1 Phân tích sự cố

Trong case này được cung cấp 4 foder ứng với 4 máy . Check các IP các máy trong Key được như sau

SQLServer : 192.168.170.142

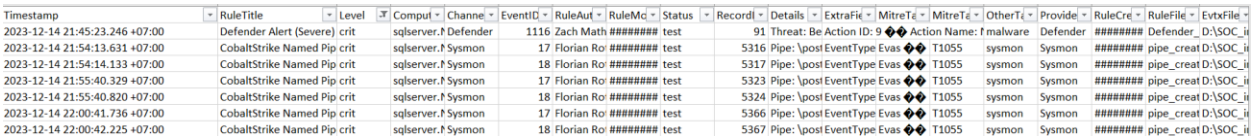
FileSever:192.168.170.138

DevPC:192.168.170.186

DC01:192.168.170.124

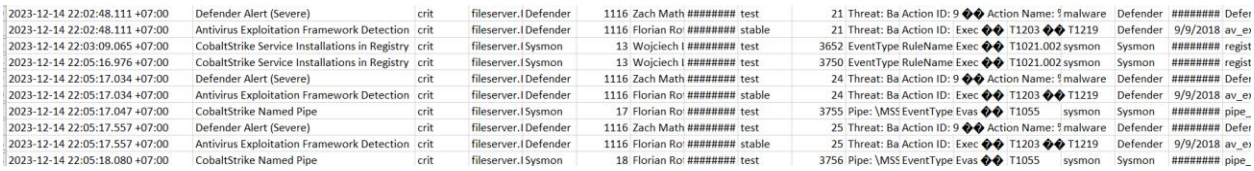
Sử dụng hayabusa parse winevt log của 4 computer và filter alert Level mức critical

SQLServer



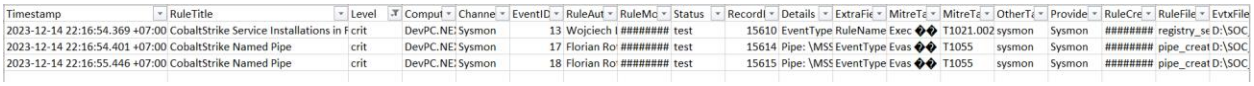
Timestamp	RuleTitle	Level	Comput	Channe	EventID	RuleAut	RuleMc	Status	Record	Details	ExtraFie	MitreTa	MitreTa	OtherTa	Provide	RuleCre	RuleFile	EvtxFile
2023-12-14 21:45:23.246 +07:00	Defender Alert (Severe)	crit	sqlserver.N	Defender	1116	Zach Math	########	test	91	Threat: Be	Action ID: 9 ◆◆	Action Name: ¶	malware		Defender	########	Defender_	D:\SOC_it
2023-12-14 21:54:13.631 +07:00	CobaltStrike Named Pip	crit	sqlserver.N	Sysmon	17	Florian Ro	########	test	5316	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_creat	D:\SOC_it
2023-12-14 21:54:14.133 +07:00	CobaltStrike Named Pip	crit	sqlserver.N	Sysmon	18	Florian Ro	########	test	5317	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_creat	D:\SOC_it
2023-12-14 21:55:40.329 +07:00	CobaltStrike Named Pip	crit	sqlserver.N	Sysmon	17	Florian Ro	########	test	5323	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_creat	D:\SOC_it
2023-12-14 21:55:40.820 +07:00	CobaltStrike Named Pip	crit	sqlserver.N	Sysmon	18	Florian Ro	########	test	5324	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_creat	D:\SOC_it
2023-12-14 22:00:41.736 +07:00	CobaltStrike Named Pip	crit	sqlserver.N	Sysmon	17	Florian Ro	########	test	5366	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_creat	D:\SOC_it
2023-12-14 22:00:42.225 +07:00	CobaltStrike Named Pip	crit	sqlserver.N	Sysmon	18	Florian Ro	########	test	5367	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_creat	D:\SOC_it

FileServer



2023-12-14 22:02:48.111 +07:00	Defender Alert (Severe)	crit	fileserver.I	Defender	1116	Zach Math	########	test	21	Threat: Ba	Action ID: 9 ◆◆	Action Name: ¶	malware		Defender	########	Defe
2023-12-14 22:02:48.111 +07:00	Antivirus Exploitation Framework Detection	crit	fileserver.I	Defender	1116	Florian Ro	########	stable	21	Threat: Ba	Action ID:	Exec ◆◆	T1203 ◆◆	T1219	Defender	9/9/2018	av_ex
2023-12-14 22:03:09.065 +07:00	CobaltStrike Service Installations in Registry	crit	fileserver.I	Sysmon	13	Wojciech I	########	test	3652	EventType	RuleName	Exec ◆◆	T1021.002	sysmon	Sysmon	########	regist
2023-12-14 22:05:16.976 +07:00	CobaltStrike Service Installations in Registry	crit	fileserver.I	Sysmon	13	Wojciech I	########	test	3750	EventType	RuleName	Exec ◆◆	T1021.002	sysmon	Sysmon	########	regist
2023-12-14 22:05:17.034 +07:00	Defender Alert (Severe)	crit	fileserver.I	Defender	1116	Zach Math	########	test	24	Threat: Ba	Action ID: 9 ◆◆	Action Name: ¶	malware		Defender	########	Defe
2023-12-14 22:05:17.034 +07:00	Antivirus Exploitation Framework Detection	crit	fileserver.I	Defender	1116	Florian Ro	########	stable	24	Threat: Ba	Action ID:	Exec ◆◆	T1203 ◆◆	T1219	Defender	9/9/2018	av_ex
2023-12-14 22:05:17.047 +07:00	CobaltStrike Named Pipe	crit	fileserver.I	Sysmon	17	Florian Ro	########	test	3755	Pipe: \MSS	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_
2023-12-14 22:05:17.557 +07:00	Defender Alert (Severe)	crit	fileserver.I	Defender	1116	Zach Math	########	test	25	Threat: Ba	Action ID: 9 ◆◆	Action Name: ¶	malware		Defender	########	Defe
2023-12-14 22:05:17.557 +07:00	Antivirus Exploitation Framework Detection	crit	fileserver.I	Defender	1116	Florian Ro	########	stable	25	Threat: Ba	Action ID:	Exec ◆◆	T1203 ◆◆	T1219	Defender	9/9/2018	av_ex
2023-12-14 22:05:18.080 +07:00	CobaltStrike Named Pipe	crit	fileserver.I	Sysmon	18	Florian Ro	########	test	3756	Pipe: \MSS	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_

DevPC



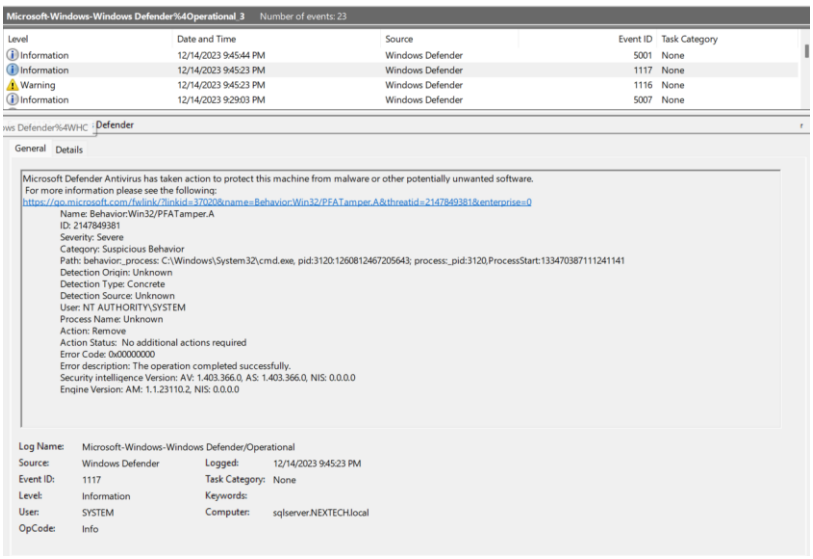
Timestamp	RuleTitle	Level	Comput	Channe	EventID	RuleAut	RuleMc	Status	Record	Details	ExtraFie	MitreTa	MitreTa	OtherTa	Provide	RuleCre	RuleFile	EvtxFile
2023-12-14 22:16:54.369 +07:00	CobaltStrike Service Installations in F	crit	DevPC.NE	Sysmon	13	Wojciech I	########	test	15610	EventType	RuleName	Exec ◆◆	T1021.002	sysmon	Sysmon	########	registry_se	D:\SOC
2023-12-14 22:16:54.401 +07:00	CobaltStrike Named Pipe	crit	DevPC.NE	Sysmon	17	Florian Ro	########	test	15614	Pipe: \MSS	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_creat	D:\SOC
2023-12-14 22:16:55.446 +07:00	CobaltStrike Named Pipe	crit	DevPC.NE	Sysmon	18	Florian Ro	########	test	15615	Pipe: \MSS	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	pipe_creat	D:\SOC

DC01

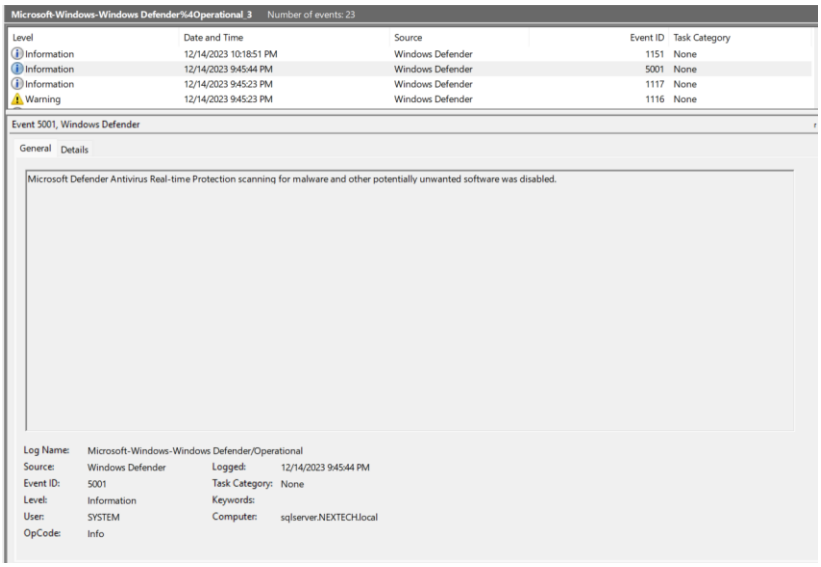
Timestamp	RuleTitle	Level	Comput	Channe	EventID	RuleAut	RuleMc	Status	Record	Details	ExtraFie	MitreTa	MitreTa	OtherTa	Provide	RuleCre	
2023-12-14 22:08:13.685 +07:00	CobaltStrike Service Installations in Registry	crit	DC01.NEX	Sysmon	13	Wojciech I	########	test	3545	EventType	RuleName	Exec ◆◆	T1021.002	sysmon	Sysmon	########	
2023-12-14 22:08:13.784 +07:00	Defender Alert (Severe)	crit	DC01.NEX	Defender	1116	Zach Math	########	test	34	Threat: Ba	Action ID: 9 ◆◆	Action Name: ¶	malware		Defender	########	
2023-12-14 22:08:13.784 +07:00	Antivirus Exploitation Framework Detection	crit	DC01.NEX	Defender	1116	Florian Ro	########	stable	34	Threat: Ba	Action ID:	Exec ◆◆	T1203 ◆◆	T1219	Defender	9/9/2018	
2023-12-14 22:08:13.828 +07:00	CobaltStrike Named Pipe	crit	DC01.NEX	Sysmon	17	Florian Ro	########	test	3551	Pipe: \MSS	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	
2023-12-14 22:08:14.855 +07:00	CobaltStrike Named Pipe	crit	DC01.NEX	Sysmon	18	Florian Ro	########	test	3554	Pipe: \MSS	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	
2023-12-14 22:12:15.504 +07:00	CobaltStrike Named Pipe	crit	DC01.NEX	Sysmon	17	Florian Ro	########	test	3571	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	
2023-12-14 22:12:15.905 +07:00	CobaltStrike Named Pipe	crit	DC01.NEX	Sysmon	18	Florian Ro	########	test	3572	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	
2023-12-14 22:13:16.598 +07:00	CobaltStrike Named Pipe	crit	DC01.NEX	Sysmon	17	Florian Ro	########	test	3588	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	
2023-12-14 22:13:17.083 +07:00	CobaltStrike Named Pipe	crit	DC01.NEX	Sysmon	18	Florian Ro	########	test	3589	Pipe: \post	EventType	Evas ◆◆	T1055	sysmon	Sysmon	########	

Quan sát output của 4 computer có những nhận xét sau có vẻ cuộc tấn công diễn ra vào ngày 12-14-2023 vào thời gian xung quanh tầm 22h . Thứ tự lần lượt các máy đưa ra alert là SQLSever – FileServer – DC01 – DevPC .

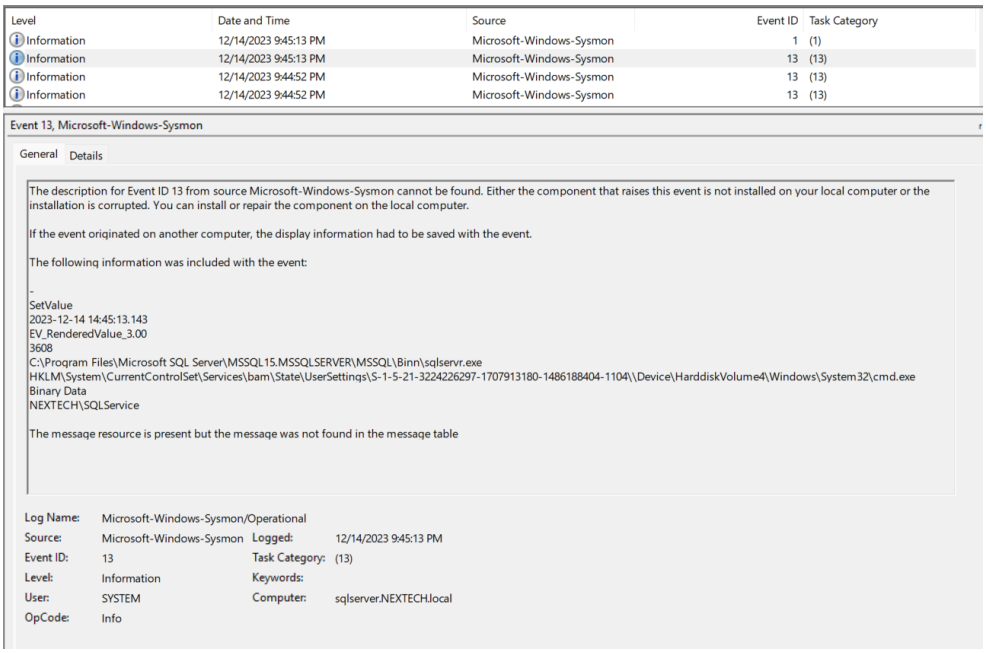
SQlSever



Vào lúc 9:45:23 PM Window defend đưa ra 1 alert là detect 1 tiến trình có hành vi độc hại được là cmd.exe .

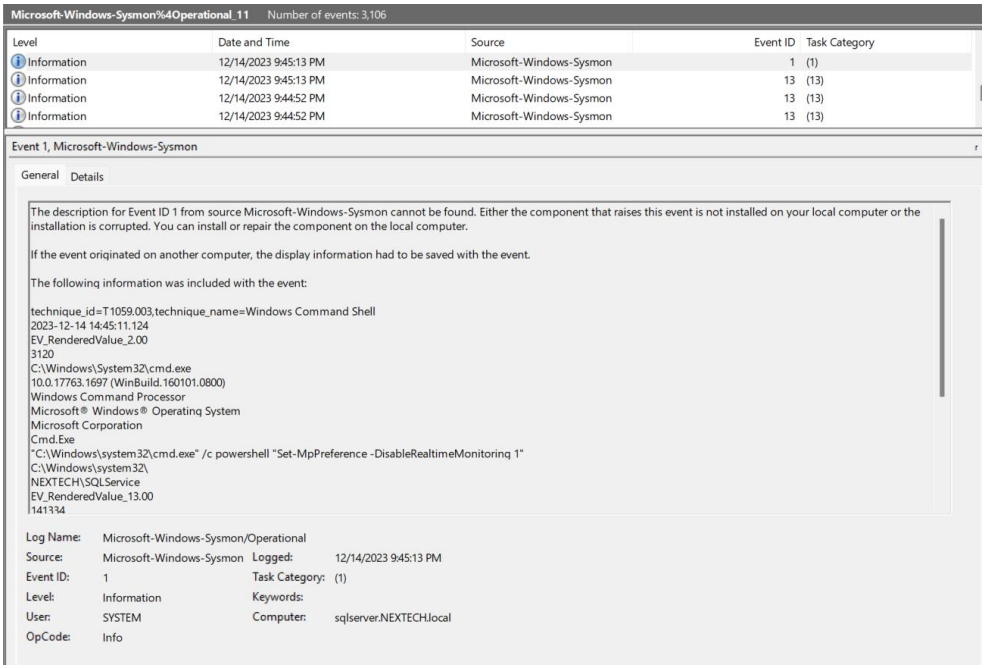


Ngay sau đó chỉ vài giây windows defend option Real-time Protection đã bị disable có thể là do hành vi của tiến trình độc hại gây ra



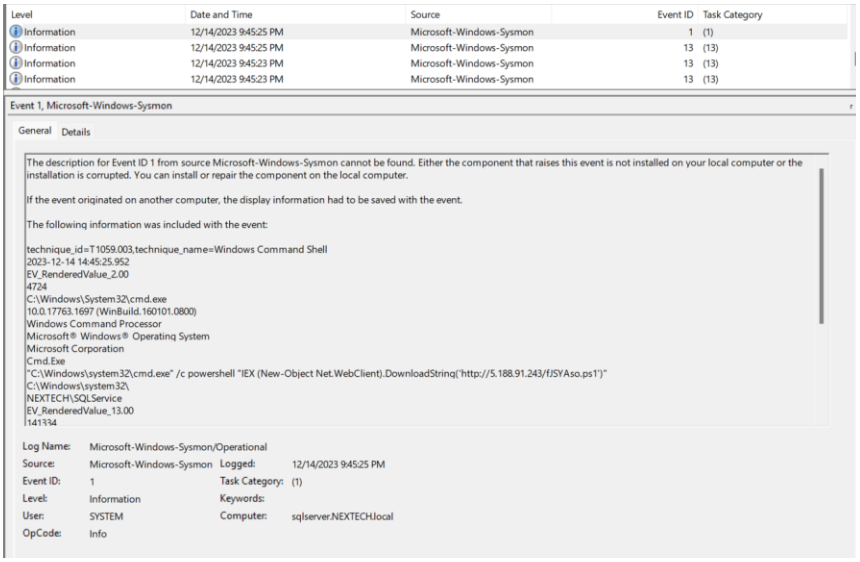
Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 9:45:13 PM	Microsoft-Windows-Sysmon	1	(1)
Information	12/14/2023 9:45:13 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 9:44:52 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 9:44:52 PM	Microsoft-Windows-Sysmon	13	(13)

Check sysmon log vào lúc 9:45:13 process sqlservr.exe đã chạy và khởi tạo 1 tiến trình con là cmd.exe và cmd này thực thi 1 command là C:\Windows\system32\cmd.exe" /c powershell "Set-MpPreference -DisableRealtimeMonitoring 1 . Đây là command set lại giá trị của DisableRealtimeMonitoring thành 1 biểu thị cho việc tắt windows defend



Microsoft-Windows-Sysmon%4Operational_11 Number of events: 3,106

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 9:45:13 PM	Microsoft-Windows-Sysmon	1	(1)
Information	12/14/2023 9:45:13 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 9:44:52 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 9:44:52 PM	Microsoft-Windows-Sysmon	13	(13)

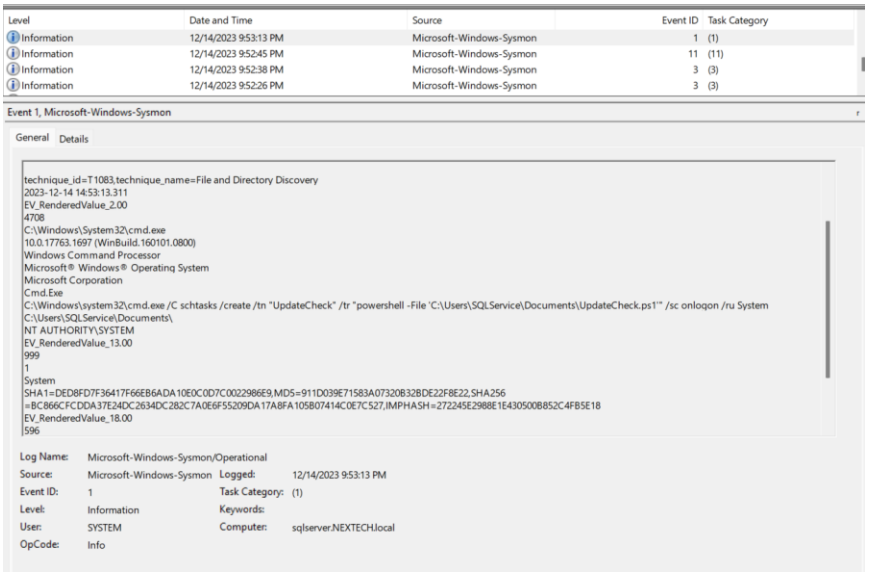


Vào lúc 9:45:25 attacker dùng cmd để thực thi1command download 1 file ps1 từ địa chỉ url http://5[.]188[.]91[.]243 có tên là FJSYAso.ps1 có vẻ như mục đích tắt window defend của attacker nhằm tải file này xuống . Đến đây chúng ta có thể chắc chắn rằng ip 5.188.91.243 là của attacker . Check log của MSSQL chúng ta phát hiện hành vi brute force của attacker

```
2023-12-14 06:43:08.76 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.76 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.76 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.76 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.76 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.76 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.76 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.76 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.76 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.76 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.77 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.77 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.77 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.77 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.77 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.77 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.77 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.77 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.77 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.77 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.77 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.77 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.77 Logon       Error: 18456, Severity: 14, State: 8.
2023-12-14 06:43:08.77 Logon       Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: 5.188.91.243]
2023-12-14 06:43:37.42 Logon       Login succeeded for user 'sa'. Connection made using SQL Server authentication. [CLIENT: 5.188.91.243]
2023-12-14 06:43:52.13 spid51      Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
2023-12-14 06:44:08.85 spid51      Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
2023-12-14 06:49:30.56 Logon       Login succeeded for user 'NT SERVICE\SQLTELEMETRY'. Connection made using Integrated authentication. [CLIENT: <local machine>]
2023-12-14 06:59:31.13 Logon       Login succeeded for user 'NT SERVICE\SQLTELEMETRY'. Connection made using Integrated authentication. [CLIENT: <local machine>]
2023-12-14 07:09:31.67 Logon       Login succeeded for user 'NT SERVICE\SQLTELEMETRY'. Connection made using Integrated authentication. [CLIENT: <local machine>]
2023-12-14 07:14:31.94 Logon       Login succeeded for user 'NT SERVICE\SQLTELEMETRY'. Connection made using Integrated authentication. [CLIENT: <local machine>]
2023-12-14 07:19:32.20 Logon       Login succeeded for user 'NT SERVICE\SQLTELEMETRY'. Connection made using Integrated authentication. [CLIENT: <local machine>]
2023-12-14 07:22:23.83 spid6s      Always On: The availability replica manager is going offline because SQL Server is shutting down. This is an informational messag
2023-12-14 07:22:23.83 spid6s      SQL Server is terminating in response to a 'stop' request from Service Control Manager. This is an informational message only. No
2023-12-14 07:22:23.97 spid14s     Service Broker manager has shut down.
2023-12-14 07:22:24.00 spid6s      .NET Framework runtime has been stopped.
2023-12-14 07:22:24.07 spid6s      SQL Trace was stopped due to server shutdown. Trace ID = '1'. This is an informational message only; no user action is required.
```

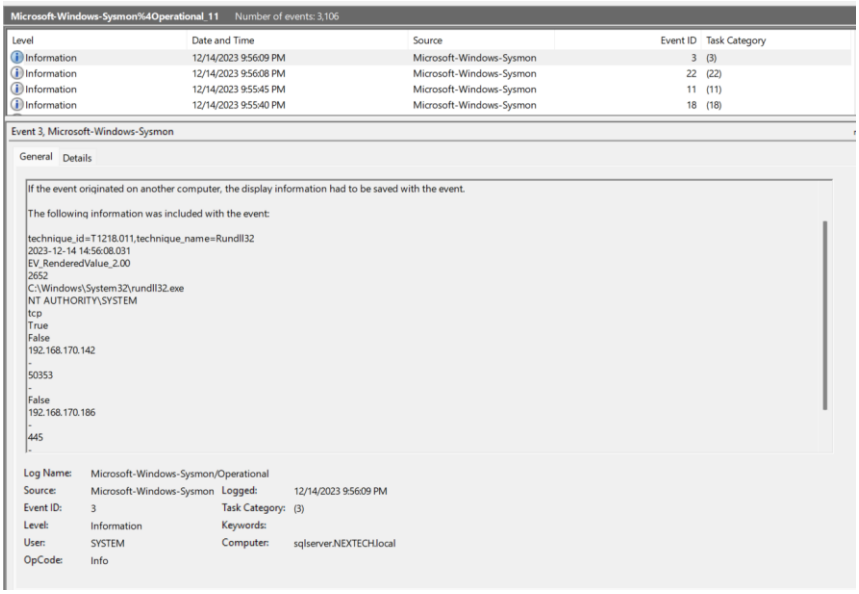
Chúng ta có thể thấy attacker đã brute force thành công tài khoản có tên user là **sa** đó là lý do tại sao attacker của nó quyền control vào máy SQLSever . Quan sát hành động của attacker sau khi bruteforce thành công thấy attacker đã sử dụng 2 option là show advanced options và xp_cmdshell . Options xp_cmdshell cho phép thực thi các lệnh hệ thống hoặc các tệp lệnh bên ngoài hệ thống thông qua lệnh "xp_cmdshell" trong môi trường T-SQL (Transact-SQL)

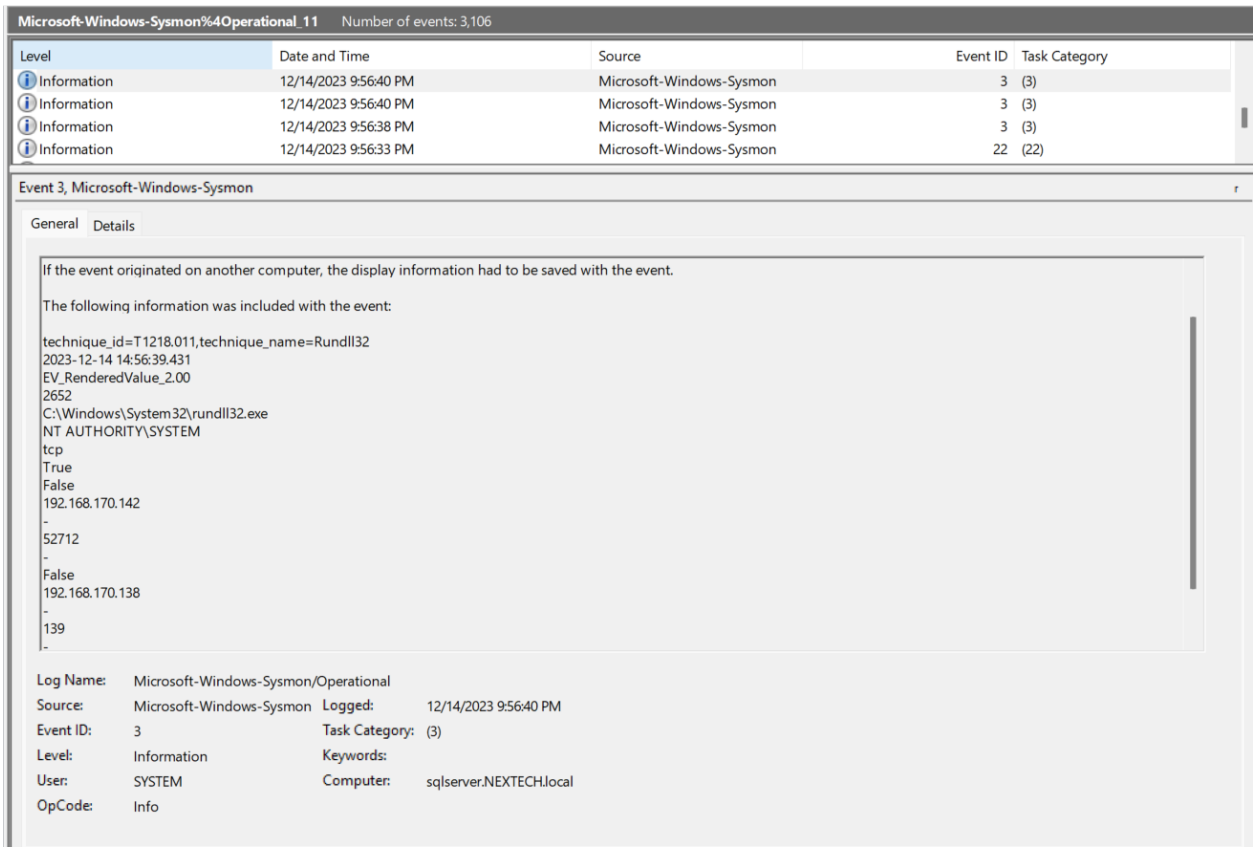
Tiếp tục check trong sysmon log vào lúc 9:53:13 phát hiện ra 1 hành động đáng nghi ngờ là của attacker đã create 1 schedule task với là UpdateCheck với việc thực thi file UpdateCheck.ps1 . Không đủ thông tin tệp UpdateCheck.ps1 làm gì do không có file mẫu nhưng có thể suy đoán nó liên quan đến file FJSYAso.ps1 mà attacker đã tải xuống nhằm mục đích persistent

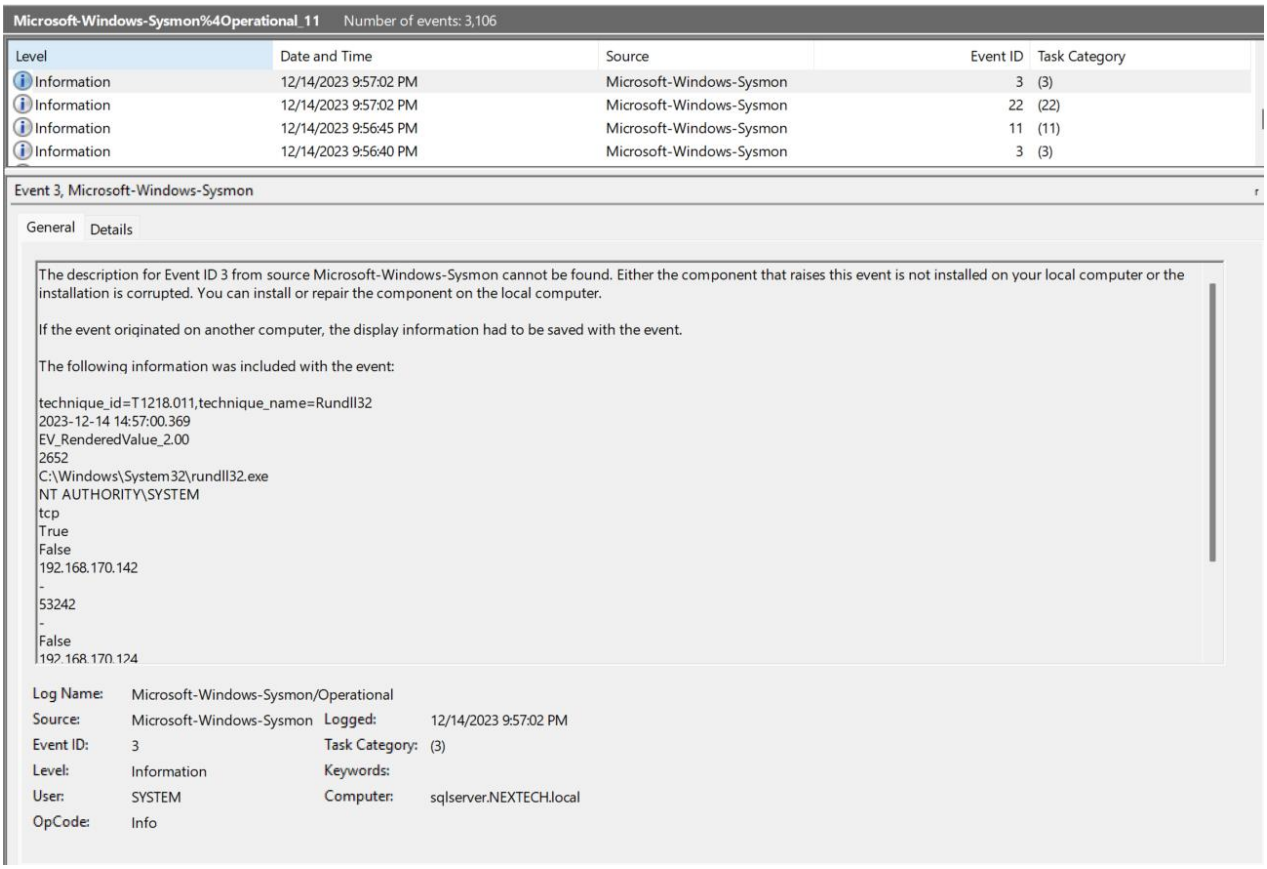


Tiếp tục phân tích log chúng ta có thể thấy attacker cố gắng connect TCP đến các máy DevPC (192.168.170.186) ,FileSever(192.168.170.138) và DC01(192.168.170.124)

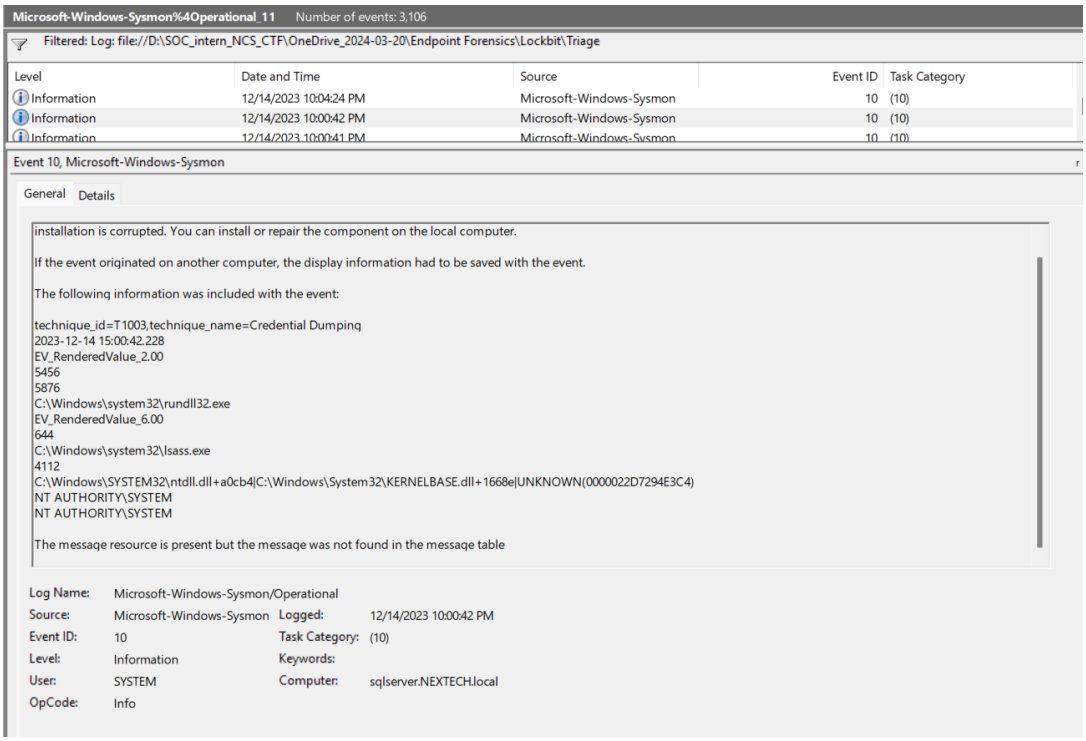
nhưng đều false



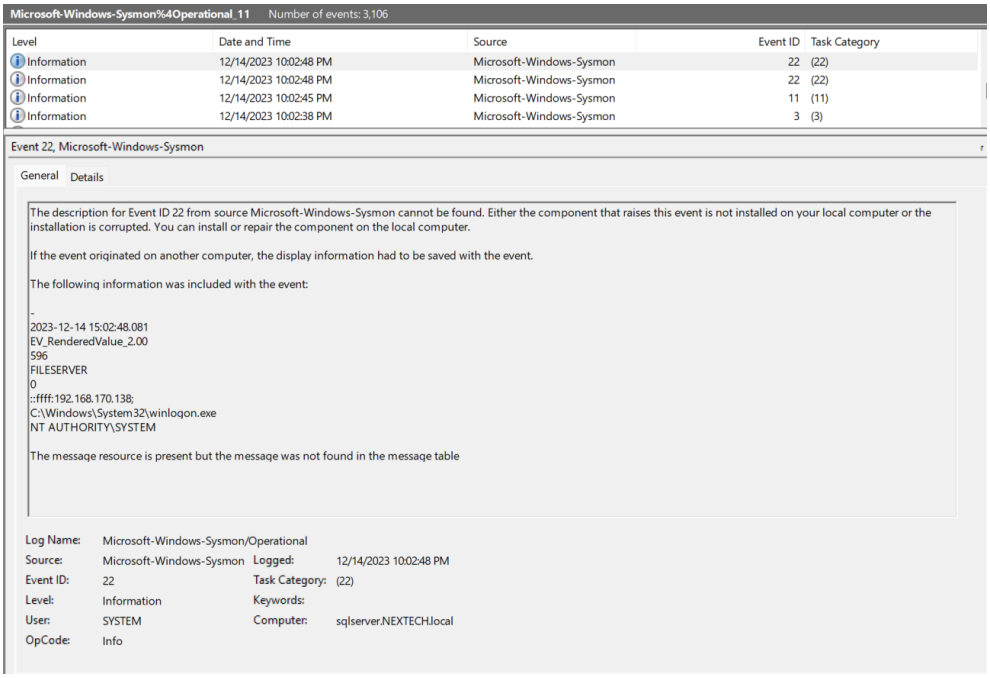

Microsoft-Windows-Sysmon%4Operational_11 Number of events: 3,106
Level Date and Time Source Event ID Task Category
Information 12/14/2023 9:56:40 PM Microsoft-Windows-Sysmon 3 (3)
Information 12/14/2023 9:56:40 PM Microsoft-Windows-Sysmon 3 (3)
Information 12/14/2023 9:56:38 PM Microsoft-Windows-Sysmon 3 (3)
Information 12/14/2023 9:56:33 PM Microsoft-Windows-Sysmon 22 (22)
Event 3, Microsoft-Windows-Sysmon
General Details
If the event originated on another computer, the display information had to be saved with the event.
The following information was included with the event:
technique_id=T1218.011,technique_name=Rundll32
2023-12-14 14:56:39.431
EV_RenderedValue_2.00
2652
C:\Windows\System32\rundll32.exe
NT AUTHORITY\SYSTEM
tcp
True
False
192.168.170.142
-
52712
-
False
192.168.170.138
-
139
-
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 9:56:40 PM
Event ID: 3 Task Category: (3)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTECH.local
OpCode: Info


Microsoft-Windows-Sysmon%4Operational_11 Number of events: 3,106
Level Date and Time Source Event ID Task Category
Information 12/14/2023 9:57:02 PM Microsoft-Windows-Sysmon 3 (3)
Information 12/14/2023 9:57:02 PM Microsoft-Windows-Sysmon 22 (22)
Information 12/14/2023 9:56:45 PM Microsoft-Windows-Sysmon 11 (11)
Information 12/14/2023 9:56:40 PM Microsoft-Windows-Sysmon 3 (3)
Event 3, Microsoft-Windows-Sysmon
General Details
The description for Event ID 3 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.
If the event originated on another computer, the display information had to be saved with the event.
The following information was included with the event:
technique_id=T1218.011,technique_name=Rundll32
2023-12-14 14:57:00.369
EV_RenderedValue_2.00
2652
C:\Windows\System32\rundll32.exe
NT AUTHORITY\SYSTEM
tcp
True
False
192.168.170.142
-
53242
-
False
192.168.170.124
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 9:57:02 PM
Event ID: 3 Task Category: (3)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTECH.local
OpCode: Info

Lúc 10:02:42 chúng ta thấy sysmon log đưa ra 1 alert Credential Dumping .Có vẻ ở đây attacker đã sử dụng mimikatz để có thể dump mem của process lsass.exe để tìm tài khoản và mật khẩu để có thể thực hiện hành vi lateral movement sang các máy khác

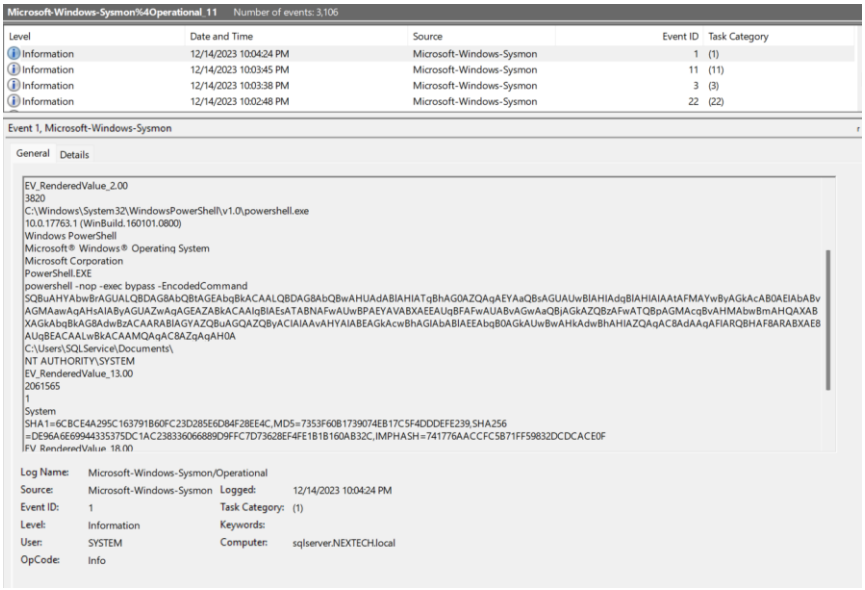


Vào lúc 10:02:48 chúng ta có thể thấy attacker đã remote thành công với computer FileServer khoảng thời gian trùng với mẫu có tên là ceabe99.exe detect trên máy FileServer mà đã đề cập ở lúc ban đầu khi check output Hayabusa

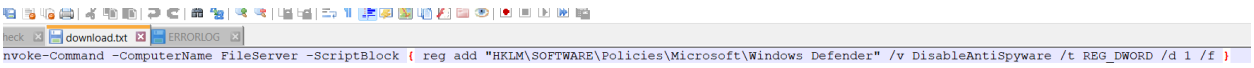


Tiếp tục phân tích sysmonlog của máy SQLSever

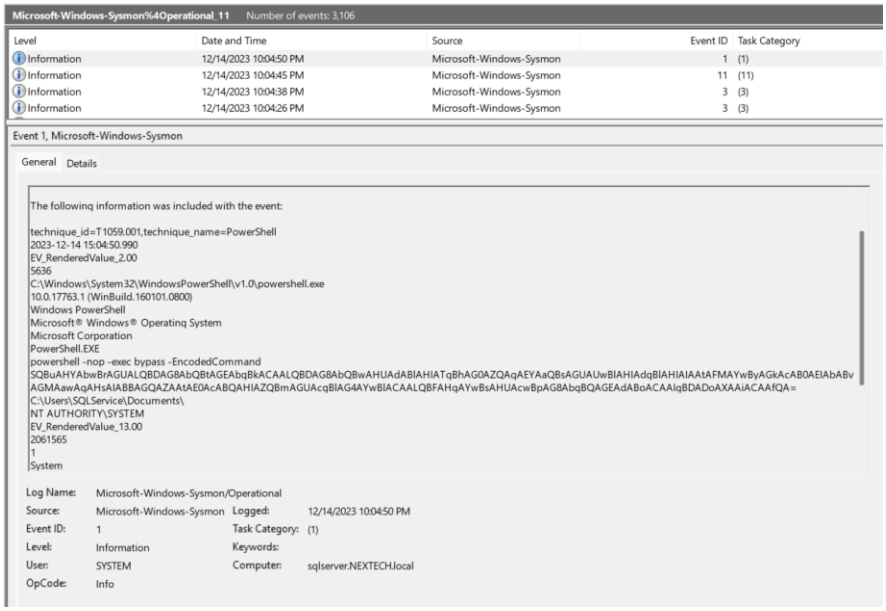
Vào lúc 10:04:24 attacker đã hiện encode 1 đoạn base64



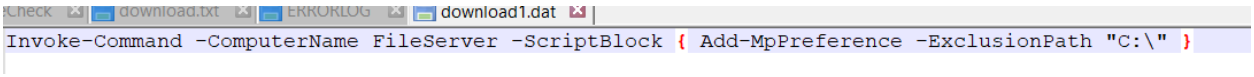
Sau khi giải mã đoạn mã trên mục đích là tắt windows defend trên máy FileServer bằng cách bật key DisableAntiSpyware



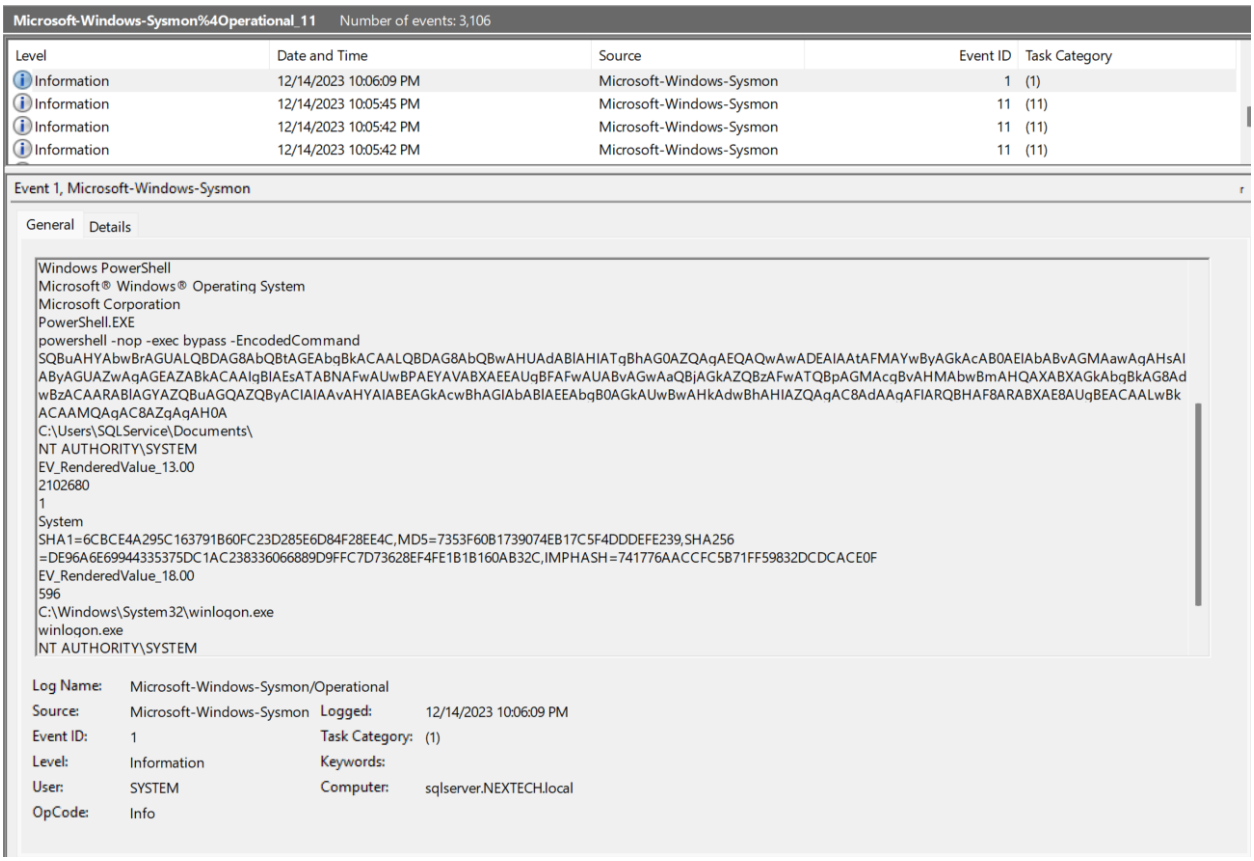
Vào lúc 10:04:50 attacker tiếp tục encode 1 đoạn base64

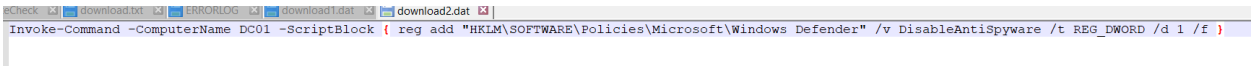


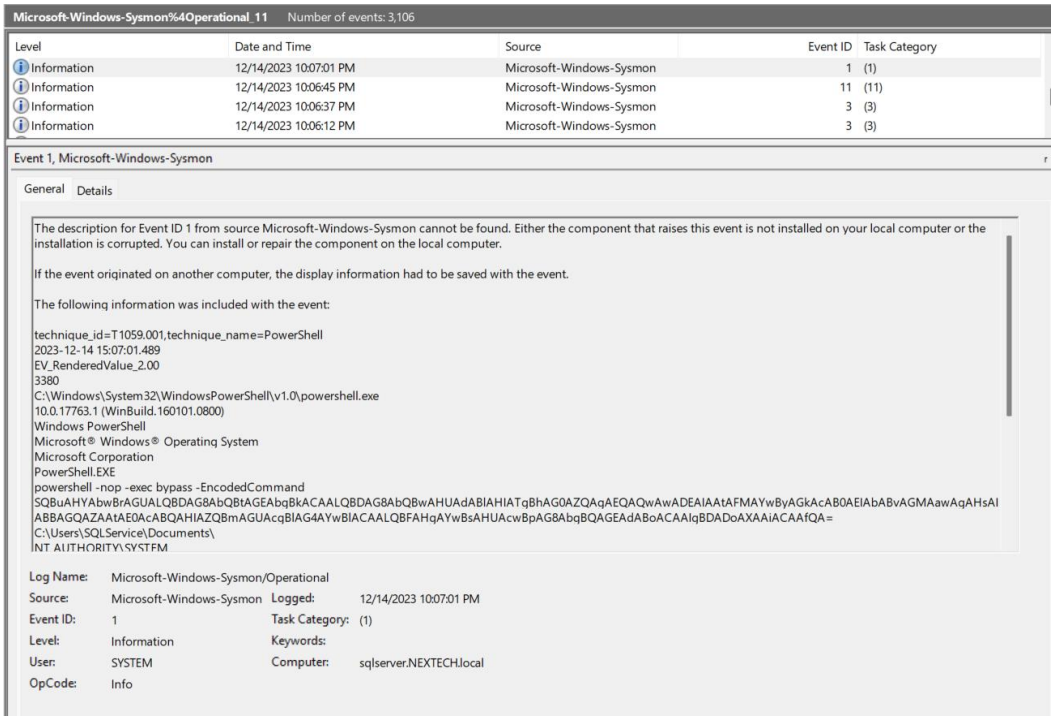
Sau khi giải mã đoạn đó thì mục đích của nó là loại trừ đường dẫn này của windows defend khiến nó không check các tệp ở đường dẫn C:\ khi thực thi



Vào lúc 10:06:09 attacker tiếp tục làm tương tự với máy DC01

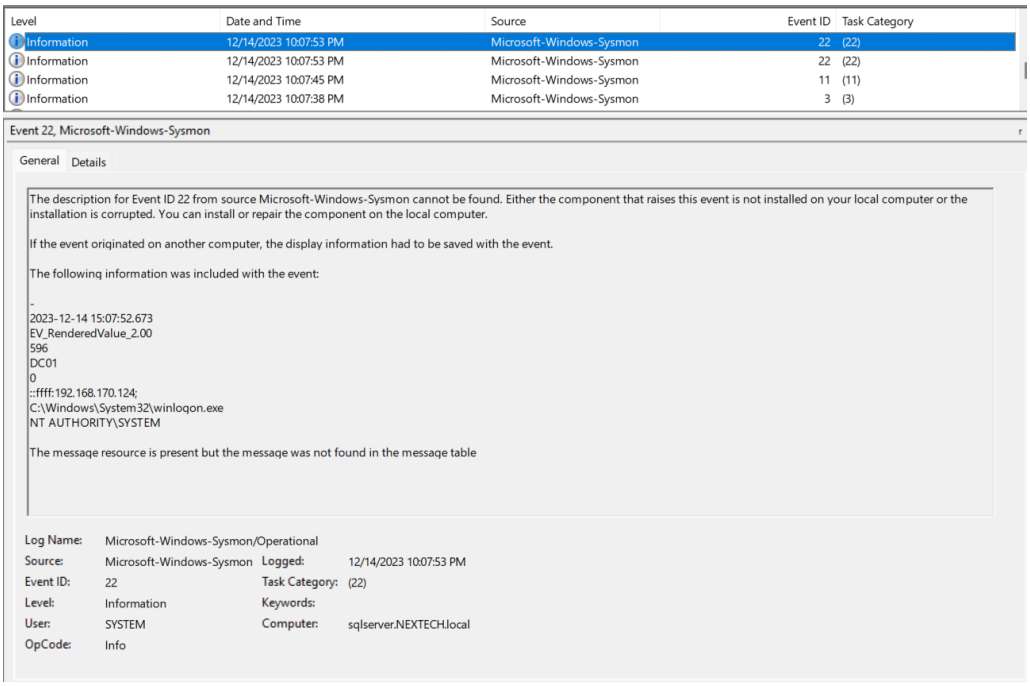




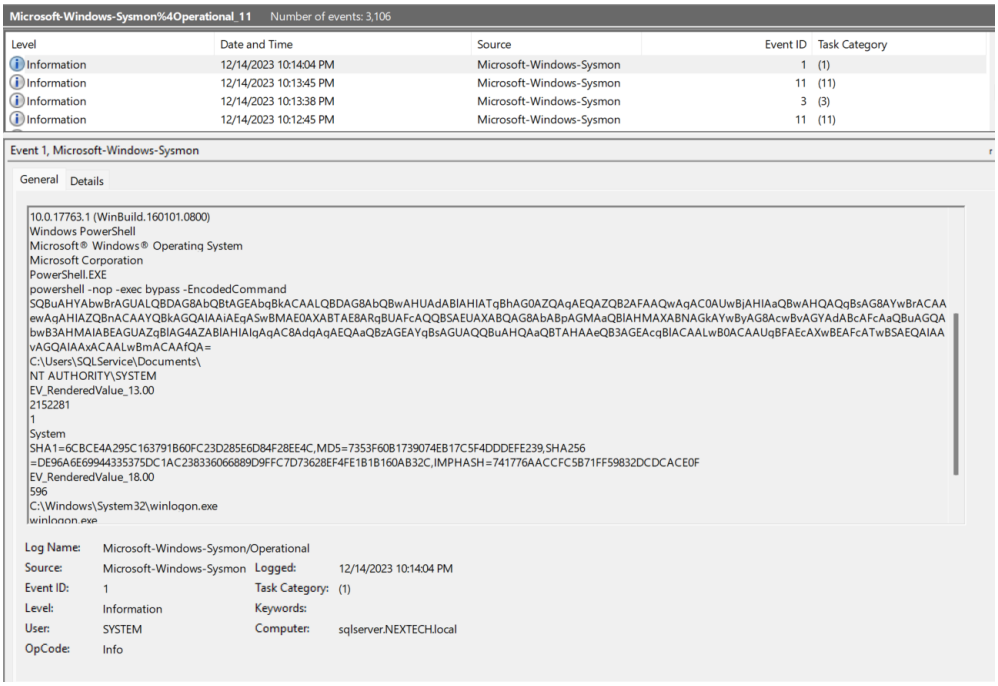



```
Invoke-Command -ComputerName DC01 -ScriptBlock { Add-MpPreference -ExclusionPath "C:\" }
```

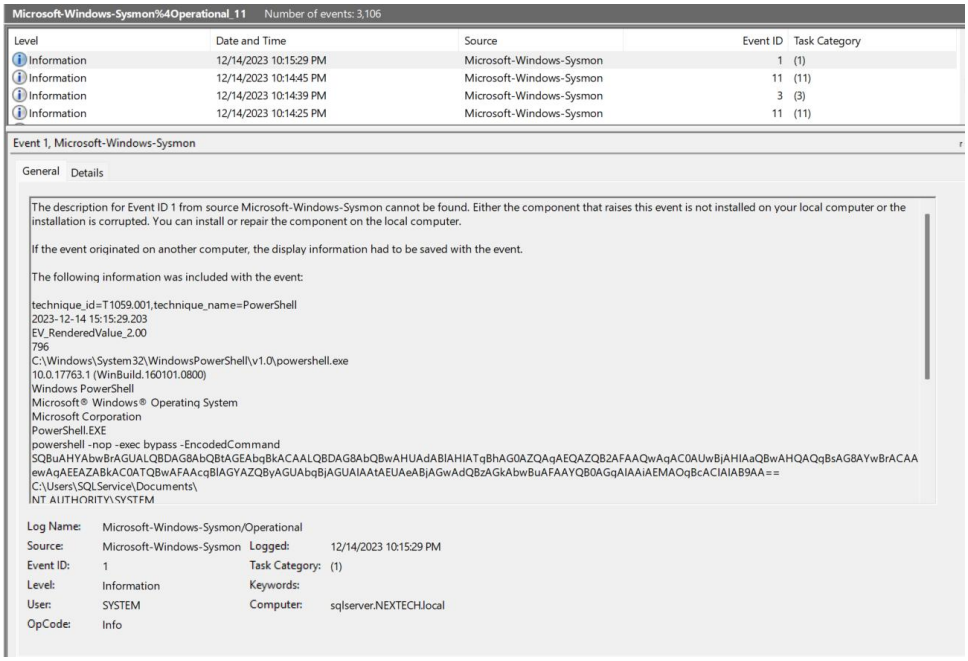
Vào lúc 10:07:53 attacker connect vào được máy DC01 và thực thi mẫu 8fe9c39.exe . Y như kết quả output của hayabusa ban đầu



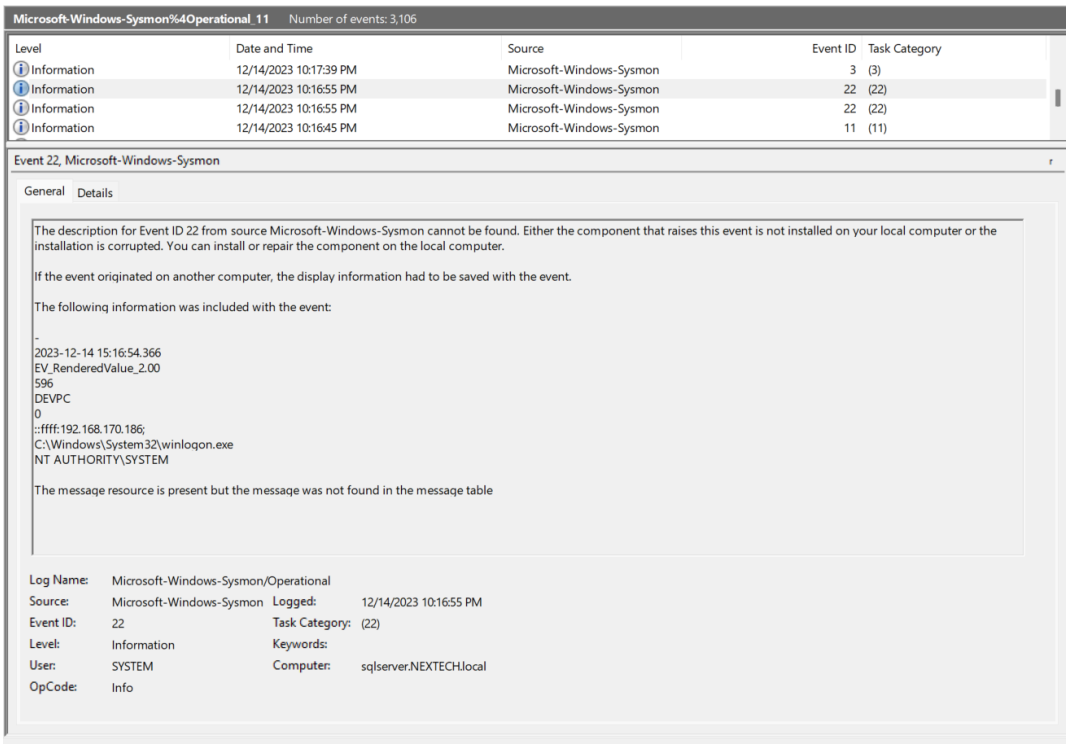
Lúc 10:14:04 attacker lại tiếp tục làm tương tự với máy DevPC




```
Invoke-Command -ComputerName DevPC -ScriptBlock { reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f }
```

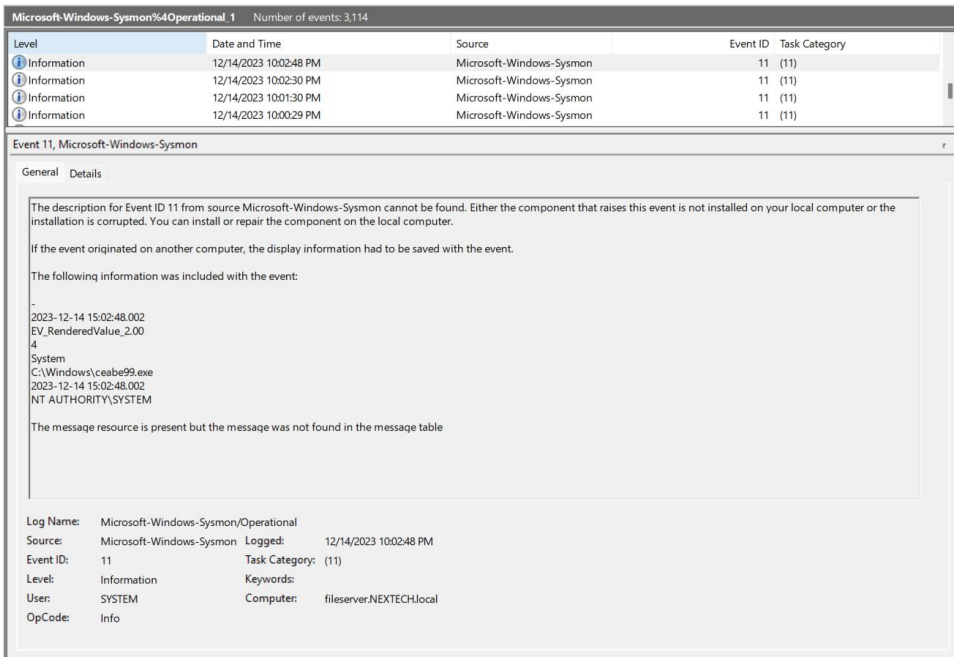



```
Invoke-Command -ComputerName DevPC -ScriptBlock { Add-MpPreference -ExclusionPath "C:\" }
```

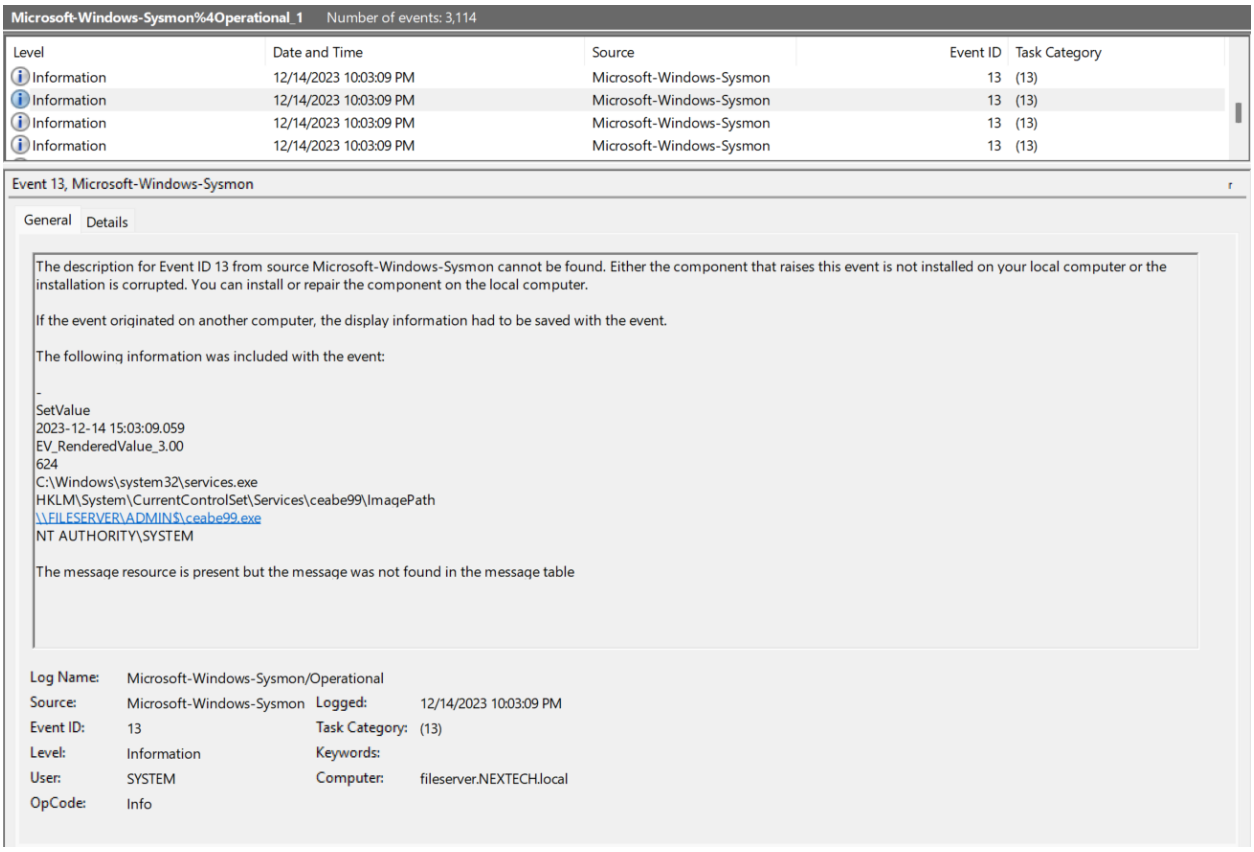


FileSever

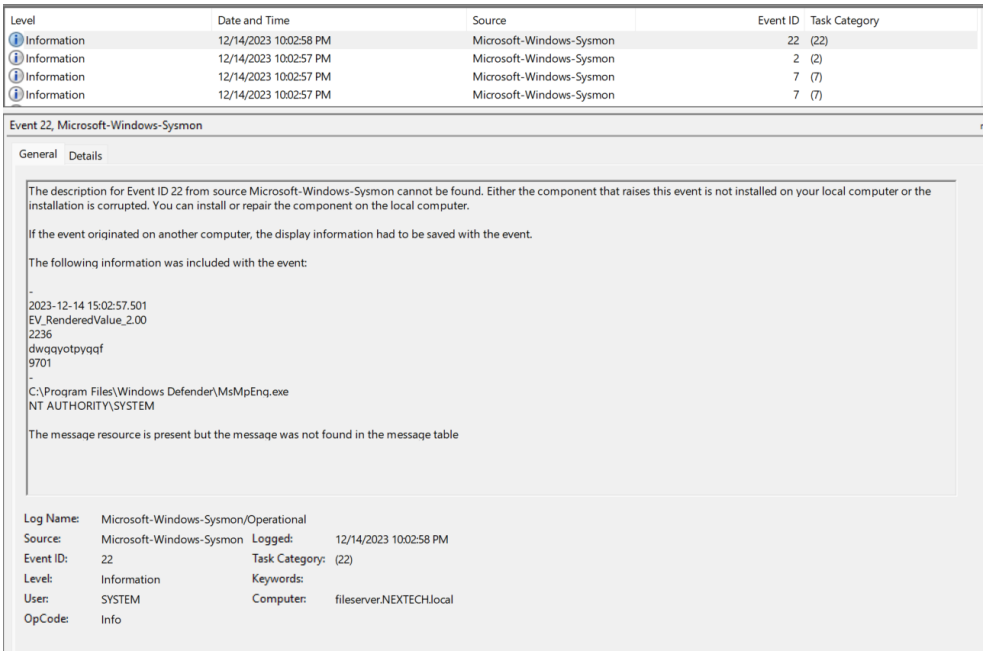
Như chúng ta đã phân tích bên trên có thể thấy vào lúc 10:02:48 1 mẫu tên là ceabe999.exe xuất hiện trên máy



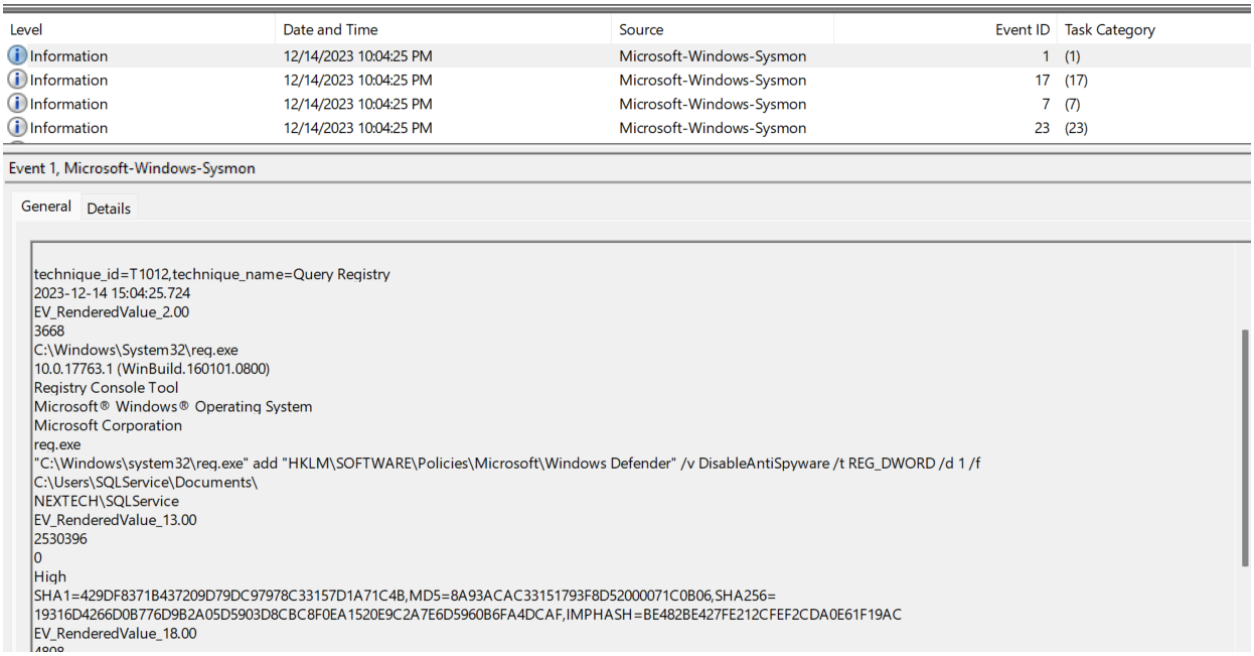
Có vẻ khi mẫu này được thực thi nó đã khởi tạo 1 service với name service là ceabe99



Nhưng mẫu này khi thực thị đã bị windows defend block đó là lý do tại sao attacker phải sử dụng các command được encode để tắt windows defend từ máy SQLServer



Đây là time mà attacker đã thực thi việc tắt windows defend để có thể thực thi mẫu mã độc trên máy FileServer do file trước đã bị block bởi windows defend



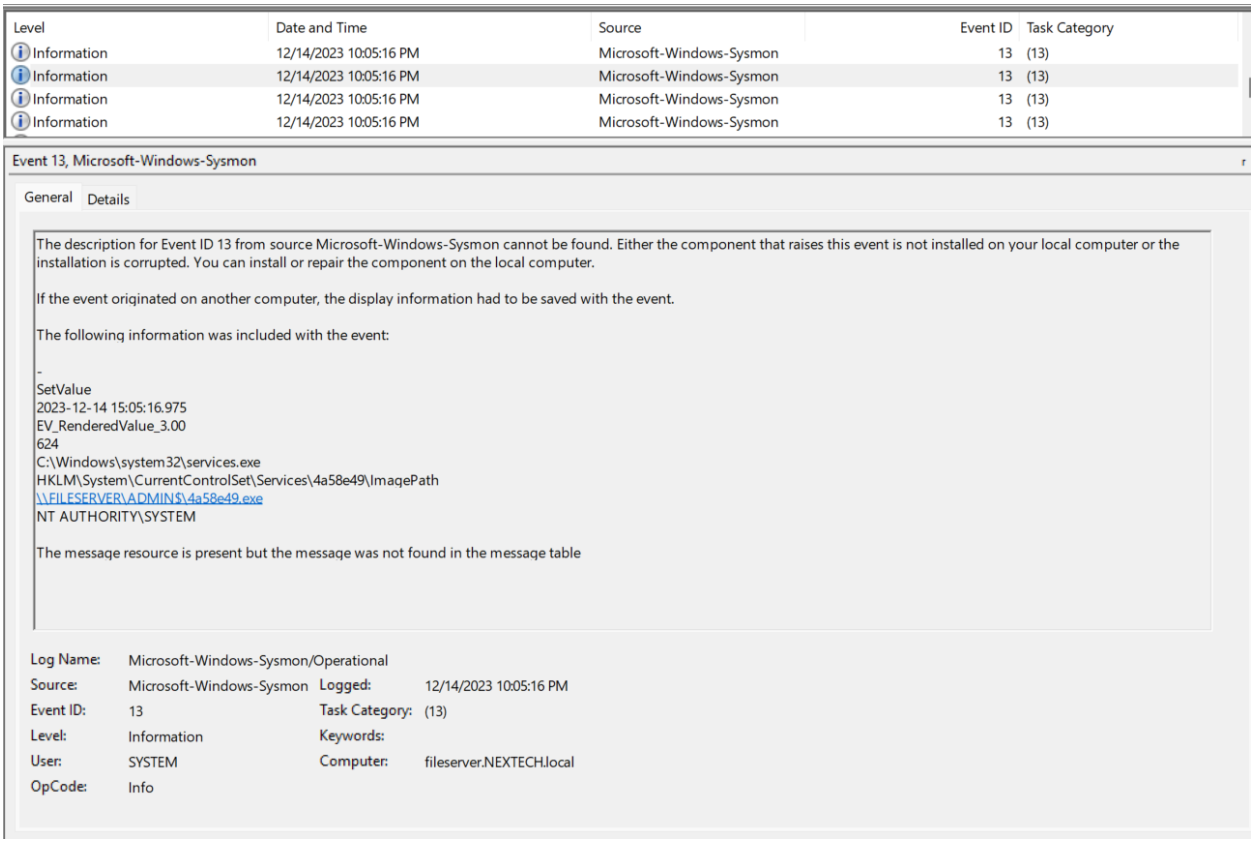
Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:04:25 PM	Microsoft-Windows-Sysmon	1	(1)
Information	12/14/2023 10:04:25 PM	Microsoft-Windows-Sysmon	17	(17)
Information	12/14/2023 10:04:25 PM	Microsoft-Windows-Sysmon	7	(7)
Information	12/14/2023 10:04:25 PM	Microsoft-Windows-Sysmon	23	(23)

Event 1, Microsoft-Windows-Sysmon

General Details

technique_id=T1012,technique_name=Query Registry
2023-12-14 15:04:25.724
EV_RenderedValue_2.00
3668
C:\Windows\System32\reg.exe
10.0.17763.1 (WinBuild.160101.0800)
Registry Console Tool
Microsoft® Windows® Operating System
Microsoft Corporation
reg.exe
"C:\Windows\system32\reg.exe" add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
C:\Users\SQLService\Documents\
NEXTECH\SQLService
EV_RenderedValue_13.00
2530396
0
High
SHA1=429DF8371B437209D79DC97978C33157D1A71C4B,MD5=8A93ACAC33151793F8D52000071C0B06,SHA256=
19316D4266D0B776D9B2A05D5903D8CBC8F0EA1520E9C2A7E6D5960B6FA4DCAF,IMPHASH=BE482BE427FE212CFEF2CDA0E61F19AC
EV_RenderedValue_18.00

Sau đó attacker đã thực thi lại 1 mẫu khác trên máy FileSever với tên là 4a58e49.exe .



Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:05:16 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 10:05:16 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 10:05:16 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 10:05:16 PM	Microsoft-Windows-Sysmon	13	(13)

Event 13, Microsoft-Windows-Sysmon

General Details

The description for Event ID 13 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

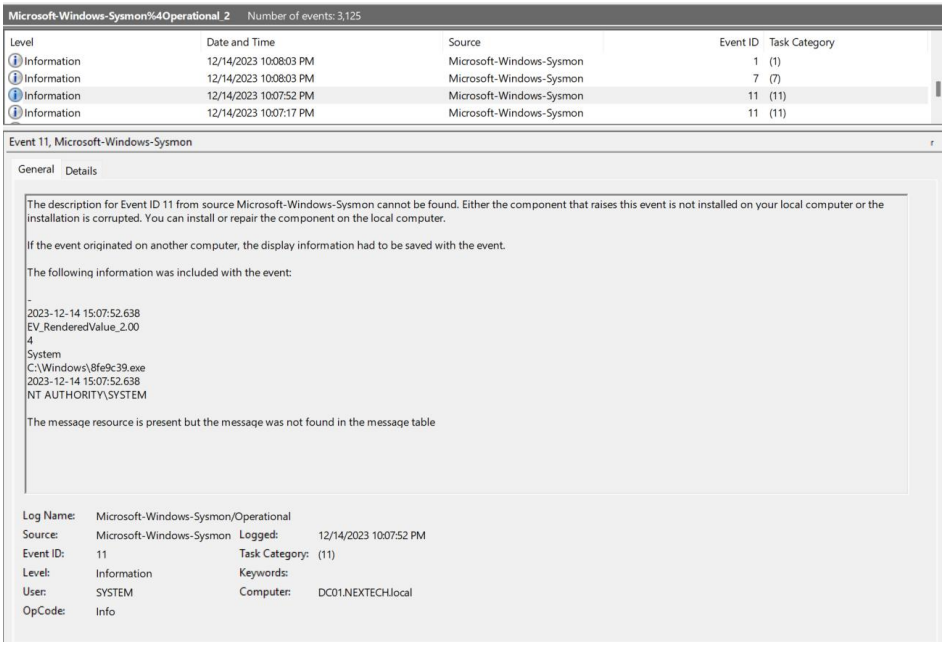
The following information was included with the event:

-
SetValue
2023-12-14 15:05:16.975
EV_RenderedValue_3.00
624
C:\Windows\system32\services.exe
HKLM\System\CurrentControlSet\Services\4a58e49\ImagePath
\\FILESERVER\ADMIN$\4a58e49.exe
NT AUTHORITY\SYSTEM

The message resource is present but the message was not found in the message table

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Microsoft-Windows-Sysmon	Logged:	12/14/2023 10:05:16 PM
Event ID:	13	Task Category:	(13)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	fileserver.NEXTECH.local
OpCode:	Info		

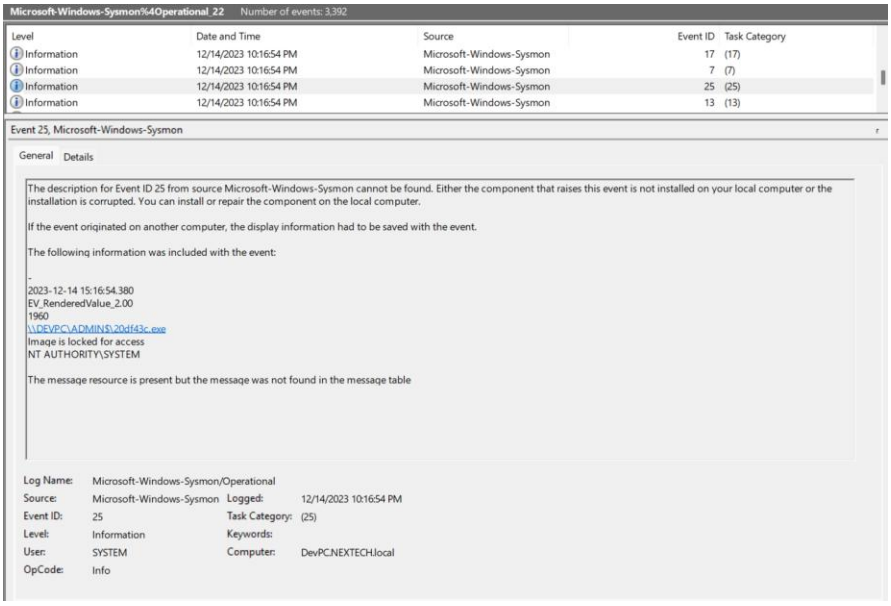
DC01



Đây là mẫu 8fe9c39.exe mà attacker đã drop trên máy DC01 và cho thực thi nó . Về cơ bản thì log tiếp theo sẽ giống với các hành vi mà attacker đã remote như phân tích ở máy SQLSever

DEVPC

Tương tự ứng với trên máy DevPC là mẫu có tên là 20df43c.exe



Sau khi các mẫu ở các máy chạy thì nó sẽ ra 1 file txt là với tên là HHuYRxB06.README.txt . Về cơ bản khi các mẫu được drop ở các máy chạy nó sẽ kết

nối tới miền IP của attacker và khởi tạo 1 service . Ở các máy chúng ta đều thấy attacker sử dụng kỹ thuật credential dumping để có dump mật khẩu từ trong mem ngoài ra attacker cũng đã Process Injection vào process winlogon.exe từ powershell

2 Mitre&ATTCK mapping

Brute Force: Password Guessing Brute Force: Password Guessing, Sub-technique T1110.001 - Enterprise | MITRE ATT&CK®

OS Credential Dumping OS Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK®

Lateral Tool Transfer Lateral Tool Transfer, Technique T1570 - Enterprise | MITRE ATT&CK®

Scheduled Task/Job Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®

Command and Scripting Interpreter Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®

Obfuscated Files or Information Obfuscated Files or Information, Technique T1027 - Enterprise | MITRE ATT&CK®

Impair Defenses: Disable or Modify Tools Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®

Process Injection Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®