|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Source | Event ID | EventType or EventDescription | EventField | Details |
| Sysmon | 12 | CreateKey | TargetObject | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe |
| Sysmon | 13 | SetValue | TargetObject | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe\Debugger |
| Sysmon | 1 | Process Create | CommandLine | reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v "Debugger" /t REG\_SZ /d "C:\windows\system32\cmd.exe" /f |
| Sysmon | 1 | Process Create | ParentImage  CommandLine | Winlogon.exe  C:\windows\system32\cmd.exe sethc.exe 211 |

Same for other accessibility features such as utilman.exe, osk.exe, Magnify.exe, Narrator.exe, DisplaySwitch.exe, AtBroker.exe

Just need to replace sethc.exe with the executable in question.

Maybe Parent Process for a cmd can also be the said accessibility executable, as of now it showed parent process winlogon.exe

parent\_process = "C:\windows\system32\setchc.exe" OR parent\_process\_name = " C:\windows\system32\osk.exe" OR parent\_process\_name = " C:\windows\system32\utilman.exe" OR parent\_process\_name = " C:\windows\system32\Magnify.exe" OR parent\_process\_name = " C:\windows\system32\DisplaySwitch.exe" OR parent\_process\_name = " C:\windows\system32\AtBroker.exe") OR (process\_name = "setchc.exe" OR process\_name = "osk.exe" OR process\_name = "utilman.exe" OR process\_name = "Magnify.exe" OR process\_name = "DisplaySwitch.exe" OR process\_name = "AtBroker.exe") AND

target\_object CONTAINS ('HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options' AND 'Debugger')