TLP:CLEAR

Volt Typhoon Chinese APT

4TH JULY 2025

CERT_CTI_2025_31

PREPARED BY: MAHACYBER

Table Of Contents

Introduction

The Chinese state-sponsored Advanced Persistent Threat (APT) organization Volt Typhoon is well-known for attacking vital infrastructure in the US and its allies, mostly for espionage and possible disruption. An overview of Volt Typhoon's covert cyber operations is given in this paper. To avoid detection and preserve long-term access, the group mostly relies on living off the land tactics.

Their emphasis on industries like communications, energy, and transportation, as well as their congruence with more general geopolitical goals, are important lessons learned. For cybersecurity experts, government organizations, and infrastructure operators who must comprehend the nature of this threat, strengthen their defensive posture, and foresee future nation-state cyber strategies, this paper is a must-read.

Purpose

The objective of this report is to examine and provide a comprehensive understanding of Volt Typhoon, a state-sponsored APT group from China, by exploring its background, goals, and operational strategies. This report seeks to illuminate the group's strategic aims of cyber espionage and convert positioning within critical infrastructure.

The report encompasses Volt Typhoon's established tactics, techniques, and procedures (TTPs), the sectors it targets, and the attack campaigns that have been observed, particularly those impacting the United States and its allies. Additionally, it provides insights into the wider geopolitical context that motivates such cyber activities and underscores the necessity of proactive defense strategies against subtle, ongoing threats.

Our Mission

To help people, businesses, and key infrastructure sectors identify and reduce potential cyber threats by disseminating accurate, easily comprehensible, and actionable information on the Volt Typhoon, a Chinese state-sponsored Advanced Persistent Threat (APT).

Targeted Industries and Countries

Industry	Countries Targeted
Energy	United States, Australia
Water Systems	United States
Satellite & Space Assets	United States, India
IT	India, Southeast Asia
Government Agencies	Australia, New Zealand
Defense Contractors	United States, India
Communications	United States
Transportation	United States, Guam

Timeline of attack

January 2023: Chinese APT Volt Typhoon Breached U.S. Power Utility in Prolonged Cyberattack:
The Chinese advanced persistent threat (APT) group Volt Typhoon infiltrated a U.S. power utility in Massachusetts in 2023, maintaining access for over 300 days. ***Link***

May 2023: Volt Typhoon targets US critical infrastructure with living-off-the-land techniques:
Volt Typhoon proxies all its network traffic to its targets through compromised SOHO network edge devices (including routers). ***Link***

December 2024: China's Tacit Acknowledgment:
In a private conference in Geneva in December 2024, Chinese officials subtly admitted China's role in cyberattacks targeting vital U.S. infrastructure. ***Link***

June 2025: Smart grid infrastructure in southern India:
In the middle of 2025, the Chinese APT group known as Volt Typhoon focused on smart grid infrastructure in southern India by taking advantage of weaknesses in IoT-based energy monitoring devices. ***Link***

Recent Campaigns and Exploits

- The Versa Director Zero-Day Attack (CVE-2024-39717) is a serious security flaw that hackers started exploiting in around October to December 2024 and continued into early 2025. It affects Versa Networks' software, which is used by internet providers (ISPs), managed service providers (MSPs), and IT companies to manage networks. Since the vulnerability was unknown to the public at first (a "zero-day"), attackers used it to secretly break into systems, steal data, or disrupt services before companies could patch it.

- Long-Term Utility Infiltration mapped operating systems and exfiltrated sensitive data while staying hidden for more than 300 days within Littleton Electric Light & Water, an electric utility in Massachusetts.

- Living-Off-the-Land Living and AD Credential Harvesting: Continuous use of PowerShell and other built-in Windows tools to move laterally, elevate rights, and gather credentials across vital infrastructure networks.

- Rebuilding the Infrastructure of Botnets: Volt Typhoon quickly reassembled when the FBI dismantled its router-based "KV botnet" in late 2023, breaking into SOHO routers and VPN devices once more to rebuild C2 infrastructure.

Case Study: Volt Typhoon Targeting U.S. Critical Infrastructure

Overview

In May 2023, Microsoft and the U.S. government disclosed that Volt Typhoon, a state-sponsored APT group from China, had been executing a prolonged cyberespionage initiative targeting critical infrastructure sectors in the U.S. which include communications, transportation, energy, and water systems.

Key Findings

Initial Access: Volt Typhoon employed living-off-the-land strategies, circumventing malware by utilizing built-in tools such as PowerShell, WMI, and cmd.exe.

Persistence: They sustained covert access through compromised Fortinet FortiGate devices, utilizing stolen credentials.

Targets: U.S. military installations, seaports, electric utilities, and water treatment facilities—particularly those located in the Pacific region.

Attribution: Associated with China's People's Liberation Army (PLA), indicating a strategy to preposition for future disruptions rather than solely for intelligence collection.

Significance

Demonstrated a transition in Chinese APT strategies towards pre-positioning within critical systems in anticipation of potential kinetic or political crises (for instance, the Taiwan conflict). Triggered collaborative cybersecurity advisories from the NSA, CISA, FBI, and global partners. Increased the urgency for implementing zero-trust architectures and segmented networks within national infrastructure.

Impact

The Volt Typhoon campaign revealed significant vulnerabilities in the critical infrastructure of the United States by penetrating sectors such as communications, energy, water, and transportation through discreet, malware-free methods that successfully avoided detection; it uncovered substantial cybersecurity gaps, took advantage of unaddressed hardware issues and vendor supply chains, threatened U.S. military operations (particularly in the Pacific), and prompted international reactions and policy measures aimed at enhancing cyber defenses and resilience.

Technical Details

01

Threat Actor

Volt Typhoon is a highly advanced, state-sponsored Advanced Persistent Threat (APT) group linked to the People’s Republic of China (PRC), operational since at least the middle of 2021. This group is recognized for executing covert cyber operations aimed at long-term espionage and establishing a presence within critical infrastructure networks, rather than focusing on immediate destruction or data theft.

02

Attack Overview

Volt Typhoon employs living-off-the-land strategies—utilizing legitimate system tools such as PowerShell, WMI, and command-line utilities—to evade detection and ensure ongoing access. Their attack methodology generally begins with gaining initial access through compromised edge devices (for instance, routers, firewalls, VPNs), followed by lateral movement, credential harvesting, and communication via command-and-control (C2) channels that are integrated into normal system activities.

03

Type of Attack

The group primarily partakes in: Cyber espionage – concentrating on intelligence collection. Pre-positioning operations – to sustain covert access for potential future sabotage or disruption. Zero-day exploitation – exemplified by the 2024 exploitation of Versa SD-WAN vulnerabilities (CVE-2024-39717). SOHO router hijacking – employing malware (such as KV-botnet) to create resilient botnets across small office and home networks.

Tactics & Techniques (Based on MITRE ATT&CK)

TACTICS	TECHNIQUE	MITRE ID
Initial Access	Exploit Public-Facing Applications	T1190
Execution	PowerShell	T1059.001
Persistence	Scheduled Task	T1053.005
Defense Evasion	Masquerading	T1036
Credential Access	OS Credential Dumping	T1003
Lateral Movement	Remote Services	T1021
Command & Control	Application Layer Protocol	T1071

Cyber Kill Chain

Reconnaissance:Open-source intelligence (OSINT) is carried out by Volt Typhoon, which also analyzes target networks & finds persons and systems that are susceptible to attack.

Weaponization: To avoid detection, the group creates dangerous payloads by enclosing malware or scripts in legitimate tools, frequently employing living-off-the-land tactics.

Delivery:Phishing emails, compromised devices, remote access software, or network services are some of the ways that malware or tools are distributed.

Exploitation:After delivery, Volt Typhoon uses PowerShell or credentials that have been stolen to execute code or obtain access to systems by taking advantage of flaws or configuration errors.

Installation: Installing persistence mechanisms which frequently use web shells, scheduled tasks, or builtin Windows utilities—maintains access.

Command and Control (C2): To give orders and retrieve information, secure channels are set up, frequently utilizing reputable services or encrypted communications.

Actions on Objectives: Volt Typhoon performs its ultimate goals—espionage, data theft, surveillance, or prepositioning for potential disruption of critical infrastructure.

Indicators of Compromise(IOC’s)

S.No	Hash Value	Risk Score
1	e10adc3949ba59abbe56e057f20f883e(MD5)	70
2	7c4a8d09ca3762af61e59520943dc26494f8941b(SHA-1)	70
3	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c9 (SHA-256)	70

S.No	IP Addresses	Risk Score
1	196.218.123.202	80
2	165.22.251.103	70
3	128.199.238.30	70
4	139.59.254.193	70
5	134.209.5.135	70
6	142.93.168.28	70

Recommendations

1. **Maintain Updated Systems:** Implement security updates on all devices, particularly routers and firewalls.
2. **Enforce Strong Password Policies and MFA**
   - Utilize Strong, Unique Passwords with Multi-Factor Authentication Refrain from reusing passwords across different services.
   - Activate Multi-Factor Authentication on email, banking, and cloud storage accounts.
3. **Defend Against Phishing and Social Engineering**
   - Be Cautious of Phishing Attempts and Avoid clicking on suspicious links or downloading unexpected attachments.
   - Report phishing emails to your service provider or workplace. Secure Home Routers and Internet of Things Devices Alter default credentials on all smart devices.
4. **Secure Remote Access and Edge Devices:** Disable unnecessary remote access functionalities.
5. **Trust on authentic source only**
   - Stay Informed Adhere to cyber hygiene recommendations from reliable sources such as CISA.gov or cyber.gc.ca.
   - Engage in local awareness initiatives when they are available.

Conclusion

- The Volt Typhoon campaign serves as a significant reminder that contemporary cyber threats are not only persistent and sophisticated but also increasingly strategic—designed to undermine national security and critical infrastructure without immediate detection.
- By utilizing stealthy, "Living-off-the-land" techniques and focusing on edge devices and credential misuse, Volt Typhoon illustrated how adversaries can gain long-term access and prepare for future geopolitical conflicts.
- In response, both organizations and individuals must embrace a proactive cybersecurity approach. This entails implementing zero trust architectures, securing vulnerable systems, enforcing robust authentication practices, and maintaining constant vigilance through monitoring and collaboration.
- Only through a collective effort—integrating technological defenses, public awareness, and cross-sector coordination—can we effectively mitigate such advanced threats and protect our digital and physical infrastructure from disruption.

References

- *https://www.darkreading.com/cyberattacks-data-breaches/volt-typhoon-strikes-massachusetts-power-utility*

- *https://www.darkreading.com/vulnerabilities-threats/voltzite-zaps-african-utilities-volt-typhoon-onslaught*

- *https://www.lawfaremedia.org/article/volt-typhoon-and-the-disruption-of-the-u.s.-cyber-strategy*

- *https://blog.barracuda.com/2024/03/14/volt-typhoon-future-war*

- *https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/?msockid=1c6946eb471b699929c450f746ba6848*