

Forum:[Hack Forums](#)

Thread: [\[TuT\] Make virus undetectable by HEXeditor\[TuT\]](#)

Arês™ - November 5, 2009, 3:31 am

Many people asking how to hexedit, I decided to write this little tutorial. I will try to explain how to hexedit your favourite Trojan in order to make it undetected by certain antivirus programs. I will try to put this as simple as possible so everyone understands it.

Content:

1. General info about hexediting .
2. What tools you need to get started.
3. How to hex.

-step 1

-step 2

-step 3

1. General info about hexediting?

If you want to make your server undetectable, you need to know how AVs work and how they detect your files, right? There are a few ways that AVs use to detect your server heuristics, sandboxing, etc., and one of them is using so called "definition files" that carry information about strings inside your server. Well, that's the way we are going again in this tutorial because hexing is pretty much useless for other methods of detection. So when AVs scan your files it searches for specific strings on specific parts in your server, and if strings match with strings in the AV database, your file is detected.

Let us say that detected strings are "XX" so we need to change that string to something else (e.g. "XY", "YY") that isn't in the AV definition database so the file can not be matched with any of the AV definitions and that way the file will be undetectable.

There are going to be a few tagged strings in your server - not only one, depending on what trojan you are using and how popular is. Less popular trojans tend to have less tagged parts, and with that they are easier to make it undetectable.

First of all, hexing is not the best method for undetecting files because AVs can change old tagged parts, and once your AV is updated, new definition files are downloaded and your once undetected server might become detected again. Also not all AVs use the same tagged parts - this way you need to hex your server against more AVs to make it fully undetected. This can be annoying because you need to download wanted AVs then hex it your server, then download another etc., etc. Sometimes AVs tag critical parts of the server, and if that part is altered will corrupt the server. Also, heavily edited servers can become unstable, some functions might not work, or even you can corrupt your server and make it useless.

That's why you need to check your server if it's still working after every single change you made while hexing it.

Now how to find detected strings in your server?

There are few ways you can do this: Manually cut your server in half adding parts to one half and scanning it until you find the detected string (which is slow and time consuming); use file splitters to split your server into bytes, and after that scan all split files and find out what byte is detected then alter it in original exe, or you can use an offset AV .

2. What tools we need.

- Unpacked trojan server. (That's your virus)

- Hex editor > [DOWNLOAD](#)
- File Splitter > [DOWNLOAD](#)

- AV-antivirus

3. How to hex:

Now to help you simplify the method I put this video clip TuT how can u make virus undetectable by AV , Whatch it >

[Whatch it here](#)

And please don't be annoying and pessimistic these is my first TuT enjoy?

mister.o - November 5, 2009, 3:38 am

OK is everything good tut but with that red font my eyes ?

FreestylI3R - November 5, 2009, 3:39 am

Thx for sharing very nice tut man ,

Arês™ - November 5, 2009, 3:43 am

(Nov 5, 2009 04:38 AM)mister.o Wrote: [\[CITE\]](#) OK is everything good tut but with that red font my eyes ?

tanx.. i change color a little bit to be more different , cool or some ?

(Nov 5, 2009 04:39 AM)FreestylI3R Wrote: [\[CITE\]](#) Thx for sharing very nice tut man ,
No problem ?

Michael Jackson - November 5, 2009, 3:53 am

nice i will check it ;)

gifar_ucuL - November 5, 2009, 5:49 am

wowwowow nice tut dude hihihih thx its cool

Arês™ - November 5, 2009, 5:55 am

(Nov 5, 2009 06:49 AM)gifar_ucuL Wrote: [\[CITE\]](#) wowwowow nice tut dude hihihih thx its cool
tanx man....?

flAmingw0rm - November 5, 2009, 5:56 am

Great tutorial, but you should posted this in tutorials forums. Good job anyway. :)

z1lla - November 5, 2009, 5:57 am

well,iam having a prob

my stub is detected so splitted it to 10pecies but non of those pecies r detected but when i reassemble it it get deleted by my kasper:(

so i cant like narow it dawn to one peice

Arês™ - November 5, 2009, 6:03 am

you must have option in your AV that can only scan the file but not delete file , i am not using Kasper Av so I don't know but i will post link of multi-AV here, so you can scan your file with 5 or more different AV s ...

Badhakz9T - November 5, 2009, 6:03 am

Nice TUT....i was searching for it...

Gizmo - November 5, 2009, 6:11 am

Thanks for this tutorial :)

Arês™ - November 5, 2009, 6:26 am

tanx for support guys

MooseHide - November 5, 2009, 6:33 am

I know this one But nice work with the tut dude

Arês™ - November 5, 2009, 6:39 am

(Nov 5, 2009 07:33 AM)??•D4rk357™© . Wrote: [\[CITE\]](#) I know this one But nice work with the tut dude

I apprishiate that ...

Riverthief - November 5, 2009, 6:48 am

http://globalhackers.blogspot.com/2008_08_13_archive.html

http://cracktohack.blogspot.com/2008_05_01_archive.html

Credits. Nao.

Valour - November 5, 2009, 7:53 am

yea thnxxx now we will not need to buy those 20\$ crypters to just make our files FUD

:P

thnxx

catlover - November 5, 2009, 7:56 am

thanks for sharing dude

TheInvader - November 5, 2009, 8:26 am

Great post nice tutorial.

Arês™ - November 5, 2009, 9:04 am

no problemo ... tanx for supports guys

NHILL - November 7, 2009, 3:09 pm

thanks man , but can i use it with turkojan to crypte server? and dll server ?

can u make tuto for crypting turkojan server with hexa? lol people waiting for this tuto

THANKS

Arês™ - November 7, 2009, 6:19 pm

you can try to use on turkojan, i did not try but i will check i it...

TuViciouz - November 7, 2009, 10:22 pm

It's an effective method when making a file ud manually but it can EASILY corrupt your file and doesn't work for a lot of antiviruses.

DefaceYoSite - November 7, 2009, 11:43 pm

Pictures would be nice .

Arês™ - November 8, 2009, 2:18 am

(Nov 8, 2009 12:43 AM)DefaceYoSite Wrote: [\[CITE\]](#) Pictures would be nice .
why you need picture when you have video

?Shots? - November 8, 2009, 4:18 am

(Nov 7, 2009 11:22 PM)calvinnxd Wrote: [\[CITE\]](#) It's an effective method when making a file ud manually but it can EASILY corrupt your file and doesn't work for a lot of antiviruses.

Arês™ - November 8, 2009, 6:51 am

just test that file , for me its ok

CrAzI_CaNaDiAn - January 4, 2010, 5:48 pm

hey riddick im wondering if it works for Bots from Host booters, im trying Metus Delphi atm ill let you know how it goes great tutorial. Also what are other ways that AV`s detect it besides this and are there tutorials for that too. And finally one last question. When you FUD this its runtime FUD also or no

Arês™ - January 5, 2010, 7:28 am

yes it works for any virus... don't know try to search man and find other TuTs , and no its just runtime..

V1P3R - May 26, 2010, 6:41 am

why removed the hex editor?:(
can any 1 send me the installer at xxdarkossxx@hotmail.com by email? plz D:
thank you very much =)

Itzah - September 22, 2010, 9:19 pm

Good TuT keep up the work.

Arês™ - September 23, 2010, 3:37 am

thank you mate i forgot that i make this TuT ;) it's really old thread .

pinoy - September 23, 2010, 7:17 am

hex editor download link is not working anymore. can anyone share it?

Haydn - September 23, 2010, 7:57 am

very nice and an informative tutorial, keep it up ! :)

ThE-iNFILTrATOr - September 23, 2010, 8:17 am

Nice tutorial thanks, expect that red colour. I highlighted the page then read it.

H@cker - September 23, 2010, 8:18 am

i like when idiots say "nice tutorial it works" and they even dont know that this is from 2009 and it stopped work long time ago , spammer fuck off...

133720 - September 23, 2010, 8:31 am

Oh! thanks for sharing knowledge

virusinsystem32 - October 26, 2010, 11:08 pm

Very good TUT BRo...

But the red front is not cool...

arnolddrita - October 27, 2010, 1:50 am

Great tutorial bro!

One question: Does this work for all antiviruses?

Arês™ - October 27, 2010, 4:19 am

Don't know now, i didn't test that a long time.

Sir SkinowZ - October 28, 2010, 6:08 pm

Good tut man

You are the best ?

naturalmuffin - October 28, 2010, 6:30 pm

(Nov 5, 2009 04:31 AM)Arês™ Wrote: [\[CITE\]](#) Many people asking how to hexedit, I decided to write this little tutorial. I will try to explain how to hexedit your favourite Trojan in order to make it undetected by certain antivirus programs. I will try to put this as simple as possible so everyone understands it.

Content:

1. General info about hexediting .
2. What tools you need to get started.
3. How to hex.

-step 1

-step 2

-step 3

1. General info about hexediting?

If you want to make your server undetectable, you need to know how AVs work and how they detect your files, right? There are a few ways that AVs use to detect your server heuristics, sandboxing, etc., and one of them is using so called "definition files" that carry information about strings inside your server. Well, that's the way we are going again in this tutorial because hexing is pretty much useless for other methods of detection. So when AVs scan your files it searches for specific strings on specific parts in your server, and if strings match with strings in the AV database, your file is detected.

Let us say that detected strings are "XX" so we need to change that string to something else (e.g. "XY", "YY") that isn't in the AV definition database so the file can not be matched with any of the AV definitions and that way the file will be undetectable.

There are going to be a few tagged strings in your server - not only one, depending on what trojan you are using and how popular is. Less popular trojans tend to have less tagged parts, and with that they are easier to make it undetectable.

First of all, hexing is not the best method for undetecting files because AVs can change old tagged parts, and once your AV is updated, new definition files are downloaded and your once undetected server might become detected again. Also not all AVs use the same tagged parts - this way you need to hex your server against more AVs to make it fully undetected. This can be annoying because you need to download wanted AVs then hex it your server, then download another etc., etc. Sometimes AVs tag critical parts of the server, and if that part is altered will corrupt the server. Also, heavily edited servers can become unstable, some functions might not work, or even you can corrupt your server and make it useless.

That's why you need to check your server if it's still working after every single change you made while hexing it.

Now how to find detected strings in your server?

There are few ways you can do this: Manually cut your server in half adding parts to one half and scanning it until you find the detected string (which is slow and time consuming); use file splitters to split your server into

bytes, and after that scan all split files and find out what byte is detected then alter it in original exe, or you can use an offset AV .

2. What tools we need.

- Unpacked trojan server. (That's your virus)

- Hex editor > [DOWNLOAD](#)

- File Splitter > [DOWNLOAD](#)

- AV-antivirus

3. How to hex:

Now to make more simple i add these video TuT how can u make virus undetectable by AV , Whatch it >

[Whatch it here](#)

And please don't be annoying and pessimistic these is my first TuT enjoy?
WOW I NEVER KNEW U COULD DOT HIS WIT HEX EDITOR

eXeSoul™ - November 4, 2010, 11:22 pm

Nice info :-)

easy to understand.!

dwarf - November 5, 2010, 9:14 am

does this method still work?

b3w4r3 - November 5, 2010, 10:31 am

gonna use it, for my keylogger :D

Akash - November 5, 2010, 10:35 am

I will try, hope i wont corrupt my server

Golliath808 - November 12, 2010, 1:08 pm

This is a RUNTIME or SCANTIME UD method??

My Life - November 12, 2010, 1:12 pm

Nice share mate .

Goanna try it out but I am sure it will work.

GI-jo3 - November 12, 2010, 7:25 pm

a nice tut you got there i will try it out tomorrow

orionstar - November 12, 2010, 7:33 pm

Thanx for posting this TuT I'm about to try it this weekend, my server is FUD except a stupid Avira generic I can't get rid of... I removed all API calls in the stub which made it undetectable by Avira and passed with flying colors but once I crypted the actual server it flags Avira. Already tried ResHack changing file properties and icon database, hexing it is my last resort and this is something I've been looking for, thanks again!

Arês™ - November 13, 2010, 6:37 am

Glad to help you guys .Enjoy

ak007t - November 20, 2010, 7:01 am

nice tut man keep it up.?

Shu luvs DOnutS - November 20, 2010, 7:06 am

is this technique really working because you erase some bits of your program ?

JailMaster - November 20, 2010, 7:17 am

Awsome tutorial. I think you can hex edit folders to turn it into a text file? xD

IGotHacks - November 20, 2010, 8:09 am

Really nice tutorial good to understand

Just saw your video nicely made but no HD ? even if i put it on 480p i cant really see things well enough doenload camasia studio or smth like that

if insplit the server the virus scanner doesnt even detct a virus anymore

Pulse? - November 20, 2010, 10:09 am

You've probably wanted to use red font to make it noticable. But something better is yellow color and skinny font. ?

Do0ks - December 11, 2010, 7:29 pm

Thanks man, I don't know much about making servers UD, But i really want to learn and this seems like a hell of a grate start.

Thanks a bunch, Great tut!

Ovchik - December 11, 2010, 8:02 pm

Just wondering if this method will work on Cybergate? Will the server file be FUD?

??h™ - December 11, 2010, 8:11 pm

This is cool! I'll have to try this. ?

seskanda - January 4, 2011, 10:11 pm

Well, at least i learned how AVs detect viruses

taokrk - April 25, 2011, 1:49 pm

this is so great tutorial,nice mate! regards (:

d3d0h - April 28, 2011, 12:31 pm

Does this still work? can anyone give the hex editor he is using?

11blabla - April 28, 2011, 12:34 pm

nice tutorial. trying right now. thank you so much

denominator13 - April 28, 2011, 2:49 pm

Excellent tut but the vid could do with being a little clearer maybe in HD?

Stoneman420 - July 24, 2011, 8:04 pm

I've seen it posted by a few people but there was no clear answer yet as to why this happens. When I split the file, none of them come back as detectable, how can this be resolved?

CaLLMeHZoMM - July 24, 2011, 8:48 pm

Thanks for this awesome share! Take care :)

eddieboo - January 9, 2012, 8:12 pm

I am trying to make ArdameX file which is 1.1M FUD with hexeditor, I have split the files and make them as small as I can, i even change the value and after that I tried to add the file to gmail or yahoo and it works, both client unable to detect the virus but somehow my value changes is destroying the file itself as the file doesn't work after that when I combine them back.

Is there a calculation for how to split the file? i mean what size of the split value we need to use to detect the smallest file to change the value?

Please help me fix the issue..

Thanks in advance....

starglitz - January 20, 2012, 6:55 pm

Great tutorial :D i started to learn .. Thanks for sharing. :)

Arês™ - February 22, 2012, 10:39 am

Thank you guys for your support ,I appreciate it . I update TuT a little bit :)

Hyptonix - February 22, 2012, 11:51 pm

Not bad, should add a couple pictures to clear up some issues for people.

ironangel - February 23, 2012, 4:00 am

Thanks man, nice job.

Keep up the good work.

Vlad1k - February 23, 2012, 4:03 am

Nice tutorial, but my stupid-ass didn't get a single part of it. o_O

Arês™ - February 23, 2012, 5:22 am

(Feb 23, 2012 12:51 AM)Hyptonix Wrote: [\[CITE\]](#) Not bad, should add a couple pictures to clear up some issues for people.

Maybe mate but they have video i think that's better way to understand it :)

(Feb 23, 2012 05:03 AM)Vlad1k Wrote: [\[CITE\]](#) Nice tutorial, but my stupid-ass didn't get a single part of it. o_O

Thank you , just watch video mate and you will understand better :)

Taleos - February 23, 2012, 5:41 am

Yes good tutorial , i test this virus tomorrow ;)

Arês™ - February 23, 2012, 5:51 am

It is an old method mate but it is simple and good :)

Appliance Warehouse - February 23, 2012, 3:58 pm

Looks nice. i wonder if I have to crypt then edit stub, or if it will work straight off of server?

Arês™ - February 23, 2012, 4:17 pm

No need for crypting if you use this method mate .

Anthony.gov - February 23, 2012, 8:59 pm

Wow if this works AWESOME!

Do not feel like trying to at the moment. ?

- Anthony.gov

ryck - February 23, 2012, 9:11 pm

Nice one man, i will try that out soon!

Thanks for sharing!

uglykidjoes - February 23, 2012, 10:29 pm

Goonna bookmark this for later good tut op

Blietzer - February 23, 2012, 11:44 pm

I tried this, and my server keeps getting corrupted does anyone know what I'm doing wrong?

- tried file splitting twice
- hex edited first bit (made it undetectable but also corrupted)
- combined split files

This is on DC5 rat btw

(Apr 28, 2011 12:31 PM)d3d0h Wrote: [\[CITE\]](#) Does this still work? can anyone give the hex editor he is using?

The one in the video is old, but the one he gave in the download link is called "Hex workshop" any hex editor should do though.

venkat46 - February 24, 2012, 5:34 am

thanks for your post man.. iam now gain knowledge about vires undetection ...?

stylo_asif - February 24, 2012, 8:04 am

It make corrupted Also My Server Not Work 4 me

Infinity. - February 24, 2012, 9:22 am

This is kind of cool ..i've modified 1 like this but never thought that it will be able to make a file undetectable

Thanks for the tut..

Arês™ - February 24, 2012, 9:35 am

Guys , You must understand that this method worked in the old: keyloggers, RAT, Stealers ... it does work on some new but I do not know exactly which one. This is the best way to understand how AV works and how AV detect the virus, in the future you can encode your crypter or something similar.

You may be able to reduce detection by AV for new : RAT, Keylogger, Stealer but not to make it FUD !

Thank you for support guys, I appreciate it :)

Blietzer - February 24, 2012, 11:05 am

Thanks for posting back Ares, what kind of virus/trojan do you use? I want to try it on a working server.

Arês™ - February 24, 2012, 11:09 am

I have used many different trojans, with Turkotrojan this method was working but now i am using

Dark Comet and i don't think this method will FUD DC server.exe !

Blietzer - *February 24, 2012, 11:24 am*

Yeah the dark comet servers get corrupted in the process of being FUD

Arês™ - *February 24, 2012, 11:27 am*

Yes mate, i am using Sikindar crypter and can't make it FUD it always corrupt my server.exe