

Forum:[Hack Forums](#)

Thread: [\[TUT\] Bypass avira detection \[TR/Dropper.GEN \]](#)

MoonWalker - May 19, 2011, 3:04 am

Bypass avira detection [TR/Dropper.GEN]

I've seen a lot of members having trouble in bypassing avira detection (TR/Dropper.GEN). Well here is a simple trick to fix that. Avira detects the file assembly, Use the following values in your stub and then generate the server. This time it'll be FUD.

Download RESHACKER and the replace the version info of your stub with these values.

Code VALUE "FileDescription", "Hijack This"

VALUE "FileVersion", "2.00.0002"

VALUE "InternalName", "Hijack This"

VALUE "LegalCopyright", "© 2007 Trend Micro Inc"

VALUE "OriginalFilename", "Hijack This"

VALUE "ProductName", "Hijack This"

VALUE "ProductVersion", "2.00.0002"

VALUE "Assembly Version", "2.00.0002"

This made my server 0/33. It should work for you too.

Volim te - May 19, 2011, 3:09 am

Nice TUT mate, is there A way to bypass the detection 'BDS/Backdoor.Gen' ? (Without crypting as it's a DLL lol)

wertyl11 - May 19, 2011, 3:15 am

Are you sure this is the sollution ?

Because dropper detection pretty much says for itself that it reacts on a file getting dropped. But if this tutorial worked, Great! nice share!

Gooples - May 19, 2011, 3:15 am

Hijack this worked in 07 not 11.

Banks? - May 19, 2011, 3:39 am

(May 19, 2011 03:15 AM)PinZ Wrote: [\[CITE\]](#) Hijack this worked in 07 not 11.

This. Avira isn't stupid, they don't fall for assemblies anymore. Get a new RunPE or find the code that is detected and recode it.

MoonWalker - May 19, 2011, 4:29 am

(May 19, 2011 03:15 AM)PinZ Wrote: [\[CITE\]](#) Hijack this worked in 07 not 11.

If you don't know anything about it then please don't post here.

(May 19, 2011 03:39 AM)Banksy™ Wrote: [\[CITE\]](#) This. Avira isn't stupid, they don't fall for assemblies anymore. Get a new RunPE or find the code that is detected and recode it.

I've tested this. I made a downloader and it was detected as TR/Dropper.GEN. but after doing this its FUD.

Sheikh. - May 19, 2011, 4:43 am

This is an old trick actually. Btw just use CodeDom and selfmade or undetected RunPE and its fud too.. Without assembly.

Numair - May 19, 2011, 4:46 am

Well i think many time ago Soul Collector posted the same thing to bypass Avira but using GUI.

Gooples - May 19, 2011, 5:35 am

(May 19, 2011 04:29 AM)MoonWalker Wrote: [\[CITE\]](#) If you don't know anything about it then please don't post here.

I've tested this. I made a downloader and it was detected as TR/Dropper.GEN. but after doing this its FUD.

Kid, I do know. L2 code then come back.

GoldenPhe0nix - May 19, 2011, 5:59 am

nice tut man. Thanks for the share.

Drag00n # The Hacker - May 19, 2011, 5:59 am

Cool tutorial and very useful.Thanks.

.Astro - May 19, 2011, 7:36 am

Like I haven't seen this before ..

E.R.R.O.R - May 19, 2011, 8:11 am

very old , now it dont work i have been useing another method

Ingenuity - May 19, 2011, 9:20 am

Doesn't work in the latest version of Avira. They don't fall for shit like this anymore.

Doctor Stein - May 19, 2011, 11:22 am

This Set off More Avs TR/Dropper.GEN is for your Output

Szoki333 - May 19, 2011, 12:12 pm

Not working anymore...

Now I cant bypass Avira.. -.-"

I will try to do obfuscator (or WTF :D)...

jBarrel - May 19, 2011, 3:10 pm

just change it to another assembly, the hijackthis assembly is mapped as infected by 1 year lol

sorry for my poor english

.Astro - May 19, 2011, 3:57 pm

You can try to use the OTL assembly instead.

?ystem - May 20, 2011, 7:18 am

Although, changing your file assembly to that of a well-known legitimate application does work, it sincerely isn't the an effective and suggested method for bypassing any anti-virus detection. I'm not insulting your tutorial, so please don't get that thought from this.

Lets say in the situation of if you're deciding to spread your malware through BitTorrenting by having binded your malware to a key generator/patch. Typically people will find themselves placing their mouse cursor over the file, thus revealing the file assembly. It would seem rather odd for the file from Lz0, FFF, or whomever, to have that strange assembly, thus provoking them to check up on the file by submitting it to VirusTotal, or another popular online multi anti-virus scanner, etc.

As mentioned by a few different people already, it's not only best, but also suggested for you to use an undetected RunPE. There have been numerous threads created in regards to this topic. The best detailed one probably being pr3fix's. He provides images and well detailed descriptions for obfuscating strings and encrypting API calls. [Here](#) it is.

Thank you for the tutorial regardless. It gives evidence to support the question of whether this method still works or not, considering how it had worked for you in the long run.

Raaz - May 20, 2011, 7:22 am

I hope this help's me to bypass the holy avira.

hshoo - May 20, 2011, 12:43 pm

Is there any way to know exactly which line in the source code ,being checked buy the AV so it get detected ?

Lemon ? - May 20, 2011, 5:03 pm

Yes, filesplitting and scanning for detections.

Banks? - May 20, 2011, 5:17 pm

Or commenting out the source except for one function, and scanning it to see if it's the one that is detected, and if it is, change the strings or recode it.

RussianFederation - May 20, 2011, 5:24 pm

Great tutorial, thanks alot mate.

DarkKoopa - May 21, 2011, 2:37 am

Does anybody know some alternatives to the EOF method that avira picks always up as Dropper?

Expox - June 11, 2011, 2:38 pm

Thanks for the share man !

H44Process - October 4, 2011, 5:15 pm

So Funny ? So cool , really like it , work !!

Rock ON

BreastMilk - October 4, 2011, 9:47 pm

(Oct 4, 2011 05:15 PM)H44Process Wrote: [\[CITE\]](#) So Funny ? So cool , really like it , work !!

Rock ONNo, It doesn't work. And not to mention how skiddy this is. Leave the thread to die piece fully, Not Grave dig it.