

Forum:[Hack Forums](#)

Thread: [Did I get keylogged/ratted?](#)

NA Riven - September 10, 2017, 7:14 pm

Heya,

So I got an email from Dropbox that someone logged in on my account from another location. Is it possible I got infected? Because if so you must've been very dumb to login on a Dropbox account when they know (I hope) the real owner gets an email.

Dropbox Email

Spoiler ([Click to View](#))

Logs:

FRST: <https://pastebin.com/36jxA0CW>

Addition: <https://pastebin.com/vfmYuzR4>

Sorry if I'm not clear enough xdd

Cheers.

5chn4pp - September 11, 2017, 3:48 am

I think your services and maybe drivers are fucked, do this:

Download [fixlist.txt](#) file and save it to the Desktop.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work.

NOTICE: This script was written specifically for this user, for use on that particular machine. Running this on another machine may cause damage to your operating system

Run FRST/FRST64 and press the Fix button just once and wait.

If for some reason the tool needs a restart, please make sure you let the system restart normally. After that let the tool complete its run.

When finished FRST will generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

Please download [Malwarebytes Anti-Rootkit](#) and save the file to your desktop. Please rename the file MBAR.exe to abc.exe

Right-Click abc.exe and select Run as administrator to run the installer.

Select your Desktop as the location to extract the contents and click OK. The program should open upon completion.

Click Next, followed by Update. Upon update completion, click Next.

Ensure Drivers, Sectors & System are checked and click Scan.

Do not use your computer during the scan.

Upon completion: If no malware is found, close the MBAR window.

If malware is found, ensure Create Restore Point is checked and click Cleanup. Reboot when prompted.

Two logs (mbar-log.txt and system-log.txt) will be created. Copy the contents of both logs and paste them to pastebin.com. Both logs can be found in the MBAR folder.

DrizzyFanz345 - September 11, 2017, 10:38 am

It might be just a accident on the part of someone trying to login on dropbox and made a typo.

Death - September 11, 2017, 10:40 am

Did you open up any attachment on emails before?

NA Riven - September 11, 2017, 1:05 pm

(Sep 11, 2017 03:48 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) I think your services and maybe drivers are fucked, do this:

I will when I am back in my PC

(Sep 11, 2017 10:38 AM)DrizzyFanz345 Wrote: [\[CITE\]](#) It might be just a accident on the part of someone trying to login on dropbox and made a typo.

Pretty sure you cant make a typo with this email and password.

(Sep 11, 2017 10:40 AM)linuxdaddy Wrote: [\[CITE\]](#) Did you open up any attachment on emails before?

No

5chn4pp - September 11, 2017, 1:38 pm

(Sep 11, 2017 10:38 AM)DrizzyFanz345 Wrote: [\[CITE\]](#) It might be just a accident on the part of someone trying to login on dropbox and made a typo.

He has a polymorphic infection I believe, this is probably not the case.

NA Riven - September 12, 2017, 1:40 am

(Sep 11, 2017 03:48 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#)

I think your services and maybe drivers are fucked, do this:

Download [fixlist.txt](#) file and save it to the Desktop.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work.

NOTICE: This script was written specifically for this user, for use on that particular machine. Running this on another machine may cause damage to your operating system

Run FRST/FRST64 and press the Fix button just once and wait.

If for some reason the tool needs a restart, please make sure you let the system restart normally.

After that let the tool complete its run.

When finished FRST will generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

Please download [Malwarebytes Anti-Rootkit](#) and save the file to your desktop. Please rename the file MBAR.exe to abc.exe

Right-Click abc.exe and select Run as administrator to run the installer.

Select your Desktop as the location to extract the contents and click OK. The program should open upon completion.

Click Next, followed by Update. Upon update completion, click Next.

Ensure Drivers, Sectors & System are checked and click Scan.

Do not use your computer during the scan.

Upon completion: If no malware is found, close the MBAR window.

If malware is found, ensure Create Restore Point is checked and click Cleanup. Reboot when prompted.

Two logs (mbar-log.txt and system-log.txt) will be created. Copy the contents of both logs and paste them to pastebin.com. Both logs can be found in the MBAR folder.

I just saw the Fix List and the Lion Driver thingy is for a cheat. I am not sure if its a false positive because its a cheat or not but I believe its ok

5chn4pp - September 12, 2017, 3:36 am

(Sep 12, 2017 01:40 AM)NA Riven Wrote: [\[CITE\]](#) I just saw the Fix List and the Lion Driver thingy is for a cheat. I am not sure if its a false positive because its a cheat or not but I believe its ok

Do it anyways because the files get stored in the FRST folder, if you want them back you can just copy them when your computer is clean.

Tsukiri - September 12, 2017, 3:44 am

I always feel bad for malware victims (this is a blatant lie but just go with it to make the story sound better)

but since your name is NA Riven.. I am praying that it was a banking bot combined with a cryptolocker.

<3

NA Riven - September 12, 2017, 3:45 am

(Sep 12, 2017 03:44 AM)Tsukiri Wrote: [\[CITE\]](#) I always feel bad for malware victims (this is a blatant lie but just go with it to make the story sound better)

but since your name is NA Riven.. I am praying that it was a banking bot combined with a cryptolocker.

<3

Sir that is very rude now I need to tell you to get back to botlane and buy a fucking sightstone or I will int.

@Bromo I will when I get home.

Tsukiri - September 12, 2017, 3:51 am

(Sep 12, 2017 03:45 AM)NA Riven Wrote: [\[CITE\]](#) Sir that is very rude now I need to tell you to get back to botlane and buy a fucking sightstone or I will int.

@Bromo I will when I get home.

Why no "get cancer" followed by a 1v3 engage blaming the jungler :((

You should check your startup folder and registry. If you caught malware, it will 99% of the time have startup (otherwise it will be removed once you restart your PC making it pretty useless). If you see anything suspicious there just find the path and remove the files. Run a scan using ESET NOD32 on your PC and do what bromo said.

NA Riven - September 12, 2017, 6:55 am

(Sep 12, 2017 03:51 AM)Tsukiri Wrote: [\[CITE\]](#) Why no "get cancer" followed by a 1v3 engage blaming the jungler :((

I dont lose so blaming the jungler would be useless. I only flame people so hard that they want to commit suicide.

(Sep 11, 2017 03:48 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#)I think your services and maybe drivers are fucked, do this:

Download [fixlist.txt](#) file and save it to the Desktop.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work.

NOTICE: This script was written specifically for this user, for use on that particular machine. Running this on another machine may cause damage to your operating system

Run FRST/FRST64 and press the Fix button just once and wait.
If for some reason the tool needs a restart, please make sure you let the system restart normally.
After that let the tool complete its run.
When finished FRST will generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

Please download [Malwarebytes Anti-Rootkit](#) and save the file to your desktop. Please rename the file MBAR.exe to abc.exe

Right-Click abc.exe and select Run as administrator to run the installer.

Select your Desktop as the location to extract the contents and click OK. The program should open upon completion.

Click Next, followed by Update. Upon update completion, click Next.

Ensure Drivers, Sectors & System are checked and click Scan.

Do not use your computer during the scan.

Upon completion: If no malware is found, close the MBAR window.

If malware is found, ensure Create Restore Point is checked and click Cleanup. Reboot when prompted.

Two logs (mbar-log.txt and system-log.txt) will be created. Copy the contents of both logs and paste them to pastebin.com. Both logs can be found in the MBAR folder.

I am scanning rn

5chn4pp - September 12, 2017, 10:14 am

Please download [TDSSKiller](#) and save the file to your desktop. Right-Click TDSSKiller.exe and select Run as Administrator

Click Change parameters. Place a checkmark next to Detect TDLFS file system and Verify file digital signatures.

Click Start Scan. Do not use the computer during the scan.

If objects are found, change the action to skip.

Click Continue and close the window.

A log will be created and saved to the root directory (usually C:\). Paste the file contents to pastebin.com and post the link in your next reply.

Download [fixlist.txt](#) file and save it to the Desktop.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work.

NOTICE: This script was written specifically for this user, for use on that particular machine. Running this on another machine may cause damage to your operating system

Run FRST/FRST64 and press the Fix button just once and wait.

If for some reason the tool needs a restart, please make sure you let the system restart normally. After that let the tool complete its run.

When finished FRST will generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

Please download [RogueKiller](#) and save it to your desktop. Quit all running programs.

Right-click on the program and select Run as Administrator to start and when prompted allow it to run.

Read and accept the EULA (End User License Agreement)

Click Scan to scan the system.

When the scan completes select "Report", a log will open. Close the program > Don't Fix anything!

Post the contents of the log in your next reply.

NA Riven - *September 12, 2017, 10:49 am*

I PM'd you the next logs mate ;)

Dlogreen - *September 12, 2017, 5:48 pm*

Check your processes and see if anything is eating up a lot of space. Also check your hidden files to make sure nothing is odd.