

Forum:[Hack Forums](#)

Thread: [Need a backdoor check.](#)

Emilz - July 18, 2015, 5:33 am

Hey guys im in need of someone with sublime skills to check a .exe for me if its backdoored (with rat,botnet or whatever)

Hope to find some help, for a nice reward.
Talk to you soon.

EDIT:

The file cant be checked with anubis, malwr,stealthexpert because its simply not possible.
This raised a few flags but considering the type of file im checking its not making me sketched 1000%

5chn4pp - July 18, 2015, 5:48 am

if the file has anti vm then its 99% a virus.

Emilz - July 18, 2015, 5:52 am

Thats what i thought but its regarding a private CSGO hack, that actually works.

So i wanted to find out if its binded or that the creator of the private hack just made it anti vm for competition or something.

Slachter - July 18, 2015, 5:53 am

Did you open it?

If you didn't, remove the file, because it is dangerous that file, it has anti-AV.

If you did, download Farbar Recovery Scan Tool and run a scan.

Then post the FRST.txt & Addition.txt on pastebin and give a link to it on here.

I hope this helps you.

(Jul 18, 2015 05:52 AM)Emilz Wrote: [\[CITE\]](#) Thats what i thought but its regarding a private CSGO hack, that actually works.

So i wanted to find out if its binded or that the creator of the private hack just made it anti vm for competition or something.

Did you buy the "hack" ? Who gave it to you.

Emilz - July 18, 2015, 5:54 am

Im not dumb lol i dont open shit before its 100% sure that its not infected, i just need a checkup if the file has any connections made, like connecting to a dns or a website when opened etc. I just dont know how to do that, if someone could explain me thats perfect also :)

Slachter - July 18, 2015, 5:56 am

(Jul 18, 2015 05:54 AM)Emilz Wrote: [\[CITE\]](#) Im not dumb lol i dont open shit before its 100% sure that its not infected, i just need a checkup if the file has any connections made, like connecting to a dns or a website when opened etc. I just dont know how to do that, if someone could explain me thats perfect also :)

So you are not able to scan it with any antivirus?

100% it is a virus.

5chn4pp - July 18, 2015, 5:56 am

(Jul 18, 2015 05:56 AM)Slachter Wrote: [\[CITE\]](#) So you are not able to scan it with any antivirus?

100% it is a virus.

I have a hack that works, they do exist?

Slachter - July 18, 2015, 5:58 am

(Jul 18, 2015 05:56 AM)FlareMalware Wrote: [\[CITE\]](#) I have a hack that works, they do exist?
You got it from YouTube, mate?

Tell me how please q.q

Did you search "csgo hack 2015 cracked unpatched" !?!?

5chn4pp - July 18, 2015, 6:00 am

(Jul 18, 2015 05:58 AM)Slachter Wrote: [\[CITE\]](#) You got it from YouTube, mate?

Tell me how please q.q

Did you search "csgo hack 2015 cracked unpatched" !?!?

This is off topic, but yes i got it from youtube.

Emilz - July 18, 2015, 6:01 am

I scanned it now with ReFUD and it only gives a AVG Free detection which is:Virus found win32Vblacked could be a false positive?

Even ESET doesnt detect it?

EDIT:

I didnt get it from youtube, i know the ways ;)

Im no noob i just didnt check files to be backdoored yet because i never download or open shit.

5chn4pp - July 18, 2015, 6:04 am

(Jul 18, 2015 06:01 AM)Emilz Wrote: [\[CITE\]](#) I scanned it now with ReFUD and it only gives a AVG Free detection which is:Virus found win32Vblacked could be a false positive?

Even ESET doesnt detect it?

EDIT:

I didnt get it from youtube, i know the ways ;)

Im no noob i just didnt check files to be backdoored yet because i never download or open shit.

The Packed.Win32.Black.a detection identifies files that are packed with a stolen version of the Themida software protection program.

Emilz - July 18, 2015, 6:05 am

Yeah i googled that far to.

But only 1 detect AVG FREE and AVG FREE detects it earlier then ESET, AVAST etc

I think the only real solution is to check it for connections etc but i dont know how.

Neos07 - July 18, 2015, 6:06 am

Check my tutorial: <https://hackforums.net/showthread.php?tid=4836145>

:)

5chn4pp - July 18, 2015, 6:08 am

(Jul 18, 2015 06:06 AM)Neos07 Wrote: [\[CITE\]](#) Check my tutorial:

<https://hackforums.net/showthread.php?tid=4836145>

:)

The file we are talking about has anti vm and sandbox