

Forum:[Hack Forums](#)

Thread: [\[MUST SEE\] The simplest way to check if a file is infected/binded or backdoored](#)

SaTan-INK - October 29, 2014, 9:07 am

The simplest way to check if a file is infected/binded or backdoored

Hello guys , tired and bored to read bullshits and false information about possible binded , infected or backdoored softwares by people who even don' download and check files by themselves , i decide to post this guide or these tips and tricks about a simple way to check if a file is clean or not ... read it , it will for sure help you in the future

Let's now start this quick guide ...

First of all we will need to go on your windows control panel in the folder option :

we will need to do some important changes here , so go to the second tabs and check the number 1 : " show the hidden files" , this option will be very impoortant if the file is binded , with that option enable you will be able to see all the hidden file , so the binded files (if the file is binded of course)

then be sure to UNCHECK the number 2 : " hide the known extension "

do the same as the image below :

ok , now we will need a very important software (MUST HAVE) called Sandboxie , a sandbox is a software who will allow you to run a file in a safe environnment , that means if that file is infected ,it will not infect your whole system but will stay in that sandboxed envionment , close the sandbox and the server.exe will immediately stop to work =)

Download sandboxie from the official website and install it :

<http://www.sandboxie.com/SandboxieInstall.exe>

For this tutorial i will test and analyse the next software i will share with you , a very good stealer named Black stealer v3.1 Ninja edition

to check a file with sandboxie ,simply go on the file , right click then "run sandboxed" or " run in sandbox " , a windows will appears with all the running files , if evrything is good YOU MUST ONLY SEE THE FILE YOU ARE TESTING , IF ANY OTHER THING APPEARS THAT MEANS SOMETHING IS BINDED WITH , so let's see what sandboxie show us with Black Stealer v3.1 Ninja edition :

As the image shows ,there is nothing running except the Black stealer builder so we can say that the file IS NOT BINDED !

everybody here (and on any others hacker's forums) only trust the multi antivirus scan like virus total , razor and some others , THIS IS A TOTAL MISTAKE , because we are all using some cypters to BYPASS the antivirus scans , so as i always say the virus scans are 100% USELESS and improves NOTHING !!! Of course if i crypt my file and scan it , the result will be 0/60 and people will trust me ^^

IMPORTANT TIP :

when you want to be sure the scanned file is the sme than the file to download , check the MD5 and/or the SHA1 hashes , they are some unfakable identification of the file , if they are the same , you will be sure that the files are also the same , we can fake a md5 hash !!!!!!!

To check this hash , right click on the file to check , then "properties" , then "hashes "like the picture (still with black stealer ninja edition) :

with these hashes you will be able if the scans the OP have povidе are fake or not ...

in our exemple still with Black stealer 3.1 :

[img]<http://viruscheckmate.com/image/10Rx4woHjVxs/full/img.png>[/img]

Check if the file size and the MD5 and sha1 hashes are the same to be sure the virus scan is legit , and as you can see everything is the same here

At this time, we can say this stealer builder is not binded with any other file (the sandbox show us nothing was running excepting the builder itself) and we check if the hashes were the good ones, so we can basically say with no mistake that the file seems really clean !!!

Don't be idiots and forget these shitty virus scans , if you want to really check a file there are some good scanners , impossible to fake :

-<http://malwr.com>

-<http://anubis.iseclab.org/>

-<http://www.threatexpert.com>

lets' now check that stealer on malwr.com , a powerfull scanner with an online sandbox , this scan will show us if any IP/Host/DNS is outting from the file , so let's start a scan

so the scan is now finished and available here :

<https://malwr.com/analysis/NmNkM2RkZTRIY2JINGMxZTkWmmU1NjhlYWRkMzAxZml/>

as we saw earlier in this tutorial, always check the MD5 and sha1 hashes to see if they are the same !!! (you can see they are)

the scan shows us another important thing , it shows us that no IP or Host or DNS are outting from the stealer so we can be now absolutely sure that this file is 100% Clean

Thanks you all to read and follow my tutorial as i am french , english is quite difficult for technicals details , if you have any question or need any added help , feel free to shoot me a PM , i will help you as soon as possible

Best regards

?

jasperav - October 29, 2014, 9:51 am

nice great tut :) except make soms headers so it is more easy to read and a table of contents? hope to see more of you!

mxzh - October 29, 2014, 10:01 am

Looks helpful, thanks. Screenshots might've been better if they were in english.

SaTan-INK - October 29, 2014, 11:58 am

(Oct 29, 2014 09:51 AM)jasperav Wrote: [\[CITE\]](#) nice great tut :) except make soms headers so it is more easy to read and a table of contents? hope to see more of you!

yes sir , you are right i willthink about that in the future and yes i will make some more tutorials from beginners to advanced members

don't be worry about negrep , i know people on HF do not like when the truth is said ;)

(Oct 29, 2014 10:01 AM)mxzh Wrote: [\[CITE\]](#) Looks helpful, thanks. Screenshots might've been better if they were in english.

sure sir but as my windows is in french all my system is in french i will try to edit with english language =)

btw thanks for your positive feedback about my first tutorial on hackforums , i you have any question about it , don't hesitate to PM me =)