

Forum: [Hack Forums](#)

Thread: [Fairly certain](#)

mixedBasket - August 27, 2017, 1:44 pm

Fairly certain I'm infected. Woke up this morning and I normally leave my computer on, found it opened to a few ad links; short.st and ad.fly or whatever.

No way I opened this and forgot about them.

5chn4pp - August 27, 2017, 1:52 pm

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. 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.

mixedBasket - August 27, 2017, 1:55 pm

FRST: <https://pastebin.com/XbfZckH8>

Addition: <https://pastebin.com/LtNVePG5>

Thanks

5chn4pp - August 27, 2017, 2:06 pm

Yeah you got an infected version of kmspico.

Uninstall "DragonBoost" and "RunBooster" using your control panel.

After that, 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.

mixedBasket - August 27, 2017, 2:16 pm

Wasn't able to find DragonBoost or RunBooster in the control panel.

Fixlog: <https://pastebin.com/wZBwQ95P>

5chn4pp - August 27, 2017, 2:18 pm

Weird, I have a suspicion that this is going to be hard to remove.

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.

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.

mixedBasket - August 27, 2017, 2:43 pm

From RogueKiller: <https://pastebin.com/2xesAwkG>

I'm unable to open abc.exe/mbar.exe . It says the requested resource is in use.

5chn4pp - August 27, 2017, 2:50 pm

(Aug 27, 2017 02:43 PM)mixedBasket Wrote: [\[CITE\]](#) From RogueKiller:

<https://pastebin.com/2xesAwkG>

I'm unable to open abc.exe/mbar.exe . It says the requested resource is in use.

Yep thats a hard one, make sure everything roguekiller found is selected and deleted apart from "phymem.sys"

Please download [HitmanPro](#) 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.

Click the settings tab and go into Advanced, then enable Early Warning Scoring.

Click OK and Next then select No, I only want to perform a one-time scan to check this computer.

Click Next and it should start the scan, please be patient.

When the scan completes click "Save log", and save it to your desktop. Close the program > Don't Fix anything!

Post the contents of the log in your next reply.

mixedBasket - August 27, 2017, 3:00 pm

HitmanPro: <https://pastebin.com/yi3PmCxC>

5chn4pp - August 27, 2017, 3:10 pm

(Aug 27, 2017 03:00 PM)mixedBasket Wrote: [\[CITE\]](#) HitmanPro: <https://pastebin.com/yi3PmCxC>

Lets try this, if it doesn't work we need to enter recovery mode:

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.

mixedBasket - August 27, 2017, 3:40 pm

Fixlog: <https://pastebin.com/umRqx2qV>

5chn4pp - August 27, 2017, 3:58 pm

Yeah recovery mode it is, just need new logs to see if I need to remove anything else:

Re-Scan with FRSTDoube-Click FRST.exe or FRST64.exe to run the program.

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

Upon completion, click OK, then OK on the Addition.txt pop up screen.

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to pastebin.com. Post the link here.

mixedBasket - August 27, 2017, 4:09 pm

Addition: <https://pastebin.com/RydPUS1P>

Frst: <https://pastebin.com/6RTufuUh>

NeverForgotten. - August 29, 2017, 12:37 am

Do you still need help OP?

5chn4pp - August 29, 2017, 12:41 am

(Aug 29, 2017 12:37 AM)NeverForgotten. Wrote: [\[CITE\]](#) Do you still need help OP?

I'm busy af, trying to write the post today.

NeverForgotten. - August 29, 2017, 2:40 am

(Aug 29, 2017 12:41 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) I'm busy af, trying to write the post today. Okey ?

NeverForgotten. - August 31, 2017, 5:09 pm

You still need help OP?

I'll take a look tomorrow if bromo doesn't answer.