

TryHackMe: New Hire Old Artifacts

The following writeup is for the [New Hire Old Artifacts](#) room hosted on TryHackMe. This is an intermediate level room that involves investigating an intrusion using Splunk. The scenario provided valuable practice in crafting effective queries to narrow down investigations. I hope you can find this writeup useful!

Scenario: You are a SOC Analyst for an MSSP (managed Security Service Provider) company called TryHackMe. 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 Widgets LLC's Splunk instance to see if there is anything the customer needs to be alerted on.

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

Start by opening the search and reporting app in Splunk. We can then search for 'Password Viewer' and look at the image field to see if we can find anything interesting (note I'm filtering for all time, however, you could also filter for December 2021 if the dataset was larger):

The screenshot shows a Splunk search interface. At the top, a search bar contains the query 'index="*" Password Viewer'. Below the search bar, a status bar indicates '27 events (before 7/23/24 1:25:12.000 PM)' and 'No Event Sampling'. The main content area displays a table with the following data:

Values	Count	%
C:\Users\FINANC~1\AppData\Local\Temp\11111.exe	27	100%

Additional UI elements include a 'Selected' dropdown menu with 'Yes' and 'No' options, and a 'Reports' section with links for 'Top values', 'Top values by time', 'Rare values', and 'Events with this field'. A close button (X) is visible in the top right corner of the table area.

You can see more information by looking at the raw logs:

... 20 lines omitted ...

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

FileVersion: 2.06

Description: Web Browser Password Viewer

Product: -

Company: NirSoft

What is listed as the company name?

As you can see in the previous question, the company name is listed in the raw log details, you could also create a query like as follows:

```
index="*" Password Viewer
| dedup Image
| table Image, Company
```

C:\Users\FINANC~1\AppData\Local\Temp\111111.exe

NirSoft

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)

Let's create a query that filters for the location of the previous binary (in the temp directory):

```
index=* User="DESKTOP-H1ATIJC\Finance01" Image:"\\AppData\\Local\\Temp\\*" EventCode=1
| dedup Image
| table Image, OriginalFileName, Product
```

After looking through the output, one executable stands out as suspicious:

C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe

PalitExplorer.exe

PalitExplorer

The answer is simply IonicLarge.exe,PalitExplorer.exe.

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.

To answer this question, I am going to filter for the malicious binary we found in the previous question and event ID 3 which is the Sysmon event for network connection detected. We can then look at the DestinationIp field to find what IP has 2 connections or enter:

```
index=* User="DESKTOP-H1ATIJC\Finance01" Image="C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe" EventCode=3
| stats count by Image, DestinationIp
| rename count as DestinationIpCount
```

Image #	DestinationIp #	DestinationIpCount #
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe	184.27.48.48	1
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe	127.0.0.1	79
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe	142.258.191.132	1
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe	142.258.191.286	1
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe	148.251.234.93	1
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe	9.59.53.45	2
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe	212.193.38.45	1
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe	34.117.59.81	1

Once we have identified the destination IP address that was connected to twice, we can enter it into Cyberchef using the Defang IP Addresses recipe like as follows:

Input

2.56.59.42

RBC 10 = 1

Output

2[.]56[.]59[.]42

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

To find what registry keys were changed/modified by this binary, we can filter for the event ID 13 which logs changes to a registry value:

```
index=* User="DESKTOP-H1ATIJC\\Finance01" Image="C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe" EventCode=13  
| table Image, TargetObject, Values, RuleName
```

Image	TargetObject	RuleName
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableWriteNotification	technique_id=T1089,technique_name=Disabling Security Tools
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableIOAVProtection	technique_id=T1089,technique_name=Disabling Security Tools
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableRealTimeMonitoring	technique_id=T1089,technique_name=Disabling Security Tools
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableScanOnRealTimeEnable	technique_id=T1089,technique_name=Disabling Security Tools
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableOnAccessProtection	technique_id=T1089,technique_name=Disabling Security Tools
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableBehaviorMonitoring	technique_id=T1089,technique_name=Disabling Security Tools
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\DisableAutomaticallyTakingAction	technique_id=T1089,technique_name=Disabling Security Tools
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender\\DisableAntiSpyware	technique_id=T1089,technique_name=Disabling Security Tools
C:\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	HKLM\\System\\CurrentControlSet\\Services\\Wsm\\State\\UserSettings\\5-1-5-21-1273532181-211932547-1629242413-18880\\Device\\HarddiskVolume1\\Users\\Finance01\\AppData\\Local\\Temp\\IonicLarge.exe	technique_id=T1543,technique_name=Service Creation

As you can see in the above image, majority of the registry values modified related to Windows Defender which has the key path: HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows Defender.

Some processes were killed and the associated binaries were deleted. What were the names of the two binaries? (format: file.xyz,file.xyz)

The hint lets us know to look for the 'taskkill /im' command. We can use this to significantly narrow down our results using the following query:

```
index=* CommandLine="*taskkill /im*"
| table CommandLine
```

```
"C:\\Windows\\System32\\cmd.exe" /c taskkill /im "WvmIOrcfSuILdX6SNwIRmGOJ.exe" /f & erase "C:\\Users\\Finance01\\Pictures\\Adobe Films\\WvmIOrcfSuILdX6SNwIRmGOJ.exe" & exit
```

```
"C:\\Windows\\System32\\cmd.exe" /c taskkill /im phcIAmLJMAIMSa9j9MpgJo1m.exe /f & timeout /t 6 & del /f /q "C:\\Users\\Finance01\\Pictures\\Adobe Films\\phcIAmLJMAIMSa9j9MpgJo1m.exe" & del C:\\ProgramData\\*.dll & exit
```

This outputs 2 events for which we can see the killed processes. The answer being WvmIOrcfSuILdX6SNwIRmGOJ.exe,phcIAmLJMAIMSa9j9MpgJo1m.exe.

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

This is a simple question, all we need to do is search for powershell and check the command line field for commands which relate to Windows Defender:

index=* Image="*powershell.exe"

CommandLine

X

5 Values, 4.225% of events

Selected

Yes

No






Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%	
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	2	33.333%	
powershell WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ThreatIDDefaultAction_Ids=2147735503 ThreatIDDefaultAction_Actions=6 Force=True	1	16.667%	
powershell WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ThreatIDDefaultAction_Ids=2147737007 ThreatIDDefaultAction_Actions=6 Force=True	1	16.667%	
powershell WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ThreatIDDefaultAction_Ids=2147737010 ThreatIDDefaultAction_Actions=6 Force=True	1	16.667%	
powershell WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ThreatIDDefaultAction_Ids=2147737394 ThreatIDDefaultAction_Actions=6 Force=True	1	16.667%	

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)

The answer to this question can be see in the last screenshot of the previous question:

```
powershell WMIC /NAMESPACE:\\root\Microsoft\Windows
\Defender PATH MSFT_MpPreference call Add
ThreatIDDefaultAction_Ids=2147735503
ThreatIDDefaultAction_Actions=6 Force=True
```

```
powershell WMIC /NAMESPACE:\\root\Microsoft\Windows
\Defender PATH MSFT_MpPreference call Add
ThreatIDDefaultAction_Ids=2147737007
ThreatIDDefaultAction_Actions=6 Force=True
```

```
powershell WMIC /NAMESPACE:\\root\Microsoft\Windows
\Defender PATH MSFT_MpPreference call Add
ThreatIDDefaultAction_Ids=2147737010
ThreatIDDefaultAction_Actions=6 Force=True
```

```
powershell WMIC /NAMESPACE:\\root\Microsoft\Windows
\Defender PATH MSFT_MpPreference call Add
ThreatIDDefaultAction_Ids=2147737394
ThreatIDDefaultAction_Actions=6 Force=True
```

The answer is: 2147735503,2147737010,2147737007,2147737394.

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

We can modify the query used in the second question to look for other binaries from another AppData location:

```
index=* User="DESKTOP-H1ATIJC\Finance01" Image="*\\AppData\\*"
| search NOT Image="C:\\Users\\FINANC~1\\AppData\\Local\\Temp\\*"
| dedup Image
| table Image
```

C:\Users\Finance01\AppData\Roaming\EasyCalc\EasyCalc.exe
C:\Users\Finance01\AppData\Local\Programs\Fiddler\Fiddler.exe
C:\Users\Finance01\AppData\Local\Programs\Fiddler\TrustCert.exe
C:\Users\Finance01\AppData\Local\cache\subst.exe
C:\Users\Finance01\AppData\Local\033fd62c-25ab-4ba5-9faf-a6793293e8be.exe
C:\Users\Finance01\AppData\Local\d1db597a-57e6-4233-bf9f-de9e7b0dd233.exe
C:\Users\Finance01\AppData\Local\Temp\IonicLarge.exe
C:\Users\Finance01\AppData\Local\Programs\Setup.exe
C:\Users\Finance01\AppData\Local\Programs\7z2107-x64.exe

The first binary stands out as odd, and it is also the answer to the question.

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)

To find the answer to this question, we can search for event ID 7 and the .dll file extension like as follows:

```
index=* Image="C:\\Users\\Finance01\\AppData\\Roaming\\EasyCalc\\EasyCalc.exe" EventCode=7 *.dll
```

Once you look at the ImageLoaded field, you can see the DLLs that were loaded from the binary:

ImageLoaded

10 Values, 100% of events

Selected

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Top 10 Values	Count	%	
C:\\Users\\Finance01\\AppData\\Roaming\\EasyCalc\\nw_elf.dll	15	29.412%	<div></div>
C:\\Users\\Finance01\\AppData\\Roaming\\EasyCalc\\ffmpeg.dll	13	25.49%	<div></div>
C:\\Users\\Finance01\\AppData\\Roaming\\EasyCalc\\nw.dll	13	25.49%	<div></div>

This room provided an excellent exercise in utilising Splunk to investigate a security incident. Through a series of targeted queries, it was possible to piece together the activities of a threat actor. Each step required critical thinking and effective use of Splunk's search capabilities. Through a detailed analysis of the logs, I was able to correctly answer every question.