

Forum:[Hack Forums](#)

Thread: [Downloaded a virus/RAT](#)

Snoopy - July 27, 2015, 3:40 pm

I'm pretty sure I've been infected with a virus, I've noticed random mouse movements, a command prompt (vbs.net?) running when I log in and also strange log-ins into my e-mail and PayPal (they even tried to buy something)

Scanned with MBAM multiple times but still nothing detected, can anyone please help

EDIT:

FRST: <http://pastebin.com/f6YAX8Pc>

Addition: <http://pastebin.com/WHzeFHEz>

k?'rlzm? - July 27, 2015, 3:42 pm

Download and run malware bytes

ze-slade - July 27, 2015, 3:42 pm

(Jul 27, 2015 03:40 PM)tahir. Wrote: [\[CITE\]](#) I'm pretty sure I've been infected with a virus, I've noticed random mouse movements, a command prompt (vbs.net?) running when I log in and also strange log-ins into my e-mail and PayPal (they even tried to buy something)

Scanned with MBAM multiple times but still nothing detected, can anyone please help
You're definatley infected with a rat then.

5chn4pp - July 27, 2015, 3:42 pm

(Jul 27, 2015 03:42 PM)Alpha Wolf Wrote: [\[CITE\]](#) Download and run malware bytes
are you retarded? Read the thread.

ze-slade - July 27, 2015, 3:43 pm

(Jul 27, 2015 03:42 PM)Alpha Wolf Wrote: [\[CITE\]](#) Download and run malware bytes
He already did that, read the op.

YungTrigz - July 27, 2015, 3:43 pm

(Jul 27, 2015 03:42 PM)Alpha Wolf Wrote: [\[CITE\]](#) Download and run malware bytes
MBAM Means Malware Bytes, Don't make random suggestions.

Finestquad - July 27, 2015, 3:44 pm

Hit me up with your Teamviewer or Join.me i can help you:)

k?'rlzm? - July 27, 2015, 3:44 pm

Fuck me sorry I'm tired and shit.

Give me a break

YungTrigz - July 27, 2015, 3:45 pm

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.

Please don't join that persons TV session or join.me.

Networx - July 27, 2015, 3:53 pm

PM your Skype. I can help you out.

Snoopy - July 27, 2015, 3:55 pm

(Jul 27, 2015 03:45 PM)YungTrigz Wrote: [\[CITE\]](#) 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.

Please don't join that persons TV session or join.me.

FRST: <http://pastebin.com/f6YAX8Pc>

Addition: <http://pastebin.com/WHzeFHEz>

I wouldn't think of it but thank you

President Morty - July 28, 2015, 6:18 am

Did you happen to add this to your startup?

C:\Users\Tahir\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Client.jar

C:\Users\Tahir\AppData\Roaming\1115448083.jar

Sketchy as fuck .jar

C:\Users\Tahir\AppData\Local\Temp\lose00000.exe

O_o I searched and found it as a windows process or something for a reader for like PDFs, I have no idea what that is.

Im just pointing out some odd files.

Dont do anything unless a trained malware specalist (2tired2care4spelling) comes by to review your logs.

Snoopy - July 28, 2015, 7:26 am

(Jul 28, 2015 06:18 AM)L_USER Wrote: [\[CITE\]](#) Did you happen to add this to your startup?

C:\Users\Tahir\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Client.jar

C:\Users\Tahir\AppData\Roaming\1115448083.jar

Sketchy as fuck .jar

C:\Users\Tahir\AppData\Local\Temp\ose00000.exe

O_o I searched and found it as a windows process or something for a reader for like PDFs, I have no idea what that is.

Im just pointing out some odd files.

Dont do anything unless a trained malware specialist (2tired2care4spelling) comes by to review your logs.

I'm only aware of the Client.jar and that's from myself, but the others I'm not sure. Thank you, I will wait.

YungTrigz - July 28, 2015, 7:58 am

You seem to be infected, I have no training so I wouldn't try and make you a fixlist or something like that, What I do recommend is you PM Knaut Or Charmz With a link to your thread, if you do not receive help within 12 hours I will pm you a link somewhere you will get help quicker.

Snoopy - July 28, 2015, 8:43 am

(Jul 28, 2015 07:58 AM)YungTrigz Wrote: [\[CITE\]](#) You seem to be infected, I have no training so I wouldn't try and make you a fixlist or something like that, What I do recommend is you PM Knaut Or Charmz With a link to your thread, if you do not receive help within 12 hours I will pm you a link somewhere you will get help quicker.

Will do, thank you. I haven't noticed anything strange since last night after changing all my passwords and scanning my computer. I also didn't get the "vbs.net" command prompt when I signed in this time but I'll still wait for help just to be safe

Knautschtabak - July 29, 2015, 12:05 am

Hello tahir.

Please read through the points below to ensure this process moves as quickly and efficiently as possible. Ensure you read through my instructions thoroughly, and carry out each step in the order specified.

Please 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 whilst following my instructions, please stop and inform me of the issue in as much detail as possible. Please do not hesitate to ask before proceeding.

I will notify you when I believe your computer is free of malware. Please bear in mind, absence of symptoms does not necessarily correlate to absence of malware, so please wait until the "All Clean".

You have no Antivirus installed. Is there any particular reason for it?

You have a Java Backdoor on your system that is known by the detection name Artemis Backdoor. Before we start removal I need to check some entries of your logs.

Step 1: Folder Options Press the Windows Key + r on your keyboard at the same time. Type Control Folders and click OK.

Click View. Under Hidden files and folders:

Place a checkmark next to Show hidden files, folders and drives.

Remove the checkmark next to Hide extensions for known file types.

Remove the checkmark next to Hide protected operating system Files (Recommended).

Click Apply followed by OK.

Step 2: VirusTotal UploadPlease go to [VirusTotal.com](https://www.virustotal.com).

Click Choose File and locate the following file:

C:\Users\Tahir\AppData\Local\Google\Chrome\User Data\Default\Extensions\
bknhkbghgkjlhioehiclhcgjiaooeg

Click Scan it!.

If you receive the following notification: File already analysed click Reanalyse.

Once the file has been analyzed, copy the page URL at the top of the window and paste in your next reply.

Please do the same for the files below:C:\Users\Tahir\AppData\Roaming\programs.vc

Step 3: Farbar Recovery Scan Tool (FRST) ScriptPress 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:

Folder: C:\ProgramData\E1864A66-75E3-486a-BD95-D1B7D99A84A7

Folder: C:\Users\Tahir\AppData\Roaming\4185E59E-AFA6-40EF-9F80-1F7D07CF3218

Folder: C:\ProgramData\Windows Services

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. Right-Click FRST.exe and select Run as administrator 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.

Snoopy - July 29, 2015, 11:58 am

(Jul 29, 2015 12:05 AM)Knautschtabak Wrote: [\[CITE\]](#) Hello tahir.

Please read through the points below to ensure this process moves as quickly and efficiently as possible. Ensure you read through my instructions thoroughly, and carry out each step in the order specified.

Please 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 whilst following my instructions, please stop and inform me of the issue in as much detail as possible. Please do not hesitate to ask before proceeding.

I will notify you when I believe your computer is free of malware. Please bear in mind, absence of symptoms does not necessarily correlate to absence of malware, so please wait until the "All Clean".

You have no Antivirus installed. Is there any particular reason for it?

You have a Java Backdoor on your system that is known by the detection name Artemis Backdoor. Before we start removal I need to check some entries of your logs.

Step 1: Folder Options Press the Windows Key + r on your keyboard at the same time. Type Control Folders and click OK.

Click View. Under Hidden files and folders:

Place a checkmark next to Show hidden files, folders and drives.

Remove the checkmark next to Hide extensions for known file types.

Remove the checkmark next to Hide protected operating system Files (Recommended).

Click Apply followed by OK.

Step 2: VirusTotal UploadPlease go to [VirusTotal.com](https://www.virustotal.com).

Click Choose File and locate the following file:

C:\Users\Tahir\AppData\Local\Google\Chrome\User Data\Default\Extensions\
bknhkbghgkjljioehiclhcgjiiiaoeg

Click Scan it!.

If you receive the following notification: File already analysed click Reanalyse.

Once the file has been analyzed, copy the page URL at the top of the window and paste in your next reply.

Please do the same for the files below:C:\Users\Tahir\AppData\Roaming\programs.vc

Step 3: Farbar Recovery Scan Tool (FRST) ScriptPress 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:

Folder: C:\ProgramData\E1864A66-75E3-486a-BD95-D1B7D99A84A7

Folder: C:\Users\Tahir\AppData\Roaming\4185E59E-AFA6-40EF-9F80-1F7D07CF3218

Folder: C:\ProgramData\Windows Services

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.Right-Click FRST.exe and select Run as administrator 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.

Thank you for your reply. I assumed Malwarebytes Antimalware counts as an antivirus? If not,

which one would you recommend?

When I navigate to C:\Users\Tahir\AppData\Local\Google\Chrome\User Data\Default\Extensions\bknhkbghgkjlloehiclhcgjiaooeg there is only a list of folders, this particular folder contains 2 files, Cached Theme.pak and manifest.json. It also contains an image folder which contains a few images which I recognise from a custom chrome theme I made a while back.

I'm presuming the other folders contain chrome extension files (based on the names of the files within them)

Scan for programs.vc:

<https://www.virustotal.com/en/file/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855/analysis/1438182918/>

fixlist.txt: <http://pastebin.com/2ak3hbdc>

Knautschtabak - July 29, 2015, 11:54 pm

These folders

C:\ProgramData\541099

C:\ProgramData\541199

C:\Users\Tahir\AppData\Roaming\4185E59E-AFA6-40EF-9F80-1F7D07CF3218

contain log files. The first two are definitely from the RAT, not sure about the third. You may take a look into them to see what the RAT captured. Note: The FRST fix will remove the RAT folders.

You have disabled entries in msconfig that are related to your Babylon RAT. If you really want to get rid of them, you should remove Babylon.

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:

CloseProcesses:

Reg: reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run /v "Client.jar" /f

Reg: reg delete

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder /v "Client.jar" /f

HKU\S-1-5-21-2553393960-3600394711-1477681348-1007\...\RunOnce: [Babylon RAT] =>

C:\ProgramData\Babylon RAT\client.exe

Startup: C:\Users\Tahir\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Client.jar [2015-07-27] ()

HKU\S-1-5-21-2553393960-3600394711-1477681348-1007\Software\Classes\exefile: <===== ATTENTION!

2015-07-27 01:09 - 2015-07-27 01:09 - 00244792 _____

C:\Users\Tahir\AppData\Roaming\1115448083.jar

2015-07-27 01:03 - 2015-07-27 01:03 - 00031232 _____ (Microsoft)

C:\Users\Tahir\Documents\usersdat.exe

2015-07-27 00:58 - 2015-07-27 23:19 - 00000000 __SHD C:\ProgramData\541099

2015-07-27 00:58 - 2015-07-27 00:58 - 00000006 __RSH

```
C:\ProgramData\7433cdb324b04dd5e3c3db213381216c7c539baa
2015-07-27 00:58 - 2015-07-27 00:58 - 000000 __SHD C:\ProgramData\541199
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_1600531638122434154.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_1953036125835962126.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_3109344135661366674.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_3942053402218933952.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_5122581650076520125.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_668736564603157120.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_7875434675044394057.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_8917667986274682635.dll
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. Right-Click FRST.exe and select Run as administrator 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.

Snoopy - July 30, 2015, 6:24 am

(Jul 29, 2015 11:54 PM)Knautschtabak Wrote: [\[CITE\]](#) These folders

```
C:\ProgramData\541099
C:\ProgramData\541199
C:\Users\Tahir\AppData\Roaming\4185E59E-AFA6-40EF-9F80-1F7D07CF3218
```

contain log files. The first two are definitely from the RAT, not sure about the third. You may take a look into them to see what the RAT captured. Note: The FRST fix will remove the RAT folders.

You have disabled entries in msconfig that are related to your Babylon RAT. If you really want to get rid of them, you should remove Babylon.

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:
CloseProcesses:
Reg: reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
/v "Client.jar" /f
Reg: reg delete
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder /v
```

```
"Client.jar" /f
HKU\S-1-5-21-2553393960-3600394711-1477681348-1007\...\RunOnce: [Babylon RAT] =>
C:\ProgramData\Babylon RAT\client.exe
Startup: C:\Users\Tahir\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\Client.jar [2015-07-27] ()
HKU\S-1-5-21-2553393960-3600394711-1477681348-1007\Software\Classes\exefile: <=====
ATTENTION!
2015-07-27 01:09 - 2015-07-27 01:09 - 00244792 _____
C:\Users\Tahir\AppData\Roaming\1115448083.jar _____
2015-07-27 01:03 - 2015-07-27 01:03 - 00031232 _____ (Microsoft)
C:\Users\Tahir\Documents\usersdat.exe
2015-07-27 00:58 - 2015-07-27 23:19 - 0000000 __SHD C:\ProgramData\541099
2015-07-27 00:58 - 2015-07-27 00:58 - 00000006 __RSH
C:\ProgramData\7433cdb324b04dd5e3c3db213381216c7c539baa
2015-07-27 00:58 - 2015-07-27 00:58 - 0000000 __SHD C:\ProgramData\541199
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_1600531638122434154.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_1953036125835962126.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_3109344135661366674.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_3942053402218933952.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_5122581650076520125.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_668736564603157120.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_7875434675044394057.dll
C:\Users\Tahir\AppData\Local\Temp\JNativeHook_8917667986274682635.dll
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. Right-Click FRST.exe and select Run as administrator 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.

Thank you for your reply. The folder C:\Users\Tahir\AppData\Roaming\4185E59E-AFA6-40EF-9F80-1F7D07CF3218 just contains a few .dat files, and a settings.bin file. I've also installed AVG Internet security 2015 as an antivirus alongside MBAM, and ran a whole computer scan, so maybe that's why some of the files are missing in the fixlist.txt?

I've also removed Babylon

fixlist.txt: <http://pastebin.com/NiVJXrca>

PureLegend - July 30, 2015, 9:00 am

Did u download any software from any torrent search website? Try to delete em ASAP, coz alot of russian dudes likes to put rats into cracked software. Also Knautschtabak seems to be much helpful

then me,so just follow his steps

Knautschtabak - July 30, 2015, 11:24 pm

Please check my ground rules again. They say:

Quote:Please 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.

If you are doing things on your own like system scans, you are making it hard for me to provide the best advice.

The fix seemed to work except for one detail. How is your computer doing?

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

Right-Click DeIFix.exe and click Run as administrator.

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

Place a checkmark next to the following items:Create registry backup

Click the Run button.

Reg Fix 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 Windows Registry Editor Version 5.00

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]
```

```
"Client.jar"=-
```

Click Format. Ensure Wordwrap is unchecked.

Click File, Save As and name the file regfix.reg.

Select All Files as the Save as type.

Save the file to your Desktop.

Locate regfix.reg on your Desktop. Right-Click the file and click Merge with the Registry.

Accept any prompts.

Reboot your computer for the changes to take effect.

Snoopy - July 31, 2015, 8:38 am

(Jul 30, 2015 11:24 PM)Knautschtabak Wrote: [\[CITE\]](#) Please check my ground rules again. They say:

If you are doing things on your own like system scans, you are making it hard for me to provide the best advice.

The fix seemed to work except for one detail. How is your computer doing?

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

Right-Click DelFix.exe and click Run as administrator.

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

Place a checkmark next to the following items:Create registry backup

Click the Run button.

Reg Fix 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 Windows Registry Editor Version 5.00

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]
"Client.jar"=-
```

Click Format. Ensure Wordwrap is unchecked.

Click File, Save As and name the file regfix.reg.

Select All Files as the Save as type.

Save the file to your Desktop.

Locate regfix.reg on your Desktop. Right-Click the file and click Merge with the Registry.

Accept any prompts.

Reboot your computer for the changes to take effect.

Sorry it's just that you pointed out that I had no antivirus.

I've done everything that you said so far. I know you said absence of symptoms doesn't mean I'm clean but I haven't noticed any strange behaviour or any strange logins since.

What should I do now?

Knautschtabak - July 31, 2015, 10:26 am

If you did the registry fix, post fresh FRST logs (including Addition.txt), so I can confirm that the bad entries are gone.

Farbar Recovery Scan Tool (FRST) ScanRight-Click FRST64.exe and select Run as Administrator

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.

Snoopy - July 31, 2015, 2:48 pm

(Jul 31, 2015 10:26 AM)Knautschtabak Wrote: [\[CITE\]](#) If you did the registry fix, post fresh FRST logs (including Addition.txt), so I can confirm that the bad entries are gone.

Farbar Recovery Scan Tool (FRST) ScanRight-Click FRST64.exe and select Run as Administrator

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.

FRST.txt (exceeded pastebin size limit): <http://paste2.org/ZWV1B6xg>

Addition.txt: <http://pastebin.com/sTGqjbWw>

Dedsec34 - July 31, 2015, 6:40 pm

bro just open the taskbar and search for weird name server that has exe in it and locate file delete everything and end task and your good to go even more help download AVG its free and perfect protection

Nuworld - July 31, 2015, 8:39 pm

(Jul 31, 2015 06:40 PM)Dedsec34 Wrote: [\[CITE\]](#) bro just open the taskbar and search for weird name server that has exe in it and locate file delete everything and end task and your good to go even more help download AVG its free and perfect protection

Why are you interfering with the work of an Expert?

Your advise is miss cured.

Knautschtabak - August 1, 2015, 1:15 pm

Your logs look good now.

DelFixPlease download [DeFix](#) 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).

Snoopy - August 1, 2015, 1:33 pm

(Aug 1, 2015 01:15 PM)Knautschtabak Wrote: [\[CITE\]](#) Your logs look good now.

DelFixPlease download [DeFix](#) 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).

Thank you so much for your help!