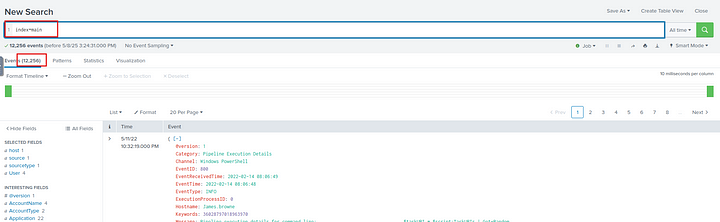
### **Investigating with Splunk — TryHackMe**

**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.

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

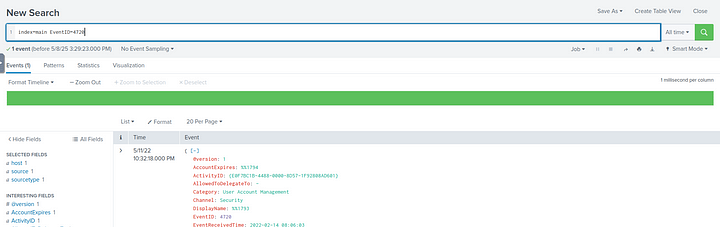
index=main



**Answer:** 12256

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

index=main EventID=4720



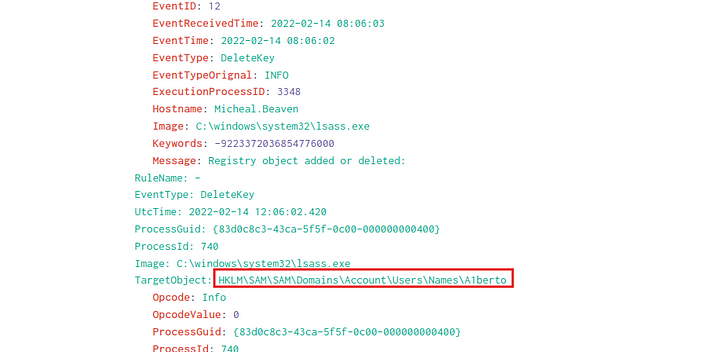
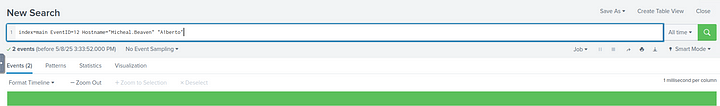
As we can see, we only have one event. If we see the details of the event, we can find the username of the new user.



**Answer:** A1berto

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

index=main EventID=12 Hostname="Micheal.Beaven" "A1berto"

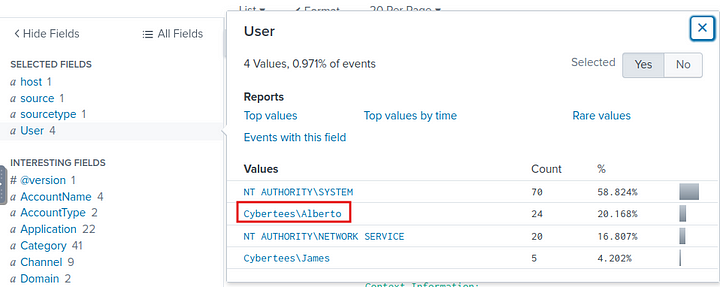


**Answer:** HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto

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

This is obvious from the name of the new account, but we can confirm by checking the Users field under the index main

index=main

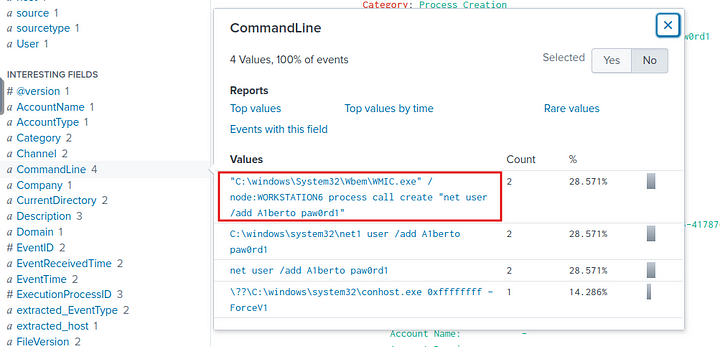


**Answer:** Alberto

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

We can check for the events with CommandLine field in them

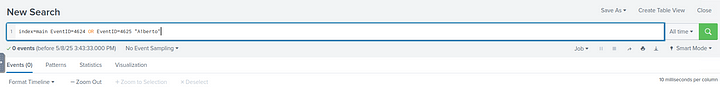
index=main "A1berto" CommandLine="\*"



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

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

index=main EventID=4624 OR EventID=4625 "A1berto"

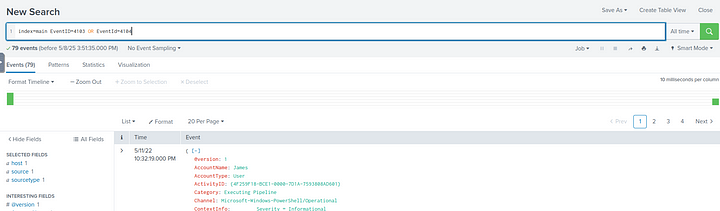


**Answer:** 0

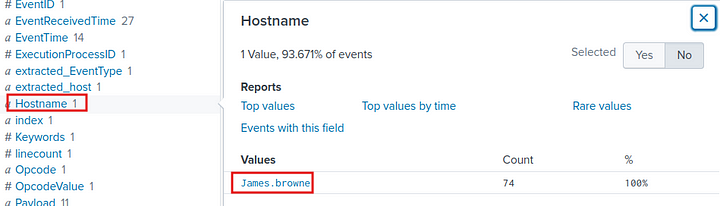
**7. What is the name of the infected host on which suspicious Powershell commands were executed?**

index=main EventID=4103 OR EventId=4104

The above filter will return events where a powershell script was run and also will return the commands executed. We can see encoded command in the events which hints at some malicious activity.



If we check the Hostname field there is only one value. This is our answer.



**Answer:** James.browne

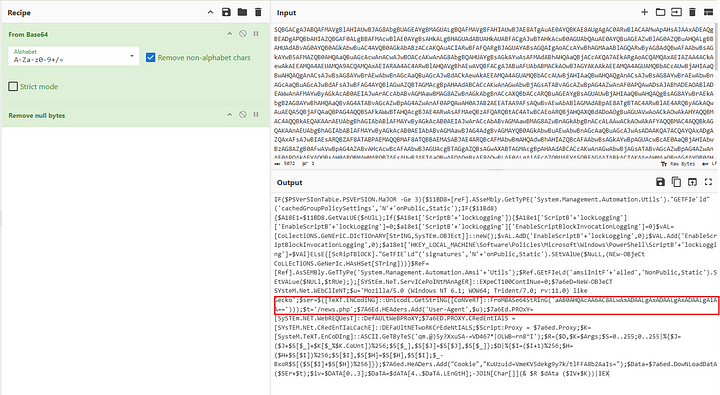
**8. PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?**

The answer to this is the number of events that returned on the previous search.

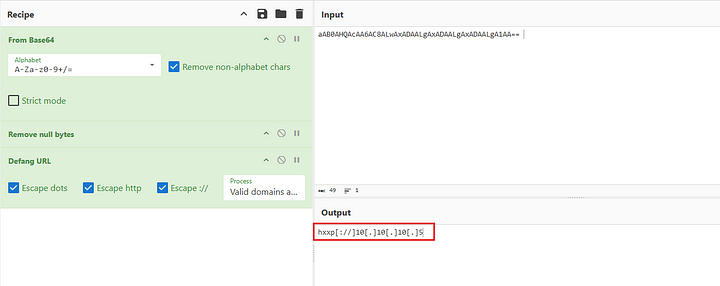
**Answer:** 79

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

In the previous search we found an encoded command execution, let us decode it using Cyberchef.



There seems to be a web request being made in this command, but the url is encoded. So let us take the encoded string and decode it.



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

This is the end of the walkthrough.