./ persistence-info.github.io

View on GitHub

MPNotify

Location:

`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`

Classification:

Criteria	Value
Permissions	Admin
Security context	System
Persistence type	Registry
Code type	EXE
Launch type	Any logon required
Impact	Non-destructive[1]
OS Version	All OS versions
Dependencies	OS only
Toolset	Scriptable

Description:

If you put `mpnotify` `REG_SZ` value into the `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` registry key, the exe will be loaded by the `winlogon.exe` process, when user logs on. After the timeout (30s) the process and its child processes are terminated.

References:

https://youtu.be/ggY3srD9dYs

Credits:

@0gtweet

See also:

Remarks:

1. Slows the logon process down by 30s, but it works. ↩