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.

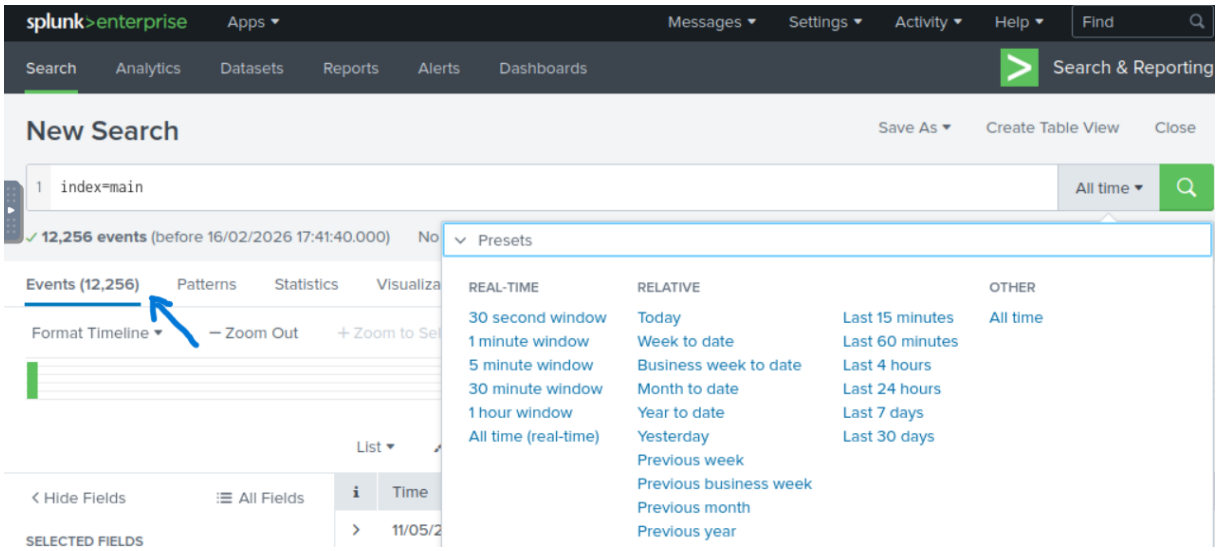
2. Scenario

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.

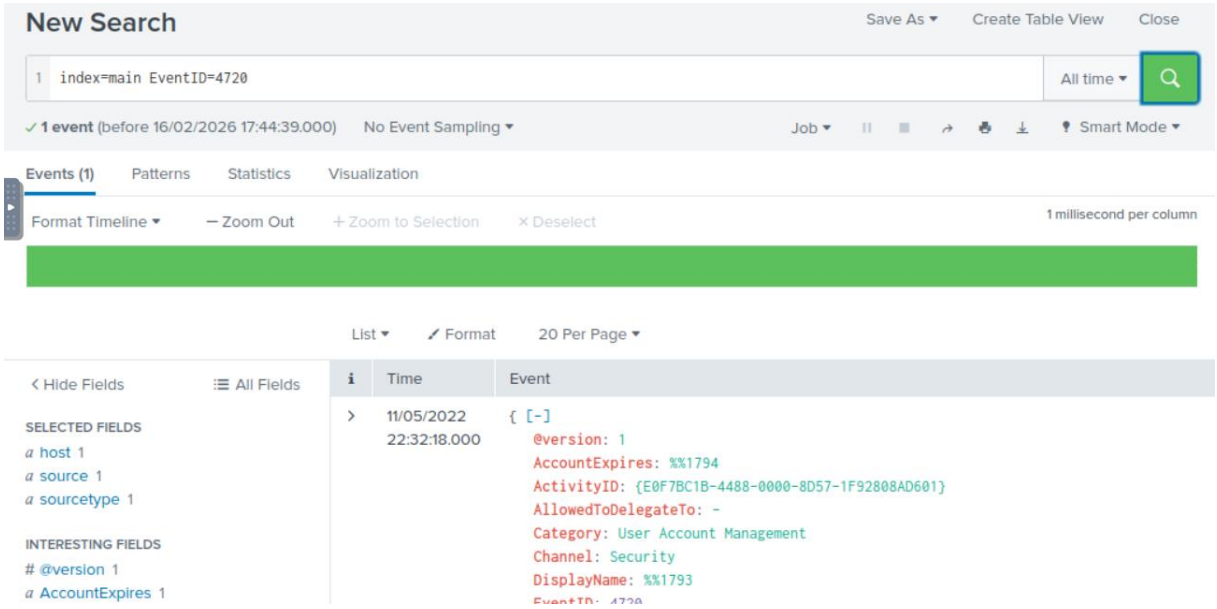


Answer: 12256

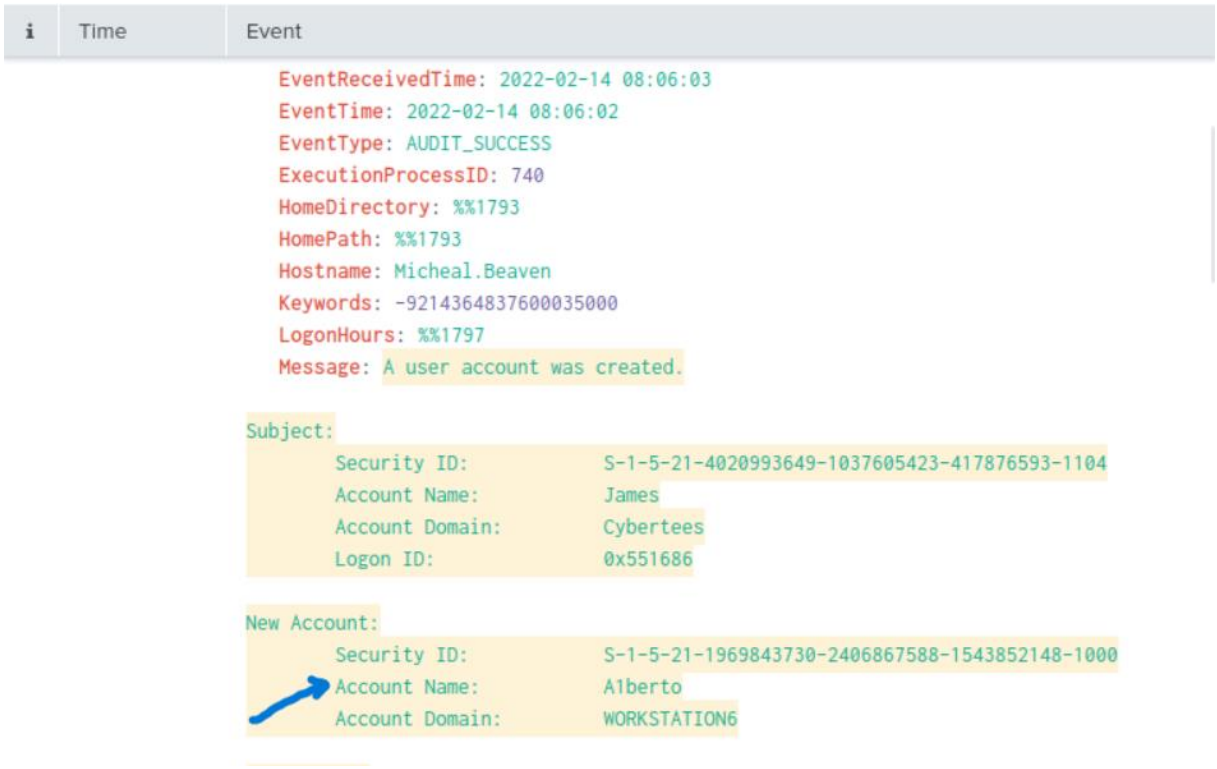
On one of the infected hosts, the adversary was successful in creating a backdoor user. What is the new username?

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.

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



And find the account name of the user created.



Answer: A1berto

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

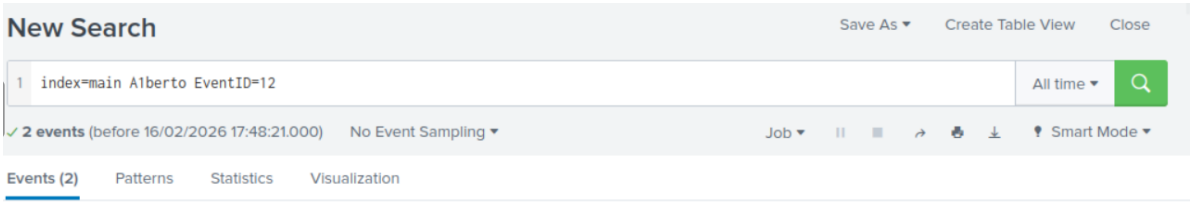
This is an event from Sysmon.

On this page

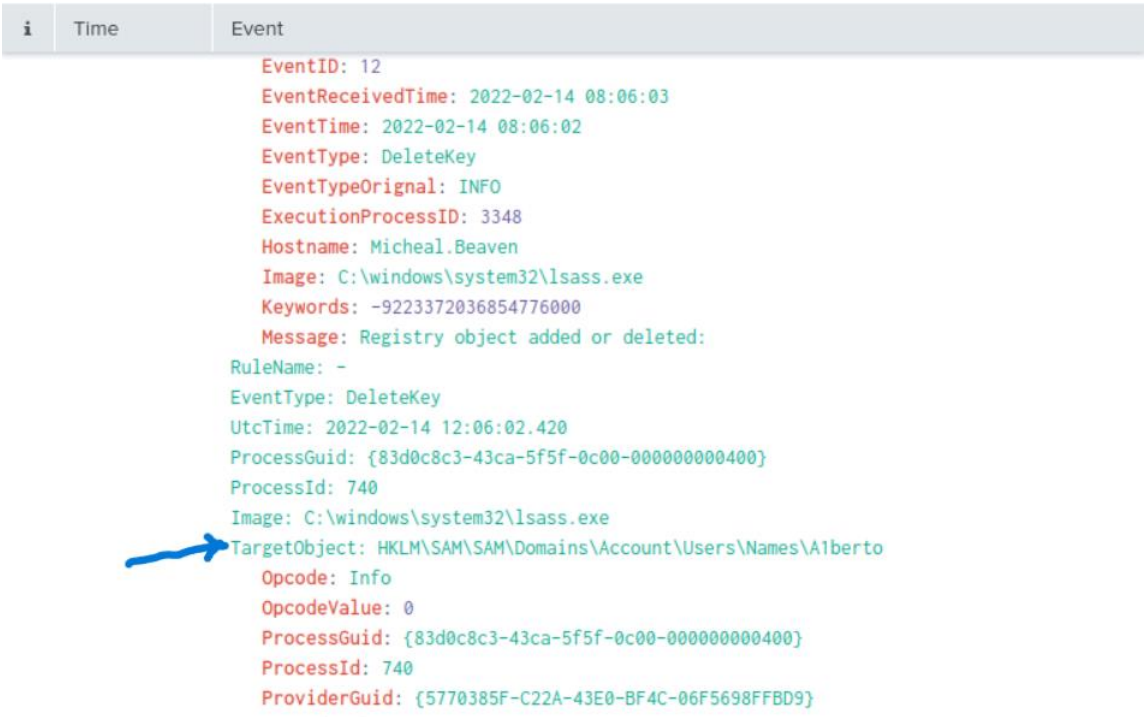
- Description of this event
- Field level details
- Examples

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*.



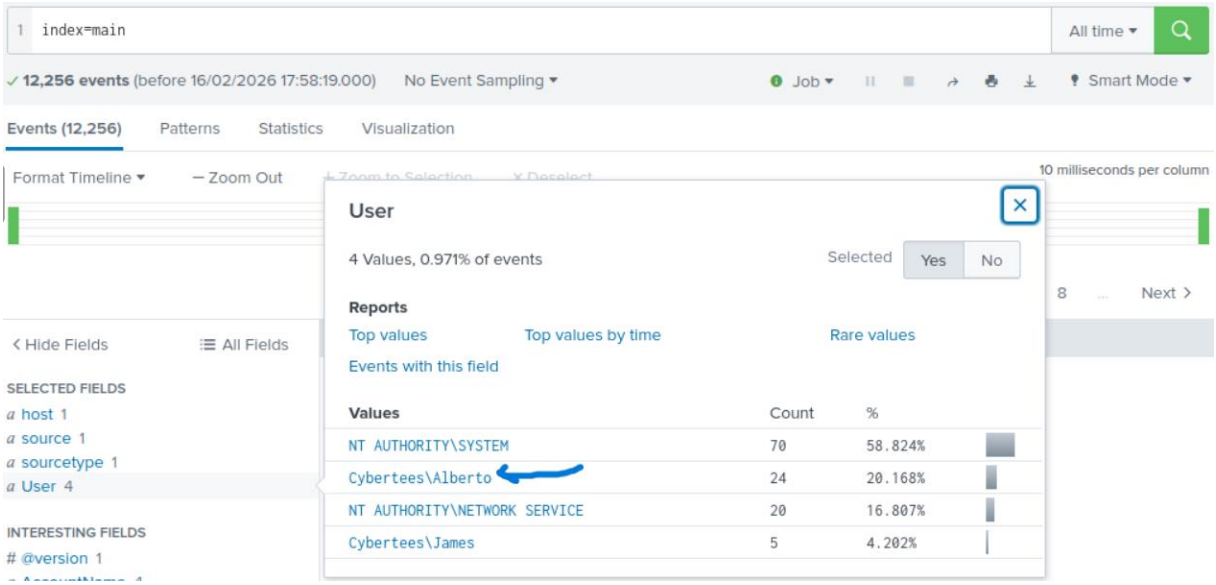
The *TargetObject* field discloses the value of the modified object.



Answer: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto

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 A1berto aims to impersonate the legitimate user Alberto.



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

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

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.

Sysmon Event ID 1

1: Process creation

Source	Sysmon

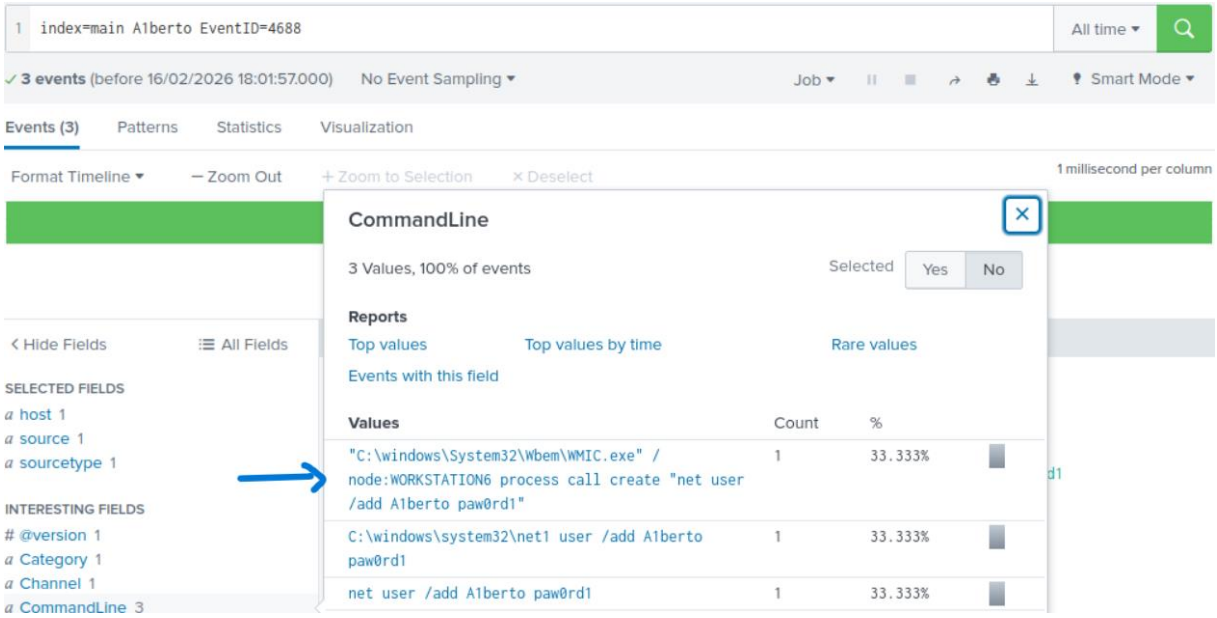
This is an event from Sysmon.

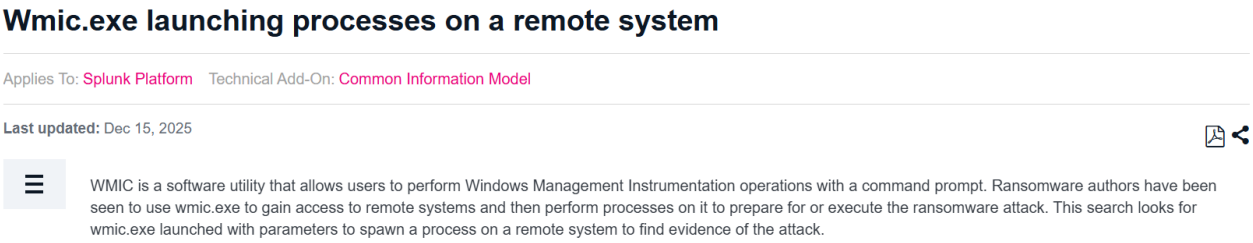
On this page

- 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.

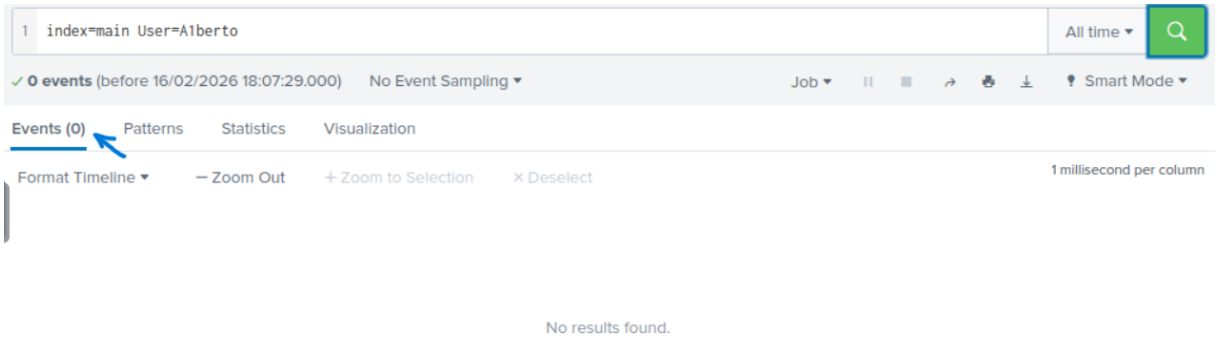




Answer: C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1

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.



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

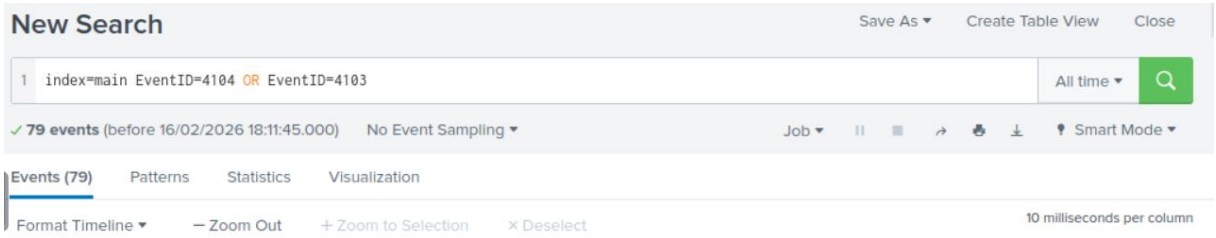
Event submitted by Event Log Doctor

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

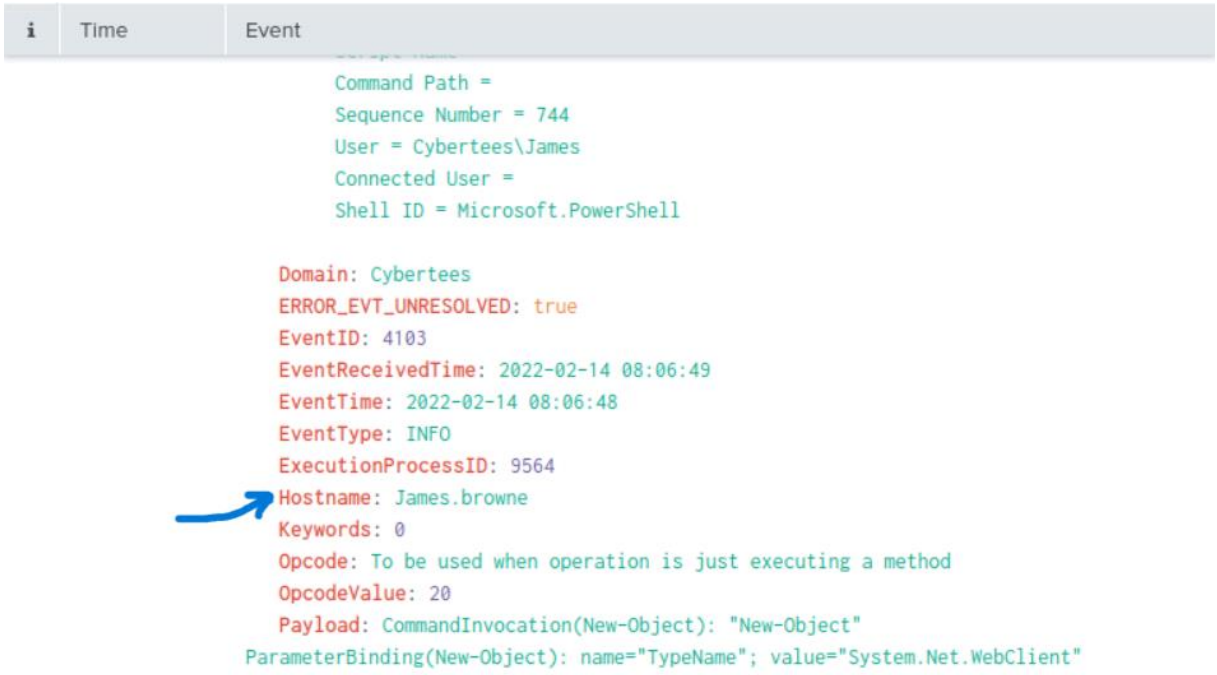
Message:
```
Creating Scriptblock text (1 of 1):
Write-Host PowerShellV5ScriptBlockLogging

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

Event 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 identificators.



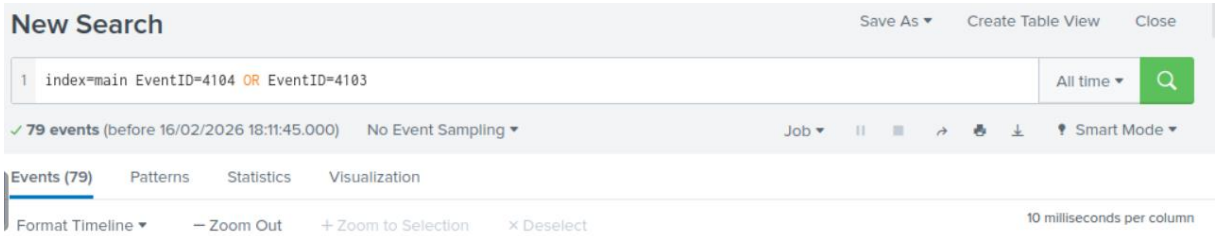
Analyzing events we can find the hostname where the Powershell commands were executed.



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.



Answer: 79

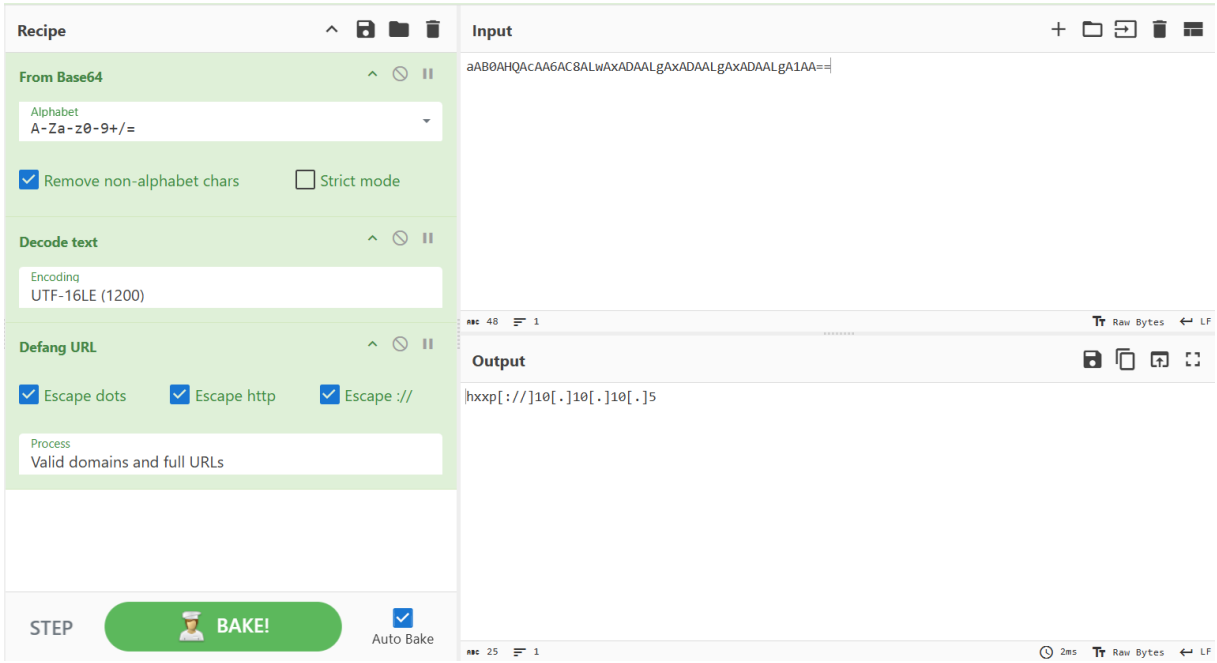
An encoded Powershell script from the infected host initiated a web request. What is the full URL?

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.

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/