

## Investigating with Splunk

SOC Analyst Johnny 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.

index=main

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

The screenshot shows a Splunk search interface. At the top, the search bar contains the query `1 index="main" EventID="4720"`. Below the search bar, the results are displayed in a table format. The first result is for Event ID 4720, which occurred on 5/11/22 at 10:32:18.000 PM. The event details are as follows:

Field	Value
@version	1
AccountExpires	%%1794
ActivityID	{E0F7BC1B-4488-0000-8D57-1F92808AD601}
AllowedToDelegateTo	-
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.
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	Alberto
Account Domain	WORKSTATION6

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

Hostname: Michael.Beaven (from user account creation)

Backdoor user: A1berto

**New Search**

1 index="main" Hostname="Micheal.Beaven" A1berto

✓ 10 events (before 12/15/22 6:19:35.000 PM) No Event Sampling

Events (10) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1
- User 1

INTERESTING FIELDS

- @version 1
- AccountName 1
- AccountType 1
- ActivityID 1
- Category 5
- Channel 2
- CommandLine 3
- Company 1
- CurrentDirectory 2
- Description 2
- Domain 1
- EventID 6
- EventReceivedTime 2

Category

5 Values, 100% of events

Selected Yes No

Reports

- Top values
- Top values by time
- Rare values

Events with this field

Values

Values	Count	%
Process Create (rule: ProcessCreate)	3	30%
Process Creation	2	20%
Registry object added or deleted (rule: RegistryEvent)	2	20%
User Account Management	2	20%
Registry value set (rule: RegistryEvent)	1	10%

417876593-1104

1 index="main" Hostname="Micheal.Beaven" A1berto Category="Registry object added or deleted (rule: RegistryEvent)"

✓ 2 events (before 12/15/22 6:21:07.000 PM) No Event Sampling

Events (2) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

```
Domain: NT AUTHORITY
EventID: 12
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:02
EventType: DeleteKey
EventTypeOriginal: INFO
ExecutionProcessID: 3348
Hostname: Micheal.Beaven
Image: C:\windows\system32\lsass.exe
Keywords: -9223372036854776000
Message: Registry object added or deleted:
RuleName: -
EventType: DeleteKey
UtcTime: 2022-02-14 12:06:02.420
ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-00000000400}
ProcessId: 740
Image: C:\windows\system32\lsass.exe
TargetObject: HKLM\SAM\Domains\Account\Users\Names\A1berto
Opcode: Info
OpcodeValue: 0
ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-00000000400}
ProcessId: 740
ProviderGuid: {5770385F-C22A-43E0-BF4C-06F5698FFBD9}
RecordNumber: 183218
RuleName: -
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: im_msvisalog
SourceName: Microsoft-Windows-Sysmon
TargetObject: HKLM\SAM\Domains\Account\Users\Names\A1berto
Task: 12
ThreadID: 4532
UserID: S-1-5-18
UtcTime: 2022-02-14 12:06:02.420
```

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

**New Search**

index="main"

✓ 12,256 events (before 12/15/22 6:37:01.000 PM) No Event Sampling ▼

Events (12,256) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

< Hide Fields All Fields

SELECTED FIELDS

- a CommandLine 19
- a host 1
- a source 1
- a sourcetype 1
- a User 4

INTERESTING FIELDS

- # @version 1
- a AccountName 4
- a AccountType 2
- a Application 22
- a Category 41

**User**

4 Values, 0.971% of events

Selected Yes No

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%

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

**New Search**

index="main"

✓ 12,256 events (before 12/15/22 6:24:44.000 PM) No Event Sampling ▼

Events (12,256) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

< Hide Fields All Fields

SELECTED FIELDS

- a CommandLine 19
- a host 1
- a source 1
- a sourcetype 1
- a User 4

INTERESTING FIELDS

- # @version 1
- a AccountName 4
- a AccountType 2
- a Application 22
- a Category 41
- a Channel 9
- a Domain 2
- # EventID 55
- a EventReceivedTime 60
- a EventTime 64

**CommandLine**

19 Values, 0.408% of events

Selected Yes No

Reports

- Top values
- Top values by time
- Rare values

Events with this field

Top 10 Values

Values	Count	%
"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	8	16%
"C:\windows\system32\backgroundTaskHost.exe" -ServerName:App.AppMtcn0h2tfby7k9kn8hxb6dmzz1zh0.mca	4	8%
C:\windows\system32\wbem\wmiprvse.exe -secured -Embedding	4	8%
\\??C:\windows\system32\conhost.exe 0xffffffff -ForceV1	4	8%
"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add Alberto paw0rd1"	4	4%
C:\Windows\System32\RuntimeBroker.exe -Embedding	2	4%
C:\Windows\System32\usocoreworker.exe -Embedding	2	4%
C:\windows\System32\svchost.exe -k NetSvc -p -s NcaSvc	2	4%
C:\windows\System32\svchost.exe -k NetworkService -p -s DoSvc	2	4%
C:\windows\system32\RAServer.exe /offerraupdate	2	4%

```

{ [-]
  @version: 1
  Category: Process Creation
  Channel: Security
  CommandLine: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add Alberto paw0rd1"
  EventID: 4688
  EventReceivedTime: 2022-02-14 08:06:03
  EventTime: 2022-02-14 08:06:01
  EventType: AUDIT_SUCCESS
  ExecutionProcessID: 4
  Hostname: James.browne
  Keywords: -9214364837600035000
  MandatoryLabel: S-1-16-12288
  Message: A new process has been created.

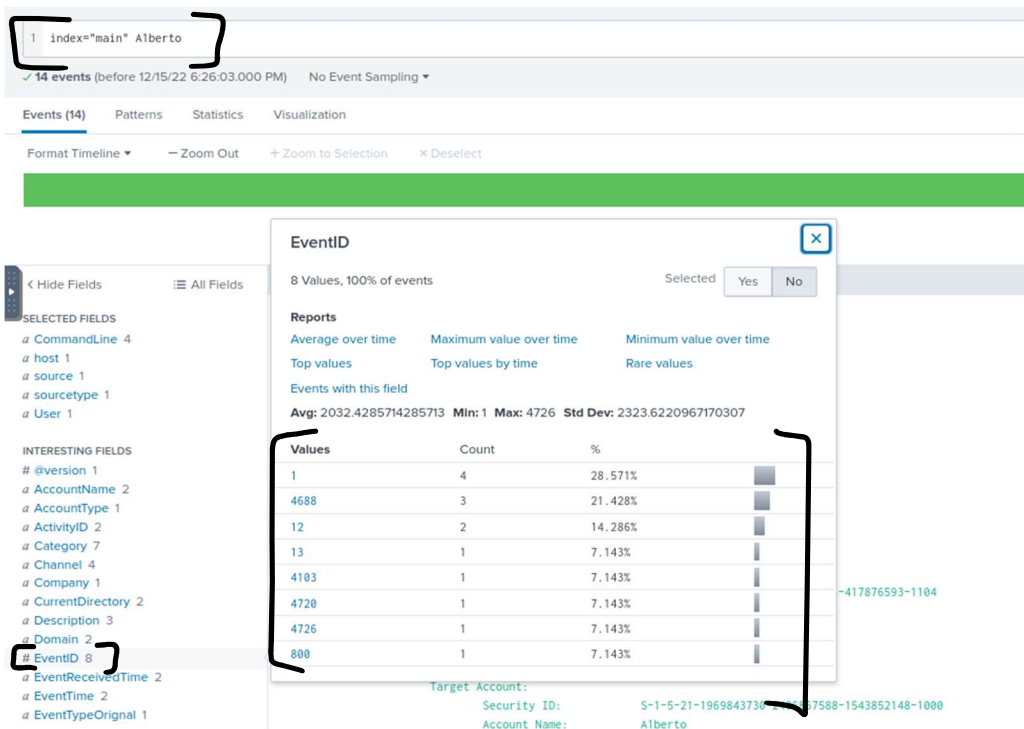
Creator Subject:
  Security ID: S-1-5-21-4020993649-1037605423-417876593-1104
  Account Name: James
  Account Domain: Cybertees
  Logon ID: 0x2CC013

Target Subject:
  Security ID: S-1-0-0
  Account Name: -
  Account Domain: -
  Logon ID: 0x0

Process Information:
  New Process ID: 0x24d4
  New Process Name: C:\Windows\System32\wbem\WMIC.exe
  Token Elevation Type: %%1937
  Mandatory Label: S-1-16-12288
  Creator Process ID: 0x255c
  Creator Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
  Process Command Line: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add Alberto paw0rd1"

```

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



Event ID 4625 documents every failed attempt at logging on to a local computer.

0 events for Event ID 4625 – Alberto

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

**New Search** PowerShell logging - Event ID 4103

`index="main" EventID="4103"`

✓ 79 events (before 12/15/22 6:52:39.000 PM) No Event Sampling ▼

Events (79) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼

	i	Time	Event
<b>SELECTED FIELDS</b> # @version 1 a host 1 a source 1 a sourcetype 1  <b>INTERESTING FIELDS</b> # @version 1 a AccountName 1 a AccountType 1 a ActivityID 79 a Category 1 a Channel 1 a ContextInfo 79 a Domain 1 a ERROR_EVT_UNRESOLVED 1 # EventID 1 a EventReceivedTime 27 a EventTime 14	>	5/11/22 10:32:19.000 PM	{ [-] @version: 1 AccountName: James 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-a0972e93916 Host Application = C:\Windows\System32\Window: SQBGACgAJABQAFMAVgBIAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAI Engine Version = 5.1.18362.752 Runspace ID = a6093660-16a6-4a60-ae6b-7e603f0: Pipeline ID = 1 Command Name = New-Object Command Type = Cmdlet Script Name =