JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China (PRC) state-sponsored cyber actors are 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.

Actions to take today to mitigate Volt Typhoon activity:

- **Apply patches for internet-facing systems**. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
- **Implement phishing-resistant MFA**.
- **Ensure logging is turned on for application, access, and security logs** and store logs in a central system.
- **Plan "end of life" for technology beyond manufacturer's supported lifecycle.**

CISA, NSA, FBI and the following partners are releasing this advisory to warn critical infrastructure organizations about this assessment, which is based on observations from the U.S. authoring agencies' incident response activities at critical infrastructure organizations compromised by the PRC state-sponsored cyber group known as Volt Typhoon (also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus):

- U.S. Department of Energy (DOE)
- U.S. Environmental Protection Agency (EPA)
- U.S. Transportation Security Administration (TSA)
- Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS), a part of the Communications Security Establishment (CSE)
- United Kingdom National Cyber Security Centre (NCSC-UK)
- New Zealand National Cyber Security Centre (NCSC-NZ)

The U.S. authoring agencies have confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations—primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors—in the continental and non-continental United States and its territories, including Guam. Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions. The U.S. authoring agencies are concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts. CCCS assesses that the direct threat to Canada's critical infrastructure from PRC state-sponsored actors is likely lower than that to U.S. infrastructure, but should U.S. infrastructure be disrupted, Canada would likely be affected as well, due to cross-border integration. ASD's ACSC and NCSC-NZ assess Australian and New Zealand critical infrastructure, respectively, could be vulnerable to similar activity from PRC state-sponsored actors.

As the authoring agencies have previously highlighted, the use of living off the land (LOTL) techniques is a hallmark of Volt Typhoon actors' malicious cyber activity when targeting critical infrastructure. The group also relies on valid accounts and leverage strong operational security, which combined, allows for long-term undiscovered persistence. In fact, the U.S. authoring agencies have recently observed indications of Volt Typhoon actors maintaining access and footholds within some victim IT environments for at least five years. Volt Typhoon actors conduct extensive pre-exploitation reconnaissance to learn about the target organization and its environment; tailor their tactics, techniques, and procedures (TTPs) to the victim's environment; and dedicate ongoing resources to maintaining persistence and understanding the target environment over time, even after initial compromise.

The authoring agencies urge critical infrastructure organizations to apply the mitigations in this advisory and to hunt for similar malicious activity using the guidance herein provided, along with the recommendations found in joint guide Identifying and Mitigating Living Off the Land Techniques. These mitigations are primarily intended for IT and OT administrators in critical infrastructure organizations. Following the mitigations for prevention of or in response to an incident will help disrupt Volt Typhoon's accesses and reduce the threat to critical infrastructure entities.

If activity is identified, the authoring agencies strongly recommend that critical infrastructure organizations apply the incident response recommendations in this advisory and report the incident to the relevant agency (see Contact Information section).

For additional information, see joint advisory People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection and U.S. Department of Justice (DOJ) press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure. For more information on PRC state-sponsored malicious cyber activity, see CISA's China Cyber Threat Overview and Advisories webpage.

For a downloadable copy of indicators of compromise (IOCs), see:

- MAR-10448362-1.v1 (JSON, 60KB)

TABLE OF CONTENTS

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 14. See Appendix C: MITRE ATT&CK Tactics and Techniques section for tables of the Volt Typhoon cyber threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Overview of Activity

In May 2023, the authoring agencies—working with industry partners—disclosed information about activity attributed to Volt Typhoon (see joint advisory People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection). Since then, CISA, NSA, and FBI have determined that this activity is part of a broader campaign in which Volt Typhoon actors have successfully infiltrated the networks of critical infrastructure organizations in the continental and non-continental United States and its territories, including Guam.

The U.S. authoring agencies have primarily observed compromises linked to Volt Typhoon in Communications, Energy, Transportation Systems, and Water and Wastewater Systems sector organizations' IT networks. Some victims are smaller organizations with limited cybersecurity capabilities that provide critical services to larger organizations or key geographic locations.

Volt Typhoon actors tailor their TTPs to the victim environment; however, the U.S. authoring agencies have observed the actors typically following the same pattern of behavior across identified intrusions. Their choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable the disruption of OT functions across multiple critical infrastructure sectors (see Figure 1).

1. **Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's network architecture and operational protocols.** This reconnaissance includes identifying network topologies, security measures, typical user behaviors, and key network and IT staff. The intelligence gathered by Volt Typhoon actors is likely leveraged to enhance their operational security. For example, in some instances, Volt Typhoon actors may have abstained from using compromised credentials outside of normal working hours to avoid triggering security alerts on abnormal account activities.
2. **Volt Typhoon typically gains initial access to the IT network by exploiting known or zero-day vulnerabilities in public-facing network** appliances (e.g., routers, virtual private networks [VPNs], and firewalls) and then connects to the victim's network via VPN for follow-on activities.
3. **Volt Typhoon aims to obtain administrator credentials within the network, often by exploiting privilege escalation vulnerabilities in the operating system or network services.** In some cases, Volt Typhoon has obtained credentials insecurely stored on a public-facing network appliance.

4. **Volt Typhoon uses valid administrator credentials to move laterally to the domain controller (DC) and other devices** via remote access services such as Remote Desktop Protocol (RDP).
5. **Volt Typhoon conducts discovery in the victim's network, leveraging LOTL binaries for stealth**. A key tactic includes using PowerShell to perform targeted queries on Windows event logs, focusing on specific users and periods. These queries facilitate the discreet extraction of security event logs into `.dat` files, allowing Volt Typhoon actors to gather critical information while minimizing detection. This strategy, blending in-depth pre-compromise reconnaissance with meticulous post-exploitation intelligence collection, underscores their sophisticated and strategic approach to cyber operations.
6. **Volt Typhoon achieves full domain compromise by extracting the Active Directory database (`NTDS.dit`) from the DC.** Volt Typhoon frequently employs the Volume Shadow Copy Service (VSS) using command-line utilities such as `vssadmin` to access `NTDS.dit`. The `NTDS.dit` file is a centralized repository that contains critical Active Directory data, including user accounts, passwords (in hashed form), and other sensitive data, which can be leveraged for further exploitation. This method entails the creation of a shadow copy—a point-in-time snapshot—of the volume hosting the `NTDS.dit` file. By leveraging this snapshot, Volt Typhoon actors effectively bypass the file locking mechanisms inherent in a live Windows environment, which typically prevent direct access to the `NTDS.dit` file while the domain controller is operational.
7. **Volt Typhoon likely uses offline password cracking techniques to decipher these hashes.** This process involves extracting the hashes from the `NTDS.dit` file and then applying various password cracking methods, such as brute force attacks, dictionary attacks, or more sophisticated techniques like rainbow tables to uncover the plaintext passwords. The successful decryption of these passwords allows Volt Typhoon actors to obtain elevated access and further infiltrate and manipulate the network.
8. **Volt Typhoon uses elevated credentials for strategic network infiltration and additional discovery, often focusing on gaining capabilities to access OT assets.** Volt Typhoon actors have been observed testing access to domain-joint OT assets using default OT vendor credentials, and in certain instances, they have possessed the capability to access OT systems whose credentials were compromised via `NTDS.dit` theft. This access enables potential disruptions, such as manipulating heating, ventilation, and air conditioning (HVAC) systems in server rooms or disrupting critical energy and water controls, leading to significant infrastructure failures (in some cases, Volt Typhoon actors had the capability to access camera surveillance systems at critical infrastructure facilities). In one confirmed compromise, Volt Typhoon actors moved laterally to a control system and were positioned to move to a second control system.

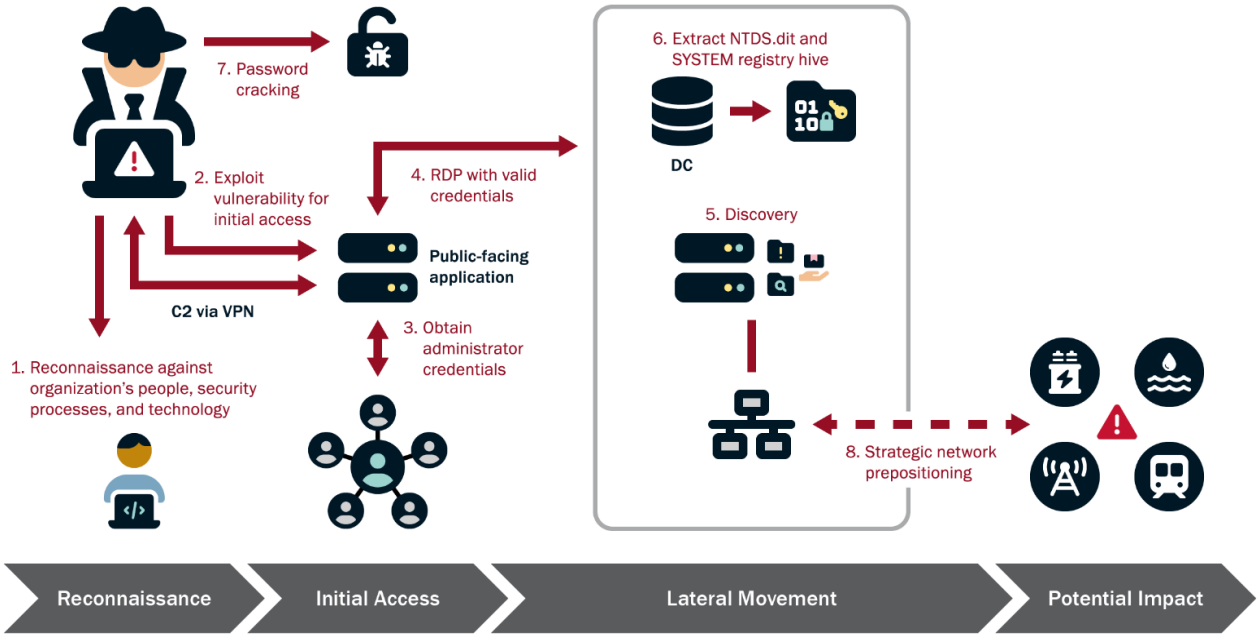

Figure 1: Typical Volt Typhoon Activity

After successfully gaining access to legitimate accounts, Volt Typhoon actors exhibit minimal activity within the compromised environment (except discovery as noted above), suggesting their objective is to maintain persistence rather than immediate exploitation. This assessment is supported by observed patterns where Volt Typhoon methodically re-targets the same organizations over extended periods, often spanning several years, to continuously validate and potentially enhance their unauthorized accesses. Evidence of their meticulous approach is seen in instances where they repeatedly exfiltrate domain credentials, ensuring access to current and valid accounts. For example, in one compromise, Volt Typhoon likely extracted `NTDS.dit` from three domain controllers in a four-year period. In another compromise, Volt Typhoon actors extracted `NTDS.dit` two times from a victim in a nine-month period.

Industry reporting—identifying that Volt Typhoon actors are silent on the network following credential dumping and perform discovery to learn about the environment, but do not exfiltrate data—is consistent with the U.S. authoring agencies' observations. This indicates their aim is to achieve and maintain persistence on the network. In one confirmed compromise, an industry partner observed Volt Typhoon actors dumping credentials at regular intervals.

In addition to leveraging stolen account credentials, the actors use LOTL techniques and avoid leaving malware artifacts on systems that would cause alerts. Their strong focus on stealth and operational security allows them to maintain long-term, undiscovered persistence. Further, Volt Typhoon's operational security is enhanced by targeted log deletion to conceal their actions within the compromised environment.

See the below sections for Volt Typhoon TTPs observed by the U.S. authoring agencies from multiple confirmed Volt Typhoon compromises.

Observed TTPs

Reconnaissance

Volt Typhoon actors conduct extensive pre-compromise reconnaissance [TA0043] to learn about the target organization [T1591], its network [T1590], and its staff [T1589]. This includes web searches [T1593]—including victim-owned sites [T1594]—for victim host [T1592], identity, and network information, especially for information on key network and IT administrators. According to industry reporting, Volt Typhoon actors use FOFA[1], Shodan, and Censys for querying or searching for exposed infrastructure. In some instances, the U.S. authoring agencies have observed Volt Typhoon actors targeting the personal emails of key network and IT staff [T1589.002] post compromise.

Resource Development

Historically, Volt Typhoon actors use multi-hop proxies for command and control (C2) infrastructure [T1090.003]. The proxy is typically composed of virtual private servers (VPSs) [T1583.003] or small office/home office (SOHO) routers. Recently, Volt Typhoon actors used Cisco and NETGEAR end-of-life SOHO routers implanted with KV Botnet malware to support their operations [T1584.005]. (See DOJ press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure for more information).

Initial Access

To obtain initial access [TA0001], Volt Typhoon actors commonly exploit vulnerabilities in networking appliances such as those from Fortinet, Ivanti Connect Secure (formerly Pulse Secure), NETGEAR, Citrix, and Cisco [T1190]. They often use publicly available exploit code for known vulnerabilities [T1588.005] but are also adept at discovering and exploiting zero-day vulnerabilities [T1587.004].

- In one confirmed compromise, Volt Typhoon actors likely obtained initial access by exploiting CVE-2022-42475 in a network perimeter FortiGate 300D firewall that was not patched. There is evidence of a buffer overflow attack identified within the Secure Sockets Layer (SSL)-VPN crash logs.

Once initial access is achieved, Volt Typhoon actors typically shift to establishing persistent access [TA0003]. They often use VPN sessions to securely connect to victim environments [T1133], enabling discreet follow-on intrusion activities. This tactic not only provides a stable foothold in the network but also allows them to blend in with regular traffic, significantly reducing their chances of detection.

Execution

Volt Typhoon actors rarely use malware for post-compromise execution. Instead, once Volt Typhoon actors gain access to target environments, they use hands-on-keyboard activity via the command-line [T1059] and other native tools and processes on systems [T1218] (often referred to as "LOLBins"), known as LOTL, to maintain and expand access to the victim networks. According to industry reporting, some "commands appear to be exploratory or experimental, as the operators [i.e., malicious actors] adjust and repeat them multiple times."[2]

For more details on LOTL activity, see the Credential Access and Discovery sections and Appendix A: Volt Typhoon LOTL Activity.

Similar to LOTL, Volt Typhoon actors also use legitimate but outdated versions of network admin tools. For example, in one confirmed compromise, actors downloaded [T1105] an outdated version of `comsvcs.dll` on the DC in a non-standard folder. `comsvcs.dll` is a legitimate Microsoft Dynamic Link Library (DLL) file normally found in the `System32` folder. The actors used this DLL with `MiniDump` and the process ID of the Local Security Authority Subsystem Service (LSASS) to dump the LSASS process memory [T1003.001] and obtain credentials (LSASS process memory space contains hashes for the current user's operating system (OS) credentials).

The actors also use legitimate non-native network admin and forensic tools. For example, Volt Typhoon actors have been observed using Magnet RAM Capture (MRC) version 1.20 on domain controllers. MRC is a free imaging tool that captures the physical memory of a computer, and Volt Typhoon actors likely used it to analyze in-memory data for sensitive information (such as credentials) and in-transit data not typically accessible on disk. Volt Typhoon actors have also been observed implanting Fast Reverse Proxy (FRP) for command and control.[3] (See the Command and Control section).

Persistence

Volt Typhoon primarily relies on valid credentials for persistence [T1078].

Defense Evasion

Volt Typhoon has strong operational security. Their actors primarily use LOTL for defense evasion [TA0005], which allows them to camouflage their malicious activity with typical system and network behavior, potentially circumventing simplistic endpoint security capabilities. For more information, see joint guide Identifying and Mitigating Living off the Land Techniques.

Volt Typhoon actors also obfuscate their malware. In one confirmed compromise, Volt Typhoon obfuscated FRP client files (`BrightmetricAgent.exe` and `SMSvcService.exe`) and the command-line port scanning utility ScanLine by packing the files with Ultimate Packer for Executables (UPX) [T1027.002]. FRP client applications support encryption, compression, and easy token authentication and work across multiple protocols—including transmission control protocol (TCP), user datagram protocol (UDP), hypertext transfer protocol (HTTP), and hypertext transfer protocol secure (HTTPS). The FRP client applications use the Kuai connection protocol (KCP) for error-checked and anonymous data stream delivery over UDP, with packet-level encryption support. See Appendix C and CISA Malware Analysis Report (MAR)-10448362-1.v1 for more information.

In addition to LOTL and obfuscation techniques, Volt Typhoon actors have been observed selectively clearing Windows Event Logs [T1070.001], system logs, and other technical artifacts to remove evidence [T1070.009] of their intrusion activity and masquerading file names [T1036.005].

Credential Access

Volt Typhoon actors first obtain credentials from public-facing appliances after gaining initial access by exploiting privilege escalation vulnerabilities [T1068] in the operating system or network services.

In some cases, they have obtained credentials insecurely stored on the appliance [T1552]. In one instance, where Volt Typhoon likely exploited CVE-2022-42475 in an unpatched Fortinet device, Volt Typhoon actors compromised a domain admin account stored inappropriately on the device.

Volt Typhoon also consistently obtains valid credentials by extracting the Active Directory database file (`NTDS.dit`)—in some cases multiple times from the same victim over long periods [T1003.003]. `NTDS.dit` contains usernames, hashed passwords, and group memberships for all domain accounts, essentially allowing for full domain compromise if the hashes can be cracked offline.

To obtain `NTDS.dit`, the U.S. authoring agencies have observed Volt Typhoon:

1. Move laterally [TA0008] to the domain controller via an interactive RDP session using a compromised account with domain administrator privileges [T1021.001];
2. Execute the Windows-native `vssadmin` [T1006] command to create a volume shadow copy;
3. Use Windows Management Instrumentation Console (WMIC) commands [T1047] to execute `ntdsutil` (a LOTL utility) to copy `NTDS.dit` and `SYSTEM` registry hive from the volume shadow copy; and
4. Exfiltrate [TA0010] `NTDS.dit` and `SYSTEM` registry hive to crack passwords offline) [T1110.002]. (For more details, including specific commands used, see Appendix A: Volt Typhoon LOTL Activity.)
   Note: A volume shadow copy contains a copy of all the files and folders that exist on the specified volume. Each volume shadow copy created on a DC includes its `NTDS.dit` and the `SYSTEM` registry hive, which provides keys to decrypt the `NTDS.dit` file.

Volt Typhoon actors have also been observed interacting with a PuTTY application by enumerating existing stored sessions [T1012]. Given this interaction and the exposure of cleartext-stored proxy passwords used in remote administration, Volt Typhoon actors potentially had access to PuTTY profiles that allow access to critical systems (see the Lateral Movement section).

According to industry reporting, Volt Typhoon actors attempted to dump credentials through LSASS (see Appendix B for commands used).[2]

The U.S. authoring agencies have observed Volt Typhoon actors leveraging Mimikatz to harvest credentials, and industry partners have observed Volt Typhoon leveraging Impacket.[2]

- Mimikatz is a credential dumping tool and Volt Typhoon actors use it to obtain credentials. In one confirmed compromise, the Volt Typhoon used RDP to connect to a server and run Mimikatz after leveraging a compromised administrator account to deploy it.
- Impacket is an open source Python toolkit for programmatically constructing and manipulating network protocols. It contains tools for Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks—as well as remote service execution.

Discovery

Volt Typhoon actors have been observed using commercial tools, LOTL utilities, and appliances already present on the system for system information [T1082], network service [T1046], group [T1069] and user [T1033] discovery.

Volt Typhoon uses at least the following LOTL tools and commands for system information, network service, group, and user discovery techniques:

- cmd
- certutil
- dnscmd
- ldifde
- makecab
- net user/group/use
- netsh
- nltest
- netstat
- ntdsutil
- ping
- PowerShell
- quser
- reg query/reg save
- systeminfo
- tasklist
- wevtutil
- whoami
- wmic
- xcopy

Some observed specific examples of discovery include:

- Capturing successful logon events [T1654].
  - Specifically, in one incident, analysis of the PowerShell console history of a domain controller indicated that security event logs were directed to a file named `user.dat`, as evidenced by the executed command `Get-EventLog security -instanceid 4624 -after [year-month-date] | fl * | Out-File 'C:\users\public\documents\user.dat'`. This indicates the group's specific interest in capturing successful logon events (event ID `4624`) to analyze user authentication patterns within the network. Additionally, file system analysis, specifically of the Master File Table (MFT), uncovered evidence of a separate file, `systeminfo.dat`, which was created in `C:\Users\Public\Documents` but subsequently deleted [T1070.004]. The presence of these activities suggests a methodical approach by Volt Typhoon actors in collecting and then possibly removing traces of sensitive log information from the compromised system.
- Executing `tasklist /v` to gather a detailed process listing [T1057], followed by executing `taskkill /f /im rdpservice.exe` (the function of this executable is not known).
- Executing `net user` and `quser` for user account information [T1087.001].
- Creating and accessing a file named `rult3uil.log` on a domain controller in `C:\Windows\System32\`. The `rult3uil.log` file contained user activities on a compromised system, showcasing a combination of window title information [T1010] and focus shifts, keypresses, and command executions across Google Chrome and Windows PowerShell, with corresponding timestamps.
- Employing `ping` with various IP addresses to check network connectivity [T1016.001] and `net start` to list running services [T1007].

See Appendix A for additional LOTL examples.

In one confirmed compromise, Volt Typhoon actors attempted to use Advanced IP Scanner, which was on the network for admin use, to scan the network.

Volt Typhoon actors have been observed strategically targeting network administrator web browser data—focusing on both browsing history and stored credentials [T1555.003]—to facilitate targeting of personal email addresses (see the Reconnaissance section) for further discovery and possible network modifications that may impact the threat actor's persistence within victim networks.

In one confirmed compromise:

- Volt Typhoon actors obtained the history file from the `User Data` directory of a network administrator user's Chrome browser. To obtain the history file, Volt Typhoon actors first executed an RDP session to the user's workstation where they initially attempted, and failed, to obtain the `C$ File Name: users\{redacted}\appdata\local\Google\Chrome\UserData\default\History` file, as evidenced by the accompanying `1016` (reopen failed) SMB error listed in the application event log. The threat actors then disconnected the RDP session to the workstation and accessed the file `C:\Users\{redacted}\Downloads\History.zip`. This file presumably contained data from the `User Data` directory of the user's Chrome browser, which the actors likely saved in the Downloads directory for exfiltration [T1074]. Shortly after accessing the `history.zip` file, the actors terminated RDP sessions.
- About four months later, Volt Typhoon actors accessed the same user's Chrome data `C$ File Name: Users\{redacted}\AppData\Local\Google\Chrome\User Data\Local State` and `$ File Name: Users\{redacted}\AppData\Local\Google\Chrome\User Data\Default\Login Data` via SMB. The Local State file contains the Advanced Encryption Standard (AES) encryption key [T1552.004] used to encrypt the passwords stored in the Chrome browser, which would enable the actors to obtain plaintext passwords stored in the Login Data file in the Chrome browser.

In another confirmed compromise, Volt Typhoon actors accessed directories containing Chrome and Edge user data on multiple systems. Directory interaction was observed over the network to paths such as `C:\Users\{redacted}\AppData\Local\Google\Chrome\User Data\` and `C:\Users\{redacted}\AppData\Local\Microsoft\Edge\User Data\`. They also enumerated several directories, including directories containing vulnerability testing and cyber related content and facilities data, such as construction drawings [T1083].

Lateral Movement

For lateral movement, Volt Typhoon actors have been observed predominantly employing RDP with compromised valid administrator credentials. **Note:** With a full on-premises Microsoft Active Directory identity compromise (see the Credential Access section), the group may be capable of using other methods such as Pass the Hash or Pass the Ticket for lateral movement [T1550].

In one confirmed compromise of a Water and Wastewater Systems Sector entity, after obtaining initial access, Volt Typhoon actors connected to the network via a VPN with administrator credentials they obtained and opened an RDP session with the same credentials to move laterally. Over a nine-month period, they moved laterally to a file server, a domain controller, an Oracle Management Server (OMS), and a VMware vCenter server. The actors obtained domain credentials from the domain controller and performed discovery, collection, and exfiltration on the file server (see the Discovery and Collection and Exfiltration sections).

Volt Typhoon's movement to the vCenter server was likely strategic for pre-positioning to OT assets. The vCenter server was adjacent to OT assets, and Volt Typhoon actors were observed interacting with the PuTTY application on the server by enumerating existing stored sessions. With this

information, Volt Typhoon potentially had access to a range of critical PuTTY profiles, including those for water treatment plants, water wells, an electrical substation, OT systems, and network security devices. This would enable them to access these critical systems [T1563]. See Figure 2.

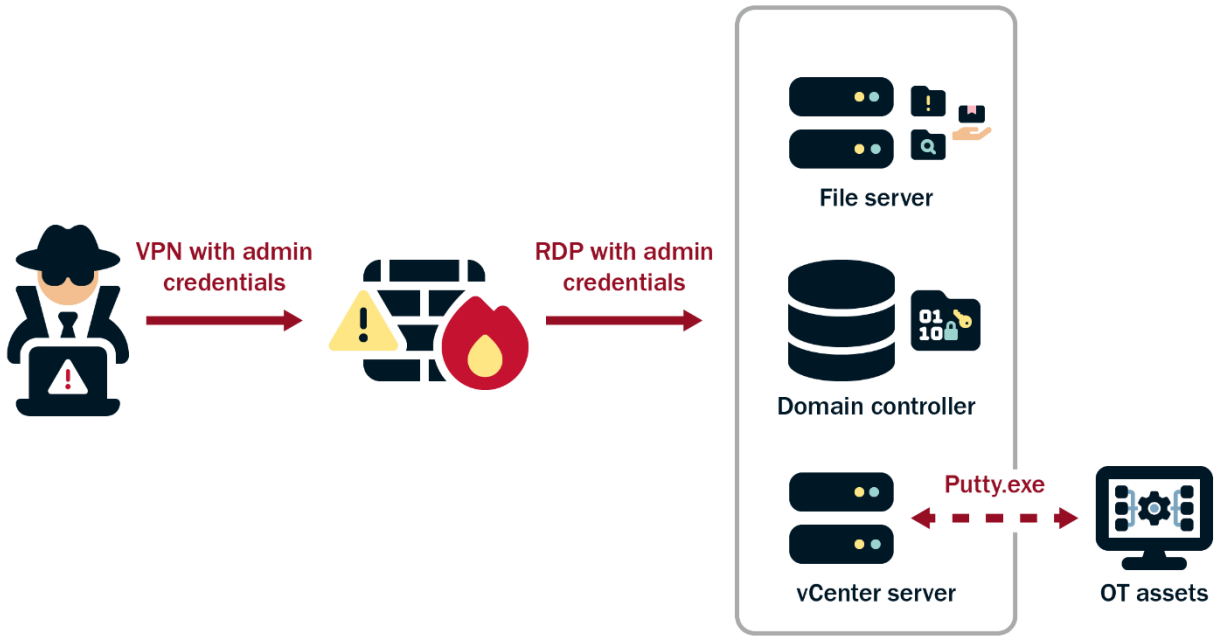

Figure 2: Volt Typhoon Lateral Movement Path File Server, DC, and OT-Adjacent Assets

Additionally, Volt Typhoon actors have been observed using PSExec to execute remote processes, including the automated acceptance of the end-user license agreement (EULA) through an administrative account, signified by the `accepteula` command flag.

Volt Typhoon actors may have attempted to move laterally to a cloud environment in one victim's network but direct attribution to the Volt Typhoon group was inconclusive. During the period of the their known network presence, there were anomalous login attempts to an Azure tenant [T1021.007] potentially using credentials [T1078.004] previously compromised from theft of `NTDS.dit`. These attempts, coupled with misconfigured virtual machines with open RDP ports, suggested a potential for cloud-based lateral movement. However, subsequent investigations, including password changes and multifactor authentication (MFA) implementations, revealed authentication failures from non-associated IP addresses, with no definitive link to Volt Typhoon.

Collection and Exfiltration

The U.S. authoring agencies assess Volt Typhoon primarily collects information that would facilitate follow-on actions with physical impacts. For example, in one confirmed compromise, they collected [TA0009] sensitive information obtained from a file server in multiple zipped files [T1560] and likely exfiltrated [TA0010] the files via Server Message Block (SMB) [T1048] (see Figure 3). Collected information included diagrams and documentation related to OT equipment, including supervisory

control and data acquisition (SCADA) systems, relays, and switchgear. This data is crucial for understanding and potentially impacting critical infrastructure systems, indicating a focus on gathering intelligence that could be leveraged in actions targeting physical assets and systems.

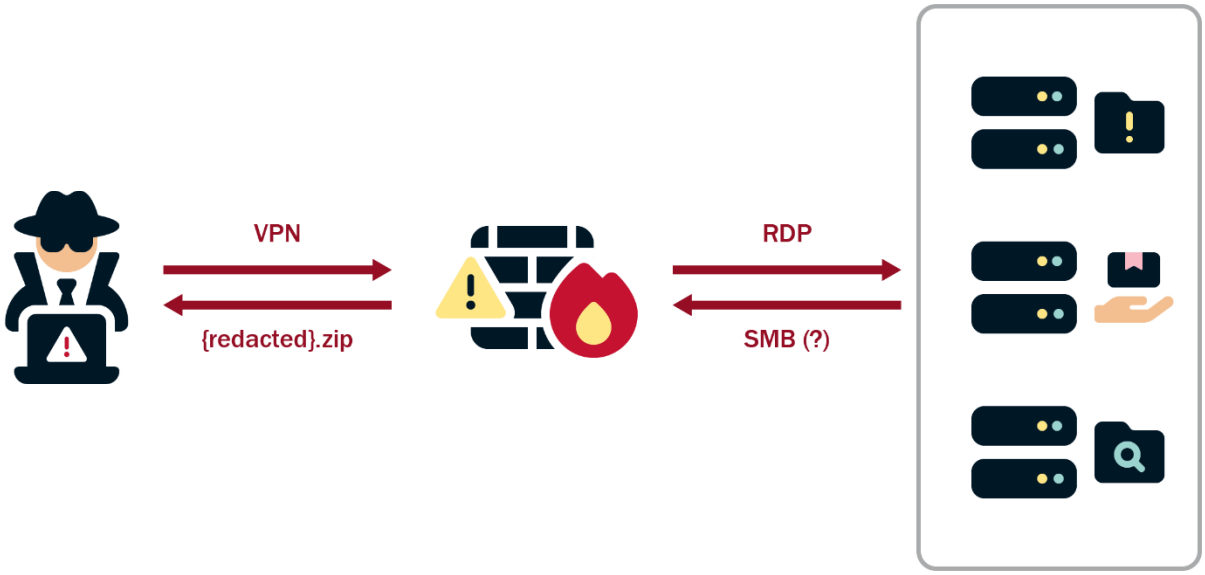

Figure 3: Volt Typhoon Attack Path for Exfiltration of Data from File Server

In another compromise, Volt Typhoon actors leveraged WMIC to create and use temporary directories (`C:\Users\Public\pro`, `C:\Windows\Temp\tmp`, `C:\Windows\Temp\tmp\Active Directory` and `C:\Windows\Temp\tmp\registry`) to stage the extracted `ntds.dit` and `SYSTEM` registry hives from `ntdsutil` execution volume shadow copies (see the Credential Access section) obtained from two DCs. They then compressed and archived the extracted `ntds.dit` and accompanying registry files by executing `ronf.exe`, which was likely a renamed version of the archive utility `rar.exe`) [T1560.001].

Command and Control

Volt Typhoon actors have been observed leveraging compromised SOHO routers and virtual private servers (VPS) to proxy C2 traffic. For more information, see DOJ press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure).

They have also been observed setting up FRP clients [T1090] on a victim's corporate infrastructure to establish covert communications channels [T1573] for command and control. In one instance, Volt Typhoon actors implanted the FRP client with filename `SMSvcService.exe` on a Shortel Enterprise Contact Center (ECC) server and a second FRP client with filename `Brightmetricagent.exe` on another server. These clients, when executed via PowerShell [T1059.001], open reverse proxies between the compromised system and Volt Typhoon C2 servers. `Brightmetricagent.exe` has

additional capabilities. The FRP client can locate servers behind a network firewall or obscured through Network Address Translation (NAT) [T1016]. It also contains multiplexer libraries that can bi-directionally stream data over NAT networks and contains a command-line interface (CLI) library that can leverage command shells such as PowerShell, Windows Management Instrumentation (WMI), and Z Shell (zsh) [T1059.004]. See Appendix C and MAR-10448362-1.v1 for more information.

In the same compromise, Volt Typhoon actors exploited a Paessler Router Traffic Grapher (PRTG) server as an intermediary for their FRP operations. To facilitate this, they used the `netsh` command, a legitimate Windows command, to create a PortProxy registry modification [T1112] on the PRTG server [T1090.001]. This key alteration redirected specific port traffic to Volt Typhoon's proxy infrastructure, effectively converting the PRTG's server into a proxy for their C2 traffic [T1584.004] (see Appendix B for details).

DETECTION/HUNT RECOMMENDATIONS

Apply Living off the Land Detection Best Practices

Apply the prioritized detection and hardening best practice recommendations provided in joint guide Identifying and Mitigating Living off the Land Techniques. Many organizations lack security and network management best practices (such as established baselines) that support detection of malicious LOTL activity—this makes it difficult for network defenders to discern legitimate behavior from malicious behavior and conduct behavior analytics, anomaly detection, and proactive hunting. Conventional IOCs associated with the malicious activity are generally lacking, complicating network defenders' efforts to identify, track, and categorize this sort of malicious behavior. This advisory provides guidance for a multifaceted cybersecurity strategy that enables behavior analytics, anomaly detection, and proactive hunting, which are part of a comprehensive approach to mitigating cyber threats that employ LOTL techniques.

Review Application, Security, and System Event Logs

Routinely review application, security, and system event logs, focusing on Windows Extensible Storage Engine Technology (ESENT) Application Logs. Due to Volt Typhoon's ability for long-term undetected persistence, network defenders should assume significant dwell time and review specific application event log IDs, which remain on endpoints for longer periods compared to security event logs and other ephemeral artifacts. Focus on Windows ESENT logs because certain ESENT Application Log event IDs (`216`, `325`, `326`, and `327`) may indicate actors copying `NTDS.dit`.

See Table 1 for examples of ESENT and other key log indicators that should be investigated. Please note that incidents may not always have exact matches listed in the Event Detail column due to variations in event logging and TTPs.

Table 1: Key Log Indicators for Detecting Volt Typhoon Activity

Event ID (Log)	Event Detail	Description
216 (Windows ESENT Application Log)	A database location change was detected from 'C:\Windows\NTDS\ntds.dit' to '\\?\GLOBALROOT\Device\{redacted}VolumeShadowCopy1\Windows\NTDS\ntds.dit'	A change in the `NTDS.dit` database location is detected. This could suggest an initial step in NTDS credential dumping where the database is being prepared for extraction.
325 (Windows ESENT Application Log)	The database engine created a new database (2, C:\Windows\Temp\tmp\Active Directory\ntds.dit).	Indicates creation of a new `NTDS.dit` file in a non-standard directory. Often a sign of data staging for exfiltration. Monitor for unusual database operations in temp directories.
637 (Windows ESENT Application Log)	C:\Windows\Temp\tmp\Active Directory\ntds.jfm-++- (0) New flush map file “C:\Windows\Temp\tmp\Active Directory\ntds.jfm” will be created to enable persisted lost flush detection.	A new flush map file is being created for `NTDS.dit`. This may suggest ongoing operations related to NTDS credential dumping, potentially capturing uncommitted changes to the `NTDS.dit` file.
326 (Windows ESENT Application Log)	NTDS-++-12460,D,100-++--++-1-++- C:\$SNAP_{redacted}_VOLUMEC$\Windows\NTDS\ntds.dit-++-0-++- [1] The database engine attached a database. Began mounting of C:\Windows\NTDS\ntds.dit file created from volume shadow copy process	Represents the mounting of an `NTDS.dit` file from a volume shadow copy. This is a critical step in NTDS credential dumping, indicating active manipulation of a domain controller’s data.

Event ID (Log)	Event Detail	Description
327 (Windows ESENT Application Log)	C:\Windows\Temp\tmp\Active Directory\ntds.dit-++-1-++- [1] The database engine detached a database (2, C:\Windows\Temp\tmp\Active Directory\ntds.dit). Completion of mounting of ntds.dit file to C:\Windows\Temp\tmp\Active Director	The detachment of a database, particularly in a temp directory, could indicate the completion of a credential dumping process, potentially as part of exfiltration preparations.
21 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session logon succeeded: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful authentication to a Remote Desktop Services session.
22 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Shell start notification received: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful start of a new Remote Desktop session. This may imply lateral movement or unauthorized remote access, especially if the user or session is unexpected.
23 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session logoff succeeded: User: {redacted}\{redacted} Session ID: {redacted}	Successful logoff of Remote Desktop session.
24 (Windows Terminal Services Local	Remote Desktop Services: Session has been disconnected: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Remote Desktop session disconnected by user or due to network connectivity issues.

Event ID (Log)	Event Detail	Description
Session Manager Operational Log)		
25 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session reconnection succeeded: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Successful reconnection to a Remote Desktop Services session. This may imply lateral movement or unauthorized remote access, especially if the user or session is unexpected.
1017 (Windows System Log)	Handle scavenged. Share Name: C$ File Name: users\{redacted}\downloads\History.zip Durable: 1 Resilient or Persistent: 0 Guidance: The server closed a handle that was previously reserved for a client after 60 seconds.	Indicates the server closed a handle for a client. While common in network operations, unusual patterns or locations (like `History.zip` in a user's downloads) may suggest data collection from a local system.
1102 (Windows Security Log)	All	All Event ID `1102` entries should be investigated as logs are generally not cleared and this is a known Volt Typhoon tactic to cover their tracks.

Monitor and Review OT System Logs

- Review access logs for communication paths between IT and OT networks, looking for anomalous accesses or protocols.
- Measure the baseline of normal operations and network traffic for the industrial control system (ICS) and assess traffic anomalies for malicious activity.
- Configure intrusion detection systems (IDS) to create alarms for any ICS network traffic outside normal operations.
- Track and monitor audit trails on critical areas of ICS.

- Set up security incident and event monitoring (SIEM) to monitor, analyze, and correlate event logs from across the ICS network to identify intrusion attempts.

Review CISA's Recommended Cybersecurity Practices for Industrial Control Systems and the joint advisory, NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems, for further OT system detection and mitigation guidance.

Use gait to Detect Possible Network Proxy Activities

Use gait[4] to detect network proxy activities. Developed by Sandia National Labs, gait is a publicly available Zeek[5] extension. The gait extension can help enrich Zeek's network connection monitoring and SSL logs by including additional metadata in the logs. Specifically, gait captures unique TCP options and timing data such as a TCP, transport layer security (TLS), and Secure Shell (SSH) layer inferred round trip times (RTT), aiding in the identification of the software used by both endpoints and intermediaries.

While the gait extension for Zeek is an effective tool for enriching network monitoring logs with detailed metadata, it is not specifically designed to detect Volt Typhoon actor activities. The extension's capabilities extend to general anomaly detection in network traffic, including—but not limited to—proxying activities. Therefore, while gait can be helpful in identifying tactics similar to those used by Volt Typhoon, such as proxy networks and FRP clients for C2 communication, not all proxying activities detected by using this additional metadata are necessarily indicative of Volt Typhoon presence. It serves as a valuable augmentation to current security stacks for a broader spectrum of threat detection.

For more information, see Sandia National Lab's gait GitHub page sandialabs/gait: Zeek Extension to Collect Metadata for Profiling of Endpoints and Proxies.

Review Logins for Impossible Travel

Examine VPN or other account logon times, frequency, duration, and locations. Logons from two geographically distant locations within a short timeframe from a single user may indicate an account is being used maliciously. Logons of unusual frequency or duration may indicate a threat actor attempting to access a system repeatedly or maintain prolonged sessions for the purpose of data extraction.

Review Standard Directories for Unusual Files

Review directories, such as `C:\windows\temp\` and `C:\users\public\`, for unexpected or unusual files. Monitor these temporary file storage directories for files typically located in standard system paths, such as the `System32` directory. For example, Volt Typhoon has been observed downloading `comsvcs.dll` to a non-standard folder (this file is normally found in the `System32` folder).

INCIDENT RESPONSE

If compromise, or potential compromise, is detected, **organizations should assume full domain compromise** because of Volt Typhoon's known behavioral pattern of extracting the `NTDS.dit` from

the DCs. Organizations should immediately implement the following immediate, defensive countermeasures:

1. **Sever the enterprise network from the internet. Note:** this step requires the agency to understand its internal and external connections. When making the decision to sever internet access, knowledge of connections must be combined with care to avoid disrupting critical functions.
   a. If you cannot sever from the internet, **shutdown all non-essential traffic between the affected enterprise network and the internet**.
2. **Reset credentials of privileged and non-privileged accounts within the trust boundary of each compromised account**.
   a. Reset passwords for all domain users and all local accounts, such as `Guest`, `HelpAssistant`, `DefaultAccount`, `System`, `Administrator`, and `krbtgt`. The `krbtgt` account is responsible for handling Kerberos ticket requests as well as encrypting and signing them. The `krbtgt` account should be reset twice because the account has a two-password history. The first account reset for the `krbtgt` needs to be allowed to replicate prior to the second reset to avoid any issues. See CISA's Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise for more information. Although tailored to FCEB agencies compromised in the 2020 SolarWinds Orion supply chain compromise, the steps are applicable to organizations with Windows AD compromise.
      i) Review access policies to temporarily revoke privileges/access for affected accounts/devices. If it is necessary to not alert the attacker (e.g., for intelligence purposes), then privileges can be reduced for affected accounts/devices to "contain" them.
   b. Reset the relevant account credentials or access keys if the investigation finds the threat actor's access is limited to non-elevated permissions.
      i) Monitor related accounts, especially administrative accounts, for any further signs of unauthorized access.
3. Audit all network appliance and edge device configurations with indicators of malicious activity for signs of unauthorized or malicious configuration changes. Organizations should ensure they audit the current network device running configuration and any local configurations that could be loaded at boot time. If configuration changes are identified:
   a. Change all credentials being used to manage network devices, to include keys and strings used to secure network device functions (SNMP strings/user credentials, IPsec/IKE preshared keys, routing secrets, TACACS/RADIUS secrets, RSA keys/certificates, etc.).
   b. Update all firmware and software to the latest version.
4. **Report the compromise to an authoring agency** (see the Contact Information section).
5. For organizations with cloud or hybrid environments, **apply best practices for identity and credential access management.**
   a. Verify that all accounts with privileged role assignments are cloud native, not synced from Active Directory.

   b. Audit conditional access policies to ensure Global Administrators and other highly privileged service principals and accounts are not exempted.
   c. Audit privileged role assignments to ensure adherence to the principle of least privilege when assigning privileged roles.
   d. Leverage just-in-time and just-enough access mechanisms when administrators need to elevate to a privileged role.
   e. In hybrid environments, ensure federated systems (such as AD FS) are configured and monitored properly.
   f. Audit Enterprise Applications for recently added applications and examine the API permissions assigned to each.
6. **Reconnect to the internet. Note:** The decision to reconnect to the internet depends on senior leadership's confidence in the actions taken. It is possible—depending on the environment—that new information discovered during pre-eviction and eviction steps could add additional eviction tasks.
7. **Minimize and control use of remote access tools and protocols** by applying best practices from joint Guide to Securing Remote Access Software and joint Cybersecurity Information Sheet: Keeping PowerShell: Security Measures to Use and Embrace.
8. **Consider sharing technical information with an authoring agency and/or a sector-specific information sharing and analysis center.**

For more information on incident response and remediation, see:

- Joint advisory Technical Approaches to Uncovering and Remediating Malicious Activity. This advisory provides incident response best practices.
- CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to U.S. Federal Civilian Executive Branch (FCEB) agencies, the playbooks are applicable to all organizations. The incident response playbook provides procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents.
- Joint Water and Wastewater Sector - Incident Response Guide. This joint guide provides incident response best practices and information on federal resources for Water and Wastewater Systems Sector organizations.

MITIGATIONS

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of Volt Typhoon activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

These mitigations are intended for IT administrators in critical infrastructure organizations. The authoring agencies recommend that software manufactures incorporate secure by design and default principles and tactics into their software development practices to strengthen the security posture for their customers.

For information on secure by design practices that may protect customers against common Volt Typhoon techniques, see joint guide Identifying and Mitigating Living off the Land Techniques and joint Secure by Design Alert Security Design Improvements for SOHO Device Manufacturers.

For more information on secure by design, see CISA's Secure by Design webpage and joint guide.

IT Network Administrators and Defenders

Harden the Attack Surface

- **Apply patches for internet-facing systems within a risk-informed span of time** [CPG 1E]. Prioritize patching critical assets, known exploited vulnerabilities, and vulnerabilities in appliances known to be frequently exploited by Volt Typhoon (e.g., Fortinet, Ivanti, NETGEAR, Citrix, and Cisco devices).
- **Apply vendor-provided or industry standard hardening guidance** to strengthen software and system configurations. **Note:** As part of CISA's Secure by Design campaign, CISA urges software manufacturers to prioritize secure by default configurations to eliminate the need for customer implementation of hardening guidelines.
- **Maintain and regularly update an inventory of all organizational IT assets** [CPG 1A].
- **Use third party assessments to validate current system and network security compliance** via security architecture reviews, penetration tests, bug bounties, attack surface management services, incident simulations, or table-top exercises (both announced and unannounced) [CPG 1F].
- **Limit internet exposure of systems when not necessary**. An organization's primary attack surface is the combination of the exposure of all its internet-facing systems. Decrease the attack surface by not exposing systems or management interfaces to the internet when not necessary.
- **Plan "end of life" for technology beyond manufacturer supported lifecycle**. Inventories of organizational assets should be leveraged in patch and configuration management as noted

above. Inventories will also enable identification of technology beyond the manufacturer's supported lifecycle. Where technology is beyond "end of life" or "end of support," additional cybersecurity vigilance is necessary, and may warrant one or more of the following:

- Supplemental support agreements;
- Additional scanning and testing;
- Configuration changes;
- Isolation;
- Segmentation; and
- Development of forward-looking plans to facilitate replacement.

Secure Credentials

- **Do not store credentials on edge appliances/devices.** Ensure edge devices do not contain accounts that could provide domain admin access.
- **Do not store plaintext credentials on any system** [CPG 2L]. Credentials should be stored securely—such as with a credential/password manager or vault, or other privileged account management solutions—so they can only be accessed by authenticated and authorized users.
- **Change default passwords** [CPG 2A] and ensure they meet the policy requirements for complexity.
- Implement and enforce an organizational system-enforced policy that:
  - **Requires passwords for all IT password-protected assets to be at least 15 characters;**
  - **Does not allow users to reuse passwords for accounts, applications, services**, etc., [CPG 2C]; and
  - **Does not allow service accounts/machine accounts to reuse passwords** from member user accounts.
- **Configure Group Policy settings to prevent web browsers from saving passwords** and disable autofill functions.
- **Disable the storage of clear text passwords in LSASS memory**.

Secure Accounts

- **Implement phishing-resistant MFA** for access to assets [CPG 2H].
- **Separate user and privileged accounts**.
  - User accounts should never have administrator or super-user privileges [CPG 2E].
  - Administrators should never use administrator accounts for actions and activities not associated with the administrator role (e.g., checking email, web browsing).
- **Enforce the principle of least privilege**.
  - **Ensure administrator accounts only have the minimum permissions** necessary to complete their tasks.
  - **Review account permissions for default/accounts for edge appliances/devices and remove domain administrator privileges,** if identified.

  - **Significantly limit the number of users with elevated privileges**. Implement continuous monitoring for changes in group membership, especially in privileged groups, to detect and respond to unauthorized modifications.
  - **Remove accounts from high-privilege groups like Enterprise Admins and Schema Admins**. Temporarily reinstate these privileges only when necessary and under strict auditing to reduce the risk of privilege abuse.
  - **Transition to Group Managed Service Accounts (gMSAs)** where suitable for enhanced management and security of service account credentials. gMSAs provide automated password management and simplified Service Principal Name (SPN) management, enhancing security over traditional service accounts. See Microsoft's Group Managed Service Accounts Overview.
- **Enforce strict policies via Group Policy and User Rights Assignments** to limit high-privilege service accounts.
- **Consider using a privileged access management (PAM) solution** to manage access to privileged accounts and resources [CPG 2L]. PAM solutions can also log and alert usage to detect any unusual activity.
- **Complement the PAM solution with role-based access control (RBAC)** for tailored access based on job requirements. This ensures that elevated access is granted only when required and for a limited duration, minimizing the window of opportunity for abuse or exploitation of privileged credentials.
- **Implement an Active Directory tiering model to segregate administrative accounts** based on their access level and associated risk. This approach reduces the potential impact of a compromised account. See Microsoft's PAM environment tier model.
- **Harden administrative workstations** to only permit administrative activities from workstations appropriately hardened based on the administrative tier. See Microsoft's Why are privileged access devices important - Privileged access.
- **Disable all user accounts and access to organizational resources of employees on the day of their departure** [CPG 2G]
- **Regularly audit all user, admin, and service accounts** and remove or disable unused or unneeded accounts as applicable.
- **Regularly roll NTLM hashes of accounts that support token-based authentication.**
- Improve management of hybrid (cloud and on-premises) identity federation by:
  - **Using cloud only administrators that are asynchronous with on-premises environments** and ensuring on-premises administrators are asynchronous to the cloud.
  - **Using CISA's SCuBAGear tool to discover cloud misconfigurations in Microsoft cloud tenants**. SCuBA gear is automation script for comparing Federal Civilian Executive Branch (FCEB) agency tenant configurations against CISA M365 baseline recommendations. SCuBAGear is part of CISA's Secure Cloud Business Applications (SCuBA) project, which provides guidance for FCEB agencies, securing their cloud business application environments and protecting federal information created, accessed, shared, and stored in those environments. Although tailored to FCEB agencies, the project provides security guidance applicable to all organizations with cloud environments. For

more information on SCuBAGear see CISA's Secure Cloud Business Applications (SCuBA) Project.
    - **Using endpoint detection and response capabilities to actively** defend on-premises federation servers.

Secure Remote Access Services

- **Limit the use of RDP and other 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.
- **Disable Server Message Block (SMB) protocol version 1 and upgrade to version 3 (SMBv3)** after mitigating existing dependencies (on existing systems or applications), as they may break when disabled.
- **Harden SMBv3** by implementing guidance included in joint #StopRansomware Guide (see page 8 of the guide).
- **Apply mitigations from the joint Guide to Securing Remote Access Software**.

Secure Sensitive Data

- **Securely store sensitive data** (including operational technology documentation, network diagrams, etc.), ensuring that only authenticated and authorized users can access the data.

Implement Network Segmentation

- **Ensure that sensitive accounts use their administrator credentials only on hardened, secure computers**. This practice can reduce lateral movement exposure within networks.
- **Conduct comprehensive trust assessments to identify business-critical trusts and apply necessary controls** to prevent unauthorized cross-forest/domain traversal.
- **Harden federated authentication by enabling Secure Identifier (SID) Filtering and Selective Authentication on AD trust relationships** to further restrict unauthorized access across domain boundaries.
- **Implement network segmentation to isolate federation servers** from other systems and limit allowed traffic to systems and protocols that require access in accordance with Zero Trust principles.

Secure Cloud Assets

- **Harden cloud assets** in accordance with vendor-provided or industry standard hardening guidance.
    - Organizations with Microsoft cloud infrastructure, see CISA's Microsoft 365 Security Configuration Baseline Guides, which provide minimum viable secure configuration baselines for Microsoft Defender for Office 365, Azure Active Directory (now known as Microsoft Entra ID), Exchange Online, OneDrive for Business, Power BI, Power Platform, SharePoint Online, and Teams. For additional guidance, see the Australian Signals Directorate's Blueprint for Secure Cloud.

  - Organizations with Google cloud infrastructure, see CISA's Google Workspace Security Configuration Baseline Guides, which provide minimum viable secure configuration baselines for Groups for Business, GMAIL, Google Calendar, Google Chat, Google Common Controls, Google Classroom, Google Drive and Docs, Google Meet, and Google Sites.
- **Revoke unnecessary public access to cloud environment.** This involves reviewing and restricting public endpoints and ensuring that services like storage accounts, databases, and virtual machines are not publicly accessible unless absolutely necessary. Disable legacy authentication protocols across all cloud services and platforms. Legacy protocols frequently lack support for advanced security mechanisms such as multifactor authentication, rendering them susceptible to compromises. Instead, enforce the use of modern authentication protocols that support stronger security features like MFA, token-based authentication, and adaptive authentication measures.
  - **Enforce this practice through the use of Conditional Access Policies**. These policies can initially be run in `report-only` mode to identify potential impacts and plan mitigations before fully enforcing them. This approach allows organizations to systematically control access to their cloud resources, significantly reducing the risk of unauthorized access and potential compromise.
- **Regularly monitor and audit privileged cloud-based accounts**, including service accounts, which are frequently abused to enable broad cloud resource access and persistence.

Be Prepared

- **Ensure logging is turned on for application, access, and security logs** (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, and VPNs) [CPG 2T]. Given Volt Typhoon's use of LOTL techniques and their significant dwell time, application event logs may be a valuable resource to hunt for Volt Typhoon activity because these logs typically remain on endpoints for relatively long periods of time.
  - For OT assets where logs are non-standard or not available, **collect network traffic and communications between those assets and other assets**.
  - Implement file integrity monitoring (FIM) tools to detect unauthorized changes.
- **Store logs in a central system**, such as a security information and event management (SIEM) tool or central database.
  - **Ensure the logs can only be accessed or modified by authorized and authenticated users** [CPG 2U].
  - **Store logs for a period informed by risk or pertinent regulatory guidelines**.
  - **Tune log alerting to reduce noise while ensuring there are alerts for high-risk activities**. (For information on alert tuning, see joint guide Identifying and Mitigating Living Off the Land Techniques.)
- **Establish and continuously maintain a baseline of installed tools and software, account behavior, and network traffic**. This way, network defenders can identify potential outliers, which may indicate malicious activity. **Note:** For information on establishing a baseline, see joint guide Identifying and Mitigating Living off the Land Techniques.

- **Document a list of threats and cyber actor TTPs relevant to your organization** (e.g., based on industry or sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats [CPG 3A].
- **Implement periodic training for all employees and contractors that covers basic security concepts** (such as phishing, business email compromise, basic operational security, password security, etc.), as well as fostering an internal culture of security and cyber awareness [CPG 2I].
  - **Tailor the training to network IT personnel/administrators and other key staff based on relevant organizational cyber threats and TTPs**, such as Volt Typhoon. For example, communicate that Volt Typhoon actors are known to target personal email accounts of IT staff, and encourage staff to protect their personal email accounts by using strong passwords and implementing MFA.
  - In addition to basic cybersecurity training, **ensure personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training** on at least an annual basis [CPG 2J].
  - **Educate users about the risks associated with storing unprotected passwords**.

OT Administrators and Defenders

- **Change default passwords** [CPG 2A] and ensure they meet the policy requirements for complexity. If the asset's password cannot be changed, implement compensating controls for the device; for example, segment the device into separate enclaves and implement increased monitoring and logging.
- **Require that passwords for all OT password-protected assets be at least 15 characters**, when technically feasible. In instances where minimum passwords lengths are not technically feasible (for example, assets in remote locations), apply compensating controls, record the controls, and log all login attempts. [CPG 2B].
- **Enforce strict access policies for accessing OT networks**. Develop strict operating procedures for OT operators that details secure configuration and usage.
- **Segment OT assets from IT environments** by [CPG 2F]:
  - **Denying all connections to the OT network by default** unless explicitly allowed (e.g., by IP address and port) for specific system functionality.
  - **Requiring necessary communications paths between IT and OT networks to pass through an intermediary**, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets.
- **Closely monitor all connections into OT networks for misuse, anomalous activity, or OT protocols**.
- **Monitor for unauthorized controller change attempts**. Implement integrity checks of controller process logic against a known good baseline. Ensure process controllers are prevented from remaining in remote program mode while in operation if possible.

- **Lock or limit set points in control processes to reduce the consequences of unauthorized controller access**.
- **Be prepared** by:
  - **Determining your critical operational processes' reliance on key IT infrastructure**:
    - Maintain and regularly update an inventory of all organizational OT assets.
    - Understand and evaluate cyber risk on "as-operated" OT assets.
    - Create an accurate "as-operated" OT network map and identify OT and IT network inter-dependencies.
  - Identifying a resilience plan that addresses how to operate if you lose access to or control of the IT and/or OT environment.
    - Plan for how to continue operations if a control system is malfunctioning, inoperative, or actively acting contrary to the safe and reliable operation of the process.
    - Develop workarounds or manual controls to ensure ICS networks can be isolated if the connection to a compromised IT environment creates risk to the safe and reliable operation of OT processes.
  - **Create and regularly exercise an incident response plan**.
    - Regularly test manual controls so that critical functions can be kept running if OT networks need to be taken offline.
  - **Implement regular data backup procedures** on OT networks.
    - Regularly test backup procedures.
- **Follow risk-informed guidance** in the joint advisory NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems, the NSA advisory Stop Malicious Cyber Activity Against Connected Operational Technology.

CONTACT INFORMATION

US organizations: To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact:

- CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870 or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.
- Water and Wastewater Systems Sector organizations, contact the EPA Water Infrastructure and Cyber Resilience Division at watercyberta@epa.gov to voluntarily provide situational awareness.
- Entities required to report incidents to DOE should follow established reporting requirements, as appropriate. For other energy sector inquiries, contact EnergySRMA@hq.doe.gov.
- For transportation entities regulated by TSA, report to CISA Central in accordance with the requirements found in applicable Security Directives, Security Programs, or TSA Order.

Australian organizations: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations: Report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand organizations: Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom organizations: Report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring agencies recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 5 through Table 17).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring agencies recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REFERENCES

[1] fofa

[2] Microsoft: Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

[3] GitHub - fatedier/frp: A fast reverse proxy to help you expose a local server behind a NAT or firewall to the internet

[4] GitHub - sandialabs/gait: Zeek Extension to Collect Metadata for Profiling of Endpoints and Proxies

[5] The Zeek Network Security Monitor

RESOURCES

Microsoft: Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

Secureworks: Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

ACKNOWLEDGEMENTS

Fortinet and Microsoft contributed to this advisory.

VERSION HISTORY

February 7, 2024: Initial Version.

March 7, 2024: Updated Mitigations section to add recommendation on “end of life” technology.

APPENDIX A: VOLT TYPHOON OBSERVED COMMANDS / LOTL ACTIVITY

See Table 2 and Table 3 for Volt Typhoon commands and PowerShell scripts observed by the U.S. authoring agencies during incident response activities. For additional commands used by Volt Typhoon, see joint advisory People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.

Table 2: Volt Typhoon Observed Commands in PowerShell Console History

Command/Script	Description/Use
Get-EventLog security -instanceid 4624 -after {redacted date} | fl * | Out-File 'C:\users\public\documents\user.dat'	PowerShell command extracts security log entries with the Event ID `4624` after a specified date. The output is formatted (`fl *`) and saved to `user.dat`. Potentially used to analyze logon patterns and identify potential targets for lateral movement.
Get-EventLog security -instanceid 4624 | Where-Object {$_.message.contains('{redacted user account}')} | select -First 1 | fl *	PowerShell command extracts security log entries with the Event ID `4624` and filters them to include only those containing a specific user account, selecting the first instance of such an event.
wminc process get name,processid	Appears to be an attempt to use the wmic command but with a misspelling (`wminc` instead of `wmic`). This command, as it stands, would not execute successfully and would return an error in a typical Windows environment. This could indicate a mistake made during manual input.
wmic process get name,processid	WMI command lists all running processes with process names and process IDs. Potentially used to find process IDs needed for other operations, like memory dumping.
tasklist /v	Command displays detailed information about currently running processes, including the name, PID, session number, and memory usage.

Command/Script	Description/Use
taskkill /f /im rdpservice.exe	Command forcibly terminates the process `rdpservice.exe`. Potentially used as a cleanup activity post-exploitation.
ping -n 1 {redacted IP address}	Command sends one ICMP echo request to a specified IP address.
ping -n 1 -w 1 {redacted IP address}	Command sends one ICMP echo request to a specified IP address with a timeout (`-w`) of 1 millisecond.
net user	Lists all user accounts on the local machine or domain, useful for quickly viewing existing user accounts.
quser query user	Displays information about user sessions on a system, aiding in identifying active users or sessions.
net start	Lists all active services.
cmd	Opens a new instance of the command prompt.
cd [Redacted Path]	Changes the current directory to a specified path, typically for navigating file systems.
Remove-Item .\Thumbs.db	PowerShell command to delete the `Thumbs.db` file, possibly for cleanup or removing traces.
move .\Thumbs.db ttt.dat	Relocates and renames the file `Thumbs.db` in the current directory to `ttt.dat` within the same directory.
del .\Thumbs.db /f /s /q	Force deletes `Thumbs.db` files from the current directory and all subdirectories, part of cleanup operations to erase traces.
del ??	Deletes files with two-character names, potentially a targeted cleanup command.

Command/Script	Description/Use
del /?	Displays help information for the `del` command.
exit	Terminates the command prompt session.
ipconfig	Retrieves network configuration details, helpful for discovery and mapping the victim's network.
net time /dom	Queries or sets the network time for a domain, potentially used for reconnaissance or to manipulate system time.
netstta -ano	Intended as `netstat -ano`; a mistyped command indicating a potential operational error.
netstat -ano	Lists active network connections and processes, helpful for identifying communication channels and potential targets.
type .\Notes.txt	Displays the contents of `Notes.txt`, possibly used for extracting specific information or intelligence gathering.
logoff	Logs off the current user session.

Table 3: Volt Typhoon Observed PowerShell Scripts

Script name and location	Contents	Description/Use
C:\{redacted}\ logins.ps1	# Find DC list from Active Directory $DCs = Get-ADDomainController -Filter * # Define time for report (default is 1 day) $startDate = (get-date).AddDays(-1)	The script is designed for user logon discovery in a Windows Active Directory environment. It retrieves a list of DCs and then queries security logs on these DCs for successful logon events (Event ID **4624**) within the last day. The script differentiates

Script name and location	Contents	Description/Use

	# Store successful logon events from security logs with the specified dates and workstation/IP in an array
	foreach ($DC in $DCs){
	$slogonevents = Get-Eventlog -LogName Security -ComputerName $DC.Hostname -after $startDate \| where {$_.eventID -eq 4624 }}
	
	# Crawl through events; print all logon history with type, date/time, status, account name, computer and IP address if user logged on remotely
	
	foreach ($e in $slogonevents){
	# Logon Successful Events
	# Local (Logon Type 2)
	if (($e.EventID -eq 4624) -and ($e.ReplacementStrings[8] -eq 2)){
	write-host "Type: Local Logon`tDate: "$e.TimeGenerated "`tStatus: Success`tUser: "$e.ReplacementStrings[5] "`tWorkstation: "$e.ReplacementStrings[11]
	}
	# Remote (Logon Type 10)
	if (($e.EventID -eq 4624) -and ($e.ReplacementStrings[8] -eq 10)){
	write-host "Type: Remote Logon`tDate: "$e.TimeGenerated "`tStatus: Success`tUser: "$e.ReplacementStrings[5] "`tWorkstation: "$e.ReplacementStrings[11] "`tIP Address: "$e.ReplacementStrings[18]
	}}
		between local (Logon Type 2) and remote (Logon Type 10) logon events. For each event, it extracts and displays details including the logon type, date/time of logon, status, account name, and the workstation or IP address used for the logon. Volt Typhoon may be leveraging this script to monitor user logon activities across the network, potentially to identify patterns, gather credentials, or track the movement of users and administrators within the network.

APPENDIX B: INDICATORS OF COMPROMISE

See Table 4 for Volt Typhoon IOCs obtained by the U.S. authoring agencies during incident response activities.

Table 4: Volt Typhoon Malicious Files and Associated Hashes

Note: See MAR-10448362-1.v1 for more information on this malware.

File Name	Description	MD5	Hashes (SHA256)
BrightmetricAgent.exe	The file is an FRP that could be used to reveal servers situated behind a network firewall or obscured through Network Address Translation (NAT).	fd41134e8ead1c18ccad27c62a260aa6	edc0c63065e88ec96197c8d7a40662a15a812a9583dc6c82b18ecd7e43b13b70
SMSvcService.exe	The file is a Windows executable "FRPC" designed to open a reverse proxy between the compromised system and the threat actor(s) C2 server.	b1de37bf229890ac181bdef1ad8ee0c2	99b80c5ac352081a64129772ed5e1543d94cad708ba2adc46dc4ab7a0bd563f1

APPENDIX C: MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 5 through Table 17 for all referenced threat actor tactics and techniques in this advisory.

Table 5: Volt Typhoon actors ATT&CK Techniques for Enterprise – Reconnaissance

Reconnaissance		
Technique Title	**ID**	**Use**
Gather Victim Host Information	T1592	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.
Gather Victim Identity Information	T1589	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's staff.
Gather Victim Identity Information: Email Addresses	T1589.002	Volt Typhoon targets the personal emails of key network and IT staff.
Gather Victim Network Information	T1590	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's network.
Gather Victim Org Information	T1591	Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization.
Search Open Websites/Domains	T1593	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.
Search Victim-Owned Websites	T1594	Volt Typhoon conducts extensive pre-compromise reconnaissance. This includes web searches, including victim-owned sites, for victim host, identity, and network information, especially for information on key network and IT administrators.

Table 6: Volt Typhoon actors ATT&CK Techniques for Enterprise – Resource Development

Resource Development		
Technique Title	**ID**	**Use**
Acquire Infrastructure: Botnet	T1583.003	Volt Typhoon uses multi-hop proxies for command-and-control infrastructure. The proxy is typically composed of Virtual Private Servers (VPSs) or small office/home office (SOHO) routers.
Compromise Infrastructure: Botnet	T1584.005	Volt Typhoon used Cisco and NETGEAR end-of-life SOHO routers implanted with KV Botnet malware to support their operations.
Compromise Infrastructure: Server	T1584.004	Volt Typhoon has redirected specific port traffic to their proxy infrastructure, effectively converting the PRTG's Detection Guidance server into a proxy for their C2 traffic.
Develop Capabilities: Exploits	T1587.004	Volt Typhoon uses publicly available exploit code, but is also adept at discovering and exploiting vulnerabilities as zero days.
Obtain Capabilities: Exploits	T1588.005	Volt Typhoon uses publicly available exploit code, but is also adept at discovering and exploiting vulnerabilities as zero days.

Table 7: Volt Typhoon actors ATT&CK Techniques for Enterprise – Initial Access

Initial Access		
Technique Title	**ID**	**Use**
Exploit Public-Facing Application	T1190	Volt Typhoon commonly exploits vulnerabilities in networking appliances such as Fortinet, Ivanti (formerly Pulse Secure), NETGEAR, Citrix, and Cisco.
External Remote Services	T1133	Volt Typhoon often uses VPN sessions to securely connect to victim environments, enabling discreet follow-on intrusion activities.

Table 8: Volt Typhoon actors ATT&CK Techniques for Enterprise – Execution

Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter	T1059	Volt Typhoon uses hands-on-keyboard execution for their malicious activity via the command-line.
Command and Scripting Interpreter: PowerShell	T1059.001	Volt Typhoon has executed clients via PowerShell.
Command and Scripting Interpreter: Unix Shell	T1059.004	Volt Typhoon has used `Brightmetricagent.exe`, which contains multiplexer libraries that can bi-directionally stream data over through NAT networks and contains a command-line interface (CLI) library that can leverage command shells such as PowerShell, Windows Management, Instrumentation (WMI), and Z Shell (zsh).
Windows Management Instrumentation	T1047	Volt Typhoon has used Windows Management Instrumentation Console (WMIC) commands.

Table 9: Volt Typhoon actors ATT&CK Techniques for Enterprise – Persistence

Persistence		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	Volt Typhoon primarily relies on valid credentials for persistence.

Table 10: Volt Typhoon actors ATT&CK Techniques for Enterprise – Privilege Escalation

Privilege Escalation		
Technique Title	**ID**	**Use**
Exploitation for Privilege Escalation	T1068	Volt Typhoon first obtains credentials from public-facing appliances after gaining initial access by exploiting privilege

		escalation vulnerabilities in the operating system or network services.

Table 11: Volt Typhoon actors ATT&CK Techniques for Enterprise – Defense Evasion

Defense Evasion		
Technique Title	**ID**	**Use**
Direct Volume Access	T1006	Volt Typhoon has executed the Windows-native `vssadmin` command to create a volume shadow copy.
Indicator Removal: Clear Persistence	T1070.009	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
Indicator Removal: Clear Windows Event Logs	T1070.001	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
Indicator Removal: File Deletion	T1070.004	Volt Typhoon created `systeminfo.dat` in `C:\Users\Public\Documents`, but subsequently deleted it.
Masquerading: Match Legitimate Name or Location	T1036.005	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity and masquerading file names.
Modify Registry	T1112	Volt Typhoon has used the `netsh` command, a legitimate Windows command, to create a PortProxy registry modification on the PRTG server.
Obfuscated Files or Information: Software Packing	T1027.002	Volt Typhoon has obfuscated FRP client files (`BrightmetricAgent.exe` and `SMSvcService.exe`) and the command-line port scanning utility ScanLine by packing the files with Ultimate Packer for Executables (UPX).
System Binary Proxy Execution	T1218	Volt Typhoon uses hands-on-keyboard activity via the command-line and use other native tools and processes on systems (often referred to as “LOLBins”), known as LOTL, to maintain and expand access to the victim networks.

Table 12: Volt Typhoon actors ATT&CK Techniques for Enterprise – Credential Access

Credential Access		
Technique Title	**ID**	**Use**
Brute Force: Password Cracking	T1110.002	Volt Typhoon has exfiltrated `NTDS.dit` and `SYSTEM` registry hive to crack passwords offline.
Credentials from Password Stores	T1555	Volt Typhoon has installed browsers saved passwords history, credit card details, and cookies.
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	Volt Typhoon has strategically targeted network administrator web browser data, focusing on both browsing history and stored credentials.
OS Credential Dumping: LSASS Memory	T1003.001	Volt Typhoon used a DLL with `MiniDump` and the process ID of Local Security Authority Subsystem Service (LSASS) to dump the LSASS process memory and obtain credentials.
OS Credential Dumping: NTDS	T1003.003	Volt Typhoon appears to prioritize obtaining valid credentials by extracting the Active Directory database file (`NTDS.dit`).
Unsecured Credentials	T1552	Volt Typhoon has obtained credentials insecurely stored on an appliance.
Unsecured Credentials: Private Keys	T1552.004	Volt Typhoon has accessed a Local State file that contains the Advanced Encryption Standard (AES) encryption key used to encrypt the passwords stored in the Chrome browser, which enables the actors to obtain plaintext passwords stored in the Login Data file in the Chrome browser.

Table 13: Volt Typhoon actors ATT&CK Techniques for Enterprise – Discovery

Discovery		
Technique Title	**ID**	**Use**
Account Discovery: Local Account	T1087.001	Volt Typhoon executed `net user` and `quser` for user account information.

Application Window Discovery	T1010	Volt Typhoon created and accessed a file named `rult3uil.log` on a Domain Controller in `C:\Windows\System32\`. The `rult3uil.log` file contained user activities on a compromised system, showcasing a combination of window title information and focus shifts, keypresses, and command executions across Google Chrome and Windows PowerShell, with corresponding timestamps.
Browser Information Discovery	T1217	Volt Typhoon has installed browsers saved passwords history, credit card details, and cookies.
File and Directory Discovery	T1083	Volt Typhoon enumerated several directories, including directories containing vulnerability testing and cyber related content and facilities data, such as construction drawings.
Log Enumeration	T1654	Volt Typhoon has captured successful logon events.
Network Service Discovery	T1046	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
Peripheral Device Discovery	T1120	Volt Typhoon has obtained the victim's system screen dimension and display devices information.
Permission Groups Discovery	T1069	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
Process Discovery	T1057	Volt Typhoon executed `tasklist /v` to gather a detailed process listing.
Query Registry	T1012	Volt Typhoon has interacted with a PuTTY application by enumerating existing stored sessions.
Software Discovery	T1518	Volt Typhoon has obtained the victim's list of applications installed on the victim's system.
System Information Discovery	T1082	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.

System Location Discovery	T1614	Volt Typhoon has obtained the victim's system current locale.
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	Volt Typhoon employs `ping` with various IP addresses to check network connectivity and `net start` to list running services.
System Owner/User Discovery	T1033	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for system information, network service, group, and user discovery.
System Service Discovery	T1007	Volt Typhoon employs `ping` with various IP addresses to check network connectivity and `net start` to list running services.
System Time Discovery	T1124	Volt Typhoon has obtained the victim's system timezone.

Table 14: Volt Typhoon actors ATT&CK Techniques for Enterprise – Lateral Movement

Lateral Movement		
Technique Title	**ID**	**Use**
Remote Service Session Hijacking	T1563	Volt Typhoon potentially had access to a range of critical PuTTY profiles, including those for water treatment plants, water wells, an electrical substation, operational technology systems, and network security devices. This would enable them to access these critical systems.
Remote Services: Cloud Services	T1021.007	During the period of Volt Typhoon's known network presence, there were anomalous login attempts to an Azure tenant potentially using credentials previously compromised from theft of `NTDS.dit`.
Remote Services: Remote Desktop Protocol	T1021.001	Volt Typhoon has moved laterally to the Domain Controller via an interactive RDP session using a compromised account with domain administrator privileges.

Use Alternate Authentication Material	T1550	Volt Typhoon may be capable of using other methods such as Pass the Hash or Pass the Ticket for lateral movement.
Valid Accounts: Cloud Accounts	T1078.004	During the period of Volt Typhoon's known network presence, there were anomalous login attempts to an Azure tenant potentially using credentials previously compromised from theft of `NTDS.dit`.

Table 15: Volt Typhoon actors ATT&CK Techniques for Enterprise – Collection

Collection		
Technique Title	**ID**	**Use**
Archive Collected Data	T1560	Volt Typhoon collected sensitive information obtained from a file server in multiple zipped files.
Archive Collected Data: Archive via Utility	T1560.001	Volt Typhoon has compressed and archived the extracted `ntds.dit` and accompanying registry files (by executing `ronf.exe`, which was likely a renamed version of `rar.exe`).
Data Staged	T1074	Volt Typhoon accessed the file `C:\Users\{redacted}\Downloads\History.zip`, which presumably contained data from the User Data directory of the user's Chrome browser, which the actors likely saved in the Downloads directory for exfiltration.
Screen Capture	T1113	Volt Typhoon has obtained a screenshot of the victim's system using two libraries (`gdi32.dll` and `gdiplus.dll`)

Table 16: Volt Typhoon actors ATT&CK Techniques for Enterprise – Command and Control

Command and Control		
Technique Title	**ID**	**Use**
Encrypted Channel	T1573	Volt Typhoon has setup FRP clients on a victim's corporate infrastructure to establish covert communications channels for command and control.

Ingress Tool Transfer	T1105	Volt Typhoon uses legitimate, but outdated versions of network admin tools. For example, in one confirmed compromise, actors downloaded an outdated version of `comsvcs.dll`, on the DC in a non-standard folder.
Proxy	T1090	Volt Typhoon has setup FRP clients on a victim's corporate infrastructure to establish covert communications channels for command and control.
Proxy: Internal Proxy	T1090.001	Volt Typhoon has used the `netsh` command, a legitimate Windows command, to create a PortProxy registry modification on the PRTG server.
Proxy: Multi-hop Proxy	T1090.003	Volt Typhoon uses multi-hop proxies for command-and-control infrastructure.

Table 17: Volt Typhoon actors ATT&CK Techniques for Enterprise – Exfiltration

Exfiltration		
Technique Title	**ID**	**Use**
Exfiltration Over Alternative Protocol	T1048	Volt Typhoon exfiltrated files via Server Message Block (SMB).