

Forum:[Hack Forums](#)

Thread: [\[Tut\] Avira Got You Stumped?](#)

Deathader - May 20, 2010, 3:10 pm

So, word on the street is that you have your server ALMOST FUD, but you have one detection stumping you. And that detection is Avira TR/Dropper.gen

How can I get past this bugger?

1) The easiest and simplist way to do so is encrypt your server with an after-market obfuscator / packer. (SmartAssembly, xenocode, etc..)

2) Check to make sure "Stub" is NOWHERE in your code. I had my server's solution named "Stub", and matter or fact, that is what was causing the detection. Change it to something like "service"

3) Use complex filesplits, such as "ïu¾¼Ç`Õ®ipfx'fè¶·ï...¹îªý". A good way to get GOOD filesplits is to open another exe in notepad, and copy/paste some of the giberish you see (be sure to rearrange it a bit). Some AV's check for the word SPLIT, FILESPLIT, SPLITTER, etc..

4) Add junk code / Add 200kb icon. These are the 2 methods I absolutely hate, because you are not only not learning how to solve problems, but you are now stuck with a HUGE stub. No stub should EVER be over 25 - 30 kb. I like having mine under 20kb, and a 200kb icon prevents that! Although they CAN make your stub FUD.

5) Stop using EOF. Avira has started to pick up on EOF, and if your file is under like 50kb, and has EOF data, it will USUALLY be picked up as a dropper. How can I prevent using EOF? Check into other methods, such as http settings files (store your settings on a server and get the stub to download it!) or use UpdateResources ([HERE](#))

If you still can't get it to compile FUD, you will have to start the trial/error method. To do this, remove a sub from your exe, compile it, and scan it. I suggest using Avira home, as it is MUCH faster than using a web based scanner (You know you are trying to beat avira, nothing else). When you come upon the detected line(s), try rearranging them, inversing if's, etc. Do what you have to do to make it different.

That's all folks. I will update this thread if I think of any other methods.

Thanks for reading!

South Park - May 20, 2010, 3:16 pm

Nice guide. I need a way to bypass avira WITHOUT editing my crypter (Just the stub). But since its detecting the EOF its going to be hard. I did but now I have 2/24, iKarus and A-Squared or some shit.

GoldStar - May 20, 2010, 3:19 pm

yeah that's about it, you said it all. nice tut.

-RC2- - May 20, 2010, 3:20 pm

just add junk code , change/remove icon, there are alot of other tutorials.

GodWall - May 20, 2010, 3:37 pm

Wow gr8 advice from you once again, so if I use something like this "ïu¾<Ç"Ö@ipfx'fè¶·ï...¹ířáý"
,out of Microsoft.Scripting.Core.dll right, lol sorry off subject,
as my split, would be gr8 to gen this up quick, like a String Builder I was searching to find what
Method would cre8 this value, do you maybe know or is it even possible? If I find it I'll post back :)
thanks

Unrated - May 20, 2010, 3:47 pm

Lmao, This is great. Nice job!

seheiahs - May 20, 2010, 4:07 pm

Great tut, thanks.

Strange think for me : I applied 2) and 3) to my personnal keylogger and it' s worse :
2/20 (NOD32 and of course avira) -> 4/20 (NOD32, avira + a² and ikarus now detect
Trojan-Dropper.MSIL)...

Beck - May 20, 2010, 4:08 pm

Yea, when I make my keyloggers, I include 3-4 lines of junk code in each sub, and I change the
strings and filesplits to text that has been encrypted by RC4 polymorphic encryption.

High Definition - May 20, 2010, 9:39 pm

Sounds good...

you may try opening a image or rar or any such with notepad...

Nice Work

Edit : I see you've suggested the same..

Deathader - May 21, 2010, 3:54 am

(May 20, 2010 09:39 PM)High Definition Wrote: [\[CITE\]](#) Sounds good...

you may try opening a image or rar or any such with notepad...

Nice Work

Edit : I see you've suggested the same..

If you open any file (other than anything plaintext) you will find hundreds, if not THOUSANDS of
GREAT splits :D

Odayleet - May 21, 2010, 5:20 am

Thanks, I never knew that Avira was detecting EOF on crypter ..

Meth - May 21, 2010, 6:14 am

(May 20, 2010 03:20 PM)robbiecee2 Wrote: [\[CITE\]](#) just add junk code , change/remove icon, there
are alot of other tutorials.

Did you not read it?

DarkSeven46 - May 21, 2010, 8:15 am

Thanks for the tutorial Deathader.

Deathader - May 21, 2010, 11:26 am

(May 21, 2010 08:15 AM)darkvista46 Wrote: [\[CITE\]](#) Thanks for the tutorial Deathader.
No problem!

Neon666 - June 8, 2010, 9:23 am

Thanks man, pretty nice ;)

Neon

JIMP - June 8, 2010, 9:33 am

Nice TUT. Really helped. Thanks for this.

rapidguide - June 8, 2010, 10:13 am

Nice You Are Good Helping Member Here But Server Size Becomes 300<?kB

check24 - June 8, 2010, 10:23 am

(May 20, 2010 03:10 PM)Deathader Wrote: [\[CITE\]](#) 5Check into other methods, such as http settings files (store your settings on a server and get the stub to download it!)

Can you explain this method`?

but thats a great tutorial

:)