

Forum:[Hack Forums](#)

Thread: [How to tell if ive been hacked](#)

broccoliMonster - January 26, 2018, 9:14 am

How would i be able to tell if my pc/phone/laptop has been hacked? would all my anonymity measures be useless if i were hacked? ?

Thanks for help! ?

vaxton - January 26, 2018, 9:19 am

you should always check your process, startup and apps.
never download strange shits from youtube,forums (not this).

your antivirus wont help you against viruses since they can easily be crypted and bypass your antivirus.. but they cant hide from processes even with runPEE you can still get them out of your machine.

use wireshark to capture all the in-coming and outcoming connecting.

PM me for more live help :)

gb106 - January 26, 2018, 11:44 am

you can also try monitoring your network traffic, if there are any weird ones that you don't recognize, look into them to see where they came from

CyberStrike - January 26, 2018, 1:07 pm

So this is pretty much "Incident Response", we won't want this machine on the internet although we will want to keep it on as we will also look at the RAM. Pretty much we here are looking at Indicators Of Compromise (IOC) so we need to check what programs are opening ports, simple netstat -anb can get us quite a bit of info. We will need SysInternals to help us a bit. You want to check using procmon (assuming Windows here) what processes are running and for child processes. Also we check out Autoruns to see what is already running, let us note that if an attacker was to use application shimming it will not appear in autoruns.

Next your registry you need to parse through it. Although you can find shims searching through the registry and using other tools and volatility. Speaking of Volatility this is a great tool you can parse through the memory and find the applications running as well as much more, and it works pretty much for a majority of OS's and it is a crossplatform tool. So wireshark or tshark this is will be helpful for analysing the traffic and yes even if it is SSL you just have to work harder. So once you start to find something that is an outlier let's say you find it is to a strange IP. Well now we go ahead and check out our threat/intel feeds and OSNIT tools. So simple stuff we plug in the IP/Domain in question into VT, see what is going on. You will see that many times it is going to have a subdomain, and this as well should be enumerated. Next we need to hit up our feeds we start plugging in that domain we plug in the IP owe plug in other things we have found, say we have a file that had a wierd connection and was identified during our registry search as well, we plug in the sha256 hash value into VT as well as our feed. Basically we are searching now for that next indicator, generally many people get infected and often it will be somewhere like say AlienVault.

Once we have an idea of what we are dealing with we will want to search each possible indicator. Also you probably can have a good idea as to what group it is, perhaps not in the home user crowd

but in corporate we often will find out who it is that we are dealing with. There is a great amount more really, as DFIR is it's own thing.

Simple common sense is not too common so using a VM with NO SHARING is the key to not getting your host OS (the garbage you log into first) infected from the VM. Also if you do not know the sender or the application/file don't run it. If you are hell bent on running something go and download and everything in a VM, remember no sharing. Also have procmon and wireshark running and use INETSIM (Internet simulator) have snapshots of your VM before you installed your garbage.

Uose - January 26, 2018, 1:57 pm

Look for other standard hacker malware, overrides, etc. Here are some other things that might occur when hacked

Fake virus messages. Either you have virus software or you don't; if you don't, such messages will automatically alert you. If you do, then provided you know what your program's messages should look like, then you'll also be alerted to the messages being fakes. Do not click on it; it's a scam to get you to release credit card details in a panic to get rid of viruses on your computer. Be aware that the hacker is already controlling your computer (see What to Do below).

Additional toolbars appear in your browser. They may carry messages about "helping" you. There should only be one toolbar. Be suspicious if they multiply.

Random and frequent pop-ups appear on your computer. You'll need to get rid of the program that is doing this.

Your anti-malware, virus software doesn't work, appears disconnected. Your Task Manager or Registry Editor may also be out of action.

People in your email address list get fake emails from you.

Money is missing from your bank account or you get bills to pay for online purchases you haven't made.

If you simply won't have any control over anything you do, prioritize the probability that you are at the receiving end of being hacked. In particular, if your mouse cursor is moving around the screen and performing real actions that have actual results, a human is at the other end manipulating this. If you've ever had to allow access to work I.T. to fix your computer remotely, you'll know what this looks like when it's done for benign purposes. If it's not authorized, then you've been hacked.

Check your personal information. Google yourself. Are there returns of personal information online that you haven't personally released? This may not show up immediately but keeping an eye on this possibility may be important if personal information is released.

jordima - January 27, 2018, 6:33 am

My laptop (when sleeping) regularly just starts up randomly (mainly at night).

Hacked?

GetASyncKeyState() - January 27, 2018, 12:21 pm

(Jan 27, 2018 07:33 AM)jordima Wrote: [\[CITE\]](#) My laptop (when sleeping) regularly just starts up randomly (mainly at night).

Hacked?

Maybe you downloaded something and got a RAT and someone's controlling your computer...

CyberStrike - January 27, 2018, 1:55 pm

(Jan 27, 2018 07:33 AM)jordima Wrote: [\[CITE\]](#) My laptop (when sleeping) regularly just starts up randomly (mainly at night).

Hacked?

Probably and they pay attention to when you are on but at least you know that they are using a gui

type of RAT and probably some kind of teamviewer/VNC if you have Windows 7/8.1/10 professional (unless you applied the patch or the person in the machine applied the patch) then they probably are not using RDP. You probably should pull the physical connection on the machine for the internet, or disconnect it from wifi.

gb106 - January 27, 2018, 3:14 pm

(Jan 27, 2018 07:33 AM)jordima Wrote: [\[CITE\]](#) My laptop (when sleeping) regularly just starts up randomly (mainly at night).

Hacked?

Start collecting logs, see if you can find out how they're getting in (what protocol they're using, which program etc etc) and if you want, trace it back.