

Forum:[Hack Forums](#)

Thread: [Think I might be ratted/keylogged \(Need some assistance\)](#)

smartwhip - November 23, 2016, 10:17 am

I keep getting login attempts on my gmail, my skype was also hacked. A little paranoid right now about the whole situation so could do with some help.

SIM-2502833 - November 23, 2016, 10:24 am

Please download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Note: You need to run the version compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator (XP users click run after receipt of Windows Security Warning - Open File). When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce logs called FRST.txt and Addition.txt in the same directory the tool is run from.

Please copy and paste the logs back here.

Shaq - November 23, 2016, 10:31 am

Before you fix anything you need a foundation to rebuild on. Here's what I'd recommend:

Tell your bank to watch out if something weird hits your account.

Go on your phone and make a new email. Do not link this to any other email. For recovery, you can put your real phone number. This email only has one use: LastPass.

Purchase LastPass Premium (it's like \$13/year, way worth it) and use your new email when signing up. Do NOT use lastpass to store that email's password.

Download the LastPass app on your phone and login.

Enable LastPass Authenticator (2-factor auth, like Google Authenticator) You may be able to use Google Authenticator with this as well.

Enable LastPass Credit Monitoring (there should be a help article on this). This will help if whoever hacked your stuff got your SSN.

As you secure your accounts, use LastPass to generate and store their logins. This way each one has a separate password.

Store your security questions/random answers in a LastPass Secure Note. I use dinopass.com to generate random answers.

SIM-2502833 - November 23, 2016, 10:34 am

(Nov 23, 2016 11:31 AM)NTFS Wrote: [\[CITE\]](#) Before you fix anything you need a foundation to rebuild on. Here's what I'd recommend:

Tell your bank to watch out if something weird hits your account.

Go on your phone and make a new email. Do not link this to any other email. For recovery, you can put your real phone number. This email only has one use: LastPass.

Purchase LastPass Premium (it's like \$13/year, way worth it) and use your new email when signing up. Do NOT use lastpass to store that email's password.

Download the LastPass app on your phone and login.

Enable LastPass Authenticator (2-factor auth, like Google Authenticator) You may be able to use Google Authenticator with this as well.

Enable LastPass Credit Monitoring (there should be a help article on this). This will help if whoever hacked your stuff got your SSN.

As you secure your accounts, use LastPass to generate and store their logins. This way each one has a separate password.

Store your security questions/random answers in a LastPass Secure Note. I use dinopass.com to generate random answers.

I feel like this is largely unnecessary, using 2 facto authorization (I prefer lastpass 2 facto auth) and having the app on your phone is more than enough.

Been using lastpass for years

<http://prntscr.com/dax7om>

GruntStyl - November 23, 2016, 10:38 am

What scans have you run, if any? And was anything detected. I would continue following MrMcShroom instructions and go from there.

Shaq - November 23, 2016, 10:45 am

(Nov 23, 2016 11:34 AM)MrMcShroom Wrote: [\[CITE\]](#) I feel like this is largely unnecessary, using 2 facto authorization (I prefer lastpass 2 facto auth) and having the app on your phone is more than enough.

Been using lastpass for years

<http://prntscr.com/dax7om>

Which part is unnecessary? In order to have the app on your phone you need premium..

ka\$h - November 23, 2016, 10:52 am

Skype got hacked, what do you mean by that?

smartwhip - November 23, 2016, 10:53 am

(Nov 23, 2016 11:24 AM)MrMcShroom Wrote: [\[CITE\]](#) Please download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Note: You need to run the version compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator (XP users click run after receipt of Windows Security Warning - Open File). When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce logs called FRST.txt and Addition.txt in the same directory the tool is run from.

Please copy and paste the logs back here.

frst - <http://pastebin.com/tDHTykCL>

addition - <http://pastebin.com/JKF4ummR>

ankok81 - November 23, 2016, 12:37 pm

If your Skype was hacked, and you are getting third party attempts on your Gmail, there is no further question whether you are hacked. Now, you need to find your recovery media [if it is not built in], and factory reset, or manually format ALL drives. This is the only way to assure you are no longer compromised. If you state your OS, I can direct you to the appropriate information to assist you with this process.

GruntStyl - November 23, 2016, 3:08 pm

I'm assuming if he's coming here he is wanting to avoid a factory reload. Of course that would ensure he would be clean for the most part. However if he's being ratted/keylogged it shouldn't be too hard to remove the infection.

smartwhip - December 14, 2016, 1:00 pm

100% am infected with a keylogger or rat, change my password pretty much twice a week and somehow someone is getting access to my accounts, Need help asap

ka\$h - December 14, 2016, 1:02 pm

(Dec 14, 2016 02:00 PM)North Face Wrote: [\[CITE\]](#) 100% am infected with a keylogger or rat, change my password pretty much twice a week and somehow someone is getting access to my accounts, Need help asap

Do you know what keylogger you installed and/or what file you installed it from?

smartwhip - December 14, 2016, 1:08 pm

(Dec 14, 2016 02:02 PM)Ka\$h Wrote: [\[CITE\]](#) Do you know what keylogger you installed and/or what file you installed it from?

I dont have a clue, been getting sign in attempts for awhile now but I 100% know something is on my computer

ka\$h - December 14, 2016, 1:16 pm

(Dec 14, 2016 02:08 PM)North Face Wrote: [\[CITE\]](#) I dont have a clue, been getting sign in attempts for awhile now but I 100% know something is on my computer

What have you done up to now just so we know

smartwhip - December 14, 2016, 1:22 pm

(Dec 14, 2016 02:16 PM)Ka\$h Wrote: [\[CITE\]](#) What have you done up to now just so we know ran a malware bytes scan, nothing found , that is all

ka\$h - December 14, 2016, 1:42 pm

(Dec 14, 2016 02:22 PM)North Face Wrote: [\[CITE\]](#) ran a malware bytes scan, nothing found , that is all

What version of Windows are you on? I would suggest running malwarebytes while your in safe mode if you didn't; I need some information about the last things you remember downloading that may have caused it.

smartwhip - December 14, 2016, 1:44 pm

(Dec 14, 2016 02:42 PM)Ka\$h Wrote: [\[CITE\]](#) What version of Windows are you on? I would suggest running malwarebytes while your in safe mode if you didn't; I need some information about the last things you remember downloading that may have caused it.

I have not got that information, It has been along time since I believe i have been infected, Windows 7 64bit

Hackoo - December 14, 2016, 2:04 pm

Hi ?

Copy and paste this batch file on your notepad and save it as STARTUP_ITEMS.bat and Execute it as administrator to generate a report that you can copy and paste to <http://pastebin.com/> or to <http://textuploader.com/>

so before executing this script close all your browsers otherwise the script will do it for you !

Source code of STARTUP_ITEMS.bat

STARTUP_ITEMS.bat ([Click to View](#))

NB : Don't forgot to share here in this thread (Not by PM :Non:) the link of your paste report :Oui:

ka\$h - December 14, 2016, 2:10 pm

(Dec 14, 2016 02:44 PM)North Face Wrote: [\[CITE\]](#) I have not got that information, It has been along time since I believe i have been infected, Windows 7 64bit

Waiting for a moment so I can get to have a look at that scan report

smartwhip - December 14, 2016, 2:19 pm

(Dec 14, 2016 03:04 PM)Hackoo Wrote: [\[CITE\]](#) Hi ?

Copy and paste this batch file on your notepad and save it as STARTUP_ITEMS.bat and Execute it as administrator to generate a report that you can copy and paste to <http://pastebin.com/> or to <http://textuploader.com/>

so before executing this script close all your browsers otherwise the script will do it for you !

Source code of STARTUP_ITEMS.bat

STARTUP_ITEMS.bat ([Click to View](#))

NB : Don't forgot to share here in this thread (Not by PM :Non:) the link of your paste report :Oui:

<http://pastebin.com/xgSHrswz>

imabeast - December 14, 2016, 2:35 pm

(Dec 14, 2016 03:19 PM)North Face Wrote: [\[CITE\]](#) <http://pastebin.com/xgSHrswz>

after a quick google search for made by hackoo 2016 thats in the bat i found out a guy named

hackoo on leakforums helping people with vbs and guess what? bat scripts.. maybe he made this? but then it would be while helping someone.

<https://leakforums.net/thread-777270>

Hackoo - December 14, 2016, 3:12 pm

(Dec 14, 2016 03:19 PM)North Face Wrote: [\[CITE\]](#) <http://pastebin.com/xgSHrswz> A quick look on your report, we can say there are no reasons to worry but if want be sure more and more of your all running process, i will recommend you an old HTA tool that i made before to check and kill process and has the ability to upload your exe files to virustotal.com

This tool is in french but i will perhaps update it and make another version in english ?

Copy and paste this code on your notepad and name it as CheckProcess+VirusTotal.hta

CheckProcess+VirusTotal.hta ([Click to View](#))

If you encounter any bug please let me know ?

smartwhip - December 14, 2016, 3:22 pm

(Dec 14, 2016 04:12 PM)Hackoo Wrote: [\[CITE\]](#) A quick look on your report, we can say there are no reasons to worry but if want be sure more and more of your all running process, i will recommend you an old HTA tool that i made before to check and kill process and has the ability to upload your exe files to virustotal.com

This tool is in french but i will perhaps update it and make another version in english ?

Copy and paste this code on your notepad and name it as CheckProcess+VirusTotal.hta

CheckProcess+VirusTotal.hta ([Click to View](#))

If you encounter any bug please let me know ?

I have got reasons to worry, I know for sure I am infected, every time I change my password somehow I get sign in attempts with that password via my gmail account.

Hackoo - December 14, 2016, 3:29 pm

(Dec 14, 2016 04:22 PM)North Face Wrote: [\[CITE\]](#) I have got reasons to worry, I know for sure I am infected, every time I change my password somehow I get sign in attempts with that password via my gmail account.

Download and scan your PC with [AntiLogger](#)

ka\$h - December 14, 2016, 3:30 pm

(Dec 14, 2016 04:22 PM)North Face Wrote: [\[CITE\]](#) I have got reasons to worry, I know for sure I am infected, every time I change my password somehow I get sign in attempts with that password via my gmail account.

Your Gmail account has 2FA enabled?

debug - December 14, 2016, 3:30 pm

(Nov 23, 2016 11:23 AM)?Kosdff Wrote: [\[CITE\]](#) Scan your system with MalwareBytes.

Install Glasswire and block any unfamiliar connections. Wow, that looks beautiful. Gonna try it out now and hopefully replace comodo.