TLP:AMBER

Situational Awareness Bulletin: Volt Typhoon Threat Update

PT-OTRB & ST ISACs

March 2024

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Purpose

The Public Transportation (PT) - Over the Road Bus (OTRB) and Surface Transportation (ST) Information Sharing and Analysis Centers (ISACs) are providing this Situational Awareness Bulletin (SAB) for your general security awareness.

Utilization of any standards or guidance discussed herein is strictly voluntary. The practices implemented by rail, transit, and OTRB systems may be more or less restrictive than any recommended practices or guidance in this document. Federal or state regulations sometimes govern portions of public transit systems' operations. In those cases, government regulations should precede the information or guidance provided herein. Organizations should consult their policies and guidance before acting based on the information presented in these documents.

This document supplements guidance and analysis already provided in daily reports produced by the PT-OTRB & ST ISACs. Of note, the last page of this report lists references for additional information.

FAIR USE: The PT-OTRB and ST ISACs provide this report to ISAC members and partners. Recipients may share this report with members of their organization who may benefit from the information; however, public dissemination is not authorized without prior author approval.

To contact ST analysts, please call 866-784-7221 or email st-isac@surfacetransportationisac.org.

To contact PT-OTRB analysts, please call 877-847-5510 or email mcanalyst@motorcoachisac.org.

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Introduction

In May 2023, the United States National Security Agency (NSA), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Federal Bureau of Investigation (FBI), and multiple allied foreign governments issued a joint Cybersecurity Advisory (CSA) highlighting the threat of a newly discovered campaign launched by advanced persistent threat (APT), Volt Typhoon. The CSA warned network defenders and critical infrastructure (CI) operators of the state-sponsored actors targeting CI in the United States and its territories. Volt Typhoon, based in the People's Republic of China (PRC), has targeted the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors to disrupt the pillars of American society. The campaign is thought to be one of the most extensive known Chinese cyber-espionage campaigns against American critical infrastructure. In May 2023, Microsoft's Threat Intelligence team assessed with moderate confidence that the APT "is pursuing [the] development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises." In early February 2023, the NSA, CISA, FBI, and allied partners in Canada, New Zealand, Australia, and the UK released an updated CSA warning that Volt Typhoon is "seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States." Additionally, various news outlets have reported that the threat actor has had access to the computer networks of "transportation hubs and other critical American infrastructure" for at least five years. Volt Typhoon is a highly sophisticated threat actor and can cut off water, power, and communications to military bases, residential homes, and businesses. It is confirmed to have been found in telecommunications systems in Guam back in early 2023.

Attack Details

Volt Typhoon primarily relies on living-off-the-land (LOTL) techniques to perform espionage and maintain access without being detected for as long as possible. LOTL attacks leverage legitimate tools within the victim's system to evade detection from the user and antivirus applications downloaded on the network. Volt Typhoon has been observed issuing "commands via the command line to collect data, including credentials from local and network systems, put the data into an archive file to stage it for exfiltration, and then… use the stolen valid credentials to maintain persistence." The APT gains initial access by compromising internet-facing Fortinet FortiGuard devices, which are currently being assessed to understand how the devices are exploited. They will then leverage the privileges within the Fortinet device to extract credentials from the Active Directory account and authenticate to other devices on the network. Volt Typhoon's success also stems from extensive pre-compromise reconnaissance. The reconnaissance aims to learn about the target's network architecture, security measures, typical user behaviors, and key network and IT staff. Additional tactics, techniques, and procedures (TTPs) utilized by the APT are routing traffic through compromised routers, firewalls, and VPN hardware to better "blend into normal network activity" and "using custom versions of open-source tools to establish a command and control (C2) channel over proxy to further stay under the radar." A figure illustrating the typical activity of Volt Typhoon is included in the Appendix at the end of this document.

Indicators of Compromise

The following is a list of indicators of compromise (IOC) for at-risk organizations:

- Exploiting vulnerabilities [T1190] in widely used software including, but not limited to:
  - CVE-2021-40539—ManageEngine ADSelfService Plus. https://www.cisa.gov/uscert/ncas/alerts/aa21-259a.
  - CVE-2021-27860—FatPipe WARP, IPVPN, MPVPN. https://www.ic3.gov/Media/News/2021/211117-2.pdf.
- Using webshells for persistence and exfiltration [T1505.003], with at least some of the webshells derived from the *Awen* webshell.
- Using living off the land tools for discovery, lateral movement, and collection activities, to include:
  - certutil
  - dnscmd
  - ldifde
  - makecab
  - net user/group/use
  - netsh
  - nltest
  - ntdsutil
  - PowerShell
  - req query/save
  - systeminfo
  - tasklist
  - wevtutil
  - wmic
  - xcopy
- Selective clearing of Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity [T1546].
- Using FRP file BrightmetricAgent.exe to reveal servers behind a network firewall or obscured through Network Address Translation (NAT).
  - Observed MD5 Hashing:
    - fd41134e8ead1c18ccad27c62a260aa6
    - edc0c63065e88ec96197c8d7a40662a15a812a9583dc6c82b18ecd7e43b13b70
- Using open source “hacktools” tools, such as:

- Fast Reverse Proxy (frp) – Probably derived from the publicly-available *fatedier* and *EarthWorm* variants.
- Impacket – To detect Impacket usage, see the joint Cybersecurity Advisory: "Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization"
- Mimikatz.exe
- Remote administration tools – Defenders should consult the joint Cybersecurity Advisory: "Protecting Against Malicious Use of Remote Monitoring and Management Software"

- Volt Typhoon custom FRP executable (SHA-256):
  - baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c
  - b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74
  - 4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349
  - c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d
  - d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af
  - 9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a
  - 450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267
  - 93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066
  - 7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5
  - 389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61
  - c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b
  - e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95
  - 6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff
  - cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984
  - 17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4
  - 8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2
  - d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295
  - 472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d
  - 3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642
- Queries to hunt these indicators of compromise in Defender are available via Microsoft.

Detection

The CSA described how network defenders can detect Volt Typhoon's malicious activity. The following list is the logging recommendations detailed by the joint advisory:

- Implement detailed logging and aggregate logs in an out-of-band, centralized location that is write-once, read-many to avoid the risk of attackers modifying or erasing logs.
- Establish and continuously maintain network, user, administrative, and application activity baselines and least privilege restrictions.

- Build or acquire automation (such as machine learning models) to continually review all logs, compare current activities against established behavioral baselines, and alert on specified anomalies.
- Reduce alert noise by fine-tuning via priority (urgency and severity) and continuously reviewing detections based on trending activity.
- Leverage user and entity behavior analytics (UEBA).
- Enhance IT and OT network segmentation and monitoring.

Mitigations

Below is a series of techniques that can help mitigate the threat posed by Volt Typhoon. According to CISA, the recommended mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). CPGs are basic cybersecurity practices and protections that all organizations should implement to ensure their systems and networks are risk-averse. For more information on CPGs, and additional recommended baseline protections, visit CISA's Cross-Sector Cybersecurity Performance Goals.

- Defenders should harden the attack surface by applying patches for internet-facing systems. Vulnerabilities in appliances frequently exploited by Volt Typhoon such as Fortinet, Ivanti, NETGEAR, Citrix, and Cisco devices should be prioritized.
    - Limiting internet exposure of all internet-facing systems will reduce the primary attack surface leveraged by Volt Typhoon actors.
- Defenders should secure credentials by requiring passwords for all IT password-protected assets to be at least 15 characters, disabling the storage of clear text passwords in LSASS (Local Security Authority Subsystem Service) memory, and ensuring that edge devices (an endpoint on a network) do not contain accounts that could provide domain admin access.
- Defenders should secure accounts by separating user and privileged accounts, enforcing the principle of least privilege, auditing all user, admin, and service accounts, and implementing multi-factor authentication (MFA) to mitigate the risk of compromised valid accounts.
    - MFA is a feature typically found within network segmentation or zero-trust models. Implementing this kind of architectural approach would divide networks into multiple segments and increase the overall security posture by limiting access to data, devices, and applications while restricting communications between networks. Network segmentation helps prevent lateral movement within a system, which could prevent further exploitation of a victim after Volt Typhoon has gained initial access.

- In addition to host-level changes, defenders should review perimeter firewall configurations for unauthorized changes and entries that may permit external connections to internal hosts.

- Defenders should secure remote access services by limiting remote desktop services. If RDP is necessary, apply best practices, including auditing the network for systems using RDP, closing unused RDP ports, and logging RDP login attempts.
- Defenders should secure cloud assets by
  - Hardening cloud assets
  - Reviewing and restricting public endpoints and ensuring that services like storage accounts, databases, and virtual machines are not publicly accessible unless necessary.
  - Regularly monitor and audit privileged cloud-based accounts

- Defenders should also look for abnormal account activity, such as logons outside of regular working hours and impossible time-and-distance logons (e.g., a user logging on from two geographically separated locations simultaneously).

- Defenders should forward log files to a hardened centralized logging server, preferably on a segmented network [2.F].

Remediations

Volt Typhoon is a highly sophisticated threat actor designed to evade detection. It is recommended that if an organization determines they were victimized, even partially, by the threat actor, they follow the below remediations:

- Sever the enterprise network from the internet. If the network cannot be severed from the Internet, all non-essential traffic between the affected enterprise network and the Internet must be shut down.
- Reset credentials for all domain users and all local accounts.
- Monitor related accounts, especially administrative accounts, for any further signs of unauthorized access.
- Audit all network appliance and edge device configurations with indicators of malicious activity for signs of unauthorized or malicious configuration changes.
- Update all firmware and software to the latest version.

Additional Resources

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure; CISA, 2/7/2024 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Volt Typhoon Targets U.S. Critical Infrastructure with Living-Off-The-Land Techniques; Microsoft, 5/24/2023 https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection; CISA, 5/24/2023 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

Layering Network Security Through Segmentation; CISA, 1/2022 https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

Appendix

Volt Typhoon Activity ***Credit: Cybersecurity and Infrastructure Security Agency***