

Forum:[Hack Forums](#)

Thread: [How to be sure that I'm not keylogged or hacked?](#)

Rathz - July 6, 2013, 7:50 am

Good Day.

Well, I just posted a thread some where on this forums, and I asked that same question which is "I think I'm keylogged or hacked, how to be sure".

I think you just understood what I want to know.

Since my PayPal, Hotmail, Yahoo, Gmail, and some other accounts got hacked, I think that I'm keylogged or got hacked.

How to be sure that I'm not keylogged? And if I'm keylogged what to do?

Thanks for the one who is going to answer/help me.

Best Regards,
Flex.

Oak? - July 6, 2013, 8:12 am

I would follow these steps in order to remove your infection completely.

1. Check your processes for any unknown programs that have been executed.
2. Open up resource manager and see if there is any program that has a lot of data being connected to you.
3. I would open up Msconfig and search for startup programs that don't belong there.
4. Boot your computer with Safemode+Networking
5. Download HitmanPro and run a scan: <http://www.surfright.nl/en>
6. I recommend also Using Kasperskys TDSSKiller which can be found here: <http://www.bleepingcomputer.com/download/tdsskiller/>
7. Try using Darkcomet/Jrat Remover.

<http://redpoisOn.com/download.php?proj=remover>

If all else fails please contact me.

Corso - July 6, 2013, 8:23 am

flexyD Wrote:Good Day.

Well, I just posted a thread some where on this forums, and I asked that same question which is "I think I'm keylogged or hacked, how to be sure".

I think you just understood what I want to know.

Since my PayPal, Hotmail, Yahoo, Gmail, and some other accounts got hacked, I think that I'm keylogged or got hacked.

How to be sure that I'm not keylogged? And if I'm keylogged what to do?

Thanks for the one who is going to answer/help me.

Best Regards,

Flex. Long answer short? Post in MRT section and have professional assistance.

Now if you want to learn some ways to look for one on your own, look into [Comodo Cleaning Essentials \(CCE\)](#) for the Comodo Autorun Analyzer and Comodo KillSwitch items within it. They will help you look through your Startup and your running processes with the network connections (inbound/outbound plus details). Reviewing this and studying/researching the lines will help you understand your PC better and to help spot out any infections and such.

sinnerz - July 6, 2013, 8:51 am

1. go to your control panel and go to the program installed area.
2. uninstall any program that your not familiar with.
3. go to msconfig and a pop up will appear. you will see an option click on services and disable all running services. and hit apply then ok it will tell you to restart your comp now it will automatically disabled unnecessary program or any files..

4. put your pc on safemode/networking and scan your pc with this online scan

<http://www.eset.com/us/online-scanner-popup/> save it to your desktop

Double-click esetsmartinstaller_enu.exe to execute the program.

Tick Yes, I accept the Terms of Use.

Click Start.

If this is your first time installing the scanner, allow the ActiveX Control to install.

Database download may take some time.

When done, make sure that the option Remove found threats is ticked. Under the and Advanced Settings, please put a check on the following options:

Scan for potentially unwanted applications

Enable Anti-Stealth Technology

Click Start.

Wait for the scan to finish

5. it should show u all of the detected threatened files viruses

6. go ahead restart you pc again and go back to your start up and type in msconfig and u will the same pop up box and click on normal start up and that will allow all of your regular app and files to run back normal

7. the comp will restart again let it restart back to normal window then download this

<http://www.malwarebytes.org/> this is a very good virus killer do a full scan .

when is finish make sure you restart your pc again to take a full effect on removing the viruses

8. download this free trial <http://www.bitdefender.com/toolbox/> it is the best and top of the market comp protection

9. bitdefender has alot of features you can use to maintain a good security check on your pc on the daily day this protection is a very good protection and it will allow you to even download some of the free tools they have and also have a good monitoring support team that open 24 hrs .

well hope your comp will get better for any question just feel free to pm me..

and btw i read some thread on here u might wanna check it also and vouch for them

<https://hackforums.net/showthread.php?tid=3600691>

Oak? - July 6, 2013, 9:14 am

@Sinnerz

Are you foreign because I can barely understand what you want him to do.

I get the idea of what you are saying but you worded everything really poorly.

sinnerz - July 6, 2013, 9:32 am

thank you for reading it glad you took your time and recognized my foreign self :)

Rathz - July 7, 2013, 2:21 am

Really appreciated, thank you guys, but still can't do that steps xD

If anyone interested to help me, post here, or PM me to give him my Skype or TV Information.

TheSocialGenius - July 7, 2013, 2:34 am

(Jul 6, 2013 08:12 AM)Oak? Wrote: [\[CITE\]](#) I would follow these steps in order to remove your infection completely.

1. Check your processes for any unknown programs that have been executed.
2. Open up resource manager and see if there is any program that has a lot of data being connected to you.
3. I would open up Msconfig and search for startup programs that don't belong there.
4. Boot your computer with Safemode+Networking
5. Download HitmanPro and run a scan: <http://www.surfright.nl/en>
6. I recommend also Using Kasperskys TDSSKiller which can be found here:
<http://www.bleepingcomputer.com/download/tdsskiller/>
7. Try using Darkcomet/Jrat Remover.

<http://redpois0n.com/download.php?proj=remover>

If all else fails please contact me.

When I did a online virus scan of that website posted this is what popped up smh:

<http://sitecheck.sucuri.net/results/redpois0n.com/>

web site: redpois0n.com/

status: Site infected with malware

web trust: Site blacklisted.

Malware found in the URL:

<http://redpois0n.com/projects.php>

Known javascript malware.

Details: <http://sucuri.net/malware/entry/MW:JS:GEN2>

<p>A simple (and buggy!) PHP "Obfuscator" that can base64 encode php pages (eval(base64_decode()))), trim lines, and encode ' and " strings. </p>

JakeHD - July 7, 2013, 2:53 am

this isnt very helpfull just trying to Help, Install EsetNod32, Then install malwarebytes, Do a Quick scan with them.

If you do not have time to install a load of anti virus go here

<https://hackforums.net/showthread.php?tid=3417997>

Kind Regards,
JakeHd

im abcd - July 7, 2013, 4:55 am

(Jul 7, 2013 02:34 AM)TheSocialGenius Wrote: [\[CITE\]](#) When I did a online virus scan of that website posted this is what popped up smh:

<http://sitecheck.sucuri.net/results/redpois0n.com/>

web site: redpois0n.com/
status: Site infected with malware
web trust: Site blacklisted.

Malware found in the URL:
<http://redpois0n.com/projects.php>

Known javascript malware.

Details: <http://sucuri.net/malware/entry/MW:JS:GEN2>

<p>A simple (and buggy!) PHP "Obfuscator" that can base64 encode php pages (eval(base64_decode())), trim lines, and encode ' and " strings. </p>

Redpoison's site and his JRAT remover is completely legit and safe. Its probably because it also provides the download link for various crypters and binders.