

Forum:[Hack Forums](#)

Thread: [Think im keylogged as one of my accounts was hacked](#)

~HF~ - June 15, 2012, 8:41 am

Hey so a game i play got hacked by someone (Runescape) so i just wanted a general checkup to see if im keylogged or RAT'd ill download and do all the anti-virus stuff ect.. please help :D

Thanks!

InfectedWorld - June 15, 2012, 8:42 am

If you pm me your teamvieww i can try to help you out :)

KingKratom - June 15, 2012, 8:51 am

Hi,

Please visit [Malwarebytes Anti-Malware](#) Run a quick scan.

[ESET Online Scanner](#) tick remove found threats.

[SpyBot S&D](#) Update then check for problems <make sure to run as administrator.>

[Vulcans Scanner](#) This will detect Blackshades and other RATs

- Wooter

??g????!? - June 15, 2012, 8:53 am

Look on msconfig for sospicious startup key. (also taskmanager)

Do a virus scann or use MalwareByte.

For further help pm me your tv dettails.

G.L.

~HF~ - June 15, 2012, 10:25 am

ok thanks guys im going to do some of the stuff you said later today thanks :D

Que. - June 15, 2012, 5:08 pm

--

Hello, my name is qW. and i will try to assist you the best i can.

Please follow these steps below.

1. Open up [Task Manager](#) and locate the infected process(es) and then kill the process from task manager and then delete the file which you located, if your not sure what process looks dodgy or not, simply grab a picture of the whole process list and post it here. Also you could follow this mini tutorial "[Using Netstat to find viruses \[MINI-TUTORIAL\]](#)", by [cobija](#)

2. If you're not allowed to open up the task manager or simply cannot find the malware process, Open up [System Configuration](#), by typing "msconfig" in the search box in the start menu and then press enter or you can open it by typing the same in the [Command Prompt](#) (cmd) and then press

enter, when the System configuration window appears, go to the [Startup Tab](#) and deactivate all the dodgy app's from running on startup's, and from there you can also locate the malware files and then delete them, or you can go to the location "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup" and do the exact same, deleting the shortcut or so, if your not sure what application that is dodgy or not, you can provide us pictures of the "msconfig >> startup" tab and the "startup folder".

3. If you cannot delete the malware files in normal mode, try booting up in safe mode and try to delete the files from there, if you know the location of the files tho. By booting up in safe mode, restart you're computer and enter the boot menu by pressing the default key "F8", and select "safe mode with cmd/internet"

4. If all of the steps above failed, you can try to remove the malware from you're system by running a scan with [\[color=#FFA500\]Superantispyware](#), Download either the Trial edition or the free edition, doesn't matter, after the download is complet, install it and then open up the software, run an update to assure the software is up-to date, then run a full scan and see if it detects the malware, if the scan result comes up as blank, go on to step 5.

5. Other scanners you can try to remove the malware with is, [Malwaresbytes](#), Download the software and install it, then update it to assure it's up-to date, and then run a quick scan with it, a full scan is not necessary, the second scanner you can try is [ESET Online Scanner](#), download it and run it, then start a scan with it. The last scanner you could try is the [Spybot - Search & Destroy](#), run it and do a scan with it.

6. If you still think you're infected, please post all of you'er logs here so we can assist you further.

--

For RAT infections

Download [Comodo's Firewall](#), The firewall allows you to monitor/block outbound connections and inbound connections.

For malware infections with keyhooks (keyloggers)

Download [KeyScrambler](#), the software will spooof all the entered keys so the when the author gets the logs it will be displayed.. for an example "1"-123fwi&#"ed!"!DQ" instead of what you actual typed, letters/numbers/symbols.

For Adwares

Most adwares out there often redirect their slaves via the hosts file, also the malicious codes replaces or modifies the hosts file, you can easily spot this my checking the file yourself, Go to the location C:\Windows\System32\drivers\etc\ "Hosts" and right click the "Hosts" file and open it in notepad, copy + paste everything and post it here afterwards.

For more difficult infections like Rootkits and Bootkits

Please download [GMER](#), then run it and do a scan with it, then post the log here after the scan is complet. You could also download [TDSSKiller](#), the software is well known to get rid of rootkits and other diffcoul malwares.

--

I Hope this helps, and good luck.

-qW.

Viral Dragon - June 16, 2012, 2:39 am

Op:

First, I would like to suggest downloading the following: [Malwarebytes' Anti-Malware](#). Update it and run a quick scan. Remove everything it finds.

[ESET Online Scanner](#). Download the executable and run it. It will start downloading its database. Once it is done, check all options for removal and proceed with the scan. This is a free scan that will remove any found threats.

[Spybot Search&Destroy](#). Download this and run it. Click on the first box "Search & Destroy". The click on "Check for problems". It will ask you if it can delete any non-used temporary files. Click on yes. (This is ok). Let it run. Check all boxes that pop up and click on "Fix Selected Problems".

[Comodo AV and Firewall](#). This is Comodo AV and Firewall. Download this, let it update it's virus database and then proceed to run a full scan. This could take a while. Quarantine any of the files it finds.

Please also note that if you have a second computer or have another way to get on to the internet to post here, it is highly advised to disconnect from the internet on your infected machine and relay all information from the other machine instead. (You can transfer the downloads from PC to PC using a external hard drive or USB/CD/DVD). If you cannot access the internet from another machine, that is fine. I then suggest just downloading the files and disconnecting from the internet until all scans are done.

To further increase the amount of damage reduction, you could open up your start menu and traverse to your msconfig to remove the item from startup, if it exist. You can do this by going to Start -> Search -> msconfig -> Enter (or for XP, Start -> Run -> msconfig -> Enter). In doing so a window will popup. When it does please proceed to do the following:

Click on the fourth (4th) tab that says "Startup" and then proceed to go through the list, unchecking any check boxes you do not recognize. Then click on "Apply". And proceed to restart. Upon restarting this should prevent the program from starting up allowing you safe passage to the internet again. However, this is only if you found the correct startup item. But we're not out the woods yet. After you've done the above, please do the next following set of things:

Please read and follow [this](#) and a trained HJT Helper will be there to assist you. Remember to describe your problem with as much detail as possible. Paste the logs at [PasteBin](#) separately. Post links to all logs in a new thread at the [HijackThis Log Analyzer and Tutorials Section](#).

Next thing you should know, RAT's and Keyloggers tend to have themselves binded to the registry and either the %AppData% folder, /Temp/ folder, or the Windows/System32 folders. If you attempt to delete the .exe from one of these folders and you notice it comes back it means it has persistence and it is in a registry key somewhere. DO NOT attempt to look for the registry key, let a trained HJT

Helper do so for you. Registries can be dangerous if you do not know what you're doing.

Last warning I should give you as well; Do NOT under ANY circumstances, reinstall or reformat the OS. This will in NO way help you. It is time consuming, a hassle, and just generally not needed. Ignore any and ALL post who say to do so.

Lastly, be sure to clear your system restore point. Malware now adays have started infecting system restore points it recommended to just wipe the current restore points you have and just make a new one after you're done being disinfected. To do so, do the following:

Clear system restore points: Go to Start > All Programs > Accessories > System Tools > System Restore

Select Create a restore point, and Ok it.

Next, go to Start > Run and type in cleanmgr

choose your root drive (normally C:)

after it calculates how much space you will save it will open up a new window

Select the More options tab at the top of the window

Choose the option to clean up system restore and OK it.

go back to the disk clean up tab

put a checkmark in all - except compress old files (leave this unchecked)

click Ok then click yes

This will remove all restore points except the new one you just created and clean unneeded files.

-Viral.

McFlurry - June 16, 2012, 7:28 am

Remote Access Trojan (RAT) Warning

Your computer has multiple infections... one of the identified infections is related to a Remote Access Trojan.

Remote Access Trojans... are very dangerous because they provide a means of accessing a computer system that bypasses security mechanisms and steal sensitive information like passwords, personal and financial data which they send back to the hacker.

Remote attackers use these Trojans as part of an exploit to gain unauthorized access to a computer and take control of it without your knowledge.

Please read the [Danger: Remote Access Trojans](#).

If your computer is used for online banking, has credit card information or other sensitive data on it, you should:

Immediately disconnect from the Internet until your system is cleaned.

All passwords should be changed immediately, include those used for banking, email, eBay and

forums.

You should consider them to be compromised.

Change these passwords by using a different computer and not the infected one.

If not, an attacker may get the new passwords and transaction information.

Banking and credit card institutions should be notified of the possible security breach.

Que. - *June 16, 2012, 7:31 am*

Now you allot got usefull materials here OP.

Hopefully you'll manage to get rid of the infection.

-qW.

~HF~ - *June 16, 2012, 7:31 am*

ok thanks guys i found it and removed it :D thanks