

Forum:[Hack Forums](#)

Thread: [How To Detect A Backdoored Tool](#)

NinjaEdits - April 19, 2015, 6:30 am

WRITEN BY MY HOMIE ?ClockworkK.

SO DON'T COMMENT ABOUT I STEALED THIS.

1) 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

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

3) open it with a hex editor , at the start of a PE header theirs 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 something like this: %.t.e.m.p.%.x.x...e.x.e or file1.exe/file2.exe then its def binded

4) run it in sandboxie ,when a file is ran'd 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 doesn't include sandboxie rpcss/dcom launch processes,those are legit and needed for some programs) , thats 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 immdiately click file>terminate all processes from the sandboxie menu , if a file refuses to run in sandboxie or its suppose to be a program and it runs without GUI then it would probably be best to delete it

Raz3r - April 19, 2015, 6:33 am

I wouldn't recommend running it sandboxed, most RATs/key loggers have an anti VM or sandboxie setting.

I would highly suggest to use a VM+ Sandboxie.

Odin - April 20, 2015, 9:19 pm

Good tips, and maybe upload it to virustotal, just incase if it is crypted you can make it un fud. Helps out others