

Forum: [Hack Forums](#)

Thread: [Parent's Computer Infected with adware, Still Infected](#)

Sennheiser - July 21, 2015, 7:41 pm

When it was infected by the adware

I ran
Malwarebytes Scan
Adwcleaner
JRT
then reset internet settings
deleted all junky programs that were unneeded

(there is hijackthis on there, but I didn't use it as I don't know how)

I ran an FRST scan after this so these logs are up to date with no changes made after the logs were posted

FRST Logs: <http://pastebin.com/uXH8ghM2>
Addition Logs: <http://pastebin.com/15rRm3Tq>

(Set to expire in a week)

After all I did, the adware or worse is still on there.

Thanks

Sleeping With Sirens - July 21, 2015, 7:42 pm

If the adware is gone, you should be good. You went a bit overkill with the software, so I'm almost 100% it's gone.

Sennheiser - July 21, 2015, 7:48 pm

(Jul 21, 2015 07:42 PM)Sleeping With Sirens Wrote: [\[CITE\]](#) If the adware is gone, you should be good. You went a bit overkill with the software, so I'm almost 100% it's gone.
Just wanting to make sure there aren't any more problems with the PC

like hidden malware or anything out of the ordinary.

Still get some ads popped on a new page on occasion but not as excessive as before the scans

.waste - July 21, 2015, 8:02 pm

There are still some remnants of AdWare.

C:\Program Files\shopperz20072015\Rofdhowal.exe (I recommend deleting the directory)

lel.exe is located in %APPDATA%

Not sure why its there, but I'm sure you can remove it without harm to the system.

Sennheiser - July 21, 2015, 11:19 pm

Still need help with this

Getting a few pop up's still where they shouldn't be

Knautschtabak - July 22, 2015, 12:45 pm

The core of your problem is (imo) your cracked software. As long as you keep it, I don't think that cleaning will have much effect (is your OS legally activated?). I could still attempt to clean the computer, though.

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".

Step 1: Potentially Unwanted

The following programs are potentially unwanted. They may bundle third party software, show ads, be on your computer without your consent or have questionable policies and behaviour. Please tell me for each of the following programs if you want to keep it. Shop for HP Supplies

HP Games

Sennheiser - July 22, 2015, 1:01 pm

(Jul 22, 2015 12:45 PM)Knautschtabak Wrote: [\[CITE\]](#) The core of your problem is (imo) your cracked software. As long as you keep it, I don't think that cleaning will have much effect (is your OS legally activated?). I could still attempt to clean the computer, though.

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".

Step 1: Potentially Unwanted

The following programs are potentially unwanted. They may bundle third party software, show ads, be on your computer without your consent or have questionable policies and behaviour. Please tell me for each of the following programs if you want to keep it. Shop for HP Supplies

HP Games

Only thing that was cracked was the microsoft word, that has been there for over a year now.

Everything else was legitimate, the OS is legitimate

this is the pop up by the way

happens randomly, same one on any website i go to.

This started occuring almost a month ago

Knautschtabak - July 22, 2015, 1:17 pm

Please answer my question in Step 1. I need to know that before I give further instructions.

Sennheiser - July 22, 2015, 1:19 pm

(Jul 22, 2015 01:17 PM)Knautschtabak Wrote: [\[CITE\]](#) Please answer my question in Step 1. I need to know that before I give further instructions.

Just uninstalled both, neither have been used or ever will be

Knautschtabak - July 22, 2015, 1:33 pm

Before proceeding, please refer to the following instructions on how you can backup your Favourites/Bookmarks.

Chrome: [Backup Chrome Bookmarks](#)

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. Google Chrome

Follow the prompts.

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

Reboot if necessary.

Step 2: 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:

Task: {35452BF9-F991-42D2-94EB-3B334557D195} - \UHOWNOIMD1 No Task File <====

ATTENTION

Task: {462E5313-515C-4550-B764-4DCE3250F552} -

System32\Tasks\{A67787CD-A164-433A-9909-AB5F4899E317} => pcalua.exe -a F:\setup.exe -d F:\

Task: {58554D59-239B-4052-AB7F-B9667A5CE017} - System32\Tasks\FileInspect =>

c:\programdata\{e1bdf08d-aacb-44f9-e1bd-df08daacc236}\7924848117679966134b.exe <====

ATTENTION

c:\programdata\{e1bdf08d-aacb-44f9-e1bd-df08daacc236}

Task: {603A0DAA-F350-42F7-971F-7897D35A33BD} - System32\Tasks\LearningBuddy =>

c:\programdata\{a920362e-836d-3059-a920-0362e836d8ba}\sky full of stars.exe <====

ATTENTION

c:\programdata\{a920362e-836d-3059-a920-0362e836d8ba}

Task: {70EB27CF-6A85-4CCD-9F2A-4B7725BBD5E0} -

System32\Tasks\E8471924-F9BB-4F74-824A-61FF96368878 => C:\Users\Muya

Family\AppData\Local\E8471924-F9BB-4F74-824A-61FF96368878\E8471924-F9BB-4F74-824A-61FF96368878.exe <==== ATTENTION

C:\Users\Muya Family\AppData\Local\E8471924-F9BB-4F74-824A-61FF96368878

Task: {97E9625A-093F-4E93-AE2D-D74470D0123C} - \QQNFUKGLJYSQVWRQ No Task File

<==== ATTENTION

Task: {B32C7C4E-5B93-4878-AC16-D0BF5C0AC528} -

System32\Tasks\{2D9A134D-EEBB-44AF-A392-6B5525C9BF39} => pcalua.exe -a "C:\Users\Muya Family\AppData\Local\Temp\Temp1_Read_Aloud_2[1].zip\setup.exe"

Task: {CF44606A-D4C5-418E-97A8-B51BF8D3328B} -

System32\Tasks\{D8290197-B144-4D7C-81D6-D35E27297515} => pcalua.exe -a

C:\PROGRA~2\Yahoo!\Common\UNATT_~1.EXE

Task: C:\Windows\Tasks\LearningBuddy.job =>

c:\programdata\{a920362e-836d-3059-a920-0362e836d8ba}\sky full of stars.exe <====

ATTENTION

Task: C:\Windows\Tasks\QQNFUKGLJYSQVWRQ.job =>

C:\ProgramData\Service1291\Service1291.exe <==== ATTENTION

C:\ProgramData\Service1291

C:\Users\Muya Family\AppData\Local\Temp\Temp1_Read_Aloud_2[1].zip

ShellIconOverlayIdentifiers: [DropboxExt1] -> {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}

=> No File

ShellIconOverlayIdentifiers: [DropboxExt2] -> {FB314EDA-A251-47B7-93E1-CDD82E34AF8B}

=> No File

ShellIconOverlayIdentifiers: [DropboxExt3] -> {FB314EDB-A251-47B7-93E1-CDD82E34AF8B}

=> No File

ShellIconOverlayIdentifiers: [DropboxExt4] -> {FB314EDC-A251-47B7-93E1-CDD82E34AF8B}

=> No File

CHR HKLM\SOFTWARE\Policies\Google: Policy restriction <===== ATTENTION

HKU\S-1-5-21-1255986293-1186383839-1666926913-1001\Software\Microsoft\Internet

Explorer\Main,Secondary Start Pages = http://aol.com/

SearchScopes: HKLM -> {37B0E162-0ECD-4FF8-B1CB-139434BB2D5C} URL =

http://www.bing.com/search?q={searchTerms}&form=HPDTRDF&pc=HPDTRDF&src=IE-SearchBox

SearchScopes: HKLM-x32 -> {37B0E162-0ECD-4FF8-B1CB-139434BB2D5C} URL =

http://www.bing.com/search?q={searchTerms}&form=HPDTRDF&pc=HPDTRDF&src=IE-SearchBox

SearchScopes: HKU\DEFAULT -> DefaultScope {0633EE93-D776-472f-A0FF-E1416B8B2E3A}

URL =

SearchScopes: HKU\S-1-5-19 -> DefaultScope {0633EE93-D776-472f-A0FF-E1416B8B2E3A} URL

=

SearchScopes: HKU\S-1-5-20 -> DefaultScope {0633EE93-D776-472f-A0FF-E1416B8B2E3A} URL

=

Toolbar: HKU\S-1-5-21-1255986293-1186383839-1666926913-1001 -> No Name -

{7FEBEFE3-6B19-4349-98D2-FFB09D4B49CA} - No File

FF HKLM-x32\...\Firefox\Extensions: [{1457d95f-dd62-4e3c-820f-ccef2bea9201}] - C:\Program Files\shopperz20072015\Firefox

C:\Program Files\shopperz20072015

FF HKLM\...\Firefox\Extensions: [{1457d95f-dd62-4e3c-820f-ccef2bea9201}] - C:\Program Files\shopperz20072015\Firefox

S3 Rofdhawal; C:\Program Files\shopperz20072015\Rofdhawal.exe [X]

S1 njchnjyz; \??\C:\Windows\system32\drivers\njchnjyz.sys [X]

C:\Windows\system32\drivers\njchnjyz.sys

S1 rwfvacnz; \??\C:\Windows\system32\drivers\rwfvacnz.sys [X]

C:\Windows\system32\drivers\rwfvacnz.sys

Folder: C:\KVRT_Data

Folder: C:\Program1

C:\Users\Muya Family\AppData\Roaming\lcl.exe

C:\Users\Muya Family\AppData\Roaming\Adobe Flash Player Update.il

2011-10-10 22:41 - 2011-10-10 22:41 - 0006207 _____ () C:\Users\Muya Family\AppData\Local\tmpFOOTBALL7.0

2011-10-10 22:41 - 2011-10-10 22:41 - 0005434 _____ () C:\Users\Muya Family\AppData\Local\tmpFOOTBALL7.JPG

2013-08-23 01:55 - 2013-08-23 01:55 - 1662380 _____ () C:\Users\Muya Family\AppData\Local\tmpIMG_0100.0

2013-08-23 01:55 - 2013-08-23 01:55 - 0596356 _____ () C:\Users\Muya Family\AppData\Local\tmpIMG_0100.1

2013-08-23 01:55 - 2013-08-23 01:55 - 0596353 _____ () C:\Users\Muya Family\AppData\Local\tmpIMG_0100.10

2013-08-23 01:55 - 2013-08-23 01:55 - 0596383 _____ () C:\Users\Muya Family\AppData\Local\tmpIMG_0100.2

2013-08-23 01:55 - 2013-08-23 01:55 - 0596311 _____ () C:\Users\Muya Family\AppData\Local\tmpIMG_0100.3

2013-08-23 01:55 - 2013-08-23 01:55 - 0596311 _____ () C:\Users\Muya Family\AppData\Local\tmpIMG_0100.4

2013-08-23 01:55 - 2013-08-23 01:55 - 0596311 _____ () C:\Users\Muya Family\AppData\Local\tmpIMG_0100.5

2013-08-23 01:55 - 2013-08-23 01:55 - 0596353 _____ () C:\Users\Muya Family\AppData\Local\tmpIMG_0100.6

2013-08-23 01:55 - 2013-08-23 01:55 - 0596353 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0100.7
2013-08-23 01:55 - 2013-08-23 01:55 - 0596353 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0100.8
2013-08-23 01:55 - 2013-08-23 01:55 - 0596353 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0100.9
2013-08-23 01:55 - 2013-08-23 01:55 - 0596353 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0100.JPG
2013-08-23 01:55 - 2013-08-23 01:55 - 2008728 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0105.0
2013-08-23 01:55 - 2013-08-23 01:55 - 0770063 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0105.1
2013-08-23 01:55 - 2013-08-23 01:55 - 0770021 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0105.2
2013-08-23 01:55 - 2013-08-23 01:55 - 0770025 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0105.3
2013-08-23 01:55 - 2013-08-23 01:55 - 0770107 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0105.JPG
2013-08-23 01:54 - 2013-08-23 01:53 - 1867599 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0106.0
2013-08-23 01:54 - 2013-08-23 01:54 - 0718919 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0106.1
2013-08-23 01:54 - 2013-08-23 01:54 - 0718892 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0106.2
2013-08-23 01:54 - 2013-08-23 01:54 - 0718919 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0106.JPG
2011-04-14 23:27 - 2011-04-14 23:27 - 0101731 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0376.0
2011-04-14 23:27 - 2011-04-14 23:27 - 0040055 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0376.JPG
2012-01-10 10:54 - 2012-01-10 10:53 - 2176959 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0480.JPG
2011-03-21 18:08 - 2011-03-21 18:08 - 2824769 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0541.JPG
2011-03-21 18:07 - 2011-03-21 18:04 - 3166717 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_0544.JPG
2011-01-12 21:36 - 2011-01-12 21:36 - 2445495 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_1460.0
2011-01-12 21:36 - 2011-01-12 21:36 - 0922769 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_1460.JPG
2012-10-07 21:32 - 2012-10-07 21:31 - 1909241 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_4246.JPG
2014-05-12 00:51 - 2014-05-12 00:51 - 1140633 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_4329.JPG
2014-05-12 00:51 - 2014-05-12 00:51 - 0005647 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_4329_navi.JPG
2014-05-12 00:50 - 2014-05-12 00:50 - 1669011 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_4330.0
2014-05-12 00:50 - 2014-05-12 00:50 - 0705346 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_4330.1
2014-05-12 00:50 - 2014-05-12 00:50 - 0705207 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_4330.JPG
2014-05-12 00:50 - 2014-05-12 00:50 - 0008691 _____ () C:\Users\Muya

Family\AppData\Local\tmpIMG_4330_navi.JPG

2014-10-21 15:57 - 2014-10-21 15:57 - 000000 _____ () C:\Users\Muya Family\AppData\Local\{36754B80-A07E-4C65-9F72-CD0AE90A2634}
C:\Users\Muya Family\acrobatreader.exe
C:\Users\Muya Family\googleupdate.exe
C:\Users\Muya Family\jqcs.exe
C:\Users\Muya Family\teamviewer.exe
C:\Users\Muya Family\vlcplayer.exe
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Rofdhowal => ""="service"
AlternateDataStreams: C:\ProgramData\Temp\DFC5A2B2
CMD: bitsadmin /reset /allusers
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. 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.

Lorenzon - July 22, 2015, 1:38 pm

This might be a MITM attack since in my previous experience running
Malwarebytes Scan
Adwcleaner
JRT
then reset internet settings
deleted all junky programs that were unneeded
should get rid of 99% of adware.
What's your DNS settings on the infected computer?
Can be found by writing ipconfig /all
Also, how does your hosts file look like?

Knautschtabak - July 22, 2015, 1:42 pm

Quote:What's your DNS settings on the infected computer?
Also, how does your hosts file look like?

This is already shown by the given logs.
How do you want to fight malware if you don't even read the initial post properly?

Lorenzon - July 22, 2015, 1:48 pm

(Jul 22, 2015 01:42 PM)Knautschtabak Wrote: [\[CITE\]](#) This is already shown by the given logs.
How do you want to fight malware if you don't even read the initial post properly?
Sorry, just went through the post quickly and didn't read the logs and that's what came up on my

mind.

Sennheiser - July 22, 2015, 1:54 pm

I ran that fixlog and am going on the sites i usually use to make sure its gone

Knautschtabak - July 22, 2015, 1:58 pm

Please post the fixlog. We are not done yet. I included diagnostic instructions to it as well.

Edit: Also let me know how things are doing now.

Sennheiser - July 22, 2015, 1:59 pm

does bleeping computer get ads normally?

If so, I think it is all good now

Knautschtabak - July 22, 2015, 2:02 pm

(Jul 22, 2015 01:59 PM)Sennheiser Wrote: [\[CITE\]](#) does bleeping computer get ads normally?

If so, I think it is all good now

It should not show ads. And as I said, we are not done.

Sennheiser - July 22, 2015, 2:10 pm

(Jul 22, 2015 02:02 PM)Knautschtabak Wrote: [\[CITE\]](#) It should not show ads. And as I said, we are not done.

ok

ill run another frst scan so we can have updated logs

Additions: <http://pastebin.com/RSCsCtxH>

FRST: <http://pastebin.com/H3tNwFHg>

sorry, here is the fixlog as well <http://pastebin.com/jwZLEajM>

Knautschtabak - July 22, 2015, 10:55 pm

Sennheiser, this what normal advertisement on bleepingcomputer looks like:

While I was searching for ads yesterday, I did not find any, but these sponsored advertisements are in the download section.

If it is just that, you are fine.

You can now reinstall Chrome from here: <http://www.google.com/chrome/>

There is still something left.

Step 1: 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:

Task: C:\Windows\Tasks\FileInspect.job =>

```
c:\programdata\{e1bdf08d-aacb-44f9-e1bd-df08daacc236}\7924848117679966134b.exe <====  
ATTENTION  
c:\programdata\{e1bdf08d-aacb-44f9-e1bd-df08daacc236}  
Task: {CF44606A-D4C5-418E-97A8-B51BF8D3328B} -  
System32\Tasks\{D8290197-B144-4D7C-81D6-D35E27297515} => pcalua.exe -a  
C:\PROGRA~2\Yahoo!\Common\UNATT_~1.EXE  
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.

Step 2: RogueKillerDownload [RogueKiller \(x64\)](#) and save the file to your Desktop.

Close any running programs.

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

Allow the Prescan to complete. Upon completion, a window will open. Click Accept.

A browser window may open. Close the browser window.

Click . Upon completion, click .

Close the program. Do not fix anything!

A log (RKreport.txt) will be open. Copy the contents of the log to pastebin.com, click Submit and paste the link to it in your next reply.

Sennheiser - July 23, 2015, 2:51 pm

rougekiller log: <http://pastebin.com/ytV9srT2>

fixlog: <http://pastebin.com/PUHZyxAf>

Black_Georg - July 23, 2015, 2:54 pm

The only way to get rid of that malware is to FORMAT HDD! Do a clean system installation, it'll take you less time then searching for good anti-malware software.

Sennheiser - July 23, 2015, 2:57 pm

(Jul 23, 2015 02:54 PM)Black_Georg Wrote: [\[CITE\]](#) The only way to get rid of that malware is to FORMAT HDD! Do a clean system installation, it'll take you less time then searching for good anti-malware software.

<https://hackforums.net/showthread.php?tid=4557247>

focuss - July 23, 2015, 6:56 pm

These are the steps I would follow:

1. Go through Add/Remove program and remove any programs that look dodgy.
2. Do a full Malwarebytes Scan.
3. Go to start-->run and type in msconfig and click on the start-up tab and see if there is anything that doesn't look like a legit program there.
4. Right-click on your browser and go to properties and check the Target field.
If your using Firefox it should be something like this:
"C:\Program Files (x86)\Mozilla Firefox\firefox.exe"

Sometimes the path is modified with a spammy website.

5. Do a complete browser reset (recommend that you to save your bookmarks if you need them)
Depending on the browser your using the steps for this is different. Do a quick Google search on how to restore settings to default on your browser.

6. If you are still having issues it may be that Adobe Flash has been infected. Reinstall it.

Let me know if this did not fix the issues.

Knautschtabak - July 24, 2015, 8:05 am

RogueKiller FixClose any running programmes.

Right-Click RogueKiller.exe and select Run as administrator to run the programme.

Allow the Prescan to complete.

A browser window may open. Close the browser window.

Click .

Upon completion, do the following:

Click and place a checkmark next to the following items. Ensure any other items are unchecked.
[PUM.SearchPage] (X64)
HKEY_USERS\S-1-5-21-1255986293-1186383839-1666926913-1001\Software\Microsoft\Internet Explorer\Main | Search Bar : Preserve -> Found

[PUM.SearchPage] (X86)
HKEY_USERS\S-1-5-21-1255986293-1186383839-1666926913-1001\Software\Microsoft\Internet Explorer\Main | Search Bar : Preserve -> Found

[PUP] (X64) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows |
AppInit_DLLs : C:\ProgramData\FishBeats\FishBeats64.dll [x] -> Found

Click .

Click .

Copy the contents of the log and paste in your next reply.

Sennheiser - July 26, 2015, 3:40 pm

(Jul 24, 2015 08:05 AM)Knautschtabak Wrote: [\[CITE\]](#) RogueKiller FixClose any running programmes.

Right-Click RogueKiller.exe and select Run as administrator to run the programme.

Allow the Prescan to complete.

A browser window may open. Close the browser window.

Click .

Upon completion, do the following:

Click and place a checkmark next to the following items. Ensure any other items are unchecked.

[PUM.SearchPage] (X64)

HKEY_USERS\S-1-5-21-1255986293-1186383839-1666926913-1001\Software\Microsoft\Internet Explorer\Main | Search Bar : Preserve -> Found

[PUM.SearchPage] (X86)

HKEY_USERS\S-1-5-21-1255986293-1186383839-1666926913-1001\Software\Microsoft\Internet Explorer\Main | Search Bar : Preserve -> Found

[PUP] (X64) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows |
AppInit_DLLs : C:\ProgramData\FishBeats\FishBeats64.dll [x] -> Found

Click .

Click .

Copy the contents of the log and paste in your next reply.

done

<http://pastebin.com/1aK1D43t>

Knautschtabak - July 26, 2015, 11:14 pm

Well done.

Are there any outstanding issues with your computer?

You may re-run the adware cleaning tools now to get rid of leftovers.

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.

AdwCleaner Please 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.

Sleeping With Sirens - July 26, 2015, 11:15 pm

(Jul 23, 2015 02:54 PM)Black_Georg Wrote: [\[CITE\]](#) The only way to get rid of that malware is to FORMAT HDD! Do a clean system installation, it'll take you less time then searching for good anti-malware software.

I really suggest you leave this forum, bud.

Sennheiser - July 27, 2015, 1:38 am

JRT Logs: <http://pastebin.com/CzTYCgxV>

adwcleaner: <http://pastebin.com/Uav4rw6T>

I think it may be gone now, hasn't come up from what i've seen yet

Knautschtabak - July 27, 2015, 1:44 am

Looks good to me too. I think your computer is clean.

Let's wrap this up.

You have no AV installed. I suggest you get one.

Your current version of Flash Player is vulnerable. Update it to avoid infections via recent Flash exploits: <https://get.adobe.com/flashplayer/>

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).

Sennheiser - July 31, 2015, 7:57 pm

Ok, so after a few days.

The ads still keep popping up, however at a very small rate and random

meaning it is not as obtrusive as it was originally.

Any way to remove these ads?

They occur on sites they never did before

School site and aol

Sennheiser - August 6, 2015, 12:06 am

still getting the adware pop ups out of nowhere

i need help! ?

Starki - August 6, 2015, 12:27 am

Run fresh FRST logs, so we can try identify why you are still having this problem. ?

Sennheiser - August 14, 2015, 8:30 pm

(Aug 6, 2015 12:27 AM)Jam Jar Wrote: [\[CITE\]](#) Run fresh FRST logs, so we can try identify why you are still having this problem. ?

Additions log <http://pastebin.com/qBrU7fF3>

FRST Log <http://pastebin.com/ASQ8NXwV>

Sennheiser - August 17, 2015, 4:57 pm

i reposted the frst logs...

help me pls?