Cyberattack Case Study

CIS3360 - Security in Computing

Spring 2025
Michael McAlpin

Allan Aquino Vieira
al255459

The increasingly sophisticated nature of cyber threats highlights the critical importance of robust cybersecurity measures, particularly for critical infrastructure sectors like telecommunications. Recent high-profile attacks have demonstrated the devastating impact of advanced persistent threats (APTs) on both public and private sectors. Among these, the Salt Typhoon campaign, attributed to state-sponsored actors affiliated with the People's Republic of China (PRC), exemplifies the complex and ever evolving threat landscape. This campaign went unnoticed for years, and targeted telecommunications infrastructure across multiple countries, leveraging zero-day vulnerabilities, advanced backdoors, and tailored malware frameworks to exfiltrate sensitive data and undermine national security.

The cyber espionage campaign led by Salt Typhoon has drawn global attention due to its extensive reach, affecting major telecommunications companies and government entities in countries like the United States, Malaysia, and Taiwan. The attackers exploited critical vulnerabilities such as ProxyLogon and Ivanti Connect Secure, deploying highly modular tools like DEMODEX and GHOSTSPIDER to maintain persistence and evade detection. As a result, the campaign exposed significant gaps in the security of modern telecommunications networks and underscored the pressing need for enhanced visibility, proactive hardening measures, and international collaboration to counter such threats.

This paper examines the Salt Typhoon campaign, analyzing its methods, impact, and the defensive actions taken to prevent future incidents. By delving into the technical intricacies of the attack, this case study highlights the broader implications of state-sponsored cyber espionage on global security.

On November 13, 2024, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint statement addressing a series of cyberattacks targeting multiple U.S. telecommunications companies (Cybersecurity and Infrastructure Security Agency, November 13, 2024). These breaches involved the unauthorized access and exfiltration of sensitive data, including customer mobile phone metadata, private communications of individuals involved in government or political activities, and court-approved wiretap information (Cybersecurity and Infrastructure

Security Agency, November 13, 2024). As reported by *The Wall Street Journal* on August 27, the attacks were classified as part of an expansive cyber espionage campaign. The perpetrators were identified as foreign actors affiliated with the People's Republic of China (PRC), specifically the Advanced Persistent Threat (APT) group known as Salt Typhoon, a designation recognized by Microsoft (Microsoft, n.d.).

This disclosure marked a critical turning point, shedding light on a sophisticated and long-running operation that had not only targeted the U.S. telecommunications sector but also extended its reach to other industries and nations. Understanding the history and evolution of Salt Typhoon's tactics offers valuable insight into their operational strategy and the broader implications of their activities.

History of Salt Typhoon and its complex attacks

While the 2024 telecommunications attacks thrust Salt Typhoon into the international spotlight, the group's activities have a much deeper history, spanning several years and multiple aliases. Their activities first drew the attention of security researchers shortly after the disclosure of ProxyLogon vulnerability, January of 2021. This set of chained vulnerabilities allowing remote code execution (RCE) in Microsoft Exchange servers (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065), quickly weaponized by many APTs.

Exploiting ProxyLogon, two days after its patch release, March 2nd 2021, and a novel Windows kernel rootkit, dubbed Demodex, that hid malware traces from security analysis, a sophisticated multi-stage malware framework granting remote control over the infected servers, and Cheat Engine ,an open-source project that bypasses Windows Driver Signature Enforcement, GhostEmperor, as tracked by Kaspersky, has been associated with numerous Southeast Asian high-profile organizations, as well as governmental entities and telecommunication companies in Egypt, Afghanistan and Ethiopia (Lechtik, et al, 2021).

Concurrently Matthieu Faou and Tahseen Bin Taj, ESET researchers, discovered FamousSparrow, a new cyberespionage group leveraging ProxyLogon, the day after the patch release. This group also employed a never-before-seen custom backdoor, named

SparrowDoor, and two custom versions of Mimikatz, a powerful credential extraction and privilege escalation utility. These unique set of tools became the defining fingerprint linking FamousSparrow to attacks on hotels, governments, international organizations, engineering companies and law firms in France, Lithuania, the UK, Israel, Saudi Arabia, Brazil, Canada, Guatemala, Taiwan, and Burkina Faso (ESET Research, 2021).

By 2023, researchers at Trend Micro uncovered a new cyberespionage APT group, Earth Estries, targeting government and technology organization in regions such as the Philippines, Taiwan, Malaysia, South Africa, Germany, and the US. Targeting public-facing services, Using DLL Sideloading, and Cobalt Strike, PlugX, or Meterpreter, hosted by VPS services in 5 continents (North America, Europe, Africa, Asia, and Oceania), providing remote control, to avoid detection they employ PowerShell downgrade attacks, and obfuscate IP address through Fastly CDN (also used by other APT41-groups) and numerous domains, using public services such as Github, Gmail, AnonFiles, and File.io to transfer commands. Trend Micro analysts also uncovered the use of new malware like: Zingdoor, a cross-platform, anti-analysis techniques, HTTP backdoor that registers as a Windows service, capable of gathering system information, managing files, and executing arbitrary commands, developed in Go and heavily obfuscated by a custom obfuscator engine. TrillClient is an information stealer designed to register as a Windows service "Net Connection", and extract browser data. It reaches out to a GitHub repository to retrieve commands and supports updating its version, command execution, and uploading stolen data to the attacker's email account. HemiGate another backdoor that uses DLL sideloading for execution, it communicates with its command-and-control server over port 443 and can operate through proxies. It retrieves its configuration from an encrypted file and supports functionalities like file management and command execution. Also employing Server Message Block (SMB) and WMI command line (WMIC), allowed propagation throughout the network. Archiving and uploading the collected data to online repositories, cleaning the existing backdoors at the end of each round of operation, and redeploying the malware at the start of every new round (Lee, T, et al, 2023).

AhnLab’s ‘Threat Trend Report on APT Groups: October 2023 “Major Issues on APT Groups,” connected the Tropic Trooper group (APT23) to FamousSparrow, based on ITOCHU investigation of the attacks to the semiconductor and precious metal-related industries in East Asia. Where Tropic Trooper used Xiangoop Loader to load Cobalt Strike Beacon or EntryShell, and SparrowDoor Loader for CrowDoor (Ahnlab, 2023, pp 10-11) indicating a possible shared toolkit or collaboration between APTs.

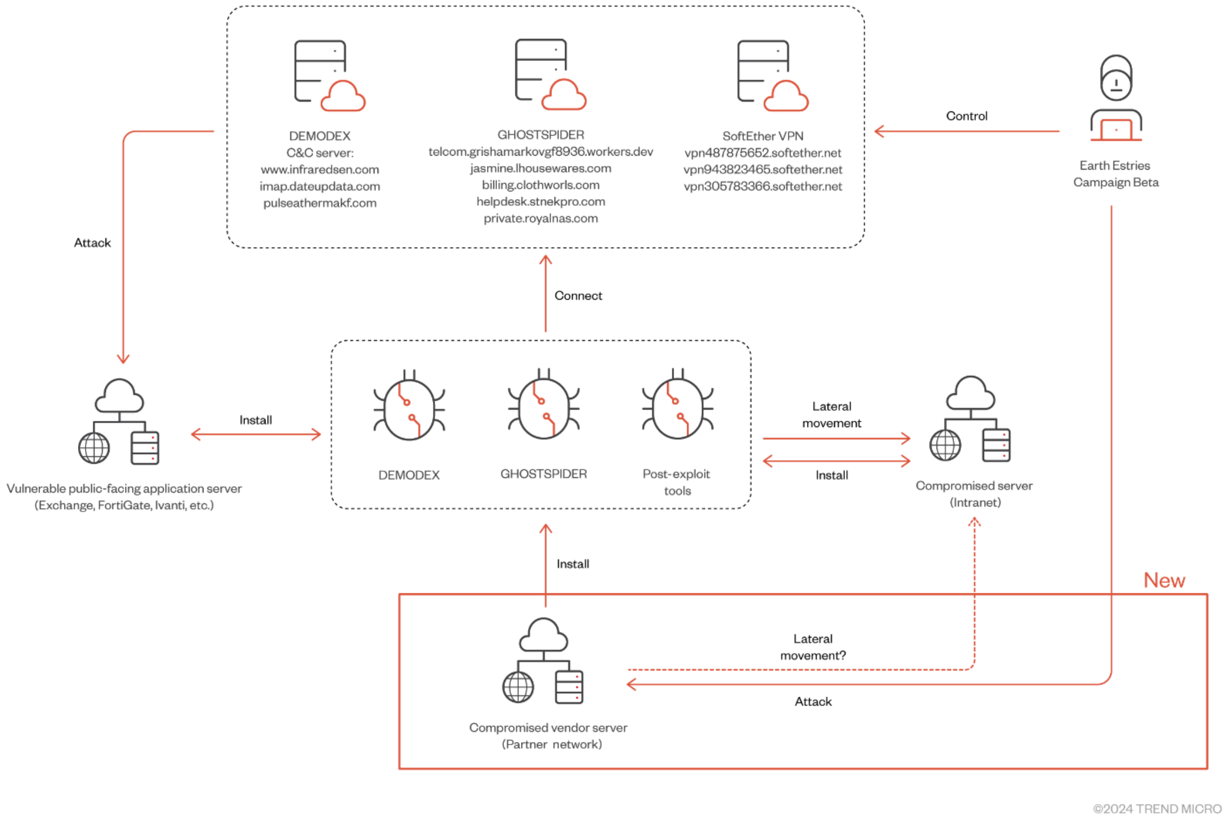
In October 2023, Mandiant identified UNC4841, actively exploiting a zero-day vulnerability in Barracuda Email Security Gateway (ESG) appliances (CVE-2023-2868), which allowed remote command injection in email attachments. Combined with a suite of custom malware, like SeaSpy, a passive backdoor, and Saltwater, a novel malware variant designed for undetectable command-and-control communications and data exfiltration. Mandiant researchers quickly identified significant infrastructure overlap between UNC4841 and UNC2286, APT tracked by Microsoft as Salt Typhoon. Also, primarily targeted governmental and organizations in high-value intelligence sectors, such as critical infrastructure and telecommunications, across North America, Europe, and Asia (Austin, Larsen, et al, 2023).

This intricate web of overlapping tools, and evolving techniques highlights the adaptability and persistence of these threats. Their ability to leverage shared infrastructure and exploit emerging vulnerabilities suggests that these APT groups may operate as part of a larger, unified strategy orchestrated by China.

Tactics, Techniques, and Procedures

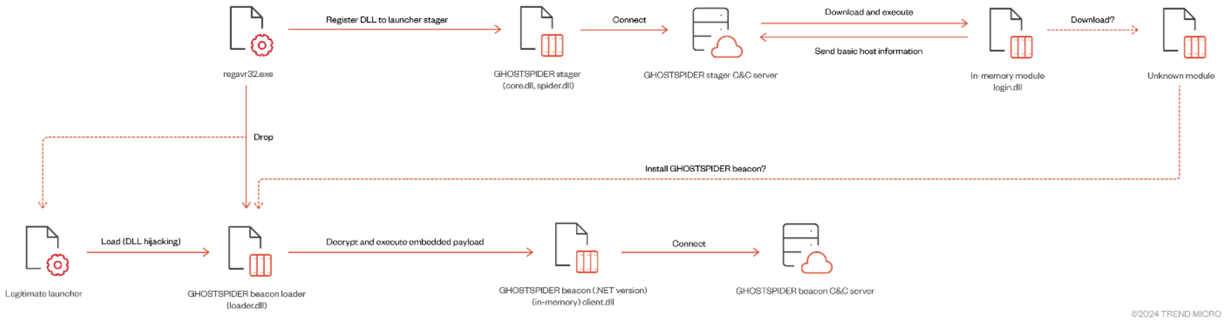
Although little technical information related to the U.S. telecom breach has been released. Many aspects parallel Trend Micro findings on the attacks to the Southeast Asian telecommunications ongoing since 2023. The researchers claim that these telecommunications companies have been compromised for years. Congruent to Anne Neuberger, deputy national security adviser, December 4th statement: “likely one to two years. China has hacked telcos in a couple of dozen countries” (@ericjgeller.com, 2024). Targeting edge devices and leveraging vulnerabilities like ProxyLogon and to a lesser extent (Chang, L. M., 2024):

Vulnerability	Description
Ivanti Connect Secure VPN Exploitation (CVE-2023-46805 and CVE-2024-21887)	Chaining authentication bypass, crafting of malicious requests, and remote code execution with elevated privileges.
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection.
CVE-2022-3236	Code injection vulnerability in the User Portal and Webadmin of Sophos Firewall allowing remote code execution.
ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)	Set of chained vulnerabilities allowing remote code execution (RCE) in Microsoft Exchange servers



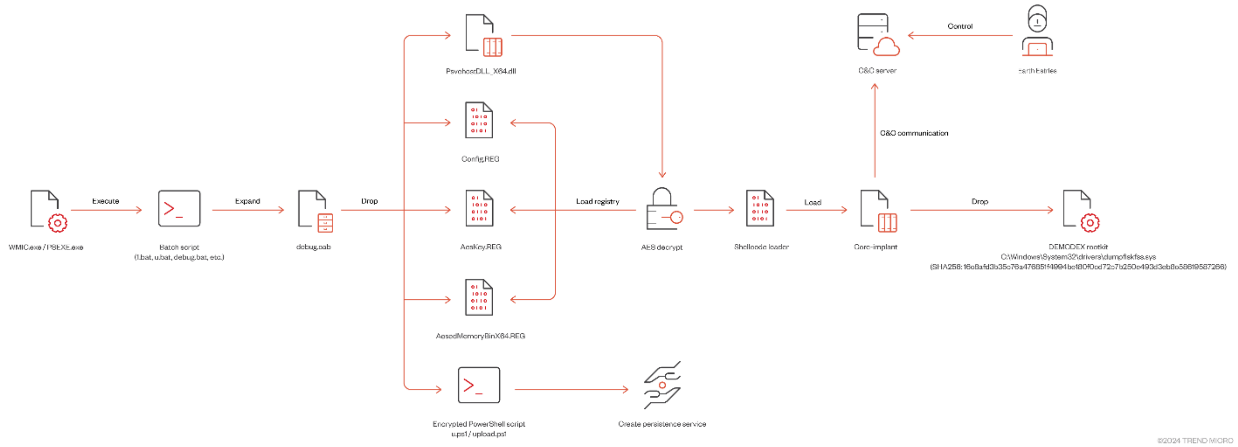
(Chang, 2024)

After obtaining control over the vulnerable resource, it was common practice to deploy DEMODEX, but recent investigations into Southeast Asian telecommunications breaches revealed a new purpose driven multi-modular backdoor. GHOSTSPIDER is a highly modular and stealthy backdoor tailored for adaptability and evasion. Its multi-stage structure allows purpose driven deployment, providing flexibility while evading detection. The initial infection involves the use of regsvr32.exe to install a stager DLL, which validates the execution environment through hardcoded hostnames, activating only on targeted systems. Once operational, the stager establishes a connection with its command-and-control (C2) server, exchanging basic endpoint data and entering a waiting for subsequent payloads. To execute its beacon loader, the malware utilizes DLL search order hijacking, deploying a legitimate executable alongside a malicious DLL. This loader decrypts and executes additional modules entirely in memory. GHOSTSPIDER's communication protocol is just as sophisticated, employing encrypted custom formats for data exchange. The beacon capabilities are extended through command codes directing modular functionalities, such as uploading payloads, managing processes, or maintaining persistence. And by segmenting its components into dynamically retrieved isolated modules from the C2 server, it provides greater operational flexibility, reduced detection footprint, and obfuscates its full scope from security analysts (Chang, L. M., 2024).


Register DLL to launcher stager
Connect
Download and execute
Send basic host information
Download?
regsvr32.exe
GHOSTSPIDER stager (core.dll, spider.dll)
GHOSTSPIDER stager C&C server
In-memory module login.dll
Unknown module
Drop
Install GHOSTSPIDER beacon?
Load (DLL hijacking)
Decrypt and execute embedded payload
Connect
Legitimate launcher
GHOSTSPIDER beacon loader (loader.dll)
GHOSTSPIDER beacon (.NET version) (in-memory) client.dll
GHOSTSPIDER beacon C&C server

©2024 TREND MICRO

This attack also revealed a new DEMODEX variant, discarding the PowerShell script in favor of more secure installation method by bundling critical registry data, like the encrypted configuration and shellcode payload, in a CAB file. Which is deleted after the installation, preventing forensic analysis (Chang, L. M., 2024).

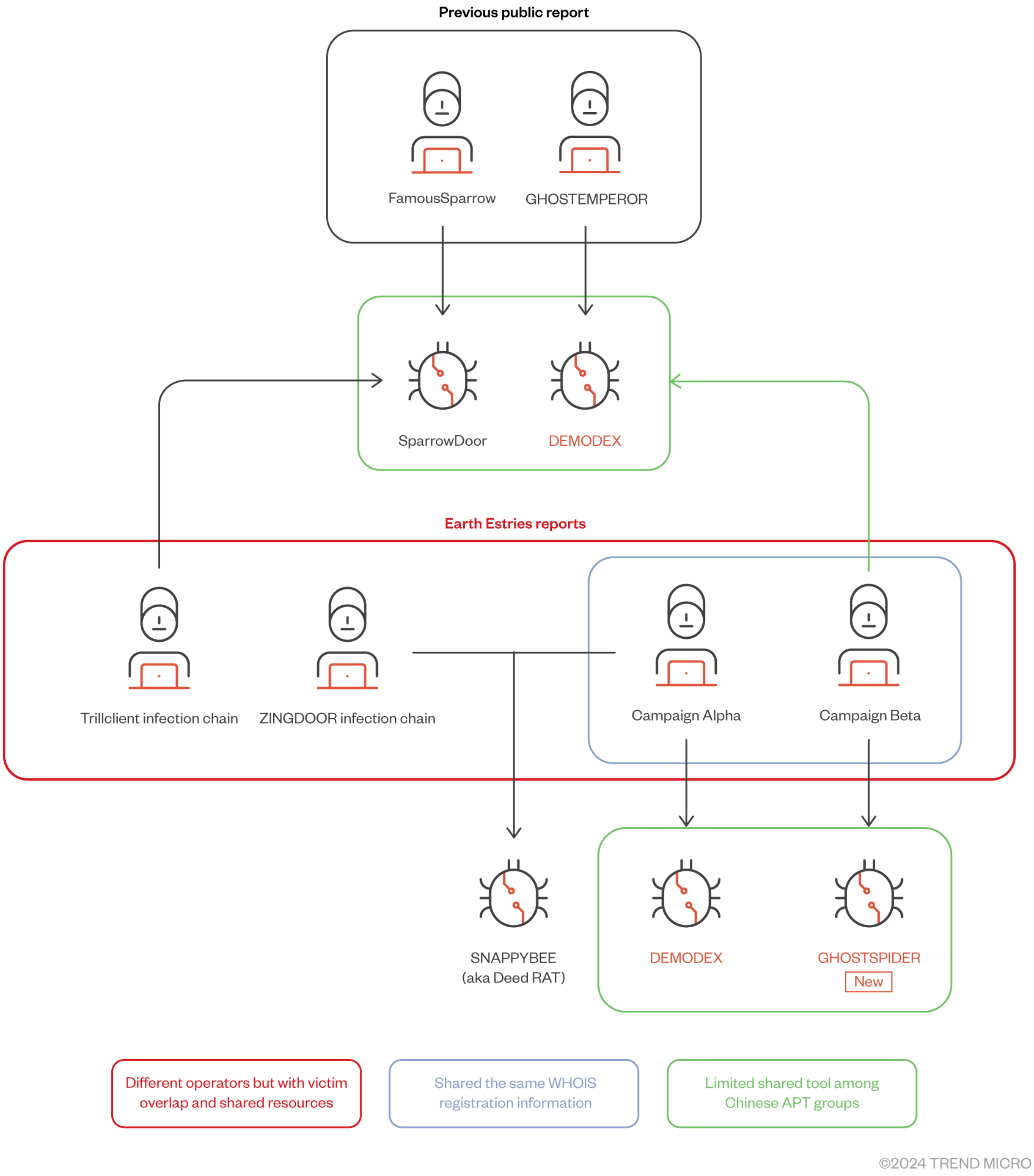


Investigations of C2 infrastructure employed on a series of contemporary attacks targeted at governments led to a novel Linux backdoor, also used in the telco attacks (*name: dash_board, SHA256:44ea2e85ea6cffba66f5928768c1ee401f3a6d6cd2a04e0d681d695f93cc5a1f*), a Linux variant of the Windows based MASOL RAT, identified in 2020 but inactive since 2021. (Chang, L. M., 2024).

Intended Domain and Purpose

The FBI, CISA and many leading cybersecurity firms, have concurring opinions about Salt Typhoon (aka Earth Estries) motivation, despite the broad victim profile, including hotels, technology, consulting, legal, chemical, telecommunications, transportation industries, government agencies, as well as non-profit organizations from countries like: Afghanistan, Brazil, Eswatini, India, Indonesia, Malaysia, Pakistan, The Philippines, South Africa, Taiwan, Thailand, US, and Vietnam. There is clear focus on the exfiltration of intelligence and privileged information, pointing to a well-coordinated state-sponsored cyberespionage campaign.

Moreover, the shared infrastructure and pattern of exploiting public-facing services and devices, leveraging newly disclosed or zero-day vulnerabilities, alongside advanced custom malware like SparrowDoor, Zingdoor, SnappyBee, and Saltwater, which are tailored for stealth, persistence, and command-and-control operations, identified by researchers across multiple security firms. Strongly indicate a unified operational strategy leading to the conclusion that Salt Typhoon, FamousSparrow, GhostEmperor (Microsoft, n.d.), and UNC2286 (Fortinet, n.d.), are likely aliases or subdivisions of the same overarching APT.



Remediation measures

To address the vulnerabilities exploited by advanced persistent threats, multiple agencies, including CISA, NSA, and the FBI, have issued detailed guidance “Enhanced Visibility and Hardening Guidance for Communications Infrastructure” on December 4th 2024. These recommendations focus on improving network visibility, securing configurations, and implementing defense-in-depth strategies. Organizations are encouraged to monitor and audit network devices rigorously, enforce role-based access control (RBAC), and disable unused or plaintext protocols such as Telnet and FTP. Patch management has been highlighted as a critical measure, with an emphasis on addressing known exploits promptly. In addition, robust encryption protocols, multi-factor authentication, and secure logging practices are advocated to minimize the attack surface and improve response capabilities. Specific measures for securing communications infrastructure include isolating management networks, employing VLAN-based segmentation, and utilizing out-of-band management to limit lateral movement. By following these best practices and adopting a proactive, secure-by-design approach to software and hardware configurations, organizations can significantly strengthen their defenses against sophisticated cyber threats (Cybersecurity & Infrastructure Security Agency, December 2025).

Punitive Actions

On January 17, 2025, the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC) imposed sanctions on Juxinhe Network Technology Co., a cybersecurity firm implicated in facilitating the breaches, and Yin Kecheng, a Shanghai-based hacker associated with China’s Ministry of State Security. Effectively freezing any U.S.-based assets of the designated parties and prohibited American entities from engaging in transactions with them.

However, this is not the first time US has sanctioned Chinese companies and individuals:

On January 3, 2025 OFAC sanctioned the Integrity Technology Group, Incorporated (Integrity Tech), a Beijing-based cybersecurity company, for providing the infrastructure, between the summer of 2022 and fall 2023, used by Flax Typhoon to perpetrate multiple computer intrusions (Solomon, 2025).

December 10, 20204 OFAC sanctioned Sichuan Silence Information Technology, a Chengdu-based cybersecurity firm, and one of its employees, Guan Tianfeng, for their alleged involvement in a 2020 global cyberattack that exploited zero-day vulnerabilities in firewalls. The US Department of the Treasury and the Department of Justice (DOJ), which also unsealed an indictment against Guan (Constantin 2025).

March 24, 2024 OFAC sanctioned Wuhan Xiaoruizhi Science and Technology Company, Limited (Wuhan XRZ), a Wuhan-based front company for Ministry of State Security (MSS), and Zhao Guangzong and Ni Gaobin associated with multiple malicious cyber operations (Swain, 2024).

References:

Cybersecurity and Infrastructure Security Agency. (2024, November 13). Joint statement from FBI and CISA on the People's Republic of China (PRC) targeting of commercial telecommunications infrastructure. U.S. Department of Homeland Security. Retrieved from https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications

Drew, J., & Nakashima, E. Chinese government hackers penetrate U.S. internet providers to spy. The Washington Post, 2024, August 27. https://www.washingtonpost.com/technology/2024/08/27/chinese-government-hackers-penetrate-us-internet-providers-spy/

Sarah, Krouse, et al. "U.S. Wiretap Systems Targeted in China-Linked Hack." The Wall Street Journal, The Wall Street Journal, 4 Oct. 2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b

Krouse, S., & Volz, D. T-Mobile hacked in massive Chinese breach of telecom networks: Carrier joins growing list of known victims, including AT&T and Verizon, of the major Chinese spying operation. The Wall Street Journal, 2024, November 15. https://www.wsj.com/politics/national-security/t-mobile-hacked-in-massive-chinese-breach-of-telecom-networks-4b2d7f92

Volz, D, et al. How Chinese hackers graduated from clumsy corporate thieves to military weapons: Massive ‘Typhoon’ cyberattacks on U.S. infrastructure and telecoms sought to lay groundwork for potential conflict with Beijing, as intruders gathered data and got in position to impede response and sow chaos. The Wall Street Journal, 2025, January 4. https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95

Geller, E. J. [@ericjgeller.com]. (2024, December 4). The Salt Typhoon activity "has been underway for some time," a senior administration official said -- "likely one to two years." China [BlueSky]. BlueSky: https://bsky.app/profile/ericjgeller.com/post/3lciyxt3i5s24

Chang, L. M., Chen, T., Bermejo, L., Lee, T. (2024, November 25). Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions. Treand Micro Global Threat Research. https://www.trendmicro.com/en_us/research/24/k/earth-estries.html

Microsoft. (n.d.). Microsoft threat actor naming. Microsoft Learn. Retrieved [2024, January 14], from https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming

Fortinet. (n.d.). Salt Typhoon. FortiGuard Threat Intelligence. Retrieved [2024, January 19], from https://www.fortiguard.com/threat-actor/5557/salt-typhoon

Lechtik, Mark, et al. "GhostEmperor: From ProxyLogon to kernel mode." SECURELIST by Kaspersky, Kaspersky, 30 Sept. 2021, http://www.securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/.

ESET Research. (2021, September 23). ESET Research discovers FamousSparrow APT group spying on hotels, governments and private companies from https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-discovers-famoussparrow-apt-group-spying-on-hotels-governments-and-private-companies/

Lee, T., Bermejo, L., Hiroaki, H., Chang, L. M., Sison, G. (2023, August 30). Earth Estries Targets Government, Tech for Cyberespionage. Treand Micro Global Threat Research. https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html

AhnLab (2023, November 9) Threat Trend Report on APT Groups: October 2023 Major Issues on APT Groups. https://asec.ahnlab.com/wp-content/uploads/2023/12/2023_Oct_Threat-Trend-Report-on-APT-Groups.pdf

Austin, Larsen, et al. "Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868)." Google Cloud Threat Intelligence, Mandiant, 9 Aug. 2023, http://www.cloud.google.com/blog/topics/threat-intelligence/unc4841-post-barracuda-zero-day-remediation

Cybersecurity & Infrastructure Security Agency. (2024, December 4). Enhanced Visibility and Hardening Guidance for Communications Infrastructure. America’s Cyber Defense Agency: https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

Solomon, H (2025 January 17) US hits back against China’s Salt Typhoon group. CSOOnline: https://www.csoonline.com/article/3631635/us-government-sanctions-chinese-cybersecurity-company-linked-to-apt-group.html

Constantin, Lucian (2025 January 3) US government sanctions Chinese cybersecurity company linked to APT group. CSOOnline: https://www.csoonline.com/article/3631635/us-government-sanctions-chinese-cybersecurity-company-linked-to-apt-group.html

U.S. Department of Justice (20204 December 10) China-Based Hacker Charged for Conspiring to Develop and Deploy Malware That Exploited Tens of Thousands of Firewalls Worldwide. U.S. DOJ: https://www.justice.gov/opa/pr/china-based-hacker-charged-conspiring-develop-and-deploy-malware-exploited-tens-thousands

Swain, Gyana (2024 December 10) US sanctions Chinese cybersecurity firm over global malware campaign. CSOOnline: https://www.csoonline.com/article/3621864/us-sanctions-chinese-cybersecurity-firm-over-global-malware-campaign.html

U.S. Department of the Treasury (2024 March 25) Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure. U.S. Department of the Treasury: https://home.treasury.gov/news/press-releases/jy2205

ChatGPT was used to revise contents for plagiarism, reference and APA guidelines compliance.