





/Wlrmrdr.exe

☆ Star

7,060

Execute

Windows Logon Reminder executable

Paths:

c:\windows\system32\wlrmrdr.exe

Resources:

- <https://twitter.com/0gtweet/status/1493963591745220608>
- <https://twitter.com/Oddvarmoe/status/927437787242090496>
- <https://twitter.com/falsneg/status/1461625526640992260>
- <https://docs.microsoft.com/en-us/windows/win32/api/shellapi/ns-shellapi-notifyicondataw>

Acknowledgements:

- Grzegorz Tworek ([@0gtweet](#))
- Oddvar Moe ([@Oddvarmoe](#))
- Freddy ([@falsneg](#))

Detections:

- Sigma: [proc_creation_win_lolbin_wlrmrdr.yml](#)
- IOC: wlrmrdr.exe spawning any new processes

Execute

Execute calc.exe with wlrmrdr.exe as parent process

```
wlrmrdr.exe -s 3600 -f 0 -t _ -m _ -a 11 -u calc.exe
```

Use case:	Use wlrmrdr as a proxy binary to evade defensive countermeasures
Privileges required:	User
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	T1202: Indirect Command Execution