

Forum: [Hack Forums](#)

Thread: [Computer strange after installing and uninstalling a program](#)

Disgusting - January 31, 2016, 11:17 am

So i installed a VPN: <https://www.safervpn.net/>

It didn't work for me so i uninstalled it directly, after that all my bookmarks on my internet got removed, a few files changed icons on my desktop and so on, so just wanted to check if there's something wrong with my computer

Here is Farbar notes:

<http://pastebin.com/hgxuw8Mf>

I didn't want to scan with TDSS since i have Imminent monitor on my computer (R.A.T program)

Would be awesome if someone could help out!

5chn4pp - January 31, 2016, 12:06 pm

Is this your rat?

C:\Users\VilleH\AppData\Roaming\system32\Runtime broker

Disgusting - January 31, 2016, 12:24 pm

(Jan 31, 2016 01:06 PM)Ezic Wrote: [\[CITE\]](#) Is this your rat?

C:\Users\VilleH\AppData\Roaming\system32\Runtime broker

Yeah, i used it on myself for selfpurposes

5chn4pp - January 31, 2016, 12:31 pm

I only see that rat and some trovi adware, do you want me to remove them both?

Disgusting - January 31, 2016, 1:29 pm

(Jan 31, 2016 01:31 PM)Ezic Wrote: [\[CITE\]](#) I only see that rat and some trovi adware, do you want me to remove them both?

Yeah that would be nice since i don't really know how to remove my own rat ._.

5chn4pp - January 31, 2016, 1:32 pm

Please create a text file called fixlist.txt and copy/paste the contents in the code box below. (Do not include "Code:")

Code CreateRestorePoint:

CloseProcesses:

HKU\S-1-5-21-4213653681-496083930-3201317036-1001\...\Run: [Runtime broker] =>

C:\Users\VilleH\AppData\Roaming\system32\Runtime broker [308224 2015-12-19] (Microsoft)

C:\Users\VilleH\AppData\Roaming\system32\Runtime broker

CHR HomePage: Default ->

hxxp://www.trovi.com/?gd=&ctid=CT3325585&octid=EB_ORIGINAL_CTID&ISID=MA7D7E416-4779-4176-92A3-4FFD0BBDD42B&SearchSource=55&CUI=&UM=5&UP=SPED998D6B-DBDA-4FD7-B A11-BFF4C94D42C7&SSPV=

CHR StartupUrls: Default ->

"hxxp://www.trovi.com/?gd=&ctid=CT3325585&octid=EB_ORIGINAL_CTID&ISID=MA7D7E416-4779-4176-92A3-4FFD0BBDD42B&SearchSource=55&CUI=&UM=5&UP=SPED998D6B-DBDA-4FD7-BA11-BFF4C94D42C7&SSPV="

EmptyTemp:

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 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 next reply.

Please download [Junkware Removal Tool](#) and save it to your desktop.

Shut down your protection software now to avoid potential conflicts. Run the tool by right-mouse clicking JRT.exe and select "Run as Administrator".

The tool will open and start scanning your system.

Please be patient as this can take a while to complete depending on your system's specifications.

On completion, a log (JRT.txt) is saved to your desktop and will automatically open.

Post the contents of JRT.txt into your next message.

Disgusting - January 31, 2016, 2:18 pm

(Jan 31, 2016 02:32 PM)Ezic Wrote: [\[CITE\]](#) Please create a text file called fixlist.txt and copy/paste the contents in the code box below. (Do not include "Code:")

Code CreateRestorePoint:

CloseProcesses:

HKU\S-1-5-21-4213653681-496083930-3201317036-1001\...\Run: [Runtime broker] =>

C:\Users\VilleH\AppData\Roaming\system32\Runtime broker [308224 2015-12-19] (Microsoft)

C:\Users\VilleH\AppData\Roaming\system32\Runtime broker

CHR HomePage: Default ->

hxxp://www.trovi.com/?gd=&ctid=CT3325585&octid=EB_ORIGINAL_CTID&ISID=MA7D7E416-4779-4176-92A3-4FFD0BBDD42B&SearchSource=55&CUI=&UM=5&UP=SPED998D6B-DBDA-4FD7-BA11-BFF4C94D42C7&SSPV=

CHR StartupUrls: Default ->

"hxxp://www.trovi.com/?gd=&ctid=CT3325585&octid=EB_ORIGINAL_CTID&ISID=MA7D7E416-4779-4176-92A3-4FFD0BBDD42B&SearchSource=55&CUI=&UM=5&UP=SPED998D6B-DBDA-4FD7-BA11-BFF4C94D42C7&SSPV="

EmptyTemp:

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 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 next reply.

Please download [Junkware Removal Tool](#) and save it to your desktop.

Shut down your protection software now to avoid potential conflicts. Run the tool by right-mouse clicking JRT.exe and select "Run as Administrator".

The tool will open and start scanning your system.

Please be patient as this can take a while to complete depending on your system's specifications.

On completion, a log (JRT.txt) is saved to your desktop and will automatically open.

Post the contents of JRT.txt into your next message.

Code Fix result of Farbar Recovery Scan Tool (x64) Version:27-01-2016

Ran by VilleH (2016-01-31 22:55:38) Run:1

Running from C:\Users\VilleH\Desktop\F

Loaded Profiles: VilleH (Available Profiles: VilleH)

Boot Mode: Normal

=====

fixlist content:

CreateRestorePoint:

CloseProcesses:

HKU\S-1-5-21-4213653681-496083930-3201317036-1001\...\Run: [Runtime broker] =>

C:\Users\VilleH\AppData\Roaming\system32\Runtime broker [308224 2015-12-19] (Microsoft)

C:\Users\VilleH\AppData\Roaming\system32\Runtime broker

CHR HomePage: Default ->

hxxp://www.trovi.com/?gd=&ctid=CT3325585&octid=EB_ORIGINAL_CTID&ISID=MA7D7E416-4779

-4176-92A3-4FFD0BBDD42B&SearchSource=55&CUI=&UM=5&UP=SPED998D6B-DBDA-4FD7-B

A11-BFF4C94D42C7&SSPV=

CHR StartupUrls: Default ->

"hxxp://www.trovi.com/?gd=&ctid=CT3325585&octid=EB_ORIGINAL_CTID&ISID=MA7D7E416-477

9-4176-92A3-4FFD0BBDD42B&SearchSource=55&CUI=&UM=5&UP=SPED998D6B-DBDA-4FD7-

BA11-BFF4C94D42C7&SSPV="

EmptyTemp:

Restore point was successfully created.

Processes closed successfully.

HKU\S-1-5-21-4213653681-496083930-3201317036-1001\Software\Microsoft\Windows\CurrentVersion\Run\Runtime broker => value removed successfully
C:\Users\VilleH\AppData\Roaming\system32\Runtime broker => moved successfully
Chrome HomePage => removed successfully
Chrome StartupUrls => removed successfully
EmptyTemp: => 6.6 GB temporary data Removed.

The system needed a reboot.

==== End of Fixlog 22:59:02 ====

Code ~~~~~
Junkware Removal Tool (JRT) by Malwarebytes
Version: 8.0.2 (01.06.2016)
Operating System: Windows 8.1 Pro x64
Ran by VilleH (Administrator) on 2016-01-31 at 23:11:04,34
~~~~~

File System: 3

Successfully deleted: C:\end (File)  
Successfully deleted: C:\Users\VilleH\AppData\Roaming\imminent (Folder)  
Successfully deleted: C:\Users\VilleH\AppData\Roaming\speedrunnerslog.txt (File)

Registry: 1

Successfully deleted:  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\GoogleChromeAutoLaunch\_6A2FE0B44054DBCD65BC02D84B3CFD8E (Registry Value)

~~~~~  
Scan was completed on 2016-01-31 at 23:12:34,69
End of JRT log
~~~~~

**5chn4pp** - January 31, 2016, 2:51 pm  
Is the rat and trovi gone?

**GunVein** - January 31, 2016, 3:54 pm  
might be something malware in the installer, but idk :D

**Disgusting** - February 1, 2016, 1:54 am  
(Jan 31, 2016 03:51 PM)Ezic Wrote: [\[CITE\]](#) Is the rat and trovi gone?

Yeah i think so, thanks!

(Jan 31, 2016 04:54 PM)GunVein Wrote: [\[CITE\]](#) might be something malware in the installer, but idk :D

Yeah it could be, probably was

**5chn4pp** - February 1, 2016, 7:26 am

Then i do not see any other malware on your system, you should be clear.

**Disgusting** - February 1, 2016, 5:40 pm

(Feb 1, 2016 08:26 AM)Ezic Wrote: [\[CITE\]](#) Then i do not see any other malware on your system, you should be clear.

Thanks alot mate!