

Forum:[Hack Forums](#)

Thread: [how to hide malware from windows ???](#)

Twisted-Spider - September 11, 2021, 4:12 am

i recently created a ransomware and was scratching my head all day on how to hide it any ideas or suggestions ??

Terry A. Davis - September 11, 2021, 3:30 pm

Take a step back, look at what you're doing, you're doing something common, you've likely followed a simple play by play tutorial.

Look at how you could hook explorer to bypass certain functions, look at how you could disable anti-virus engines, look at things it's detecting, reduce the import table, load libraries and functions dynamically instead of statically.

There is plenty you can do, and if you created a "ransomware" like you said, then you should understand enough to know what I am saying.

Twisted-Spider - September 12, 2021, 6:34 pm

(Sep 11, 2021 03:30 PM)Depressed Wrote: [\[CITE\]](#) Take a step back, look at what you're doing, you're doing something common, you've likely followed a simple play by play tutorial.

Look at how you could hook explorer to bypass certain functions, look at how you could disable anti-virus engines, look at things it's detecting, reduce the import table, load libraries and functions dynamically instead of statically.

There is plenty you can do, and if you created a "ransomware" like you said, then you should understand enough to know what I am saying.

I mean trying to make the ransomware work without admin privilege's so anti-virus engines I tried to load libraries and functions dynamically but that didn't work I also tried to crypt the payload to XOR and then decrypt it while executing that didn't help i also tried to hide it in the new vulnerability CVE-2021-40444. any other ideas ???

i forgot to mention I am using .net

Terry A. Davis - September 13, 2021, 12:04 am

Why not use a UAC bypass and then cripple any anti-virus, look at how they handle exclusions and either inject your own as an exclusion, uninstall it, hook things in it that check to see if it's been tampered with?

XOR is quite common and the algorithm for it is easy to find in a file, so yet again, common thing, very easy to detect.

Also, that's not a 0day so odds are most anti-virus vendors will detect it.

I'm not going to hand hold you in this, this is all on you buddy.

spongebob - September 13, 2021, 8:26 am

Ransomwares' discussion is not allowed here. Please read [Help Docs](#)

