

Forum:[Hack Forums](#)

Thread: [Question about Generic detections](#)

Mr Relic - December 8, 2018, 5:59 am

Hi!

I'm currently working on my own crypter and it's going quite well actually.

Scantime detections: ESET

Runtime detections: ESET & Dr. Web AV

All the rest are FUD, even bypasses Windows Defender.

However I had a small question regarding Generic detections.

I takes me a good recrypt or 5 everytime per stub to find assembly info/ICO to avoid getting Generic detections.

Anyone knows if there's any keywords to avoid etc?

Thanks in advance!

g3ntl3m4n - December 8, 2018, 6:32 am

The problem you have is based of your codeflow or api chains

What you could try is do a Control flow obfuscation..

If you have this correct you dont need a assembly or ico at all...

Mr Relic - December 8, 2018, 6:34 am

(Dec 8, 2018 07:32 AM)th3j3st3r Wrote: [\[CITE\]](#) The problem you have is based of your codeflow or api chains

What you could try is do a Control flow obfuscation..

If you have this correct you dont need a assembly or ico at all...

Hmm I see..

I'll take a look at that right now.

I personally host my own direct download link and use a macro exploit to get the exe on a computer so it's not like the assembly or ico has to be convincing anyway.

But would be helpful if I didn't need to put any in the first place.

Thanks!

g3ntl3m4n - December 8, 2018, 6:36 am

If you just dont want to put the effort in it everytime finding an assembly just use anti tampering a lot of obfuscators do have this option