

Forum:[Hack Forums](#)

Thread: [Free Insight on Crypters](#)

benio - March 9, 2022, 3:41 pm

Alright im going to save you time and money.

1. If a crypter is using registry key persistence it will not bypass WD at runtime, do not touch it with a 10ft pole.
2. If the crypted file is dropping itself to disk after its run, then it will get detected by WD behavioral analysis. Your dropped file must be signed with a trusted signature.
3. If the crypter does not have AMSI solution then you will probably get decked at runtime.

Say it does bypass it for a few hours. After distribution, the dropped file will get caught by WD.

In 2022, the crypter must use a fileless technique or you must perform DLL hijacking to get a true bypass. Your persistence must also be unique like WMI event subscription. The main .exe must not have the dropper code inside it, it will get caught even when obfuscated. The .exe must be a shell that holds the dropper code inside it. Most of these skids have no clue how to code something complex enough to bypass AV in 2022 for more than a few hours. Just a little rant after I looked at the marketplace here.

Do not believe the bullshit scan results either, in 2022 most AV's detect behavior. I cannot believe some of these skids are selling a GUI for 75-150\$ a month marketing it as a crypter. What if I jump on here and sell you guys an actually working product can i charge 500?

SIM549839 - March 11, 2022, 12:55 am

(Mar 9, 2022 04:41 PM)benio Wrote: [\[CITE\]](#) Alright im going to save you time and money.

1. If a crypter is using registry key persistence it will not bypass WD at runtime, do not touch it with a 10ft pole.
2. If the crypted file is dropping itself to disk after its run, then it will get detected by WD behavioral analysis. Your dropped file must be signed with a trusted signature.
3. If the crypter does not have AMSI solution then you will probably get decked at runtime.

Say it does bypass it for a few hours. After distribution, the dropped file will get caught by WD.

In 2022, the crypter must use a fileless technique or you must perform DLL hijacking to get a true bypass. Your persistence must also be unique like WMI event subscription. The main .exe must not have the dropper code inside it, it will get caught even when obfuscated. The .exe must be a shell that holds the dropper code inside it. Most of these skids have no clue how to code something complex enough to bypass AV in 2022 for more than a few hours. Just a little rant after I looked at the marketplace here.

Do not believe the bullshit scan results either, in 2022 most AV's detect behavior. I cannot believe some of these skids are selling a GUI for 75-150\$ a month marketing it as a crypter. What if I jump on here and sell you guys an actually working product can i charge 500?

Dll hijacking is the proper way to bypass most AV's, and it is not that hard to find ;p

jmark7 - March 11, 2022, 8:18 am

(Mar 11, 2022 01:55 AM)SIM549839 Wrote: [\[CITE\]](#) Dll hijacking is the proper way to bypass most AV's, and it is not that hard to find ;p

can you elaborate more on how you can do it?

Comrade - March 11, 2022, 8:29 am

Now that's what we can call quality thread....

Thanks for the knowledge.

Comrade

SIM549839 - March 11, 2022, 8:50 am

(Mar 11, 2022 09:18 AM)jmark7 Wrote: [\[CITE\]](#) can you elaborate more on how you can do it?

You gotta exploit existing files that are signed.. usually side loading is quite easy to detect with tools like : procmon etc.

anderz2912 - March 11, 2022, 11:22 am

yo send me ur discord bro...

Basilisk - March 11, 2022, 1:36 pm

Speaking of which, can you recommend a good crypter?

Jhonnycash779 - March 14, 2022, 5:46 pm

Very interesting thread, i'll have a look on dll hijacking.

There is demand for quality, if you are able to build this kind of 'perfect' product, and to prove it, you should start your business, here, and surely also not here for more ..

sn0ffleren - March 31, 2022, 4:48 pm

thank you brother :)))) +1