

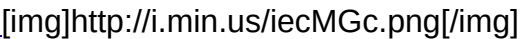
Forum:[Hack Forums](#)

Thread: [\[TuT\] How to check if a file is infected \[TuT\]](#)

Rrrrrrocket boi - January 15, 2011, 9:35 pm

Well I'm not like a professional white hat or anything like that, but I'd just like to share some tips on what I do before I open a suspicious file.

1) Look at the user's post count and join date. If they joined within the last month, then you already have a clue it's probably not legit, but don't prejudge mind you.

Example : Spoiler [\(Click to View\)](#)

Already got deleted from it being infected, but serves as a good example. Join date was in December, and only had 14 posts.

2) Now you're unsure if it is clean or not but you download anyway. Next step is to head to [VirusTotal](#). Upload it there and see if anything is detected. Most of the time, this is where you will realize it is infected. Even if this scan comes up as 0/43, it still could be crypted.

Spoiler [\(Click to View\)](#)

3) If you don't have [sandboxie](#), go get it. It is a tool that allows you to run programs in a sandbox basically, so if it is infected, it won't infect your computer. Run the suspect file in sandboxie and look for anything suspicious. If anything other than the program shows up, e.g. firefox.exe or explorer.exe, then it is infected. Also, if there are still things open after closing the program, it is infected. Examples below

As I open it:

Spoiler [\(Click to View\)](#)

Even after I close it:

Spoiler [\(Click to View\)](#)

4) Always have a reliable anti virus running on your computer, and do regular scans with [MalwareBytes](#) and [SuperAntiSpyware](#). For a reliable anti virus I use [Avira AntiVir](#), but there are many others that are just as good or better, such as [Comodo Firewall](#), which also tells you when something tries to connect to a DNS (so if it could be a RAT). And by regular scans, I mean at least once a month.

If you do believe you are infected, disconnect from the internet, and then run scans with both MalwareBytes and SuperAntiSpyware, and also check your startup to see if it has been injected there. To do this, go to run and type msconfig, then go to the startup tab. If this doesn't cure the infection head to the [White Hat Help Section](#) while in safe mode with networking.

If you are not sure if you are infected, use a packet sniffer such as [Commview](#) or [WireShark](#) and look for any suspicious IPs on your network.

Hopefully this tutorial will reduce the amount of infections here, and reduce the work load on the HJT Team.

wisd0m - January 15, 2011, 9:36 pm

Seems you put effort into this, also I suggest you add comodo firewall in there, it is one of the best Internet ones you can get, and is free ware.

Rrrrrrocket boi - January 15, 2011, 9:37 pm

Done. Thanks for that, I was drawing a blank on some of the good AVs I knew of haha.

bb123 - January 15, 2011, 9:47 pm

good tutorial bro pretty smart.

Impuhsive - January 15, 2011, 9:49 pm

Nice tutorial, really helpful...(you should also include where you can find these programs) Great Job!?

Charity - January 15, 2011, 9:53 pm

I'd also add something about Anubis scans and packet sniffing. Good tutorial for newbies though.

Rrrrrrocket boi - January 15, 2011, 9:55 pm

(Jan 15, 2011 10:53 PM)Charity Wrote: [CITE](#) I'd also add something about Anubis scans and packet sniffing. Good tutorial for newbies though.

The only thing I don't like about packet sniffing is that you are seeing if it is infected after running it which kind of worries me. Anubis scanning is a good idea though. I'll add that in as soon as I figure out how to use it myself lol.

Charity - January 15, 2011, 9:57 pm

I'm pretty sure that you can run programs packet sniffers within Sanboxie, but most (should) do it in a VM to avoid infection any way.

Kill?Muvz - May 26, 2011, 9:59 am

There's an easy method to bypass that. Simple running on SandBoxie is not going to do much. Yet I'm not going to reveal it, but I'm sure many of you know it.

Alphaseek - March 21, 2012, 10:03 am

Thank you for sharing the knowledge with us.

uglykidjoes - March 21, 2012, 11:35 am

I found a virus once by listening to the PC's fan! It was sounding fast even tho PC was idel. So I checked taskmanager and saw a none normal file running so I right click n open file location and then scanned it with online scanner then deleted it as it was a infection. Trusty fans. Good tutorial op