

Forum:[Hack Forums](#)

Thread: [Best Persistence Technique?](#)

Neik111 - December 12, 2023, 8:43 pm

Hey Guys,

I have a problem with startup of my exe.

Its completly fud, but when i use a reg key for startup it gets detected.

Startupfolder also gets detected.

How can i avoid this or use another technique?

osn64698 - December 12, 2023, 9:31 pm

Nobody will share his own method, but you can start by using .bat/.vbs files etc.

DramaKing - December 13, 2023, 6:49 am

Need to know the AV in question. These are legitimate ways to run apps at startup, so it's hard to say.

gangushbo - December 13, 2023, 12:59 pm

which av? watchdog tried?

neonbytes - December 14, 2023, 4:13 pm

maybe you can use an intermediate lolbin to create it for your malware

trojan > lolbin > create reg key

this could detach the action from your malware

Neik111 - December 14, 2023, 7:57 pm

(Dec 14, 2023 05:13 PM)neonbytes Wrote: [\[CITE\]](#) maybe you can use an intermediate lolbin to create it for your malware

trojan > lolbin > create reg key

this could detach the action from your malware

Yea i tried this, setting the key is undetected, just when you reboot, then its detected

Wacatac - December 14, 2023, 8:46 pm

(Dec 14, 2023 08:57 PM)Neik111 Wrote: [\[CITE\]](#) Yea i tried this, setting the key is undetected, just when you reboot, then its detected

Because your malware that you're trying to put on startup is detected, not the LOLBIN.

NyQuil - December 23, 2023, 2:27 am

(Dec 14, 2023 09:46 PM)Tentco Wrote: [\[CITE\]](#) Because your malware that you're trying to put on startup is detected, not the LOLBIN.

run as admin, kek

DramaKing - December 23, 2023, 5:41 pm

Not to beat a dead horse, but based on the available info, it may not be completely FUD. It could be detected at runtime without the execution method having anything to do with it. Or the registry key

could push the heuristics just enough to trigger detection. Maybe try creating a scheduled task.