

Forum:[Hack Forums](#)

Thread: [\[tut\]keep file FUD WITHOUT crypter \[tut\]](#)

jay1994 - November 2, 2014, 8:01 am

hey everyone, i havent been here for a while and looking back on this tut-ish post i made i realized someone said it should be posted here, so i will be doing that right now.

each of these methods ARE NOT my own, i just found them and used them together to make my rat scantime/runtime FUD and thought that this would be better than buying crypter all the time, so i hope you guys enjoy!!!

requirements:

winrar

file splitter/joiner

hex editor

and a file to make fud

i just googled for a free file splitter/joiner and i use hxd portable as my hex editor

to start, we want to make the file runtime fud using hex editing, i used this tutorial to learn:

<http://www.youtube.com/watch?v=34JuwNg9ECU>

once this file is created, we then need to make it scantime fud, which i figured out how to do using this tutroial:

<http://gapsecurities.blogspot.com/2013/0...ypter.html>

(in the tut the person who made it complains about hex editing, but the hex editing itself isnt scantime fud, so this still applies)

if anyone for any reason needs help or clarification, ive already done this and tested it so if you need help either pm me or add me on skype: jay4901

i know this isnt a good tutorial, more of just sharing information but i think this can help alot of people out!

BY THE WAY: with the hex editing, its said to work on anything, but i am a bit sceptical, so test the file after you use the hex method just to make sure its working properly! (it basically works on everything!)

original post: <https://hackforums.net/showthread.php?tid=4222320>

the first time i did this people were asking if id do it for them, if you want me to make your file fud using these methods pm me, or add me on skype. hope this helps people here

BTW: i will be asking roughly .03 (10 usd) of btc if you have me do it for you. not because i'm an ass but because its very simple to do this yourself.

hexm4ster - November 2, 2014, 9:00 am

Nice, i respect the part of you doing your own thing. If you write your own code, it makes it auto FUD until an AV vendor mines it off some end users system and profiles it. The FUD obsession here tells me that hardly anyone actually codes anything.

jay1994 - November 2, 2014, 9:42 am

(Nov 2, 2014 10:00 AM)hexm4ster Wrote: [\[CITE\]](#) Nice, i respect the part of you doing your own thing. If you write your own code, it makes it auto FUD until an AV vendor mines it off some end users system and profiles it. The FUD obsession here tells me that hardly anyone actually codes anything.

yes i agree, and i code but im strong in python, and writing a crypter is insanely annoying if your not using c/c++ or vb, so i figured id share the method ive used :)

(Nov 2, 2014 10:00 AM)hexm4ster Wrote: [\[CITE\]](#) Nice, i respect the part of you doing your own thing. If you write your own code, it makes it auto FUD until an AV vendor mines it off some end users system and profiles it. The FUD obsession here tells me that hardly anyone actually codes anything.

yes i agree, and i code but im strong in python, and writing a crypter is insanely annoying if your not using c/c++ or vb, so i figured id share the method ive used :)

Zero_Luffy - November 2, 2014, 2:41 pm

Well python is really strong, have you heard about MSF ENCODER In metasploit ?

jay1994 - November 2, 2014, 6:51 pm

(Nov 2, 2014 03:41 PM)Zero_Luffy Wrote: [\[CITE\]](#) Well python is really strong, have you heard about MSF ENCODER In metasploit ?

I have not, care to elaborate? I haven't messed with metasploit too much yet

hexm4ster - November 3, 2014, 8:40 am

It provides the ability to generate polymorphic instances of any executable you may have lying around, and can make payloads so many different ways you wouldn't believe it. Once again I wonder, because that was big seriously like 6 or 7 years ago now, at least 5 I know.

jay1994 - November 3, 2014, 9:00 am

(Nov 3, 2014 09:40 AM)hexm4ster Wrote: [\[CITE\]](#) It provides the ability to generate polymorphic instances of any executable you may have lying around, and can make payloads so many different ways you wouldn't believe it. Once again I wonder, because that was big seriously like 6 or 7 years ago now, at least 5 I know.

interesting, so its like a polymorphic engine? it takes your executable and gives it the ability to use polymorphism?

hexm4ster - November 3, 2014, 10:40 am

I haven't played with it extensively but essentially it should handle the problem of FUD in at least scan time situations. It's like this, you can take a binary and generate copy after copy of it that are all different. I'm not sure how it would hold up to these crypters floating around here but I'm sure it would be an interesting tool for you to play with. If I remember right the MSF encoder is mostly about shellcode and the polymorphism might be found elsewhere in the metasploit framework, but it's there so look into it if you're interested.

Uiqueblhats - November 5, 2014, 6:29 am

Thanks man I might wana check it. Thanks though

P1R4T3 - November 5, 2014, 7:37 am

Bookmarking this for later, thanks for the share!

jay1994 - November 5, 2014, 7:51 am

thanks for the replies, ill hopefully be posting more threads like this soon! and good luck! :)

W00dL3cs - November 5, 2014, 7:52 am

(Nov 2, 2014 10:00 AM)hexm4ster Wrote: [\[CITE\]](#) Nice, i respect the part of you doing your own thing. If you write your own code, it makes it auto FUD until an AV vendor mines it off some end users system and profiles it. The FUD obsession here tells me that hardly anyone actually codes anything.

BIG UP FOR THIS.

I've written a keylogger from scratch 4 years ago, and still it's completely FUD nowadays, just because I have used it for personal purposes, and the code is not available publicly.

Btw back on topic, I really like the tutorial: I'm curious to know more about.

In particular way, which sections of the PE are edited.. and most important, why it's possible to achieve such a kind of result with just these "simple steps" (wondering about a possible automation etc)

jay1994 - November 5, 2014, 8:00 am

(Nov 5, 2014 08:52 AM)W00dL3cs Wrote: [\[CITE\]](#) BIG UP FOR THIS.

I've written a keylogger from scratch 4 years ago, and still it's completely FUD nowadays, just because I have used it for personal purposes, and the code is not available publicly.

Btw back on topic, I really like the tutorial: I'm curious to know more about.

In particular way, which sections of the PE are edited.. and most important, why it's possible to achieve such a kind of result with just these "simple steps" (wondering about a possible automation etc)

automation would actually be somewhat easy, for rats like darkcomet etc. i just need to make a program that reads hex and finds the hex value getting detected and switch it. but with the winrar i'm not too sure how i'd automate that.

but yes, hexm4ster is correct and if you need additional info just message via skype or pm me :D

Fizure - November 5, 2014, 9:45 am

MM very interesting the info that you are sharing here very usefull btw...

ArtMachine - November 5, 2014, 9:48 am

Thanks for the method, I might try this.

basha - November 5, 2014, 11:56 am

im gonna check and wanted to know if any problem occurs so u here for troubleshooting also?

jay1994 - November 5, 2014, 12:06 pm

(Nov 5, 2014 12:56 PM)basha Wrote: [\[CITE\]](#) im gonna check and wanted to know if any problem occurs so u here for troubleshooting also?

Well I can help if you have an issue, you just need to tell me what said issue is :)

jay1994 - September 14, 2016, 11:02 am

updated links!

updated hex tutorial:

<http://anonyd38.blogspot.com/2012/10/make-file-fud-using-hex-editing-tut.html>

updated winrar tutorial:

<https://www.youtube.com/watch?v=RJUAsh3iC-U>

kpown - September 14, 2016, 11:59 am

OP check out veil evasion payloads. Good post!

jay1994 - September 14, 2016, 1:17 pm

(Sep 14, 2016 11:59 AM)kpown Wrote: [\[CITE\]](#) OP check out veil evasion payloads. Good post! I shall and thank you! :)

O?tis - September 15, 2016, 3:23 am

(Sep 14, 2016 11:59 AM)kpown Wrote: [\[CITE\]](#) OP check out veil evasion payloads. Good post! Aren't they kind of detected nowadays? At least for me...

yaropolk - September 15, 2016, 5:51 am

If you write your own code, it makes it auto FUD until an AV vendor mines it off some end users system and profiles it. The FUD obsession here tells me that hardly anyone actually codes anything.

kpown - September 15, 2016, 5:58 am

(Sep 15, 2016 03:23 AM)TheDoctor541 Wrote: [\[CITE\]](#) Aren't they kind of detected nowadays? At least for me...

Most are, however I've bypassed industry level AVs such as Sophos endpoint security with the c payloads and the python payloads have been still FUD 1-0/35 and bypass ESET with ease.

I've recently heard about two nice sounding alternatives to veil: thefatrat and unicorn. Will be checking these out in the next few days.

DopplerAF - September 15, 2016, 6:42 am

OP as far as the Hex editing method is conserved it will completely break the file and the file will not be functional anymore...

Already tried that method in DC server few years ago and it totally break the file making it useless.