

Investigating with Splunk
TryHackMe Challenge
Write-Up
Pavel Pecheniuk

1. Introduction

This room offers to investigate logs from infected Windows machines to identify anomalous behaviour with the help of the famous SIEM tool Splunk. This challenge provides a nice opportunity to put a participant into shoes of a SOC Analyst in a controlled environment, an exposure to one of the most popular SIEM, as well as to improve log analysis skills for efficient threat detection and proper response to the threat.

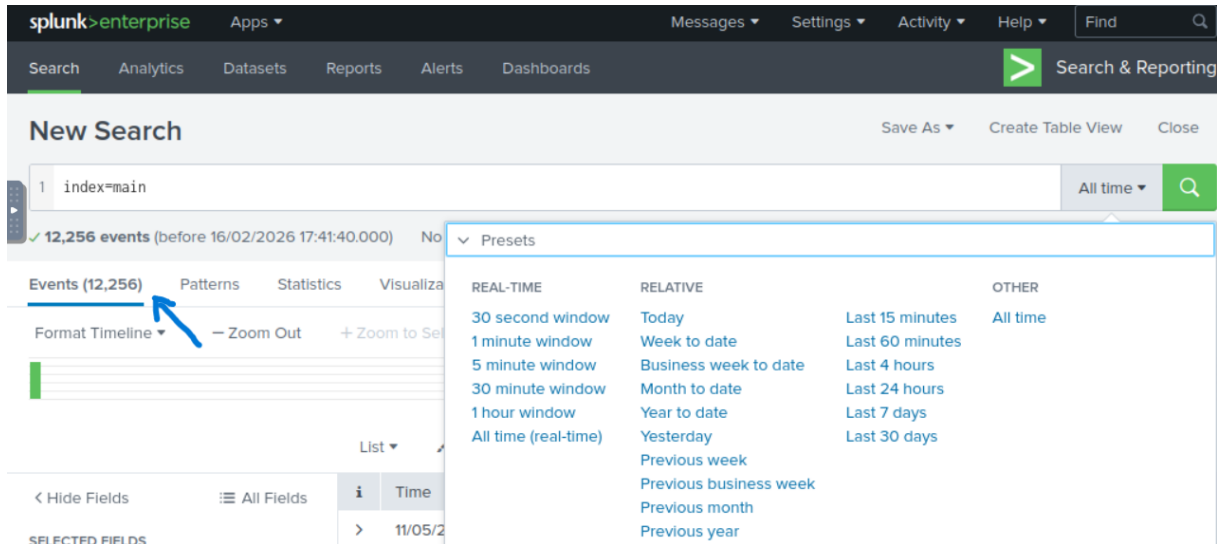
2. Scenario

SOC Analyst Johny has observed some anomalous behaviours in the logs of a few windows machines. It looks like the adversary has access to some of these machines and successfully created some backdoor. His manager has asked him to pull those logs from suspected hosts and ingest them into Splunk for quick investigation. Our task as SOC Analyst is to examine the logs and identify the anomalies.

3. Investigation

How many events were collected and Ingested in the index main?

Let's query the main index by setting a corresponding filter. Initially, the time was set to today, so we need to take care of it and set the appropriate time range.

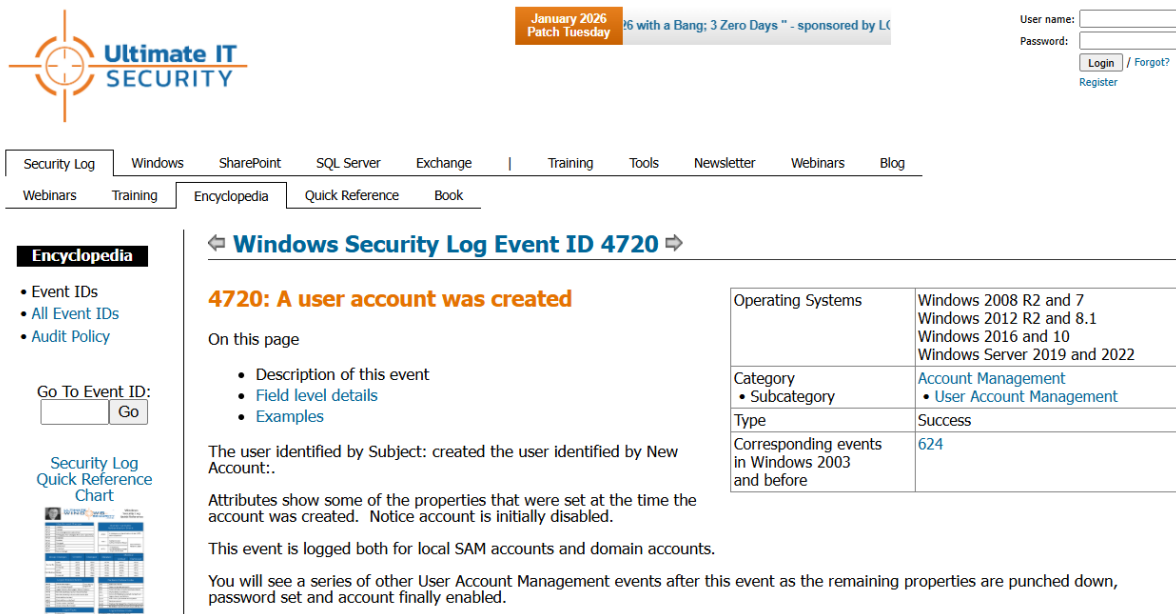


The screenshot shows the Splunk Enterprise Search interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items. Below that, a 'New Search' section contains a search bar with 'index=main'. A status bar indicates '12,256 events (before 16/02/2026 17:41:40.000)'. A 'Presets' dropdown menu is open, displaying a grid of time range options under 'REAL-TIME', 'RELATIVE', and 'OTHER' categories. A blue arrow points to the 'Events (12,256)' tab in the search results area.

Answer: 12256

On one of the infected hosts, the adversary was successful in creating a backdoor user. What is the new username?

Creation of a backdoor user account implies the log entry documenting this event. In Windows event with an ID 4720 is logged if a user account was created.



The screenshot shows the Ultimate IT Security website. At the top, there's a navigation bar with various links. Below that, a login form is visible with fields for 'User name:' and 'Password:', and buttons for 'Login', 'Forgot?', and 'Register'. The main content area features an article titled 'Windows Security Log Event ID 4720'. The article includes a sub-header '4720: A user account was created' and a list of links: 'Description of this event', 'Field level details', and 'Examples'. A table on the right side of the article provides details about the event, including 'Operating Systems', 'Category', 'Subcategory', 'Type', and 'Corresponding events'. The 'Examples' section describes the event and its attributes.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category	Account Management
Subcategory	User Account Management
Type	Success
Corresponding events in Windows 2003 and before	624

Let's examine the logs in Splunk and find the corresponding event.

New Search Save As Create Table View Close

1 index=main EventID=4720 All time Q

✓ 1 event (before 16/02/2026 17:44:39.000) No Event Sampling Job || → ↓ Smart Mode

Events (1) Patterns Statistics Visualization

Format Timeline — Zoom Out + Zoom to Selection x Deselect 1 millisecond per column

List ✓ Format 20 Per Page

	Time	Event
>	11/05/2022 22:32:18.000	{ [-] @version: 1 AccountExpires: %%1794 ActivityID: {E0F7BC1B-4488-0000-8D57-1F92808AD601} AllowedToDelegateTo: - Category: User Account Management Channel: Security DisplayName: %%1793 EventID: 4720

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
@version 1
a AccountExpires 1

And find the account name of the user created.

i	Time	Event
		<p>EventReceivedTime: 2022-02-14 08:06:03</p> <p>EventTime: 2022-02-14 08:06:02</p> <p>EventType: AUDIT_SUCCESS</p> <p>ExecutionProcessID: 740</p> <p>HomeDirectory: %%1793</p> <p>HomePath: %%1793</p> <p>Hostname: Micheal.Beaven</p> <p>Keywords: -9214364837600035000</p> <p>LogonHours: %%1797</p> <p>Message: A user account was created.</p> <p>Subject:</p> <p>Security ID: S-1-5-21-4020993649-1037605423-417876593-1104</p> <p>Account Name: James</p> <p>Account Domain: Cybertees</p> <p>Logon ID: 0x551686</p> <p>New Account:</p> <p>Security ID: S-1-5-21-1969843730-2406867588-1543852148-1000</p> <p>Account Name: Alberto</p> <p>Account Domain: WORKSTATION6</p>

Answer: Alberto

On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?

The Windows registry operations, such as registry creation and value changes, are logged with EventID 12 and 13.

← Sysmon Event ID 12 →

12: RegistryEvent (Object create and delete)

Source	Sysmon
--------	--------

This is an event from Sysmon.

On this page

- Description of this event
- [Field level details](#)
- [Examples](#)

Registry key and value create and delete operations map to this event type, which can be useful for monitoring for changes to Registry autostart locations, or specific malware registry modifications.

← Sysmon Event ID 13 →

13: RegistryEvent (Value Set)

Source	Sysmon
--------	--------

This is an event from Sysmon.

On this page

- Description of this event
- [Field level details](#)
- [Examples](#)

This Registry event type identifies Registry value modifications. The event records the value written for Registry values of type DWORD and QWORD.

Let's check these events in the logs starting with *EventID* = 12.

New Search

Save As ▼ Create Table View Close

1 index=main Alberto EventID=12

All time ▼

✓ 2 events (before 16/02/2026 17:48:21.000) No Event Sampling ▼

Job ▼ || Smart Mode ▼

Events (2)

Patterns

Statistics

Visualization

The *TargetObject* field discloses the value of the modified object.

i	Time	Event
		<div>EventID: 12</div> <div>EventReceivedTime: 2022-02-14 08:06:03</div> <div>EventTime: 2022-02-14 08:06:02</div> <div>EventType: DeleteKey</div> <div>EventTypeOriginal: INFO</div> <div>ExecutionProcessID: 3348</div> <div>Hostname: Micheal.Beaven</div> <div>Image: C:\windows\system32\lsass.exe</div> <div>Keywords: -9223372036854776000</div> <div>Message: Registry object added or deleted:</div> <div>RuleName: -</div> <div>EventType: DeleteKey</div> <div>UtcTime: 2022-02-14 12:06:02.420</div> <div>ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-00000000400}</div> <div>ProcessId: 740</div> <div>Image: C:\windows\system32\lsass.exe</div> <div>TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto</div> <div>Opcode: Info</div> <div>OpcodeValue: 0</div> <div>ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-00000000400}</div> <div>ProcessId: 740</div> <div>ProviderGuid: {5770385F-C22A-43E0-BF4C-06F5698FFBD9}</div>

Answer: HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto

Examine the logs and identify the user that the adversary was trying to impersonate.

We can find the list of users in the *User* field. Obviously, the malicious user account named Alberto aims to impersonate the legitimate user Alberto.

The screenshot shows a security log viewer interface. At the top, there's a search bar with 'index=main' and a filter for 'All time'. Below that, a status bar indicates '12,256 events (before 16/02/2026 17:58:19.000)' and 'No Event Sampling'. The main area displays a 'User' field report. The report shows 4 values, representing 0.971% of events. The values are listed in a table with columns for the value, count, and percentage. A blue arrow points to the row for 'Cybertees\Alberto'.

Values	Count	%
NT AUTHORITY\SYSTEM	70	58.824%
Cybertees\Alberto	24	20.168%
NT AUTHORITY\NETWORK SERVICE	20	16.807%
Cybertees\James	5	4.202%

Answer: Alberto

What is the command used to add a backdoor user from a remote computer?

Here we need to find created processes related to the backdoor user. Process creation are logged with EventID 4688 (and also with EventID 1).

Windows Security Log Event ID 4688

4688: A new process has been created

On this page

- Description of this event
- [Field level details](#)
- [Examples](#)

Event 4688 documents each program that is executed, who the program ran as and the process that started this process.

When you start a program you are creating a "process" that stays open until the program exits. This process is identified by the Process ID:. You can correlate this event to other events by Process ID to determine what the program did while it ran and when it exited (event 4689).

Win2012R2 adds Process Command Line.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022 Windows Server 2025
Category • Subcategory	Process Tracking • Process Creation
Type	Success
Corresponding events in Windows 2003 and before	592

Sysmon Event ID 1

1: Process creation

Source	Sysmon
--------	--------

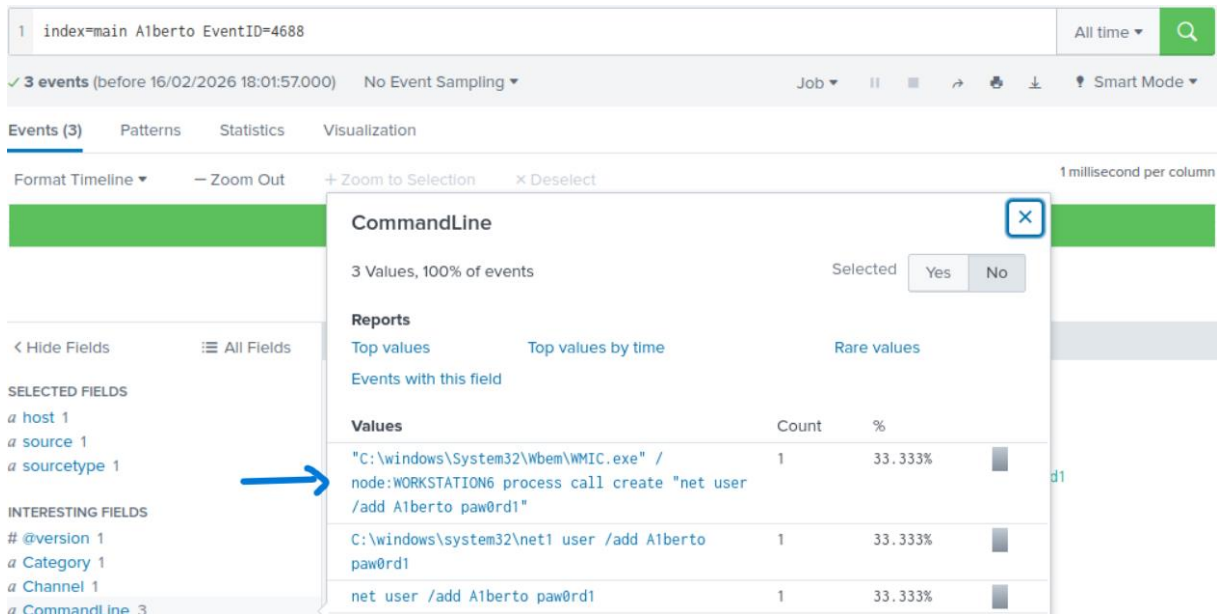
This is an event from Sysmon.

On this page

- Description of this event
- [Field level details](#)
- [Examples](#)

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.

Let's filter these events and take a look on the CommandLine field as we are interested in finding the specific command. The upper command contains the trace of using WMIC.exe utility, which is used by the malicious actors to gain access to remote systems. Hence that's the needed command.



Search: `index=main A1berto EventID=4688` All time

3 events (before 16/02/2026 18:01:57.000) No Event Sampling

Events (3) Patterns Statistics Visualization

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

Selected Yes No

Reports
Top values Top values by time Rare values
Events with this field

Values	Count	%
"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"	1	33.333%
C:\windows\system32\net1 user /add A1berto paw0rd1	1	33.333%
net user /add A1berto paw0rd1	1	33.333%

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
@version 1
a Category 1
a Channel 1
a CommandLine 3

Wmic.exe launching processes on a remote system

Applies To: [Splunk Platform](#) Technical Add-On: [Common Information Model](#)

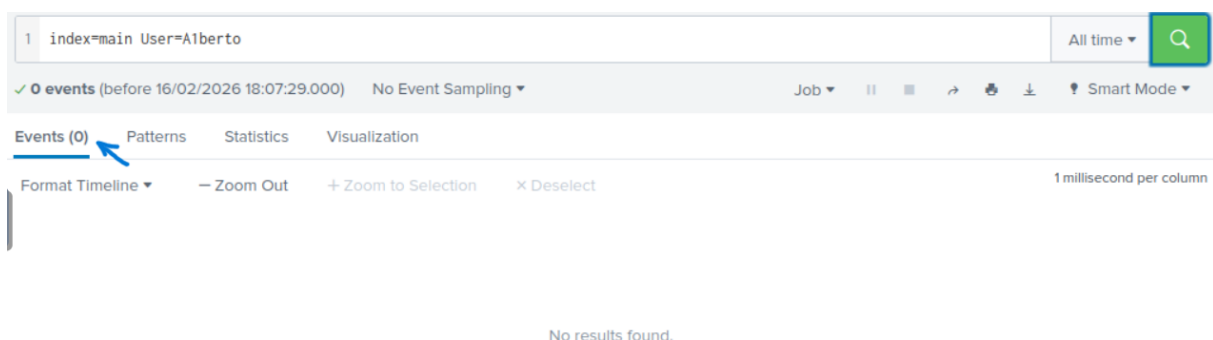
Last updated: Dec 15, 2025

WMIC is a software utility that allows users to perform Windows Management Instrumentation operations with a command prompt. Ransomware authors have been seen to use wmic.exe to gain access to remote systems and then perform processes on it to prepare for or execute the ransomware attack. This search looks for wmic.exe launched with parameters to spawn a process on a remote system to find evidence of the attack.

Answer: `C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1`

How many times was the login attempt from the backdoor user observed during the investigation?

Here we can simply track the activity from the backdoor user by filtering with the corresponding username.



Search: `index=main User=A1berto` All time

0 events (before 16/02/2026 18:07:29.000) No Event Sampling

Events (0) Patterns Statistics Visualization

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

No results found.

Note: This simple approach worked for this task, although the more reliable solution here would be to filter with EventID 4624 and 4625, corresponding to the successful and failed logon attempt respectively.

Windows Security Log Event ID 4624

4624: An account was successfully logged on

On this page

- Description of this event
- [Field level details](#)
- [Examples](#)

This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events [4634](#) and [4647](#) using Logon ID.

Win2012 adds the Impersonation Level field as shown in the example.

Win2016/10 add further fields explained below.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022 Windows Server 2025
Category • Subcategory	Logon/Logoff • Logon
Type	Success
Corresponding events in Windows 2003 and before	528 , 540

Windows Security Log Event ID 4625

4625: An account failed to log on

On this page

- Description of this event
- [Field level details](#)
- [Examples](#)

This is a useful event because it documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022 Windows Server 2025
Category • Subcategory	Logon/Logoff • Logon
Type	Failure
Corresponding events in Windows 2003	529 , 530 , 531 , 532 , 533 , 534 , 535 , 536 , 537 , 539

Answer: 0

What is the name of the infected host on which suspicious Powershell commands were executed?

Execution of a Powershell command can be logged with EventID 4104 or 4103. Also, there is an article by Splunk confirming these findings:

https://www.splunk.com/en_us/blog/security/hunting-for-malicious-powershell-using-script-block-logging.html



Event ID: 4104
Source: Microsoft-Windows-PowerShell
Category: Execute a Remote Command
Log: Microsoft-Windows-PowerShell/Operational

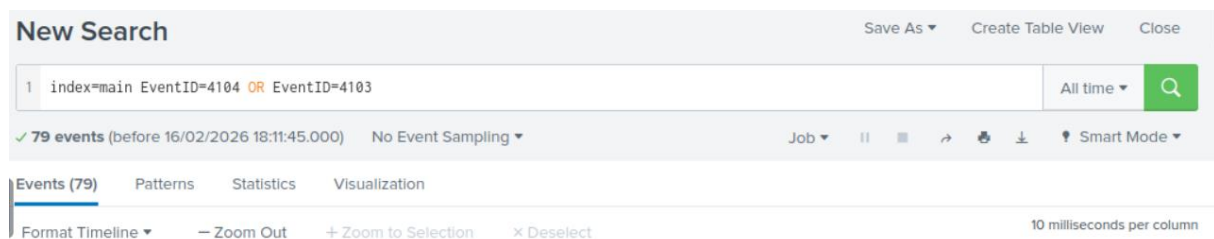
Message: Creating Scriptblock text (1 of 1):
Write-Host PowerShellV5ScriptBlockLogging

ScriptBlock ID: 6d90e0bb-e381-4834-8fe2-5e076ad267b3
Path:

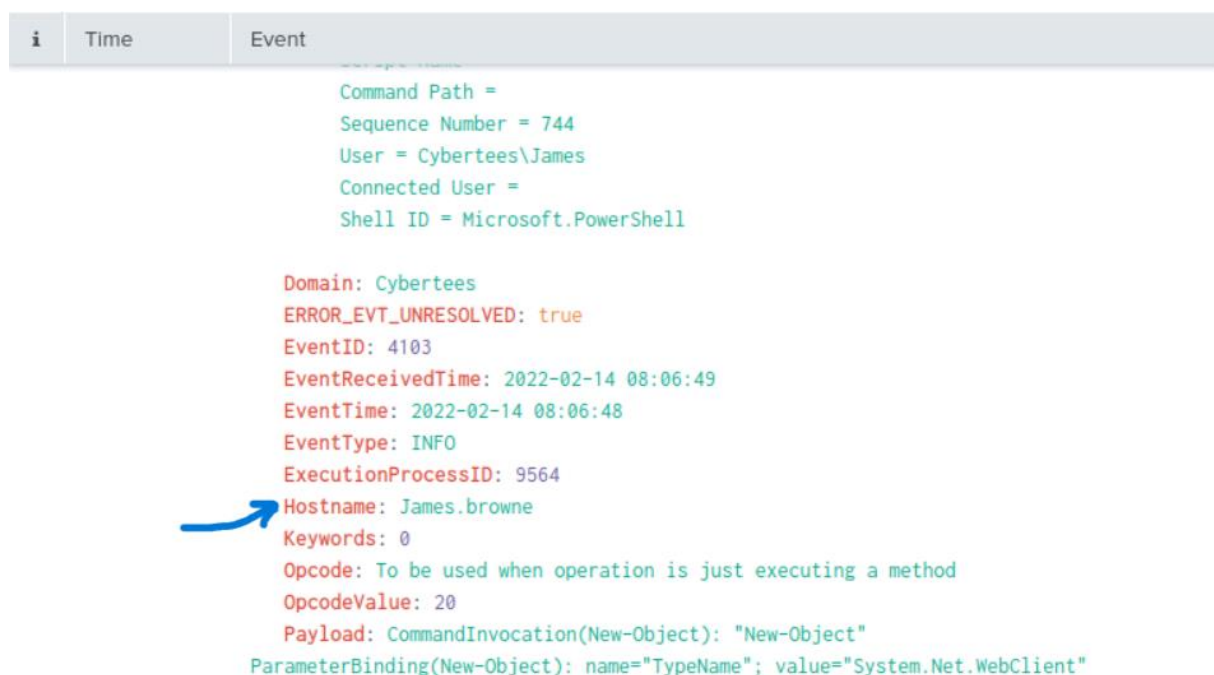
Event submitted by Event Log Doctor

Event ID: 4103
Source: Microsoft-Windows-PowerShell
Category: Executing Pipeline
Message: CommandInvocation(Write-Host): "Write-Host"
 ParameterBinding(Write-Host): name="Object"; value="TestPowerShellV5"

Let's filter Powershell events with the corresponding identifiers.



Analyzing events we can find the hostname where the Powershell commands were executed.



Answer: James.browne

PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?

We already know how many events were captured related to the malicious Powershell execution. Let's reuse the query from the previous task.

New Search Save As Create Table View Close

1 index=main EventID=4104 OR EventID=4103 All time Q

✓ 79 events (before 16/02/2026 18:11:45.000) No Event Sampling ▾ Job || ■ → 🖨 ⬇ Smart Mode ▾

Events (79) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 10 milliseconds per column

Answer: 79

An encoded Powershell script from the infected host initiated a web request. What is the full URL?

Here is the event from the infected host. Indeed, there was a *powershell.exe* executed script that have participated in the exchange of the encoded data.

	Event
022	{ [-]
3.000	<pre> @version: 1 AccountName: James AccountType: User ActivityID: {4F259F18-BCE1-0000-7D1A-7593808AD601} Category: Executing Pipeline Channel: Microsoft-Windows-PowerShell/Operational ContextInfo: Severity = Informational Host Name = ConsoleHost Host Version = 5.1.18362.752 Host ID = 0f79c464-4587-4a42-a825-a0972e939164 Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBIAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwBIAACAAMwApAHs/ AFgAeAB1AFMAQQAtAD0AVgBEADQANgA3ACoAFABPAEwAVwBCAH4AcgBuADgAXgBJACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwB; Engine Version = 5.1.18362.752 Runspace ID = a6093660-16a6-4a60-ae6b-7e603f030b6f Pipeline ID = 1 Command Name = New-Object Command Type = Cmdlet Script Name = Command Path = </pre>

Let's use CyberChef, a web app for manipulating data, including encoding, decoding, compression and etc. Let's set the filters (Recipes) *from Base64* and *Decode text* and decode the data.

We need to find details of the web request. The sequence highlighted with yellow may refer to the domain name encoded with Base64, especially considering the presence of */news.php*, which indicates a subdirectory or a part of the URL.

Let's decode the highlighted sequence with CyberChef again with the additional recipe *Defang URL*, as it is recommended by the hint THM provided us.

The final reconstructed URL is the answer.

Answer: `hxxp[://]10[.]10[.]10[.]5/news[.]php`

4. References

- <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
- https://lantern.splunk.com/Security_Use_Cases/Security_Monitoring/Detecting_a_ransomware_attack/Wmic.exe_launching_processes_on_a_remote_system
- https://www.splunk.com/en_us/blog/security/hunting-for-malicious-powershell-using-script-block-logging.html
- <https://www.myeventlog.com/>
- <https://gchq.github.io/CyberChef/>