

Forum:[Hack Forums](#)

Thread: [\[Must See \]HOW TO DETECT A BACKDOOR ON A TOOL \[simple \]](#)

T3eS 2 - March 13, 2011, 1:03 am

H!!

I am back again..

I want to share this with HF members..

How to detect a backdoor on a tool <EXCLUSIVE for HF>

FIRST METHOD:

Right click it, if you got winrar installed and you see "open with winrar" then this means it was binded with winrar so def backdoored

SECOND METHOD:

Open it with a resource editor such as resource hacker/restorator/pe explorer and check the rcdata section, if there's 1 & 2 entries in it then it's binded

THIRD METHOD:

Open it with a hex editor, at the start of a PE header there's always this line "This program cannot be run in DOS mode", search for it, if it exists more than once then it might be binded. It depends on the specific app, for example it's not unusual for binders/crypters to have the stub file attached in the resources. Also search for .exe and inspect the results, a binded file drops the files to a temp folder before executing them, so if you find something like this: %t.e.m.p%..x.x...e.x.e or file1.exe/file2.exe then it's def binded

FOURTH METHOD:

Run it in sandboxie, when a file is ran'd in sandboxie it's isolated (can't access your files/registry, first click the sandboxie tray icon to open up its Window, then right click the file and click "run with sandboxie" if you see another process name in the sandboxie Window then it's probably backdoored (this doesn't include sandboxie rpcss/dcom launch processes, those are legit and needed for some programs), that's not all, the file may drop another when one of the buttons in the program GUI is clicked or after you close it, so click all the buttons and close it just to make sure, if you do see other processes then immediately click file>terminate all processes from the sandboxie menu, if a file refuses to run in sandboxie or it's supposed to be a program and it runs without GUI then it would probably be best to delete it :::

IF THIS HELPED YOUUU..

DONT FORGET TO LEAVE A REPLY..? ENJOY

SIM-668047 - *March 13, 2011, 1:05 am*

Nice tutorial!

It looks nice!

lemmerule86 - *March 13, 2011, 1:14 am*

good one for fud bakdoors ..thanks

T3eS 2 - *March 13, 2011, 1:16 am*

thanks mate..

replys are accepted ..

-mothered- - *March 13, 2011, 1:36 am*

Nice and simplistic methods mate, which are all known to myself and are very well written.

Thanks.

irrationalByte - *March 13, 2011, 1:39 am*

Thanks For The Share I Was DoubtFull About It! Neat xD

T3eS 2 - *March 13, 2011, 1:42 am*

thanks frnds.... all suggesstions are welcome

GreenLee - *March 13, 2011, 3:37 am*

Thanks bro for all this suggestions :) I will try it rightaway

X Makube - *March 13, 2011, 6:57 am*

about the resource editor >>> resource hacker/restorator/pe explorer...
where did I find the rcdata section?

nice tutorial, Thanks

DeadlyDeath - *March 13, 2011, 7:06 am*

Thanks for the tut mate, very usefull.

validbj - *March 13, 2011, 7:33 am*

thanks a lot very helpfull

kingibi - *March 13, 2011, 7:37 am*

thanks man. this will be helpful

angelotiti - *March 13, 2011, 12:42 pm*

thanks for this but open with winrar doesnt mean its backdored

do_rrr_die - *March 14, 2011, 8:28 am*

Thanks for the helpful tut:)

PHARAOH47 - *March 14, 2011, 2:35 pm*

thank you, i was thinking about this problem for few days and have asked some more experienced friends than i am and they didnt know the answer.

M-88 - March 14, 2011, 3:58 pm

although all of them are known before but it's nice of you to combine them in one single thread .
Thank you

Itzah - March 14, 2011, 6:47 pm

Pretty common and self explanatory. Thanks

Ghost Protocol - March 14, 2011, 6:56 pm

thats awesome bro great!!

Rixxon - March 14, 2011, 11:22 pm

I'll take a closer look at this very soon. Thanks a lot for posting this, will definitely come in handy in the future.

Royal King - March 15, 2011, 3:11 am

Had read this somewhere before. Thanks anyways :)

albert6014 - March 15, 2011, 3:19 am

Yep, basic, but for the noob like me, very informative?

Lightangel - March 15, 2011, 3:34 am

Thanks for the useful information bro, now I think some HF members would be getting less infected.

araf - March 15, 2011, 3:42 am

very basic but good tutorial thanks xD

djmayur - March 15, 2011, 9:18 am

too simple n nice methods...thanx mate....

counterpoint - March 15, 2011, 9:19 am

Great job. Nice and simple - easy to understand.

MultiJocke123 - March 15, 2011, 10:11 am

thanks, very nice tut mate

llllllllllll - March 25, 2011, 9:00 am

nice tut thanks a bunch :)

HappyMan - March 25, 2011, 9:04 am

oh thanks<3(No Homo), I didnt know this :)

T3eS 2 - November 30, 2011, 4:28 am

Bumping this up..

Have it and enjoy. Thanks

CaLLMeHZoMM - November 30, 2011, 4:32 am

i never knew about the first one. Thanks!

DAMESHOT - November 30, 2011, 5:18 am

Thank man! I really needed something like this.

raks - November 30, 2011, 6:45 am

likes ur tut very much..
expect good ones in future

noober1001 - November 30, 2011, 9:40 am

Thanks for this nice tut.
Keep it up.

lechi1980 - November 30, 2011, 10:25 am

Thank you. I just got sandboxie. Gonna start using that to check my files.

MagicMushroom™ - November 30, 2011, 12:08 pm

looks nice...Keep it up! mate ?

\$SUFIS - November 30, 2011, 12:36 pm

excellent tutorial thanks man for this..keep it up!!

Lokeal - November 30, 2011, 1:22 pm

Seen it before but forgot about it, thanks a lot.

-Shadow- - November 30, 2011, 1:59 pm

great tutorial, well and deeply explained.

daehaking - November 30, 2011, 2:10 pm

Very nice tips here ;)
Nice thread bro :D

T3eS 2 - December 1, 2011, 12:50 am

Thanks guys!..

Hope you enjoy these..

T-rom - December 1, 2011, 2:14 am

Dang, I didn't even think of the first two :P

Thank you for this :]

Prince™ - December 1, 2011, 2:18 am

Really a good tutorial on how to detect if a tool is backdoor'ed or not , I'm sure you saved many of our members being infected.

bernardbear - December 1, 2011, 8:46 pm

put some image to make noob understand :D anyway nice posting

Falconite - December 6, 2011, 4:56 am

Thanks For The Share I Was DoubtFull About It! Neat xD

Techie - December 6, 2011, 6:31 am

Useful info !

Bookmarked for future Reference !

NPA - *December 6, 2011, 6:50 am*

thanks for nice share..

it helped me a lot..