

# TryHackMe: Conti Room - Threat Hunting Project Report

---

## 1. Introduction

This report outlines the step-by-step threat hunting investigation conducted in the TryHackMe 'Conti' Splunk room. The goal was to investigate a ransomware attack against a Microsoft Exchange Server using Splunk logs. Tasks included identifying the ransomware, tracing execution, uncovering attacker persistence, and identifying the vulnerabilities (CVEs) exploited.

## 2. Objectives

- Identify the location of the ransomware.
- Determine the Sysmon event ID for the file creation.
- Retrieve the MD5 hash of the ransomware.
- Identify files saved across multiple directories.
- Discover the command used to add a new user.
- Identify process migration details.
- Detect the deployed web shell.
- Uncover the command line that executed the web shell.
- Identify the CVEs leveraged during exploitation.

## 3. Methodology

### 3.1 Splunk Access and Time Range Setup

Accessed the provided Splunk instance. Initial searches returned no data due to incorrect time filters. Adjusted the time range to 'All Time' and confirmed log availability using broad queries like `index=\*`.

### 3.2 Locating the Ransomware

Used the following query to identify suspicious executables:

```
'index=* EventCode=11 TargetFilename="*.exe"
```

The ransomware was found at:

```
'C:\Users\Administrator\Documents\cmd.exe'
```

Splunk query: index=\* EventCode=11 TargetFilename="\*.exe"

```
| table _time TargetFilename Image User
```

✓ 8 events (before 6/29/25 4:47:25.000 AM) No Event Sampling			Job	Smart Mode
Events	Patterns	Statistics (B)	Visualization	
20 Per Page	Format	Preview		
_time #	TargetFilename #	Image #	User #	
2021-09-08 12:54:18	C:\Users\ADMINI-1.BEL\AppData\Local\Temp\0866ff10-0412-4762-a1ab-8a1d288e1310\DiskHost.exe	C:\Windows\system32\cleanmgr.exe	NOT_TRANSLATED	
2021-09-08 12:49:02	C:\Windows\SYSTEMC-1\METWOR-1\appdata\Local\Temp\upan-8d1a62c.exe	C:\Program Files\Windows Defender\MpCmdRun.exe	NOT_TRANSLATED	
2021-09-08 12:48:52	C:\Windows\SYSTEMC-1\METWOR-1\appdata\Local\Temp\upan-e1bdf6df.exe	C:\Program Files\Windows Defender\MpCmdRun.exe	NOT_TRANSLATED	
2021-09-08 13:08:43	C:\Windows\SYSTEMC-1\METWOR-1\appdata\Local\Temp\upan-12a45010.exe	C:\Program Files\Windows Defender\MpCmdRun.exe	NOT_TRANSLATED	
2021-09-08 13:08:35	C:\Windows\SYSTEMC-1\METWOR-1\appdata\Local\Temp\upan-69a0ed8.exe	C:\Program Files\Windows Defender\MpCmdRun.exe	NOT_TRANSLATED	
2021-09-08 12:55:08	C:\Users\Administrator\Documents\cmd.exe	C:\Windows\system32\lwpexecapp.exe	NOT_TRANSLATED	
2021-09-08 12:35:40	C:\Windows\SYSTEMC-1\METWOR-1\appdata\Local\Temp\upan-94344dc.exe	C:\Program Files\Windows Defender\MpCmdRun.exe	NOT_TRANSLATED	
2021-09-08 12:35:30	C:\Windows\SYSTEMC-1\METWOR-1\appdata\Local\Temp\upan-cdc089d.exe	C:\Program Files\Windows Defender\MpCmdRun.exe	NOT_TRANSLATED	

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

ENG IN 17:17 29-06-2025

### 3.3 Sysmon Event ID Identification

Event ID 11 was confirmed as the Sysmon event for file creation.

### 3.4 Retrieving the MD5 Hash

Hashes were not returned using standard fields. Instead, searched for hash-like strings:

```
'index=* | regex _raw="(?i)[a-f0-9]{32}"'
```

MD5 hash found: `290C7DFB01E50CEA9E19DA81A781AF2C`

Query: index=\* EventCode=1 Image="C:\Users\Administrator\Documents\cmd.exe"

```
| table _time Image CommandLine Hash
```

New Search			Save As	Create Table View	Close
<input 2="" _raw"="" _time="" c:\users\administrator\documents\cmd.exe"="" table="" type="text" value="1 index=* "  =""/>			All time		
<b>✓ 23 events (before 6/29/25 5:07:16.000 AM) No Event Sampling</b>					
Events	Patterns	Statistics (23)	Visualization		
20 Per Page	Format	Preview			
_time #	_raw #				
2021-09-08 13:08:23	09/08/2021 04:08:23 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=11 EventID=4 ComputerName=WN-A0QKG2AS2Q7.bellybear.local User=NOT_TRANSLATED SidS=1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=FileCreation RecordNumber=3213 Keywords=None TaskCategory=File created (rule: FileCreate) OpCode=Info Message=File created:				

10.10.104.94:8000/en-US/app/search/search?earliest=0&latest=&q=search index=\* "C:\Users\Administrator\Documents\cmd.exe">%0A|table \_...\_raw.general.type=statistics&display.page.search.tab=statistics&display.prefs.events.count=50&display.events.type=list&sid=175198836.79#

```

20 Per Page ▾ Format Preview ▾
_time # _raw
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=3136
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpcodeInfo
Message=Process Create:
RuleName=
UtcTime: 2021-09-08 20:05:32.431
ProcessId: (72893baa-17bc-6139-b402-00000000c00)
ProcessId: 15548
Image: C:\Users\Administrator\Documents\cmd.exe
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
CommandLine: cmd.exe
CurrentDirectory: c:\Users\Administrator\Documents\
User: NT AUTHORITY\SYSTEM
LogonGuid: {72893baa-111d-6139-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5:00070F0B15C6EAE5E50A31A731F0C SHA256:5381C1B2F41A7FC300E57D036E57539453FF82801003F64BF87F4896BF9CA22,IMPHASH:23F8157850B238377F4513BE540B4574
ParentProcessId: (72893baa-17bc-6139-7192-00000000c00)
ParentProcessId: 7408
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe

```

### 3.5 Detecting Replicated Files

To find files saved to multiple locations:

`index=\* EventCode=11 TargetFilename="\*.txt" | stats count by TargetFilename`

Answer: `readme.txt`

While i was on the same query I observed that repeated readme.txt files were saved.

```

20 Per Page ▾ Format Preview ▾
_time # _raw
EventID=4
ComputerName=WIN-AOKGQ2AS2Q7.bellybear.local
User=NOT_TRANSLATED
SID=S-1-5-18
SNTType=18
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=3213
Keywords=None
TaskCategory=File created (rule: FileCreate)
OpcodeInfo
Message=File created:
RuleName: Downloads
UtcTime: 2021-09-08 20:08:23.762
ProcessId: (72893baa-17bc-6139-b402-00000000c00)
ProcessId: 15548
Image: c:\Users\Administrator\Documents\cmd.exe
TargetFilename: C:\Users\Public\Downloads\readme.txt
CreationTime: 2021-09-08 20:08:23.759
2021-09-08 13:08:23
09/08/2021 04:08:23 PM
LogonGuid=Microsoft-Windows-Syman\Operational
EventCode=11
EventID=4
ComputerName=WIN-AOKGQ2AS2Q7.bellybear.local
User=NOT_TRANSLATED
SID=S-1-5-18
SNTType=18
SourceName=Microsoft-Windows-Syman
Type=Information
RecordNumber=3212

```

### 3.6 Attacker User Creation

Searched for net user commands:

`index=\* EventCode=1 CommandLine="\*net user\*"`

Identified the malicious account creation command.

Query:index=\* EventCode=1 Image="\*cmd.exe"

| table \_time Image CommandLine User

The screenshot shows the Splunk 8.2.2 interface with a search bar containing the query: `index=\* EventCode!=0 | search CommandLine=="net\* OR CommandLine=\*add\* | table \_time CommandLine` and a search result table below it.

**Search Results:**

_time	CommandLine	User
2021-09-08 13:07:58	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts	NOT_TRANSLATED NT AUTHORITY\LOCAL SERVICE
2021-09-08 13:07:22	"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:06:16	"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:05:54	"netsh* interface tcp show global	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:05:15	"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:04:15	"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	NOT_TRANSLATED NT AUTHORITY\SYSTEM

The screenshot shows the Splunk 8.2.2 interface with a search bar containing the query: `index=\* EventCode!=0 & q=search index%3D\* EventCode%3D1%20%0A| search CommandLine%3D"net\* OR CommandLine%3D\*add\*%0A` and a search result table below it.

**Search Results:**

_time	CommandLine	User
2021-09-08 13:05:54	"netsh* interface tcp show global	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:05:15	"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:04:15	"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:04:11	C:\Windows\system32\net1 localgroup "Remote Desktop Users" "securityninja" /add	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:04:11	net localgroup "Remote Desktop Users" "securityninja" /add	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:04:10	C:\Windows\system32\net1 localgroup administrators securityninja /add	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:04:10	net localgroup administrators securityninja /add	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:04:10	C:\Windows\system32\net1 user /add securityninja hardToHack123\$	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:04:10	net user /add securityninja hardToHack123\$	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:03:15	"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	NOT_TRANSLATED NT AUTHORITY\SYSTEM
2021-09-08 13:02:15	"C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe"	NOT_TRANSLATED NT AUTHORITY\SYSTEM

### 3.7 Process Migration

Tried EventCode=10 (ProcessAccess) but found no logs. Used EventCode=8 (CreateRemoteThread) as hinted:

`index=\* EventCode=8`

Found process injection from `powershell.exe` into `webscrab.exe`, leading to the answer: `webscrab.exe, powershell.exe`

Query: index=\* EventCode=1

```
| table _time ParentImage Image CommandLine
```

```
| sort _time
```

### 3.8 Identifying the Web Shell

Analyzed IIS POST requests:

`index=\* sourcetype=iis cs\_method=POST`

Web shell identified: `i3gfPctK1c2x.aspx`

_time	cs_method	cs_uri_stem	cs_uri_query	clientip
2021-09-08 12:51:58	POST	/owa/auth/i3gfPctK1c2x.aspx	&CorrelationID=<empty>;&cafeReqId=e4f48fdc-0910-4b2e-9481-8802eee61b57;&encoding=	
2021-09-08 12:51:58	POST	/owa/auth/i3gfPctK1c2x.aspx	&CorrelationID=<empty>;&cafeReqId=3e3e8de6-8ffd-4a75-9719-de8fb420a4d9;&encoding=	
2021-09-08 12:51:41	POST	/owa/auth/i3gfPctK1c2x.aspx	&CorrelationID=<empty>;&cafeReqId=afab08cf1-bfd0-48c7-bc3e-210f5663a4d2;&encoding=	
2021-09-08 12:51:36	POST	/owa/auth/i3gfPctK1c2x.aspx	&CorrelationID=<empty>;&cafeReqId=520cd2ae-eff4-45cf-a7fd-8866a3e3c0fe;&encoding=	

### 3.9 Web Shell Execution Command

Searched for the execution command via EventCode=1:

`attrib.exe -r \\win-aoqkg2as2q7.bellybear.local\C\$\...\\i3gfPctK1c2x.aspx`

The screenshot shows the Splunk Enterprise search interface. The search bar at the top contains the query: `1 index= EventCode=1 CommandLine="/jgPctk1c2x.aspx" 2 | table \_time Image CommandLine ParentImage` with the time range set to "All time". Below the search bar, the "Statistics" tab is selected. The search results table shows two events. Both events occurred on 2021-09-08 at 12:52:09. The first event's process is C:\Windows\System32\attrib.exe, its command line is httpd.exe -r \\\win-and-g2azn\bellybear\local\C\$\Program Files\Microsoft\Exchange Server\V15\FromEnd\HttpProxy\owaauth\1\jgPctk1c2x.aspx, and its parent image is C:\Windows\System32\cmd.exe. The second event has identical details. The interface includes various navigation and configuration buttons like "Events", "Patterns", "Format", "Preview", and "Job".

### 3.10 CVE Identification

The most challenging step. Attempted multiple chains (ProxyLogon, ProxyShell, ProxyNotShell) before external research confirmed:

`CVE-2021-34473,CVE-2021-34523,CVE-2021-31207`

Unfortunately I couldn't find the right answer to this question

### 4. Challenges Faced

- Initial lack of data due to incorrect time range.
- Missing hash values in standard fields.
- Difficulty confirming the CVEs without clear evidence.
- No EventCode=10 logs made process injection harder to confirm.

### 5. Conclusion

The room provided hands-on experience in using Splunk to hunt threats in Windows environments. Despite challenges with log completeness and CVE confirmation, a methodical approach led to successful identification of ransomware activity, attacker persistence, and web shell exploitation.

Answer the questions below

Can you identify the location of the ransomware?

✓ Correct Answer

💡 Hint

What is the Sysmon event ID for the related file creation event?

✓ Correct Answer

Can you find the MD5 hash of the ransomware?

✓ Correct Answer

What file was saved to multiple folder locations?

✓ Correct Answer

What was the command the attacker used to add a new user to the compromised system?

✓ Correct Answer

The attacker migrated the process for better persistence. What is the migrated process image (executable), and what is the original process image (executable) when the attacker got on the system?

✓ Correct Answer

💡 Hint

The attacker migrated the process for better persistence. What is the migrated process image (executable), and what is the original process image (executable) when the attacker got on the system?

✓ Correct Answer

💡 Hint

The attacker also retrieved the system hashes. What is the process image used for getting the system hashes?

✓ Correct Answer

💡 Hint

What is the web shell the exploit deployed to the system?

✓ Correct Answer

💡 Hint

What is the command line that executed this web shell?

✓ Correct Answer

💡 Hint

What three CVEs did this exploit leverage? Provide the answer in ascending order.

✍ Submit

💡 Hint