.. /Wlrmdr.exe

Execute

Windows Logon Reminder executable

Paths:
c:\windows\system32\wlrmdr.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: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_wlrmdr.yml
- IOC: wlrmdr.exe spawning any new processes

Execute

Execute calc.exe with wlrmdr.exe as parent process

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

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