

# Forum:[Hack Forums](#)

Thread: [\[READ\] \[BHCPU\] Am I Infected?](#)

-Hyperion - December 16, 2014, 8:06 pm

Hey guys, it's -Hyperion :Victoire: I have run my own security company doing Pentesting and malware removal for the past 3 years and I now work for a Fortune 500 company.

I have decided to write this quick guide since there seems to be a lot of confusion over what an actual infection is verses windows messing up. There is also a panic that sets in that needs to be addressed on what you do when actually infected.

If asking for help follow all instructions! You are not clean just because a few scans said so! Please wait for the ok from an expert and read everything carefully!!!

Am I infected?

I could write out a long list on symptoms of infection but Kaspersky has already worded it perfectly which I will share with you.

**Unexpected Crashes:** If you've ever experienced this, you probably already know the hard way that your system crashing or regularly switching to the terrifying blue screen of death is a major red flag that something is very wrong. If it's happening to you now, immediately scan your system for infections.

**Slow System:** If you're not running any resource-heavy applications on your system but it's running slowly anyway, it may be because your system is infected with a virus.

**Excessive Hard Drive Activity:** Similarly, if you notice a lot of hard drive activity even when your computer is idle, this is a warning sign of a potential infection.

**Strange Windows:** If strange windows pop up during the booting process, particularly those that warn you of lost access to various drives on your system, something is wrong.

**Peculiar Messages:** If those troubling dialogue boxes crop up when your system is running alerting you that various programs or files won't open, this is also a bad sign.

**Bad Program Activity:** If your programs go missing, are corrupted, or start to open themselves without your initiation, and/or if you receive notification that a program is attempting to access the Internet without your command, this is a serious warning sign that you are the victim of malware. If you receive notification that a program is attempting to access the Internet without your command, this is a serious warning sign that you are the victim of malware.

**Random Network Activity:** If your router is constantly blinking indicating a high level of network activity when you aren't running any significant programs or accessing high amounts of Internet data, something might be wrong.

**Erratic Email:** If your emails aren't sent, or you hear from your contacts that they're getting strange emails from you that you did not send yourself, this is a strong indication that your system has been compromised (or that your email password has been stolen).

**Blacklisted IP Address:** If you receive notification that your IP address has been blacklisted, consider this about as sure a sign as any that your PC is not in good hands — there's a very good chance it means your system has been compromised and is being used as one tentacle in a far-reaching, spam-sending botnet. I would like to add on to this with blocked websites and having websites redirected to other sites. This can be a sign that the host files have been edited or that a browser hijacker is present.

Unexpected Antivirus Disabling: Many malware programs are designed to disable the antivirus suites that would otherwise eradicate them, so if your antivirus system is suddenly not operating this could be a sign of a much larger problem.

### [Source](#)

You may also wonder what I am infected with or just what do these terms mean? You can read/learn more about the various malware/virus types and variants on [VeraCode's website](#).

The only real way to be sure is to get an in-deep check-up (and by that, I do not mean run to run Malwarebytes and Avira then call it good/clean if nothing is being returned, or even if something is being returned) by an expert/professional of the malware removal field.

I am infected, now what?

So if you believe that you are indeed infected, what should you do ?

You should start by following these steps, in order:

Shut down your computer until you are ready to remove the infection (or at least, receive assistance to get it removed);

Get on a clean and secure computer, gather the necessary tools/programs and ask for help/assistance;

Change the passwords of all your accounts;

Enable 2FA (Two-Factor Authentication) where it's available (most major websites and services like games, online payments, emails, etc. supports 2FA. For more information about it you can always look up on their website for the right procedure to follow or go to your account Security settings); Click here to [read more about 2FA](#) and find a lists of sites that support it.

Be prepared to check other computers/laptops on your network (in case you get infected with a spreading-type virus, such as a worm);

Always be ready to back-up your data (securely) and reinstall Windows. Sometimes, malware/virus cannot be removed and the only way to get rid of them is to do a clean formatting and re-partitioning of your hard drive and reinstalling Windows, sadly;

In most situations, you'll be asked by [Aur?](#) to follow the instructions in his thread below, and post the log either here or there:

[\[BHCPU\] Program/Software advices and recommendations Help Desk](#) by [Aur?](#)

Then, you'll most likely get redirected to my tutorial/guide for generic malware removal, here:

[\[BHCPU\] Brotherhood Academy - Lesson 3: Removing Malware](#) by [-Hyperion](#)

How can I get assistance here?

There are lots of ways to get assistance on here and other reputed websites (mainly forums). Some tips include: Only follow directions/instructions from one person (multiple instructions may cause issues and make the clean-up procedure more lengthy)

Follow all instructions to the letter, do not cut any corners thinking it will save time and if you're not sure about an instruction, don't be afraid to ask the person that is helping you to be more clear;

Save every logs you're getting from the scans you're running, then copy/paste them on either [Pastebin](#) or [PrivatePaste](#) and post them in your thread. You have no idea how many intel this gives to the person assisting you, so please do it;

I am no longer infected, what now?

Even with an expert looking at it there, depending of what malware you are infected with (we're talking about risky ones here, like polymorphic viruses, not adwares, spywares, some backdoor trojans, etc.), there's no way to be 100% sure that your system is indeed clean. However, if you are being helped by a reliable and professional helper, yes, you can be sure of it ONCE, and only ONE he declares you clean. After a clean up it is highly recommended that you get a reputable Antivirus product installed, but also patch your security where it's failing (firewall, Antimalware, browser extensions, etc). I also recommend scanning with an Antimalware, such as Malwarebytes, once a week.

Once a month you can also run [Tron](#)

You may also need to fix any residual problems caused by an infections such as browser setting and registry problems. If this is the case, you are totally free to update your thread with these issues, and the member who assisted you will help you fix them.

Also, I suggest you to take a look at Aura's thread below to make sure to know what to do when requesting assistance here, and also, how to receive assistance properly:

[\[Read\] What you need to know when receiving assistance in the White Hat Help section](#) by [Aur?](#)

Feel free to shoot me or Aura any questions that you may have.  
Thank you and have a good day.

Thread formatting and editing done by [Aur?](#)

**Aura** - December 16, 2014, 8:12 pm

Good thing that I edited this thread ?

**Grin** - December 16, 2014, 8:15 pm

ABSOLUTELY WONDERFUL AND INFORMATIVE THREAD. THANK YOU FOR CONTRIBUTING HIGH QUALITY CONTENT TO THIS FORUM AND HELPING MEMBERS! THANK YOU AURA TOO!

**aguila** - December 16, 2014, 8:16 pm

This is a very informative thread for us users,nice :)

**Roger Waters** - December 16, 2014, 8:22 pm

Impressive Length, Hyperion. Next time you should have [xadamxk](#) make a layout for you instead of that black hat. ?

**Aura** - December 16, 2014, 8:25 pm

(Dec 16, 2014 09:22 PM)Roger Waters Wrote: [\[CITE\]](#) Impressive Length, Hyperion. Next time you should have [xadamxk](#) make a layout for you instead of that black hat. ?

Yeah, and bother Adam's for every threads we make, LOL. These are minimalist format, it's good

enough for that section, since more fancy stuff would probably lose the users.

**-Hyperion** - December 16, 2014, 8:27 pm

(Dec 16, 2014 09:25 PM)Aur? Wrote: [\[CITE\]](#) Yeah, and bother Adam's for every threads we make, LOL. These are minimalist format, it's good enough for that section, since more fancy stuff would probably lose the users.

Idk Aura some flashing shockwave might really jazz the place up

**Aura** - December 16, 2014, 8:29 pm

(Dec 16, 2014 09:27 PM)-Hyperion Wrote: [\[CITE\]](#) Idk Aura some flashing shockwave might really jazz the place up

Because we obviously want people to have Adobe Shockwave Player installed and enabled in their browser for a tutorial ... Nope, at least, not for me, lol.

**-Hyperion** - December 17, 2014, 6:58 pm

Finished this thread and am now taking any questions from it.

**tosher1011** - December 17, 2014, 7:01 pm

(Dec 17, 2014 07:58 PM)-Hyperion Wrote: [\[CITE\]](#) Finished this thread and am now taking any questions from it.

Just a general question for you or Aura. After getting the the items you suggest on the flash drive and disinfecting the computer is there a possible change that a usb spreader was installed? If so what steps do we take from there to protect other computers the flash drive will enter.

**-Hyperion** - December 17, 2014, 7:15 pm

(Dec 17, 2014 08:01 PM)tosher1011 Wrote: [\[CITE\]](#) Just a general question for you or Aura. After getting the the items you suggest on the flash drive and disinfecting the computer is there a possible change that a usb spreader was installed? If so what steps do we take from there to protect other computers the flash drive will enter.

You can either use junk USB sticks eg 2 GB or less(they cost less then a buck on amazon now) or include the USB in your scans. There is always the chance it could be infected. Also remember that if it does have a usb spreader then any other media you plugged in could be infected to.

**tosher1011** - December 17, 2014, 7:18 pm

(Dec 17, 2014 08:15 PM)-Hyperion Wrote: [\[CITE\]](#) You can either use junk USB sticks eg 2 GB or less(they cost less then a buck on amazon now) or include the USB in your scans. There is always the chance it could be infected. Also remember that if it does have a usb spreader then any other media you plugged in could be infected to.

Link me to this less then a buck USB stick

**Aura** - December 17, 2014, 7:19 pm

(Dec 17, 2014 08:15 PM)-Hyperion Wrote: [\[CITE\]](#) You can either use junk USB sticks eg 2 GB or less(they cost less then a buck on amazon now) or include the USB in your scans. There is always the chance it could be infected. Also remember that if it does have a usb spreader then any other media you plugged in could be infected to.

This.

Unless you were infected with worm, spreader or media injector, you don't really have to worry about it, but these are still viable probabilities.

**-Hyperion** - December 17, 2014, 7:43 pm

[http://www.amazon.com/Flash-Memory-Drive-Swivel-Design/dp/B00D4I0DYI/ref=sr\\_1\\_3?s=pc&ie=UTF8&qid=1418874199&sr=1-3](http://www.amazon.com/Flash-Memory-Drive-Swivel-Design/dp/B00D4I0DYI/ref=sr_1_3?s=pc&ie=UTF8&qid=1418874199&sr=1-3) here you go they also sell a big pack of 10 for 25 bucks

I personally use these <https://store.customusb.com/shop/gigs2go/>

**rapidfire08** - December 17, 2014, 7:47 pm

Nicely written. Cheers to you guys.

**Aura** - December 20, 2014, 2:28 pm

Oh wow, you even paid for that one too?

**SantyMan** - December 25, 2014, 3:05 pm

A really nice and informative thread keep up the good work! :)

**anojh12** - December 28, 2014, 12:02 pm

Thank you for the nice imformative thread. I'm pretty you guys just saved my ass :P

**NoScript** - December 29, 2014, 11:36 pm

Very informative thread you have here, You guys should follow his advice!

**Autonomous** - December 29, 2014, 11:38 pm

Thanks for the informative thread! ?

**-Hyperion** - January 9, 2015, 8:08 pm

going to updated this thread since the stickied one gone

**Aura** - January 9, 2015, 8:09 pm

(Jan 9, 2015 09:08 PM)-Hyperion Wrote: [\[CITE\]](#) going to updated this thread since the stickied one gone

Looks like I'll have more editing to do. Yay!

**-Hyperion** - January 12, 2015, 6:43 pm

updated for readability and changed the title since assassins thread is gone :(

**Aura** - January 13, 2015, 3:17 am

(Jan 12, 2015 07:43 PM)-Hyperion Wrote: [\[CITE\]](#) updated for readability and changed the title since assassins thread is gone :(

The thread actually got deleted and not just unstickied?

**-Hyperion** - January 13, 2015, 3:17 am

(Jan 13, 2015 04:17 AM)Aur? Wrote: [\[CITE\]](#) The thread actually got deleted and not just unstickied? I don't think so but I could not find it.

**Aura** - January 13, 2015, 3:22 am

(Jan 13, 2015 04:17 AM)-Hyperion Wrote: [\[CITE\]](#) I don't think so but I could not find it. Here it is, it still exist ? I have it linked in my sticky:

[PC Running Slow and/or Think You Are Infected? Read This!](#) by [AsSaSs@iN](#)

**-Hyperion** - January 25, 2015, 6:53 am

Re launching the program help desk today

**Crashes** - January 25, 2015, 7:05 am

I thought that this was some sort of challenge at first. :(  
Nice informative thread Hyperion.

**5h1t\_warrior** - April 5, 2015, 3:36 am

really usefull guide thanx alot 10/10!

