

Forum:[Hack Forums](#)

Thread: [How to remove false positives on your crypted stub](#)

Glyco - November 23, 2016, 5:47 pm

This tutorial is to show you how to remove false positives in scan reports of your crypted file. Often times you will find your stub not being fud because its detected by false positives. These could be for many reasons the icon/assembly or it could because of the crypter in most instances it not because of the crypter its because of something else. Those false positives you might come across on come in different names which like below Gen:Variant.Zusy.33605

Gen:Variant.Razy.108032

EE:Malwr.Heur.Razy.108032

Today I will be demonstrating on how to add a digital signature to your stub. Basically what the digital signature does to your stub is it just makes it look more trustworthy when it is scanned upon AV's

Lets begin:

[Click here to download](#)

[Viruscan](#)

Do not add shortcut of the program. Add the actual file location

You can determine whether a program has a digital signature or not just by clicking on it it should look like this.

I have already created my stub, but it does not have a signature here is the scan result I get.

Now watch what happens when I add the signature.

4/35 you can remove the rest of the detections by changing the icon or assembly. If all else fail again it might be the crypter.

Sky Summers - November 23, 2016, 5:55 pm

Nice tutorial right here. I'll try this later on

holybishop - November 24, 2016, 5:17 am

Nice tutorial, icon and assembly are always first culprits. Is frustrating trying different icons and assembly many times to get Fud but at the end of the day, is definitely worth it.

For those using exploits to spread, using default windows application (exe) icon and a good assembly will mostly get your exe FUD, since it wouldn't show on the target pc, you have nothing to be concerned about.

Always avoid well known applications icons or icons and assemblies from applications that need admin right to run.

Codefuser - November 24, 2016, 7:36 am

It is not false positive if it is malware.

And Gen is still a code detection, even if it could be removed with an icon/assembly.

AliensGb - November 24, 2016, 5:31 pm

Thanks For Sharing Broooooother

InteNt - December 2, 2016, 5:20 pm

Link doesn't work for the klash digital signature

XLMLCode - December 10, 2016, 9:00 am

Yeah and I believe if you obfuscate it, it may help too.

If you want it to be hidden though, I'd suggest not using an icon because if looking for it in task manager it's an easy find.