

Forum:[Hack Forums](#)

Thread: [Think you're infected? Read this thread!](#)

Yakz - August 22, 2015, 7:07 pm

This thread is for all the new users in this board, if you have come into contact with this user: "Lanchester" (UID: 2846080) and went on his Teamspeak (and downloaded a plugin) you should immediately scan/check your system and see if you have been infected.

If you think you might be infected in general or wish to know what to do if it ever came to that, this thread is also for you!

Tools used.Regedit

Netstat

msconfig

CCleaner

Comodo

AV software

How can i easily check if i'm infected?

1. Run a scan on your system.
2. Check out a few well known spreading methods (in his case teamspeak) and determine whether or not you fell for it.
3. Look if any files, accounts, .. are missing.
4. If you noticed suspicious things happening such as webcam light, mouse moving, random typing, weird piano sounds or voices, ect..
5. Check your system manually for a suspicious file or connection (explained below)

I actually think i got infected by that person (or other person)!

Don't worry, we are going to get rid of the intruder. First go to Windows start and type in "cmd", command prompt should show up in the list, right click it and select "run as administrator". Command prompt should now open.

Now that cmd prompt is open there's one last thing we should do as preparation to make our life easier.

Close all programs that are connected with the internet (browsers, skype, steam, ect..) You may even go as far as closing all programs that are connected to the internet for updating purposes.

Once you think most is closed you want to open cmd prompt and type in the following..

Code netstat -b

As you can see a list of connections will appear, this will probably not be much since you closed most programs connected to the internet, now it'll be easier to spot the stub.

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

Go through the list and look for a filename that looks odd or that you think you have downloaded recently and shouldn't be having an active connection.

Once you found the program in the list you want remember the name, write down the ip connected to it and immediately pull out your internet cable (closing your internet connection).

Open your AV and run a scan on your system, if a virus comes up, get it removed. When all is removed put in your internet cable and download Comodo, if you already have comodo, restart your computer.

Now when you restart your computer comodo should tell you every incoming and outgoing connection upon starting your computer, if you see any connection that could be from a RAT it means that it was not successfully removed and that the stub is probably either run-time or scan-time crypted. If you don't see anything suspicious and the rat is removed, congrats!

For those who didn't succeed by trying the previous, don't worry you have a few options left, let's go through them.

Remember we wrote down the name of the stub when using netstat earlier? Look for that file on your system and upload it to virustotal, this will result in the stub being detected and the file being removed once you run a new scan, note that it's smart to keep your internet use minimal during the time AV's update and the stub gets detected. (You can find the file by partially following the steps below)

If you're more of a hands on person and don't want to sit around waiting and rather do everything yourself, you can do the following..

Open msconfig and go to the "Startup" tab, you should see the following..

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

Look for a program that looks suspicious by keeping an eye on "startup item" and "manufacturer" if the startup item is a weird name and the manufacturer is unknown it may be a RAT. To be sure keep looking and if nothing else looks out of the ordinary, uncheck all files (if they're checked) and select the suspicious file you spotted earlier and click on "disable all". Make sure you write down the name and location of the suspected stub!

Now go to the "boot" tab and select safe mode.

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

What you do next is run msconfig in safemode, if the rat is persistent it'll still be in the list but it WON'T be running since we are in safemode atm. Now it's just a matter of finding the source.

Make sure you're still in safemode and open "Regedit" (make sure you have "show hidden files and folders" enabled or you won't find it)

If you successfully opened regedit you should be looking at something like this..

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

Remember we also were able to see the file location back in msconfig? Look at the file location again (in msconfig) and navigate to it (in regedit).

The location should somewhat look like this..

Code HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\...

If you navigated to the location correctly you should be seeing this..

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

You should now have spotted the file (you saw in msconfig) in this list. If not look at the location again and make sure it's the correct one.

Now right click on the stub and click modify and you should see this..

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

Now if you're not completely sure if it is indeed the stub, put a ":" or something in front of it to disable it but still have it on your system (in case it's something else).

If you are sure it's the stub, you can completely delete it instead of modifying.

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

To make sure it's gone go back to msconfig and see if it's in the startup list, it should be completely gone now, if not you did something wrong in previous steps and you should go over it again or just following the previous method.

Now for the last step we are going to download CCleaner and scan for issues in our registry. Hit the "registry" tab and click on "scan for issues", you should see something like this..

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

When all is done, hit "Fix selected issues" and you should be done.

Hope this was useful to any of you who dealt with Lanchester or think they're infected or want to know what to do if it ever came to that.

Remember, always stay secure and think twice before blindly opening files.

Peace & much love ?

Kush.

Lipton's Ice Tea™ - August 22, 2015, 7:13 pm

This is really kind and helpful of you Op. If you posted this 10 days ago I wouldn't of reinstalled win10 :(

Yakz - August 22, 2015, 7:18 pm

(Aug 22, 2015 07:13 PM)Sarah Manning Wrote: [\[CITE\]](#) This is really kind and helpful of you Op. If you posted this 10 days ago I wouldn't of reinstalled win10 :(

So sorry that happened to you, good to know for next time ;)

?Syria - August 22, 2015, 10:49 pm

Nice thread op!

This is why never to deal or work with new members.

sirarduin - August 23, 2015, 1:55 am

The best Threads I have read in the last week. HQ post.

Cordially SirArduin

derpcoin90 - August 23, 2015, 3:28 am

Really nice of you to do this, you're a good dutchie :P

Incendiary. - August 23, 2015, 3:33 am

VERY HQ!

I highly recommend you also post this in the White Hat section. Everyday people are complaining that they are infected over there!

Yakz - August 23, 2015, 6:14 am

Thanks for all the feedback everyone!

(Aug 23, 2015 03:33 AM)Incendiary. Wrote: [\[CITE\]](#) VERY HQ!

I highly recommend you also post this in the White Hat section. Everyday people are complaining that they are infected over there!

Good idea.

Christina Perri - August 23, 2015, 6:18 am

This is a great thread in general, its nice of you to help for that specific user/situation but this thread is great in general, you should have it stickied or archived or something :3 Im sure you get what im saying haha

Yakz - August 23, 2015, 6:19 am

(Aug 23, 2015 06:18 AM)Christina Perri Wrote: [\[CITE\]](#) This is a great thread in general, its nice of you to help for that specific user/situation but this thread is great in general, you should have it stickied or archived or something :3 Im sure you get what im saying haha

I'm actually thinking about cleaning it up some more and posting it in the malware removal section.

Thanks for the feedback.

Christina Perri - August 23, 2015, 6:21 am

(Aug 23, 2015 06:19 AM)OG Kush´ Wrote: [\[CITE\]](#) I'm actually thinking about cleaning it up some more and posting it in the malware removal section.

Thanks for the feedback.

I mean its a small guide so i dont really see a need to...but maybe you can number the corresponding steps to the instructions

Gilbo - August 23, 2015, 6:22 am

Nice thread :)

I saw this guy post on a couple of threads trying to help people with rat setup, glad he is out now though.

Yakz - August 23, 2015, 6:37 am

(Aug 23, 2015 06:21 AM)Christina Perri Wrote: [\[CITE\]](#) I mean its a small guide so i dont really see a need to...but maybe you can number the corresponding steps to the instructions

Will see if i can edit this in a few.

(Aug 23, 2015 06:22 AM)wepnet Wrote: [\[CITE\]](#) Nice thread :)

I saw this guy post on a couple of threads trying to help people with rat setup, glad he is out now though.

Thanks bud.

#Skyline - August 23, 2015, 7:44 am

Nice find, glad this will be able to help users resolve there issues with this immature user who thinks infecting HF users is cool, when it's not.

Armada - August 23, 2015, 7:47 am

Users who suspect infection should report to the white hat section immediately

Cheeb - August 23, 2015, 7:49 am

Very nice thread, great job.

Yakz - August 24, 2015, 9:43 am

(Aug 23, 2015 07:47 AM)A?mªĐa Wrote: [\[CITE\]](#) Users who suspect infection should report to the white hat section immediately
What he said ?

(Aug 23, 2015 07:49 AM)Cheeb Wrote: [\[CITE\]](#) Very nice thread, great job.
Thanks for your feedback.

Kush.

Incendiary. - September 28, 2015, 5:55 am

Very helpful thread, i highly recommend that everyone bookmarks thing, just in case.

ToeCrusher - September 28, 2015, 6:39 am

Bookmarked this right away, well written guide covering every aspect of an infection