

Forum:[Hack Forums](#)

Thread: [\[c++\] What is the best persistence method for a botnet on Windows?](#)

loomixx - January 26, 2025, 1:08 am

Hey guys. I'm new here. Recently I have coded my own botnet in c++. It was going pretty well until I faced a problem: what persistence method do i use, so it's:

- 1) Undetected, legitimate-looking (like dll side loading into legitimate process)
- 2) User mode (no admin rights needed for dropper)
- 3) Works on windows 7, 8, 10, 11

I tried side loading into OneDrive (drop malicious botnet dll - cscapi.dll into %LOCALAPPDATA%\Microsoft\OneDrive, so when one drive launches, it loads malicious cscapi.dll instead of loading from system folder)

However, this works only on windows 10 because only there OneDrive is installed and is at autorun by default.

I don't know if it is good idea to change botnet program from dll to exe, because obviously while exe-based persistence is simpler, it inherently carries a higher risk of detection, so it's better to sideload (dll) into legitimate process.

So I'm eager to learn from the expertise within this community. Any insights into advanced persistence mechanisms that meet the above criteria would be invaluable.

Thank you for your time and consideration.

Bastille - January 26, 2025, 1:10 am

Please stick to one thread : <https://hackforums.net/showthread.php?tid=6290312>

Do not cross-post, if you need more visibility you can use the bump feature : see the [Help Docs](#)

Thanks