

Forum: [Hack Forums](#)

Thread: [\(Windows\) How to check if your payload is running raw or crypted?](#)

neonbytes - April 3, 2026, 2:37 pm

hey guys

i'm looking for a way to check if my payload is running raw or encrypted

i was thinking, one method to know if running raw, would be to get PPID (parent process id) and from there get the parent process, if the parent process is: explorer.exe it's raw and ran manually (double clicked)

cmd.exe it's raw and ran manually (from the cli) conhost.exe it's raw and ran manually proxying with conhost (from the cli)

etc

but it does not seem to be a very reliable way, as i would need to know all the methods that can execute a file from disk (for example using lolbins)

any ideas that can guide me in the right direction?

thanks

DramaKing - April 4, 2026, 6:02 am

I dispute your method, but you do need to rewrite your post so that it says what you mean.

neonbytes - April 4, 2026, 10:10 am

(Apr 4, 2026 06:02 AM)DramaKing Wrote: [\[CITE\]](#) I dispute your method, but you do need to rewrite your post so that it says what you mean.

what is not clear?

i need to know if my payload (rat/bot/malware) is being executed raw (without crypt) or crypted (injected, self-loaded, dll sideloaded, etc)

either would be useful