.. /Eventvwr.exe

UAC bypass (GUI)

Displays Windows Event Logs in a GUI window.

Paths:
C:\Windows\System32\eventvwr.exe
C:\Windows\SysWOW64\eventvwr.exe

Resources:
- https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
- https://github.com/enigma0x3/Misc-PowerShell-Stuff/blob/master/Invoke-EventVwrBypass.ps1
- https://twitter.com/orange_8361/status/1518970259868626944

Acknowledgements:
- Matt Nelson (@enigma0x3)
- Matt Graeber (@mattifestation)
- Orange Tsai (@orange_8361)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_uac_bypass_eventvwr.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/registry/registry_set/registry_set_uac_bypass_eventvwr.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/197615345b927682ab7ad7fa3c5f5bb2ed911eed/rules/windows/file/file_event/file_event_win_uac_bypass_eventvwr.yml
- Elastic: https://github.com/elastic/detection-rules/blob/d31ea6253ea40789b1fc49ade79b7ec92154d12a/rules/windows/privilege_escalation_uac_bypass_event_viewer.toml
- Splunk: https://github.com/splunk/security_content/blob/86a5b644a44240f01274c8b74d19a435c7dae66e/detections/endpoint/eventvwr_uac_bypass.yml
- IOC: eventvwr.exe launching child process other than mmc.exe
- IOC: Creation or modification of the registry value HKCU\Software\Classes\mscfile\shell\open\command

UAC bypass

. During startup, eventvwr.exe checks the registry value HKCU\Software\Classes\mscfile\shell\open\command for the location of mmc.exe, which is used to open the eventvwr.msc saved console file. If the location of another binary or script is added to this registry value, it will be executed as a high-integrity process without a UAC prompt being displayed to the user.

```
eventvwr.exe
```

Use case: Execute a binary or script as a high-integrity process without a UAC prompt.
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
ATT&CK® technique: T1548.002
Tags: Application: GUI

. During startup, eventvwr.exe uses .NET deserialization with %LOCALAPPDATA%\Microsoft\EventV~1\RecentViews file. This file can be created using https://github.com/pwntester/ysoserial.net

```
ysoserial.exe -o raw -f BinaryFormatter - g DataSet -c calc > RecentViews & copy RecentViews
%LOCALAPPDATA%\Microsoft\EventV~1\RecentViews & eventvwr.exe
```

Use case: Execute a command to bypass security restrictions that limit the use of command-line interpreters.
Privileges required: Administrator
Operating systems: Windows 7, Windows 8, Windows 8.1, Windows 10
ATT&CK® technique: T1548.002
Tags: Application: GUI