

Forum:[Hack Forums](#)

Thread: [How to detect a backdoor on a tool](#)

th3.g4m3_0v3r - September 7, 2009, 1:14 am

Right click on the any suspicious tool and if you have winrar installed and if it shows "open with winrar" then this means it was binded with winrar so that tool is backdoored.

2) open it with a resource editor such as resource hacker/restorator/pe explorer and check the rcdata section,if theres 1 & 2 entries in it then its binded.

3) open it with a hex editor , at the start of a PE header theres always this line "This program cannot be run in DOS mode" , search for it,if it exists more then once then it might be binded
it depends on the specific app,for example its 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 em , so if you find somethin like this: %t.e.m.p%\x.x...e.x.e or file1.exe/file2.exe then its binded.

4) run it in sandboxie ,when a file is executed in sandboxie its isolated (cant 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 its probably backdoored (this doesnt include sandboxie rpcss/dcom launch processes,those are legit and needed for some programs)

[B]iishop - September 7, 2009, 1:24 am

or easier, scan it on novirusthanks.

CyberHacker™ - September 7, 2009, 1:26 am

(Sep 7, 2009 01:24 AM)thizzleboi Wrote: [\[CITE\]](#) or easier, scan it on novirusthanks.

-Mr Mesmer - September 7, 2009, 1:27 am

(Sep 7, 2009 01:24 AM)thizzleboi Wrote: [\[CITE\]](#) or easier, scan it on novirusthanks.

^^^^^^^^^^^^^^^^

Def, a lot more casual

riskier - September 7, 2009, 2:14 am

It's good to have some of this knowledge though.

m4tth3vv - September 7, 2009, 2:17 am

Quote: or easier, scan it on novirusthanks.

Dude, if you honestly believe that I will crypt a trojan and send it to you. Then we'll see how easy it is.

@OP

Wow. You little leech.

<http://www.technohug.net/forum/topics/few-easy-steps-to-detect-a?page=1&commentId=1987837%3AComment%3A109499&x=1#1987837Comment109499>

texasti89 - September 7, 2009, 3:23 am

Mathaeus, thanks for the link!