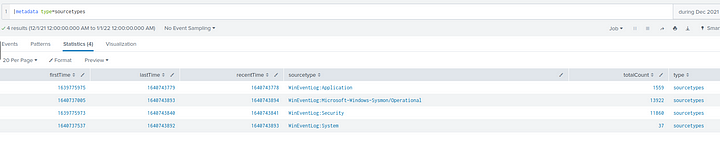
### **New Hire Old Artifacts — TryHackMe**

**Scenario:** You are a SOC Analyst for an MSSP (managed Security Service Provider) company called TryNotHackMe.

A newly acquired customer (Widget LLC) was recently onboarded with the managed Splunk service. The sensor is live, and all the endpoint events are now visible on TryNotHackMe’s end. Widget LLC has some concerns with the endpoints in the Finance Dept, especially an endpoint for a recently hired Financial Analyst. The concern is that there was a period (December 2021) when the endpoint security product was turned off, but an official investigation was never conducted.

Your manager has tasked you to sift through the events of Widget LLC’s Splunk instance to see if there is anything that the customer needs to be alerted on.



TASKS

1. **A Web Browser Password Viewer executed on the infected machine. What is the name of the binary? Enter the full path.**

Let us filter for Sysmon logs, specifically for Event Code 1.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1

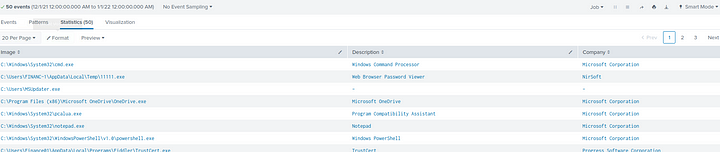
Let us now list out important fields in a table.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1

| dedup Image

| table Image Description Company

The above filter will list the executed image, the description of that image and the company that created that image. It also removes the duplicates of images as a single image might have been executed multiple times.



In the second line of the output, we can see the password viewer.



**Answer:** C:\Users\FINANC~1\AppData\Local\Temp\11111.exe

**2. What is listed as the company name?**

****

**Answer:** NirSoft

**3. Another suspicious binary running from the same folder was executed on the workstation. What was the name of the binary? What is listed as its original filename? (format: file.xyz,file.xyz)**

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1 CurrentDirectory="C:\\Users\\Finance01\\AppData\\Local\\Temp\\"

| table Image OriginalFileName

The above filter will list out all the Images that are present in the same directory as the previous executable and lists their original name.

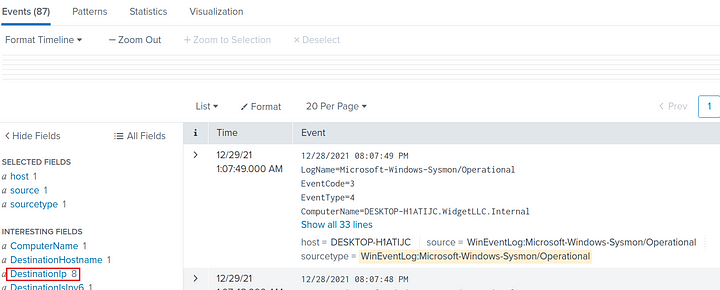


**Answer:** IonicLarge.exe,PalitExplorer.exe

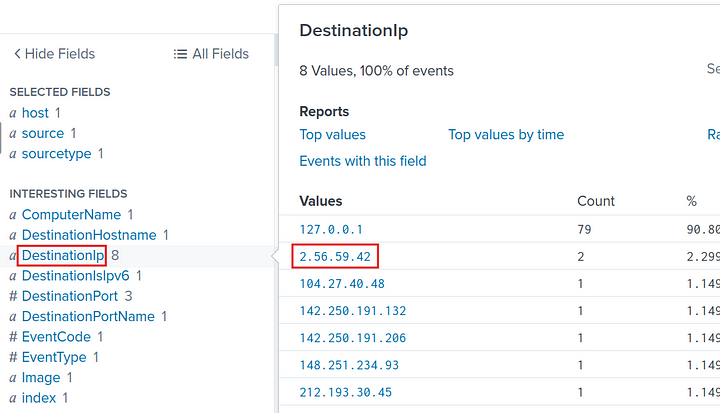
**4. The binary from the previous question made two outbound connections to a malicious IP address. What was the IP address? Enter the answer in a defang format.**

Filter for the event where the above image made network connections by filtering on Event id 3 and the image.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=3 Image="C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe"



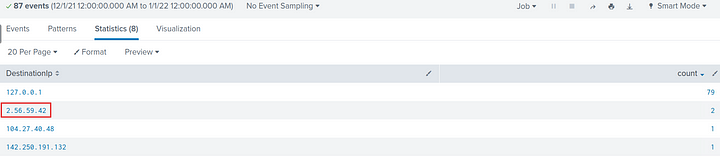
Now we can look at the Destination IP field for the IP address with two connections.



We can also use stats command to count by Destination IP’s.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=3 Image="C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe"

| stats count by DestinationIp



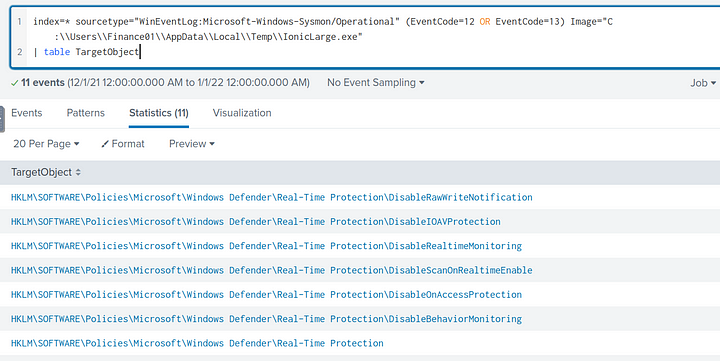
**Answer:** 2[.]56[.]59[.]42

**5. The same binary made some change to a registry key. What was the key path?**

We can filter by Event code 12 or 13 and image as the above image.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" (EventCode=12 OR EventCode=13) Image="C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe"

| table TargetObject



We can see the path to the registry key that the Image modified. There are other keys modified but this is the path that the Image mostly tried to modify.

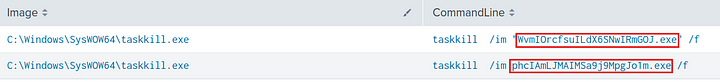
**Answer:** HKLM\SOFTWARE\Policies\Microsoft\Windows Defender

**6. Some processes were killed and the associated binaries were deleted. What were the names of the two binaries?**

While looking around, I found a value called “Terminates Processes” in the Interesting fields. So I filtered on this and found the processes taht were terminated.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" Description="Terminates Processes"

|table Image CommandLine



**Answer:** phcIAmLJMAIMSa9j9MpgJo1m.exe, WvmIOrcfsuILdX6SNwIRmGOJ.exe

**7. The attacker ran several commands within a PowerShell session to change the behavior of Windows Defender. What was the last command executed in the series of similar commands?**

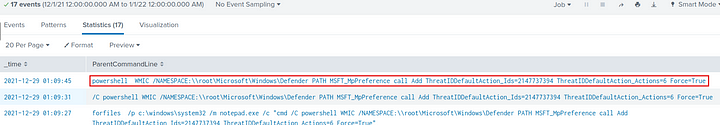
I filtered for the event with the words powershell, windows defender in them and then listed out the commands and sorted them by time.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" windows defender powershell

| where isnotnull(ParentCommandLine)

| table \_time ParentCommandLine

| sort -\_time



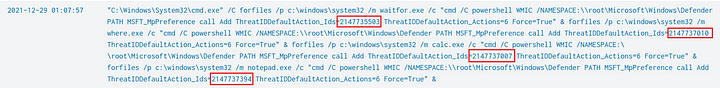
**Answer:** powershell WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT\_MpPreference call Add ThreatIDDefaultAction\_Ids=2147737394 ThreatIDDefaultAction\_Actions=6 Force=True

**8. Based on the previous answer, what were the four IDs set by the attacker? Enter the answer in order of execution. (format: 1st,2nd,3rd,4th)**

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" "ThreatIDDefaultAction\_Ids=\*"

| where isnotnull(ParentCommandLine)

| table \_time ParentCommandLine



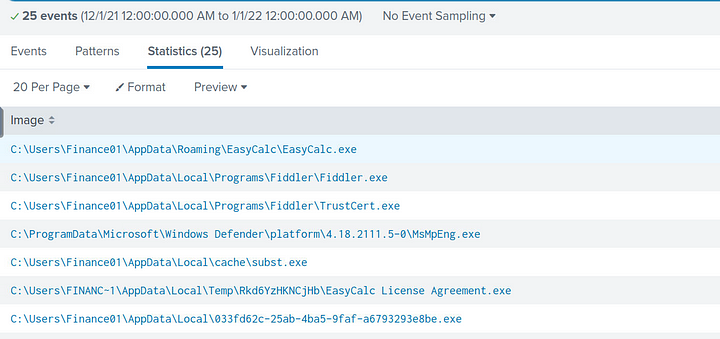
**Answer:** 2147735503,2147737010,2147737007,2147737394

**9. Another malicious binary was executed on the infected workstation from another AppData location. What was the full path to the binary?**

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" "C:\\Users\\Finance01\\AppData\\\*.exe"

| dedup Image

| table Image



We got 25 results. Now we need to look for the executable that is suspicious. I start by checking the first one.

While searching around for this executable, there is an interesting finding. That this file has many values under the OriginalFileName field.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EasyCalc.exe

| table Image OriginalFileName

| where isnotnull(OriginalFileName)



OriginalFileName is a field in PE headers which will display the previous names of the executable even if it is renamed completely. Looking at the names, it is clear that the attacker was trying to masquerade this file to look like a legitemate file.

**Answer:** C:\Users\Finance01\AppData\Roaming\EasyCalc\EasyCalc.exe

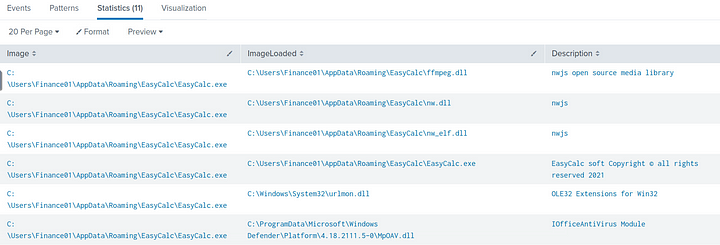
**10. What were the DLLs that were loaded from the binary from the previous question? Enter the answers in alphabetical order. (format: file1.dll,file2.dll,file3.dll)**

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EasyCalc.exe EventCode=7

| table Image ImageLoaded Description

| dedup ImageLoaded

The above filter will display a table of the Image and the Image it loaded and the description on the loaded image.



As we can see, the first three dll’s are the app’s own dll’s and the rest are system and external dll’s.

**Answer:** ffmpeg.dll,nw.dll,nw\_elf.dll

This is the end of the walkthrough.