

Conti Ransomware – Splunk Write-Up & Report



TryHackMe – Conti room

Scenario: Employees reported issues accessing Outlook, and the Exchange admin couldn't log into the Admin Center. During triage, ransom notes were found on the Exchange server, indicating a likely ransomware attack. The situation now calls for immediate investigation, log analysis, and response to identify the scope of the attack and how the threat actor gained access.

Executive Summary

This report details an investigation into a simulated Conti ransomware intrusion using Splunk log data provided in the TryHackMe environment. The objective was to expand on the given questions to further identify and understand the tactics, techniques, and procedures (TTPs) used by the attacker, following the MITRE ATT&CK framework where applicable. The investigation was approached from the perspective of a SOC analyst tasked with threat hunting, detection validation, and preliminary incident reporting.

The screenshot shows the Splunk Search interface. At the top, there are navigation tabs: Search, Analytics, Datasets, Reports, Alerts, and Dashboards. A search bar contains the query `index=* earliest=0`. Below the search bar, it indicates 28,145 events from 8/5/25 4:00:00.000 PM to 8/6/25 4:37:12.000 PM. The interface includes various controls like 'Save As', 'Create Table View', 'Close', 'Last 24 hours', 'Smart Mode', and 'No Event Sampling'. Below the search bar, there are tabs for 'Events (28,145)', 'Patterns', 'Statistics', and 'Visualization'. The main area shows a list of search results with columns for 'Time' and 'Event'. The first result is from 9/8/21 1:08:55.000 PM, with event details including LogName, EventCode, EventType, and ComputerName. The second result is from 9/8/21 1:08:55.000 PM, with similar details. The interface also includes a 'List' view, 'Format' options, and a '20 Per Page' setting.

i	Time	Event
>	9/8/21 1:08:55.000 PM	09/08/2021 04:08:55 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=WIN-AOQKG2AS2Q7.bellybear.local Show all 33 lines host = WIN-AOQKG2AS2Q7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	9/8/21 1:08:55.000 PM	09/08/2021 04:08:55 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=WIN-AOQKG2AS2Q7.bellybear.local Show all 33 lines

Question 1: Can you identify the location of the ransomware?

To begin the analysis, I perform a high-level survey of the available log data. This includes identifying all the key components in the environment such as Users, Hosts, Sources, etc. Then moving towards answering this question I started with a

simple .exe search under EventCode = 11 for file creation to get a broad overview, and was surprised with the good results.

The screenshot shows the Splunk Search & Reporting interface. At the top, there are navigation tabs: Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Search & Reporting' tab is active. Below the navigation is a 'New Search' header with options for 'Save As', 'Create Table View', and 'Close'. The search query is entered in a text box: `1 index=* earliest=0 TargetFilename=*.exe` and `2 | sort _time`. A dropdown menu shows 'Last 24 hours' and a search icon. Below the search bar, it indicates '8 events (8/5/25 5:00:00.000 PM to 8/6/25 5:40:23.000 PM)'. There are also options for 'No Event Sampling', 'Job', and 'Smart Mode'. The main content area is titled 'Events (8)' and has tabs for 'Patterns', 'Statistics', and 'Visualization'. Below this, there are zoom controls: 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect'. A timeline visualization shows a single green bar representing an event. Below the timeline, there are options for 'List', 'Format', and '20 Per Page'. The main table has columns for 'Time' and 'Event'. The first event is expanded to show details: `09/06/2021 03:35:30 PM`, `LogName=Microsoft-Windows-Sysmon/Operational`, `EventCode=11`, `EventType=4`, `ComputerName=WIN-AOQKG2AS2Q7.bellybear.local`, `User=NOT_TRANSLATED`, `Sid=S-1-5-18`, `SidType=0`, `SourceName=Microsoft-Windows-Sysmon`, `Type=Information`, `RecordNumber=802`, `Keywords=None`, `TaskCategory=File created (rule: FileCreate)`, `OpCode=Info`, `Message=File created:`, `RuleName: EXE`, `UtcTime: 2021-09-06 19:35:30.641`, `ProcessGuid: {72893ba8-6d82-6136-c202-00000000b00}`, and `ProcessId: 12644`.

Only 8 results! This is a great start as it gives a much narrower starting point.

INTERESTING FIELDS

- a ComputerName 1
- a CreationUtcTime 8
- # EventCode 1
- # EventType 1
- a Image 3
- a index 1
- a Keywords 1
- # linecount 1
- a LogName 1
- a Message 8
- a OpCode 1
- a ProcessGuid 5
- # ProcessId 5
- a punct 1
- # RecordNumber 8
- a RuleName 1
- a Sid 1
- # SidType 1
- a SourceName 1
- a splunk_server 1
- a TargetFilename 8
- a TaskCategory 1
- a Type 1
- a User 1
- a UtcTime 8

+ Extract New Fields

```

User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=802
Keywords=None
TaskCategory=File_created (rule: FileCreate)

```

TargetFilename X

8 Values, 100% of events Selected

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
C:\Users\ADMINI~1\BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\DismHost.exe	1	12.5%
C:\Users\Administrator\Documents\cmd.exe	1	12.5%
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-12a45010.exe	1	12.5%
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-69a0ed8.exe	1	12.5%
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-8d1a62c.exe	1	12.5%
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-94344dcc.exe	1	12.5%
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-cd0cd89d.exe	1	12.5%
C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\mpam-e1bdf6df.exe	1	12.5%

And already, just by simply getting narrow starting results and analyzing through the TargetFileNames listed in the fields, I have already found an unusual location which is the correct answer! Answer: C:\Users\Administrator\Documents\cmd.exe

Question 2: What is the Sysmon event ID for the related file creation event?

The last question answered this for us as I included the Sysmon EventCode in my previous search. Answer: 11

Question 3: Can you find the MD5 hash of the ransomware?

My initial thoughts in finding this hash was analyzing activity near the log where I found location of the ransomware. I did this by including a specific time in the search to analyze activity directly after the file creation.

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Create Table View Close

```
1 index=* earliest= "09/08/2021:12:59:00" latest= "09/08/2021:19:59:59"
2 | sort _time
```

Last 24 hours Q

✓ 1,323 events (9/8/21 12:59:00.000 PM to 9/8/21 7:59:59.000 PM) Job Job Smart Mode

No Event Sampling ↓

Events (1,323) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 ... Next >

	i	Time	Event
<p>< Hide Fields All Fields</p> <p>SELECTED FIELDS</p> <ul style="list-style-type: none"> a host 1 a source 6 a sourcetype 6 <p>INTERESTING FIELDS</p> <ul style="list-style-type: none"> a Account_Domain 5 a Account_Name 7 a ComputerName 1 # EventCode 41 # EventType 4 a index 1 a Keywords 3 # linecount 20 a LogName 4 	>	9/8/21 12:59:03.000 PM	2021-09-08 19:59:03 127.0.0.1 GET /mapi/emsmdb mailboxId=9b329a78-b73f-41df-bc61-4c59076bda3b@bellybear.local&CorrelationID=<empty>;&cafeReqId=cf8369e7-e2e9-4d19-b2b8-cc5a7fc127bf; 443 BELLYBEAR\HealthMailboxdf2ca 127.0.0.1 AMPProbe/Local/ClientAccess - 200 0 0 5 host = WIN-AOQKG2AS2Q7 source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex210908.log sourcetype = iis
	>	9/8/21 12:59:03.000 PM	2021-09-08 19:59:03 ::1 GET /ews/ &CorrelationID=<empty>;&cafeReqId=f16f2cba-19b2-4106-b354-28c889311956; 443 BELLYBEAR\HealthMailboxdf2ca ::1 AMPProbe/Local/ClientAccess - 200 0 0 5 host = WIN-AOQKG2AS2Q7 source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex210908.log sourcetype = iis
	>	9/8/21 12:59:03.000 PM	2021-09-08 19:59:03 ::1 GET /ecp/ReportingWebService/ &CorrelationID=<empty>;&cafeReqId=6d5a8c6c-5353-4477-a0d9-e8631df660bc;&LogoffReason=TokenCookiesGetOrF14AuthPost 443 - ::1 AMPProbe/Local/ClientAccess - 302 0 0 5

This did not end up yielding the results I wanted and wasn't narrow enough. Next, I changed the search which included "(Hash OR MD5)" to yield only results with hashes. I then broadened the time frame and went through adding each of the fields (one by one) to obtain a precise result.

New Search Save As ▾ Create Table View Close

1 index=* earliest=0 *cmd.exe (Hash OR MD5) Image="C:\Users\Administrator\Documents\cmd.exe" | Last 24 hours 🔍

✓ 1 event (8/5/25 6:00:00.000 PM to 8/6/25 6:27:11.000 PM) No Event Sampling ▾ Job ▾ || ■ ↶ ↷ ⬇ ⚙ Smart Mode ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect 1 month per column

List ▾ ↗ Format 50 Per Page ▾

< Hide Fields	☰ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		>	9/8/21 1:05:32.000 PM	09/08/2021 04:05:32 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=WIN-A0QKG2AS2Q7.bellybear.local User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=3136 Keywords=None TaskCategory=Process Create (rule: ProcessCreate) OpCode=Info Message=Process Create: RuleName: - UtcTime: 2021-09-08 20:05:32.431 ProcessGuid: {72893ba8-178c-6139-b402-00000000c00} ProcessId: 15540 Image: C:\Users\Administrator\Documents\cmd.exe FileVersion: - Description: - Product: - Company: - OriginalFileName: -

Adding the previously found "Image" field gave me the correct result and hash value.
 Answer: 290C7DFB01E50CEA9E19DA81A781AF2C

And to confirm this hash value is the ransomware, we can use VirusTotal.

61 / 70
Community Score -146

61/70 security vendors flagged this file as malicious

53b1c1b2f41a7fc300e97d036e57539453ff82001dd3feabf07f4896b1f9ca22
53b1c1b2f41a7fc300e97d036e57539453ff82001dd3feabf07f4896b1f9ca22.exe

Size: 190.00 KB | Last Analysis Date: 16 days ago

peexe detect-debug-environment runtime-modules calls-wmi direct-cpu-clock-access long-sleeps cve-2014-3931 exploit

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 18+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label [ransomware.conti/encoder](#) Threat categories [ransomware](#) [trojan](#) Family labels [conti](#) [encoder](#) [conticrypt](#)

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Ransomware/Win.Conti.R372647
Alibaba	Ransom:Win32/ContiCrypt.b7a00109	AliCloud	RansomWare
ALYac	Trojan.Ransom.Conti	Antiy-AVL	Trojan[Ransom]/Win32.Encoder
Arcabit	Trojan.Ransom.Conti.135	Arctic Wolf	Unsafe
Avast	Win32:Conti-B [Ransom]	AVG	Win32:Conti-B [Ransom]
Avira (no cloud)	HEUR/AGEN.1366989	BitDefender	Gen:Variant.Ransom.Conti.135
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Ransomware.Conti-9826703-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.ransomware.conti
%2520ac%253Aruntime-modules	Malicious (score: 100)	DnWeb	Trojan.Encoder.34230

Question 4: What file was saved to multiple folder locations?

For this question I immediately altered my search back to EventCode = 11 for file creations. I needed a way to analyze the name of a file and where it was saved to — excluding how many times it was. I ended up with this search fairly quickly.

New Search Save As Create Table View Close

```

1 index=* earliest=0 EventCode=11 ComputerName="WIN-A0QKG2AS2Q7.bellybear.local"
2 | dedup TargetFilename
3 | table TargetFilename EventCode

```

Last 24 hours

✓ 88 events (8/5/25 6:00:00.000 PM to 8/6/25 6:44:19.000 PM) No Event Sampling Job Smart Mode

Events Patterns **Statistics (88)** Visualization

100 Per Page

TargetFilename	Event
C:\Users\.NET v4.5 Classic\Downloads\readme.txt	
C:\Users\.NET v4.5\Downloads\readme.txt	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\AppxProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\AssocProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\CbsProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\CompatProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\DisMCore.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\DisMCorePS.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\DisMHost.exe	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\DisMProv.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\DmiProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\FfuProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\FolderProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\GenericProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\IBSProvider.dll	
C:\Users\ADMINI~1.BEL\AppData\Local\Temp\F0B6BF10-0412-4762-A1AB-8A1D2B8E131D\ImagingProvider.dll	

Question 5: What was the command the attacker used to add a new user to the compromised system?

I started this question with a simple EventCode = 4720 to see new user created events. I got one result which added the suspicious user *securityninja*, perfect! However, this specific log does not give me the command the attacker used. My next step is to discover the command used listed via the CommandLine field. Because I do not know the exact syntax for adding a user, I simply added securityninja to the search, along with "CommandLine=*" to find the answer. Answer: net user /add securityninja hardToHack123\$

Hide Fields All Fields List ▾ Format 50 Per Page ▾		
i	Time	Event
		ParentImage: C:\Windows\System32\net.exe ParentCommandLine: net localgroup administrators securityninja /add Show all 37 lines host = WIN-AOQKG2AS2Q7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	9/8/21 1:04:10.000 PM	09/08/2021 04:04:10 PM ... 22 lines omitted ... Company: Microsoft Corporation OriginalFileName: net.exe CommandLine: net localgroup administrators securityninja /add CurrentDirectory: C:\Windows\system32\ Show all 37 lines host = WIN-AOQKG2AS2Q7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	9/8/21 1:04:10.000 PM	... 24 lines omitted ... OriginalFileName: net1.exe CommandLine: C:\Windows\system32\net1 user /add securityninja hardToHack123\$ CurrentDirectory: C:\Windows\system32\ ... 8 lines omitted ... ParentImage: C:\Windows\System32\net.exe ParentCommandLine: net user /add securityninja hardToHack123\$ Show all 37 lines host = WIN-AOQKG2AS2Q7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	9/8/21 1:04:10.000 PM	09/08/2021 04:04:10 PM ... 22 lines omitted ... Company: Microsoft Corporation OriginalFileName: net.exe CommandLine: net user /add securityninja hardToHack123\$ CurrentDirectory: C:\Windows\system32\ Show all 37 lines

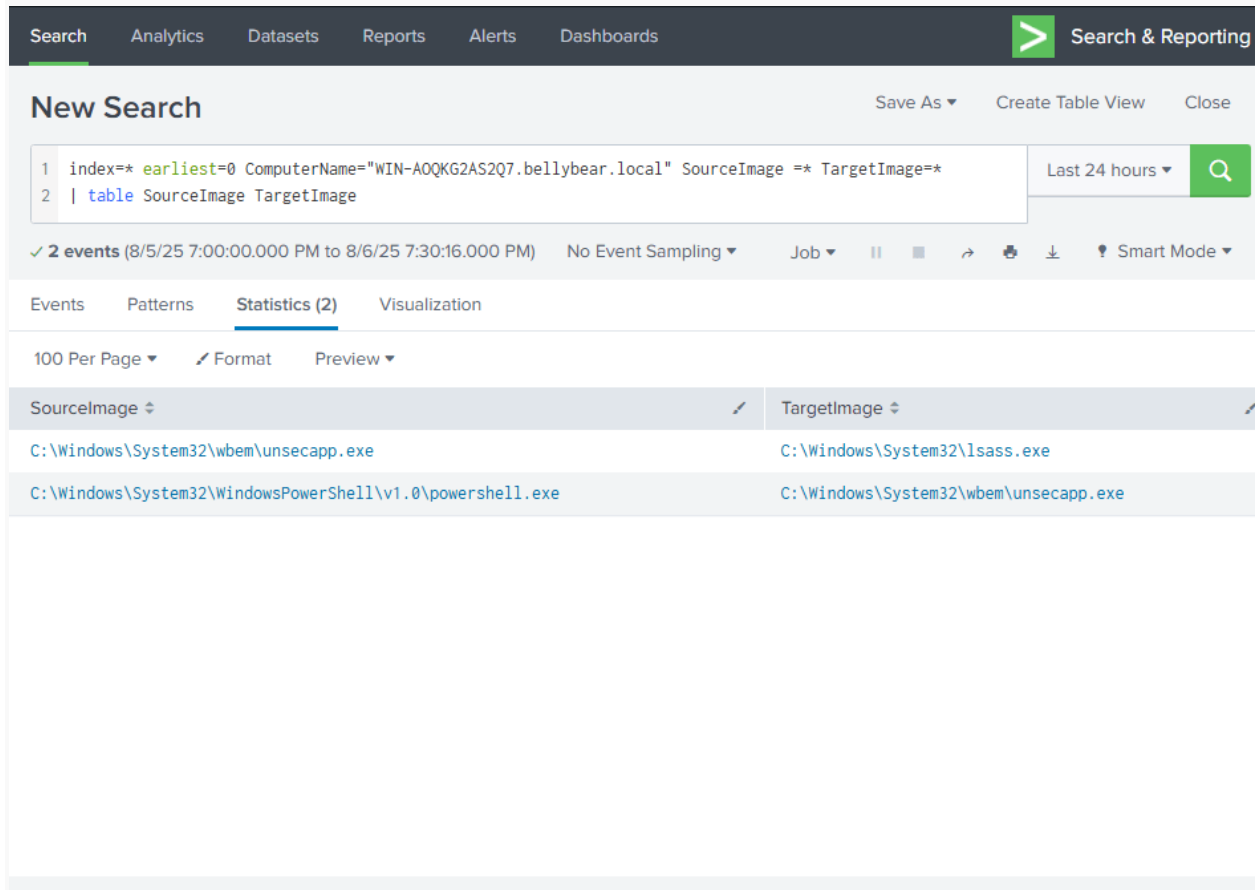
Question 6: The attacker migrated the process for better persistence. What is the migrated process image (executable), and what is the original process image (executable) when the attacker got on the system?

This answer may have been easy to get on accident as all I did was a search including SourceImage=* and TargetImage=*, and this only yielded two results. Afterwards, I consulted a couple different writeups for this room and it shows the best process is searching for EventCode = 8 for remote threads, which I now understand. Answer:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe,
 C:\Windows\System32\wbem\unsecapp.exe

The reason for this migration would be for persistence (as mentioned in the question) but how? Simply put, unsecapp.exe is a legitimate WMI (Windows

Management Instrumentation) process often abused by malware to **hide** or **persist** because it's a trusted system process.



The screenshot shows a search interface with a dark header containing navigation tabs: Search, Analytics, Datasets, Reports, Alerts, and Dashboards. A green search icon and 'Search & Reporting' text are on the right. Below the header, the 'New Search' section includes a search bar with a query: `index=* earliest=0 ComputerName="WIN-A0QKG2AS2Q7.bellybear.local" SourceImage =* TargetImage=*` and a 'Last 24 hours' filter. A 'table' button is visible. Below the search bar, a status bar shows '2 events' and various controls. The main content area has tabs for 'Events', 'Patterns', 'Statistics (2)', and 'Visualization'. Under 'Statistics (2)', there are options for '100 Per Page', 'Format', and 'Preview'. A table displays search results with columns for 'SourceImage' and 'TargetImage'. The first row shows `C:\Windows\System32\wbem\unsecapp.exe` for SourceImage and `C:\Windows\System32\lsass.exe` for TargetImage. The second row shows `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe` for SourceImage and `C:\Windows\System32\wbem\unsecapp.exe` for TargetImage.

Question 7: The attacker also retrieved the system hashes. What is the process image used for getting the system hashes?

Simply by digging deeper into the previous answer (EventCode=8), we can see going from there newly migrated directory out to `C:\Windows\System32\lsass.exe`. We can infer that this target image is the answer to the question above because `lsass.exe` is the **Local Security Authority Subsystem Service**, which is a common target for attackers to extract things like credentials and system hashes because it handles sensitive security and authentication. Answer: `C:\Windows\System32\lsass.exe`

i	Time	Event
>	9/8/21 12:55:30.000 PM	<pre> 09/08/2021 03:55:30 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=8 EventType=4 ComputerName=WIN-AOQKG2AS2Q7.bellybear.local User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=2915 Keywords=None TaskCategory=CreateRemoteThread detected (rule: CreateRemoteThread) OpCode=Info Message=CreateRemoteThread detected: RuleName: - UtcTime: 2021-09-08 19:55:30.770 SourceProcessGuid: {72893ba8-1125-6139-5d00-00000000c00} SourceProcessId: 5016 SourceImage: C:\Windows\System32\wbem\unsecapp.exe TargetProcessGuid: {72893ba8-111d-6139-0c00-00000000c00} TargetProcessId: 672 TargetImage: C:\Windows\System32\lsass.exe NewThreadId: 13980 StartAddress: 0x000001D471950000 StartModule: - StartFunction: - Collapse host = WIN-AOQKG2AS2Q7 source = WinEventlog:Microsoft-Windows-Sysmon </pre>

Question 8: What is the web shell the exploit deployed to the system?

I was unsure how to approach this question and failed to pull results from any keyword searching. Before using the “get hint” on TryHackMe, I consulted ChatGPT on what kind of shell extension I could search for such as .exe or something. ChatGPT listed off a couple different ones, and the first one I tried (.aspx) worked!

i	Time	Event
		<pre> EventCode=1 EventType=4 ComputerName=WIN-AOQKG2AS2Q7.bellybear.local User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=2788 Keywords=None TaskCategory=Process Create (rule: ProcessCreate) OpCode=Info Message=Process Create: RuleName: - UtcTime: 2021-09-08 19:52:09.748 ProcessGuid: {72893ba8-1469-6139-0b02-00000000c00} ProcessId: 13604 Image: C:\Windows\System32\attrib.exe FileVersion: 10.0.17763.1 (WinBuild.160101.0800) Description: Attribute Utility Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: ATTRIB.EXE CommandLine: attrib.exe -r \\.\win-aoqkg2as2q7.bellybear.local\C\$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\i3gfPctK1c2x.aspx CurrentDirectory: c:\windows\system32\inetsrv\ User: NT AUTHORITY\SYSTEM LogonGuid: {72893ba8-111d-6139-e703-000000000000} LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: System Hashes: MD5=3A536CC896D9C6CA2C2EE4C21CCA1DFA, SHA256=B101350BCEEB773B7E77759613BB33C28FBF1D79A13C2CB783575A9D893D52E6, IMPHASH=2CB38FE7D8F223F9DA50B7CBA9B95A6D ParentProcessGuid: {72893ba8-1469-6139-0902-00000000c00} ParentProcessId: 10116 ParentImage: C:\Windows\System32\cmd.exe </pre>

As we can see from the results of my search including .aspx, a process creation was made with a suspicious Command Line field. The attacker is modifying file permissions on the **web shell file** they dropped: i3gfPctK1c2x.aspx. Answer: i3gfPctK1c2x.aspx

Question 9: What is the command line that executed this web shell?

Easy question here and can be answered through the most recent search based on the CommandLine field. Answer: attrib.exe -r \\win-aoqkg2as2q7.bellybear.local\C\$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\i3gfPctK1c2x.aspx

Question 10: What three CVEs did this exploit leverage? Provide the answer in ascending order.

Googled “conti” AND “ransomware” AND “CVE” Answer: CVE-2020-0796,CVE-2018-13374,CVE-2018-13379. Understanding the specific vulnerabilities exploited by Conti ransomware or any other malicious actors and documenting them is essential because it enables organizations to prioritize patching, improve detection capabilities, and even develop response strategies to prevent or minimize the impact of future attacks.

Attack Conclusion:

The attacker demonstrated classic Conti ransomware tactics: initial access through exploited CVEs, lateral movement, credential dumping, persistence via user creation and process migration, and deployment of both ransomware and web shells. Using Splunk and Sysmon allowed for effective identification and mapping of the attack lifecycle, underscoring the value of centralized log analysis and endpoint visibility.

Why It Matters: Conti and other similar ransomware thrive on poor visibility. By learning how to detect these actions in Splunk, blue teamers gain the ability to respond **faster**, contain **sooner**, and **reduce impact** in real-world environments.