

Forum:[Hack Forums](#)

Thread: [\[TuT\] How to remove Rats,Malware, Adware etc. \[NOOB FRIENDLY\]](#)

Mqñster - December 25, 2013, 6:36 pm

As i have been seeing that a lot of people are having trouble removing rats, malwares, adwares (etc) i thought i would help out a bit, by following these easy steps.

[*] To remove the specific problem, head over to this [link](#) and download the file called "Hijackthis.exe".

Spoiler ([Click to View](#))

[*] Once downloaded right click the .exe file and click on "Run as admin". Now go ahead and click on: "Do a system scan and save the logfiles."

Spoiler ([Click to View](#))

[*] It should now do a system scan, and open a logfile.

Spoiler ([Click to View](#))

Keep the logfile open and COPY + PASTE everything inside the notepad, into the [this](#) "box".

Spoiler ([Click to View](#))

[*] It should now begin to analyze it, and it will tell if there is any file(s) corrupted / infected.

Spoiler ([Click to View](#)) As seen on mine, there is some Spoiler ([Click to View](#))"" Which indicates that the file is not infected nor corrupted, but that it's not a file / program which was originally created by windows 7(Xp,Vista,Windows 8), such as League of legends.

[*] Now if you did find some Spoiler ([Click to View](#))""(S) You wanna go find the corrupted file with the "X", and there it should say where / which folder it's located in.

Spoiler ([Click to View](#))

As seen with mine, it's inside the C:/Program Files (x86)/Gyazo Folder. (THIS IS NOT A VIRUS, THIS IS FOR EDUCATION ONLY. I DO NOT CLAIM THAT GYAZO IS INFECTED / CORRUPTED)

So now where we know where the corrupted / Infected file is located at, go ahead and maximise the hijackthis.exe window.

Spoiler ([Click to View](#))

And scroll around, until you find the exact folder/name as said in on the website, and check the little box in the right corner, and then press "Fix Checked".

Spoiler ([Click to View](#))

SUCCESS! THE CORRUPTED / INFECTED FILE SHOULD NOW BE DELETED / FIXED. ??

Feedback is appreciated. I know my grammar ain't the best and that the thread has a lousy design, but this is one of my first TuTs.

Thanks!

//Mqnster

Gionizer - December 25, 2013, 6:41 pm

Nice tutorial!! ??

And as you already said, your grammer isn't the best, so I'm not going to be picky about it ?

And again, thanks for this man ?

- Gionizer ?

Mqnster - December 25, 2013, 6:46 pm

(Dec 25, 2013 07:41 PM)Gionizer Wrote: [\[CITE\]](#) Nice tutorial!! ??

And as you already said, your grammer isn't the best, so I'm not going to be picky about it ?

And again, thanks for this man ?

- Gionizer ?

Np. Thank you for your feedback, appreciated mutch.

bulby13 - December 25, 2013, 7:18 pm

Although this method may solve your problem, the HiJackThis analyzer may not get Oday or new threats. Also, HiJackThis/OTL is not for the home user, it's for analysis by malware helpers.

I think you're better off using tools like Malwarebytes and AdwCleaner, as you may delete unwanted registry keys and programs by false positives (Scanners have FPs, but not as much).

Although this method works a decent amount of times, I still recommend scanners.

Aura - December 25, 2013, 8:40 pm

Nice tutorial, but as stated above, HijackThis shouldn't be used by standard users that have no idea on how to read the logs and analyze them. Also, HijackThis isn't meant for 64-bits operating system, leaving this tutorial a bit useless as most people here runs 64-bits versions of Windows.

Mqnster - December 26, 2013, 4:27 am

(Dec 25, 2013 09:40 PM)Aur? Wrote: [\[CITE\]](#) Nice tutorial, but as stated above, HijackThis shouldn't be used by standard users that have no idea on how to read the logs and analyze them. Also, HijackThis isn't meant for 64-bits operating system, leaving this tutorial a bit useless as most people here runs 64-bits versions of Windows.

Well my operative system is running with 64bit, and everything is working as intended

(Dec 25, 2013 09:40 PM)Aur? Wrote: [\[CITE\]](#) Nice tutorial, but as stated above, HijackThis shouldn't be used by standard users that have no idea on how to read the logs and analyze them. Also, HijackThis isn't meant for 64-bits operating system, leaving this tutorial a bit useless as most people here runs 64-bits versions of Windows.

My operative system runs with 64bit, and everything is working as intended

executionerhf - December 26, 2013, 6:14 am

Thanks for the tutorial man. I'll definitely try this.

En1gma - December 26, 2013, 6:47 am

Nice tutorial, this should help out a few people. You could add to it that if people can't read logs they should send it to an MRT member.

Ombra - December 26, 2013, 7:26 am

Nice tut to hjt usage :) 'll be useful for other members.

Aura - December 26, 2013, 7:34 am

(Dec 26, 2013 05:27 AM)Mqnster Wrote: [\[CITE\]](#) Well my operative system is running with 64bit, and everything is working as intended

My operative system runs with 64bit, and everything is working as intended
But if HijackThis hit 64-bits items, it will not modify it as its not made to be used on 64-bits systems.
So it will only modify 32-bits items.

Gustav. - December 26, 2013, 8:26 am

HijackThis is incredibly old & outdated on many levels. Even the simplest form of AdWare can bypass their scans- I wouldn't recommend on using it for furture security reasons.