

Forum:[Hack Forums](#)

Thread: [FIXED, THX ALOT FOR UR HELP GUYS!](#)

tyrone913 - December 21, 2015, 2:59 am

FIXED, THX ALOT FOR UR HELP GUYS!

ProtectNull™ - December 21, 2015, 3:03 am

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

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 a log called FRST.txt in the same directory the tool is run from.

Please copy and paste the log back here

The first time the tool is run it generates another log (Addition.txt - also located in the same directory as FRST.exe/FRST64.exe). Please also paste that along with the FRST.txt into your reply.

tyrone913 - December 21, 2015, 3:08 am

FIXED, THX ALOT FOR UR HELP GUYS!

ProtectNull™ - December 21, 2015, 3:15 am

(Dec 21, 2015 04:08 AM)deeznuts Wrote: [\[CITE\]](#) FRST - <http://pastebin.com/yyrieA1c>

Addition - <http://pastebin.com/Yj3N4j7u>

Do you know what akamai is?

tyrone913 - December 21, 2015, 3:15 am

FIXED, THX ALOT FOR UR HELP GUYS!

ProtectNull™ - December 21, 2015, 3:18 am

(Dec 21, 2015 04:15 AM)deeznuts Wrote: [\[CITE\]](#) No. :3

Oh I see you have AVAST installed, akamai mostly shows up when people have AVAST installed.

tyrone913 - December 21, 2015, 3:18 am

FIXED, THX ALOT FOR UR HELP GUYS!

SlaterMLG - December 21, 2015, 3:21 am

(Dec 21, 2015 04:18 AM)deeznuts Wrote: [\[CITE\]](#) Oh okay. Am i infected or something? :Di dont know but those are some nice fuckin nuts bro

Spoiler [\(Click to View\)](#)im wasted

tyrone913 - December 21, 2015, 3:22 am

(Dec 21, 2015 04:21 AM)SlaterMLG Wrote: [\[CITE\]](#) i dont know but those are some nice fuckin nuts bro

Imao hahahahahah

ProtectNull™ - December 21, 2015, 3:25 am

(Dec 21, 2015 04:18 AM)deeznuts Wrote: [\[CITE\]](#) Oh okay. Am i infected or something? :D
From the FRST logs, I see nothing, but luminositylink (is this a genuine copy?) I guess you'll have to wait for Polymorphic Plague.

I'll look further into your logs if I see anything wrong.

tyrone913 - December 21, 2015, 3:28 am

FIXED, THX ALOT FOR UR HELP GUYS!

ProtectNull™ - December 21, 2015, 3:30 am

Btw, if Poly or Knautschtabak needs a TDSSKiller log, please do so.
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.

(Dec 21, 2015 04:28 AM)deeznuts Wrote: [\[CITE\]](#) Luminositylink? I dont have that?
Really? Its saved into your desktop?

C:\users\nybruger\desktop\all my hax shit\luminositylink.exe

If you are unsure you've downloaded this, please let us know.

tyrone913 - December 21, 2015, 3:33 am

FIXED, THX ALOT FOR UR HELP GUYS!

ProtectNull™ - December 21, 2015, 3:35 am

(Dec 21, 2015 04:33 AM)deeznuts Wrote: [\[CITE\]](#) I haven't downloaded it myself, but now when i clicked it and ran it, it seems like it isn't a rat, but i'm removing it. It could be my brother tbh.
Please do a TDSSKiller Log.

tyrone913 - December 21, 2015, 3:38 am

FIXED, THX ALOT FOR UR HELP GUYS!

Knautschtabak - December 21, 2015, 4:32 am

I can check your system, but be aware that I will be slow to respond between 23. December and 1. January due to the holidays. If you want my assistance nevertheless, follow the instructions below.

Please read through the points below before we start. Read my instructions thoroughly, and carry out each step in the specified order.

Do not run any tools or take any steps other than those I provide for you. Independent efforts may make matters worse, and will affect my ability in providing the best set of instructions for you.

Please backup important files before proceeding with my instructions. Malware removal can be unpredictable at times.

If you come across any issues, please stop and inform me of the issue in detail. Do not hesitate to ask before proceeding.

I will notify you when I believe your computer is free of malware. The absence of symptoms does not necessarily mean that your computer is clean.

If I do not reply within 48 hours, write a PM. I might have just overlooked your thread. Keep in mind that we likely live in different time zones.

I might abandon your thread if you do not reply within five days. I take only as many logs as I can handle.

Step 1: Uninstall Software Press the Windows Key + r on your keyboard at the same time. Type appwiz.cpl and click OK.

Search for the following programs, right-click and click Uninstall. MyBrowser

Follow the prompts.

Note: If you are offered the choice to install additional software, ensure you decline.

Reboot if necessary.

Junkware Removal Tool (JRT) Please download [Junkware Removal Tool](#) and save the file to your Desktop.

Temporarily disable your anti-virus software. For instructions, please refer to the following [link](#).

Right-Click JRT.exe and select Run as administrator to run the program.

Follow the prompts and allow the scan to run uninterrupted.

Upon completion, a log (JRT.txt) will open on your desktop.

Re-enable your anti-virus software

Copy the contents of JRT.txt to pastebin.com and paste the link in your next reply.

AdwCleanerPlease download [AdwCleaner](#) and save the file to your Desktop.

Right-Click AdwCleaner.exe and select Run as administrator to run the program.

Follow the prompts.

Click Scan.

Upon completion, click Logfile. A log (AdwCleaner[R0].txt) will open. Briefly check the log for anything you know to be legitimate.

Ensure anything you know to be legitimate does not have a checkmark, and click Clean.

Follow the prompts and allow your computer to reboot.

After rebooting, a log (AdwCleaner[S0].txt) will open. Copy the contents of the log to pastebin.com and paste the links in your next reply.

-- File and folder backups are made for items removed using this tool. Should a legitimate file or folder be removed (otherwise known as a 'false-positive'), simple steps can be taken to restore the item. Please do not overly concern yourself with the contents of AdwCleaner[R0].txt.

In your next reply I get from youDid you successfully uninstall MyBrowser?

JRT log

AdwCleaner log

tyrone913 - December 21, 2015, 4:51 am

FIXED, THX ALOT FOR UR HELP GUYS!

Knautschtabak - December 21, 2015, 5:46 am

You have iObit software installed. iObit has a very bad reputation. See some of the articles below.

[IObit Steals Malwarebytes' Intellectual Property](#)

[IObit's Denial of Theft Unconvincing](#)

[IObit Theft Conclusion](#)

[IObit: Trusting Your Antivirus Vendor](#)

[Malwarebytes: IObit Stole Our Signatures Database](#)

[IObit accused of stealing from Malwarebytes](#)

[IObit sucks at ethics](#)

I suggest that you deinstall this software, because I would not trust this company, but the decision is up to you.

Step 1: Farbar Recovery Scan Tool (FRST) Script
Press the Windows Key + r on your keyboard at the same time. Type Notepad and click OK.

Copy the entire contents of the codebox below and paste into the Notepad document.

Code start

CreateRestorePoint:

InternetURL: C:\Users\Nybruger\AppData\Roaming\Microsoft\Windows\Start

Menu\Programs\Startup\2.com.url -> 0

HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Main,Default_Search_URL =

StartMenuInternet: IEXPLORE.EXE - iexplore.exe

CMD: ipconfig /flushdns

EmptyTemp:

end

Click File, Save As and type fixlist.txt as the File Name.

Important: The file must be saved in the same location as FRST.exe.

NOTICE: This script is intended for use on this particular machine. Do not use this script on any other machine; doing so may cause damage to your Operating System. Double-Click FRST.exe to run the program.

Click Fix.

A log (Fixlog.txt) will open on your desktop. Copy the contents of the log to pastebin.com and paste the link to it in your next reply.

Step 2: Uninstall Outdated Software
Press the Windows Key + r on your keyboard at the same time. Type appwiz.cpl and click OK.

Search for the following programs, right-click and click Uninstall. Java 8 Update 60

Follow the prompts.

Note: If you are offered the choice to install additional software, ensure you decline.

Reboot if necessary.

Step 3: Update Outdated Software

Outdated software contain security risks that must be patched. Please download and install the latest version of the programmes below. [Adobe Flash Player](#)

Step 4: Re-Scan with FRSTDouble-Click FRST64.exe to run the programme

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.

In your next reply I get from youFixlog.txt

Fresh FRST logs (Addition.txt and FRST.txt)

Please tell me if there are any outstanding issues.

tyrone913 - December 21, 2015, 6:46 am

FIXED, THX ALOT FOR UR HELP GUYS!

Knautschtabak - December 21, 2015, 6:48 am

Congratulations, your computer appears clean! :)

I no longer see signs of malware on your computer, and feel satisfied that our work here is done. The steps below will remove the tools we have used, and reset any settings changed. I have also provided a list of resources and tools that you may find useful.

DelFixPlease download [DelFix](#) and save the file to your Desktop.

Double-click DelFix.exe to run the programme.

Place a checkmark next to the following items:Remove disinfection tools

Click the Run button.

-- This will remove the specialised tools we used to disinfect your system. Any leftover logs, files, folders or tools remaining on your Desktop which were not removed can be deleted manually (right-click the file + delete).

=====

I have compiled below a list of resources you may find useful. The articles document information on computer security, common infection vectors and how you can stay safe on the Internet. [Answers to common security questions - Best Practices](#) by quietman7, MVP

[How Malware Spreads - How did I get infected?](#) by quietman7, MVP

[Simple and easy ways to keep your computer safe and secure on the Internet](#) by Lawrence Abrams, MVP

[How to Prevent Malware](#) by miekiemoes, MVP

[How to backup and restore your data using Cobian Backup](#) by YourHighness

[Slow Computer/browser? It May Not Be Malware](#) by quietman7, MVP

The following programmes come highly recommended in the security community. [AdBlock](#) is a browser add-on that blocks annoying banners, pop-ups and video ads.

[CryptoPrevent](#) places policy restrictions on loading points for ransomware (eg. CryptoWall), helping prevent the execution of malware.

[Emsisoft Antimalware](#) (free) acts as an additional on-demand scanner, and can be used in conjunction with your Anti-Virus.

[Malwarebytes Anti-Exploit](#) (MBAE) is designed to prevent zero-day malware from exploiting vulnerable software.

[Malwarebytes Anti-Malware Premium](#) (MBAM) works in real-time along side your Anti-Virus to prevent malware execution.

[NoScript](#) is a Firefox add-on that blocks the actions of malicious scripts by using whitelisting and other technology.

[Sandboxie](#) isolates programmes of your choice, preventing files from being written to your HDD unless approved by you.

[Secunia PSI](#) will scan your computer for vulnerable software that is outdated, and automatically find the latest update for you.

[SpywareBlaster](#) is a form of passive protection, designed to block the actions of malicious websites and tracking cookies.

[Unchecky](#) automatically removes checkmarks for bundled software in programme installers; helping you avoid adware and PUPs.

[Web of Trust](#) (WOT) is a browser add-on designed to alert you before interacting with a potentially malicious website.

Need a second opinion on a file or website? Scan the file/URL before clicking by using one of the following free online scanner services. [VirusTotal](#) (File & URL)

[Jotti's Malware Scan](#) [/b][b](File)

[Dr.Web Online Check](#) (URL)

[Trend Micro Site Safety Center](#) (URL)

[Norton Safe Web](#) (URL)

-- Please feel free to ask if you have any questions or concerns on computer security or the programmes above.