Recent Cyber-attack on Networking Infrastructure

A case study

Tirumala Vamsi Machavarapu
University of North Texas, Denton, TX
Tirumalavamsimachavarapu@my.unt.edu

Abstract

Recent Cyber-attacks happened on networking infrastructure like AT & T, Verizon, Lumen Technologies and T-Mobile through cisco system routers. It was discovered in late 2024 [1]. Targeted data includes president, vice president and security official's private communication and text messages [2]. Former Executive director of CISA described it as an order of magnitude worse [3]. It was caused due to unpatched devices for a known vulnerability of Fortinet and Cisco. In one instance intruders-maintained access to a system for three years. The same threat actor performed attacks for research information related to telecommunications, engineering, and technology at some universities [4]. In this case study, I will discuss this cyber-attack in a detailed way.

Introduction

Salt Typhoon is a advanced persistent threat operator believed to be a state sponsored organization. Initially these attacks were reported in late 2024. At that time the attack included at least 9 telecommunication firms and a few dozen other country firms [2]. By compromising this organizations intruder were able to access metadata of user calls and text data, time stamps, source and destination IP address and phone numbers of around million people living in Washington D.C including staff of former Vice president, phones of current president and Vice president [5]. Insikt Group researchers discovered that intruders infiltered cisco devices at few organizations including a telecom provider, UCLA, Loyala Marymount University, Utah Tech University, California State University and firms of other countries [4].

Table 1: Overview of Cyber attack

Threat actor	Salt Typhoon
Affected institutions	At least 9 telecom companies and few dozen country firms data in Late 2024. In Early 2025 a telecom firm and other universities are the firms affected.
Targeted	Officials and people data in Washington D.C, court authorized wiretapping data and research data from universities.
Attacked through	Fortinet and cisco devices. In cisco's case intruders used legitimate account credentials and multiple vulnerabilities in networking Infrastructure.

cyber-attacks on Networking infrastructure

Network Security plays a key role in cyber security. If you are not connected to any network, then risk of a cyber-attack is low. Attack vectors are the methods or paths that an attacker uses to gain unauthorized access. If an intruder accesses the network then the attack vector would be very high. Network is the first

line of defense an organization will have, most of the intruders will try to access the network immediately to increase the attack vector. Accessing a network can turn a cyber-attack into a advanced persistent threat. Intruders can move their malicious activity from a non-critical system to a critical system which affects the uptime using the network. Intruders can perform different attacks like man in the middle by accessing the network.

To provide efficient network security, a vulnerability less networking infrastructure is essential. A vulnerability in a network infrastructure can lead to a higher impact of business continuity.

There are several other significant cases in which Networking Infrastructure was targeted by the intruders. In 2022 State sponsored exploitation of network devices which affected home routers to medium and large enterprise routers [6]. Chinese state-sponsored actors repeatedly conduct cyber espionage campaigns against federal, provincial, territorial, municipal and Indigenous government networks in Canada [7]. In 2023 Russian Satellite telecom provider was hacked by Wagner group [8].

How the attack happened

The intruder gained access to core networking infrastructure and then used that infrastructure to collect variety of information. After gaining access the intruder persists in that environment for extended periods and using living off the land techniques (LOTL) [9]. They have used compromised login credentials and known vulnerabilities such as CVE-2018-0171, CVE-2023-20198, CVE-2023-20273, CVE-2023-20399 to exploit [10] . These vulnerabilities are related to Cisco IOS and IOS XE software smart Install Remote code execution vulnerability, cisco vulnerability in web UI feature and Cisco NX-OS CLI command injection vulnerability.

CVE-2018-0171 allowed to execute arbitrary code on remote devices by sending a crafted small install message [11]. CVE-2023-20399 allowed software CLI command Injection Vulnerability, A authenticated user with administrative privileges can run commands as root on underlying OS of an affected device. It uses high SSH ports to evade monitoring and executing these commands in Guest cell.

After using initial credentials, they changed configurations and captured the SNMP, TACACS/RADIUS data and decrypted weak passwords in offline. They found the upstream and downstream devices using TFTP or FTP configurations and use these details to exploit CVE-2023-20399. This configuration often contains SNMP read/write community strings and local accounts encryption type. The threat actor repeatedly modified the loopback interface and compromised to bypass Access control list (ACL) [12].

The intruder used a custom application named as “JumbledPath” by cisco to use intruder defined connections and capture the data on a required data. The initial node which is running the application on gust shell is never monitored. Sometimes the intended target can be another telecom company. Systems or hops in between them are used to compress and send the data. The logs are frequently cleared by jumbled path to reduce its footprint and evade monitoring [13].

Preventive measures

Update or patch devices as soon as possible [14]. Using MFA, since it helps as initial defense against phishing and stolen credentials [13]. To disable smart install feature which has the vulnerability use “no vstack” command [11]. If web management is not required then it’s better to disable using “no ip http server”(unencrypted traffic) and “no ip http secure-server”(encrypted server), to avoid CVE-2023-20198 vulnerability in Cisco IOS XE. Disabling guestshell when not using that feature using “guestshell disable” command to avoid running custom applications like Jumbled path by living of the land. Disable telnet and ensure its not available to any virtual Teletype (VTY) lines on cisco devices using “transport input ssh” and “transport output none”. It ensures that routers and switches are not accessible remotely. Use AAA (Authentication, Authorization and Accounting) to deny configuration modifications. Store configurations centrally and push to devices. Do not allow devices to be trusted sources of their configurations [14]. To avoid Defense Evasion of access control lists by modifying loopback address verify correctness of all management protocols like SNMP, SSH, Netconf. Monitor for Jump hosts. Encrypt all monitoring and configuration traffic to avoid exploitation of downstream and upstream devices linked to the affected device [15][16].

Using encrypted apps for communication may have reduced the attack vector. Using type 8 passwords, are recommended by NSA, which are hashed with PBKDF2, SHA-256, 80-bit salt and 20,000 iterations makes it more secure. And type 6 for TACACS+ key configuration [13] [17].

Policy and information assurance

FCC(Federal Communications Commission) chairwoman Jessica Rosenworcel has proposed a Declaratory ruling that clarifies that Section 105 of the Communications Assistance for Law Enforcement Act (CALEA) creates a legal obligation to protect telecommunication networks. FCC proposed a new compliance framework annual certification requirement for communication service providers, which requires them to create update and implement cybersecurity risk management plans. They explained that this is very serious since it impacts national security and public trust [18]. Cyber security rules should be seriously complied to avoid large fines in millions of dollars [19].

Conclusion

Salt Typhoon cyberattacks highlight the evolving threat landscape by state sponsored hacking groups which stay persistent for a long time and collect intelligence or perform espionage activities. In this case, the threat actor was able to access sensitive information by exploiting known vulnerabilities in networking infrastructure. This case explains that not only government organizations, but private organizations of a country need to be secure against Espionage activities, since this Intelligence can play a key role in national security. Cyber espionage activity might be happening now, which may not be discovered due to the stealthiness like clearing logs and jumping hosts. This case highlights the need of proactive measures for defense against espionage. As cyber security threats become more advanced, active patching and monitoring will be a necessity of organizations.

References

[1] Krouse, S., & Volz, D. (2024, November 15). *T-Mobile Hacked in Massive Chinese Breach of Telecom Networks*. The Wall Street Journal. https://www.wsj.com/politics/national-security/t-mobile-hacked-in-massive-chinese-breach-of-telecom-networks-4b2d7f92

[2] Volz, D. (2024, December 4). Dozens of Countries Hit in Chinese Telecom Hacking Campaign, Top U.S. Official Says. The Wall Street Journal. https://www.wsj.com/politics/national-security/dozens-of-countries-hit-in-chinese-telecom-hacking-campaign-top-u-s-official-says-2a3a5cca

[3] Menn, J. (2024, August 27). Chinese government hackers penetrate U.S. internet providers to spy . The Washington Post. https://www.washingtonpost.com/technology/2024/08/27/chinese-government-hackers-penetrate-us-internet-providers-spy/

[4] Wright, R. (2025, February 13). *China-backed hackers continue cyberattacks on telecom companies*. Cybersecurity Dive. https://www.cybersecuritydive.com/news/china-backed-hackers-continue-cyberattacks-on-telecom-companies/740066/

[5] Thrush, G., Goldman , A., & Barnes , J. (2024, October 25). *Chinese Hackers Are Said to Have Targeted Phones Used by Trump and Vance*. The New York Times. https://www.nytimes.com/2024/10/25/us/politics/trump-vance-hack.html

[6] NSA, CISA, and FBI expose PRC State-Sponsored exploitation of network providers, devices. (2022, June 7). National Security Agency. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3055748/nsa-cisa-and-fbi-expose-prc-state-sponsored-exploitation-of-network-providers-d/

[7] Tunney , C. (2024, October 30). China “compromised” Canadian government networks and Stole Valuable Info: Spy Agency | CBC News. CBC news. https://www.cbc.ca/news/politics/cse-cyber-threats-china-1.7367719

[8] Swinhoe, D. (2023, June 30). Russian satellite comms firm Dozer taken offline by Wagner-affiliated Hacker Group - Report. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/russian-satellite-comms-firm-dozer-taken-offline-by-wagner-affiliated-hacker-group-report/

[9] Freeman, M. (2024, December 18). *Breaking down salt typhoon*. Armis. https://www.armis.com/blog/breaking-down-salt-typhoon/
[10] Lyons, J. (2025, February 13). *More victims of China's salt typhoon cyber-spy crew emerge*. More victims of China's Salt Typhoon cyber-spy crew emerge. The Register. https://www.theregister.com/2025/02/13/salt_typhoon_pwned_7_more/
[11] Cisco IOS and IOS Xe Software Smart Install Remote Code execution vulnerability. Cisco. (2022, December 15). https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20180328-smi2.html
[12] Lakshmanan, R. (2025, February 21). Cisco confirms salt typhoon exploited CVE-2018-0171 to target U.S. Telecom Networks. The Hacker News. https://thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html
[13] Cisco Talos Blog. (2025, February 20). Weathering the storm: In the midst of a typhoon. Cisco Talos Blog. https://blog.talosintelligence.com/salt-typhoon-analysis/
[14] McMillan, R. (2025, February 20). Salt Typhoon Hackers Used Old Cisco Bug, Stolen Credentials to Hop on Routers. The Wall Street Journal . https://www.wsj.com/livecoverage/stock-market-today-dow-sp500-nasdaq-earnings-02-20-2025/card/salt-typhoon-hackers-used-cisco-bug-stolen-credentials-to-hop-on-routers-S7Nc4qISMJV785zC32bi
[15] Poireault, K. (2025, February 21). Salt typhoon exploited Cisco devices with Custom Tool. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/salt-typhoon-cisco-custom-tool/
[16] Cisco Ios XE Software Hardening Guide. Cisco . (2023, March 7). https://sec.cloudapps.cisco.com/security/center/resources/IOS_XE_hardening
[17] Cisco password types: Best practices. U.S Department of Defense. (2022, February 17). https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/1/CSI_CISCO_PASSWORD_TYPES_BEST_PRACTICES_20220217.PDF
[18] Implications of Salt Typhoon Attack and FCC Response. Federal communications commission. (2024, December 5). https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf
[19] Kapko, M. (2024, September 18). AT&T settles a 2023 data breach for $13m. recent incidents are much worse. Cybersecurity Dive. https://www.cybersecuritydive.com/news/att-telecom-cybersecurity-breach-fcc/727355/