly used a VPN to access a US-based investment management firm's network from China after which the then-employee copied sensitive information. The individual reportedly had the intention to start his own China-based investment firm. `china` `united states`

Israeli Committee advances controversial bill on digital surveillance for serious crimes

On November 10, Israel's Ministerial Committee for Legislation advanced a bill allowing police to digitally surveil suspects' devices, including with spyware, in serious crime cases, pending a sealed warrant. The bill, which excludes public corruption cases, has sparked debate over privacy, with opposition from the Attorney General and Justice Ministry officials. `israel`

Canada orders TikTok shutdown over national risk concerns

On November 6, Canada ordered TikTok to cease operations within its borders due to national security concerns over potential data risks associated with ByteDance's Canadian subsidiary. While TikTok remains accessible to Canadian users, the government cited security reviews and intelligence advice to justify the shutdown. TikTok expressed disappointment, planning to challenge the decision legally, emphasizing job losses and continued platform availability for Canadian content creators. `shutdown`

US releases AI safety framework for critical infrastructure

On November 14, the US Department of Homeland Security (DHS) introduced the “Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure,” providing guidance for secure AI deployment across the supply chain. Developed by the AI Safety and Security Board, it targets cloud providers, AI developers, critical infrastructure operators, and civil society groups, aiming to ensure safe AI integration in U.S. critical infrastructure systems. `artificial intelligence`

Interpol announces international law enforcement operation which took down 22.000 IPs

On November 5, Interpol announced an international law enforcement operation which took down 22.000 malicious IP addresses. The action was part of Operation Synergia II and specifically targeted phishing, ransomware and information stealers. The international operation was a joint effort from Interpol, private sector partners and law enforcement agencies from 95 member countries. `take down`

Over 1.000 arrests in large scale anti-cybercrime operation Serengeti

On November 26, Interpol reported that Operation Serengeti, coordinated by them and Afripol with support from the EU, resulted in 1.006 arrests across 19 African countries in September and October. The operation targeted ransomware, BEC, and online scams, dismantling 134.089 infrastructures and recovering 44 million of the 193 million US dollars stolen. Highlights include credit card fraud in Kenya, Ponzi schemes in Senegal, and forced recruitment scams in Cameroon. `arrest` `africa`

Cyberespionage

Canada reports that Chinese actors conducted reconnaissance towards Indian governmental organisations throughout 2024

On October 30, the Canadian Centre for Cyber Security (CCCS) issued its National Cyber Threat Assessment 2025-2026 in which they reported that Chinese actors conducted network-reconnaissance scanning against multiple Canadian governmental organisation throughout 2024. The report detailed cyber threats associated with state adversaries China, Russia, Iran, North Korea and India. `china`

Chinese threat actors expand Linux focus with new WolfsBane and FireWood malware

On November 21, ESET researchers revealed two Linux backdoors, WolfsBane and FireWood, linked to Chinese threat actors, including the Gelsemium group. WolfsBane, a port of Windows malware, combines stealth via rootkits with full system control capabilities, while FireWood, a broader APT tool, supports file operations, command execution, and data exfiltration, reflecting a rising trend of targeting Linux due to strengthened Windows defenses. `china`

Kaspersky uncovers QSC framework usage by BackdoorDiplomacy threat actor in targeted cyberespionage campaigns

On November 8, Kaspersky reported that the BackdoorDiplomacy group is using the QSC framework, a modular and multi-plugin malware tool, for cyberespionage in targeted campaigns, primarily within the telecommunications sector in Asia. The QSC framework, combined with the Quarian backdoor, allows in-memory loading and execution of modules such as command shells and file managers, highlighting an evolution in the group's tactics and emphasising the importance of ongoing monitoring. `china`

China-based threat actors used operational relay boxes (ORBs) to attack onward targets and obfuscate

On October 31, Sophos, a cybersecurity company, unveiled a five-year investigation tracking China-based groups targeting perimeter devices. Sophos associates the observed activity to Volt Typhoon, APT31 and APT41 and identified, with high confidence, exploit research and development activity being conducted in the Sichuan region. The threat actors used edge devices as operational relay boxes (ORBs) to attack onward targets and obfuscate the true origin of attacks. `china`

BrazenBamboo weaponizes FortiClient vulnerability to steal VPN credentials

On November 15, Volexity reported that the Chinese state-affiliated threat actor BrazenBamboo exploited a zero-day vulnerability in Fortinet"s Windows VPN client, FortiClient, to steal VPN credentials via their DEEPDATA malware. This vulnerability allowed credentials to be extracted from the client's process memory. Volexity notified Fortinet of this issue on July 18, 2024. `china`

Volt Typhoon's KV-Botnet targeting outdated routers after prior disruption

On November 12, SecurityScorecard, a US-based cybersecurity company, reported that the Chinese state-sponsored group Volt Typhoon has resumed its KV-Botnet operations, compromising outdated Cisco and Netgear routers with MIPS-based malware and webshells to establish covert communication channels after a prior disruption by US authorities in January. `china`

Singtel discloses June 2024 breach linked to China-linked Volt Typhoon threat actor

On November 5, Singtel, Singapore's largest mobile carrier, disclosed a June 2024 breach potentially tied to China-linked actor Volt Typhoon, stating no data loss or service impact occurred. The breach is suspected to have served as a trial for further targeting of U.S. telecoms, with attackers reportedly using a webshell to intercept credentials and establish persistent access. `china`

China-linked threat actor Liminal Panda targets telecom networks with SIGTRAN and GSM exploits

On November 19, CrowdStrike reported about a China-linked cyber espionage group, Liminal Panda, targeting telecommunications networks in South Asia and Africa since 2020. Leveraging custom tools like SIGTRANslator, PingPong and CordScan, the group exploits telecommunication protocols to access subscriber data, call metadata, and SMS, while also infiltrating core infrastructure through weak passwords and the interconnected nature of telecom providers' systems. `china` `telecommunications`

China-linked threat actor Salt Typhoon cyberespionage campaign targets telecommunications sector
On November 15, The Wall Street Journal reported that T-Mobile confirmed having been targeted within an ongoing industry-wide cyberespionage campaign against the telecommunications sector. While T-Mobile claims no evidence of customer data compromise, other companies, including AT&T and Verizon, reported data exfiltration by Salt Typhoon, including call logs and messages. Reports confirm Salt Typhoon also accessed US law enforcement wiretap systems for months, with the campaign first reported in September. `china` `telecommunications`

NSO Group exploits WhatsApp zero day to deploy Pegasus spyware despite lawsuits
According to court documents filed on November 7, Israeli firm NSO Group exploited multiple zero-day exploits, including "Erised," an unknown one affecting WhatsApp to deploy Pegasus spyware in zero-click attacks, despite lawsuits. NSO developed custom clients to bypass WhatsApp protections and targeted thousands of devices globally. Pegasus enabled clients to surveil targets with minimal input. WhatsApp and Apple sued NSO, and the US sanctioned the group in 2021. `psoa`

Cybercrime

Fake AI tools spread malware to steal credentials and cryptocurrency
On November 15, researchers reported about cybercriminals distributing fake AI image and video tools to infect Windows with Lumma Stealer and macOS with AMOS malware. Both steal cryptocurrency wallets, credentials, cookies, passwords, and browsing data from major browsers like Chrome and Edge. Collected data is archived and sent to attackers for use in future exploits or sale on cybercrime markets. `artificial intelligence`

New Ymir ransomware partners with RustyStealer in sophisticated cyber attacks
On November 11, Kaspersky revealed the emergence of Ymir, a new ransomware targeting systems previously compromised by RustyStealer, a credential-harvesting malware, marking a partnership in cybercrime for lateral movement and network infiltration. Ymir operates in-memory and uses the ChaCha20 cipher for file encryption, with Kaspersky warning that its use of information stealers could quickly make this new ransomware family a widespread threat.

BianLian ransomware shifts to exclusive data theft extortion
On November 21, CISA, the FBI, and the Australian Cyber Security Centre reported that the BianLian ransomware group has transitioned fully to data theft extortion, abandoning file encryption tactics since January 2024. Operating primarily from Russia, the group employs advanced techniques like privilege escalation, SOCKS5 tunneling, and PowerShell scripting, targeting Windows and ESXi systems, and pressuring victims through ransom notes, direct calls, and dark web extortion.

Critical Veeam Backup vulnerability exploited in the wild by Frag ransomware
On November 8, Sophos reported that a critical Veeam Backup & Replication (VBR) vulnerability, CVE-2024-40711, is being exploited by Frag ransomware, following its previous use in Akira and Fog ransomware attacks. Threat actors exploited the flaw to gain remote code execution on unpatched VBR servers, using stolen VPN credentials to establish accounts for lateral movement. Agger Labs noted that Frag operators heavily leverage Living Off The Land binaries, complicating detection efforts.

Firefox and Windows zero-days exploited by RomCom hackers
On November 26, BleepingComputer reported that the Russian-based RomCom cybercrime group exploited two zero-day vulnerabilities, CVE-2024-9680 in Firefox and CVE-2024-49039 in Windows Task Scheduler, to target users across Europe and North America. The attacks

leveraged a zero-day chain exploit to deliver the RomCom backdoor via malicious websites. This widespread campaign impacted multiple industries, including government, defense, and energy, and highlights RomCom's advanced capabilities and espionage focus.

Significant vulnerabilities

Critical Vulnerability in 7-Zip. A severe security flaw in the 7-Zip file compression utility allows remote attackers to execute malicious code through specially crafted archives. This vulnerability, tracked as CVE-2024-11477, has a CVSS score of 7,8. See CERT-EU's SA 2024-118.

Zero-Day Vulnerabilities in Palo Alto Networks PAN-OS. Palo Alto Networks released updates for two actively exploited zero-day vulnerabilities in PAN-OS. Exploitation could permit a remote unauthenticated attacker to gain administrator privileges or enable a PAN-OS administrator to perform actions on the firewall with root privileges. Users are advised to apply updates and restrict management web interface access to trusted internal IP addresses. See CERT-EU's SA 2024-117.

Microsoft November 2024 Patch Tuesday. Microsoft's November 2024 Patch Tuesday addressed 91 vulnerabilities, including four zero-day vulnerabilities. Notably, CVE-2024-43451 (NTLM Hash Disclosure Spoofing) and CVE-2024-49039 (Windows Task Scheduler Elevation of Privilege) have been actively exploited, potentially allowing attackers to gain unauthorized access or escalate privileges with minimal user interaction or crafted applications. See CERT-EU's SA 2024-116.

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	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.