

Forum:[Hack Forums](#)

Thread: [Camera Light on for no Reason, Slow Performance and Weird Cursor](#)

Effexion - September 4, 2017, 1:58 pm

Looks like that despite all my best intentions, I have a RAT. Can someone please do a checkup for me?

FatStacks - September 4, 2017, 2:18 pm

(Sep 4, 2017 01:58 PM)Effexion Wrote: [\[CITE\]](#) Looks like that despite all my best intentions, I have a RAT. Can someone please do a checkup for me?

Back up all current files to a external harddrive then use a data des on your main/os hard drive then reinstall windows

Effexion - September 4, 2017, 2:25 pm

(Sep 4, 2017 02:18 PM)FatSac Wrote: [\[CITE\]](#) Back up all current files to a external harddrive then use a data des on your main/os hard drive then reinstall windows

I feel backing up all my files won't solve the problem. I haven't opened anything over suspicious, so the chances are that I will click whatever it is again.

camden [™] - September 4, 2017, 2:28 pm

My camera light shows up sometimes, but I am not ratted.

I'd recommend you download Wireshark and search for DNS before you reset anything.
Good luck.

Death - September 4, 2017, 2:29 pm

Does anyone have your wifi password?
What system are you running?

Not Your Average Orange - September 4, 2017, 2:29 pm

Download [Farbar Recovery Scan tool](#)

Run as admin >

Yes to disclaimer >

Scan >

Put logs in pastebin, they will be in the same dir as FRST >

Post here

Effexion - September 4, 2017, 2:29 pm

(Sep 4, 2017 02:28 PM)SecureSeal Wrote: [\[CITE\]](#) My camera light shows up sometimes, but I am not ratted.

I'd recommend you download Wireshark and search for DNS before you reset anything.
Good luck.

Why would the camera light just come on for no reason? You might want to make a thread too, amigo.

It's not just that, my cursor is fucky as fuckery too.

(Sep 4, 2017 02:29 PM)Not Your Average Orange Wrote: [\[CITE\]](#) Download [Farbar Recovery Scan tool](#)

Run as admin >
Yes to disclaimer >
Scan >
Put logs in pastebin, they will be in the same dir as FRST >
Post here
Thanks, doing this now.

camden™ - September 4, 2017, 2:30 pm

(Sep 4, 2017 02:29 PM)Effexion Wrote: [\[CITE\]](#) Why would the camera light just come on for no reason? You might want to make a thread too, amigo.

It's not just that, my cursor is fucky as fuckery too.
I'm not sure it was a few months ago, i'm sure I wasn't ratted. But I'd really recommend using Wireshark.

Death - September 4, 2017, 2:35 pm

Nibba didnt even answer my questions.
ok.

Effexion - September 4, 2017, 3:06 pm

FRST.txt: <https://pastebin.com/Xe9RD3Y9>
Addition.txt: <https://pastebin.com/7ZyWrXT2>

Thank you!

Death - September 4, 2017, 3:18 pm

I can see that mousepoints 2

What is the installer.exe on D:

Flaws. - September 4, 2017, 3:29 pm

Just from a quick read I can see

HKU\S-1-5-21-3820243653-2334247829-3564828230-1001\...\MountPoints2:
{3d6e705a-5c6c-11e7-b9e2-806e6f6e6963} - "D:\Installer.exe"

which is uh about as sketchy as it gets not gonna lie

QQ Spitfire - September 4, 2017, 3:32 pm

Might be worth you checking the following...

Processors Under task manger
Wireshark checking dodgy connections
Virus/Malware Scan

That should give an outcome to what's going on. If not just backup your files and do a fresh install, if your on Windows 10 there's an option to create a clean install of the OS but keep your files.

Hope this helped!

Effexion - September 4, 2017, 4:00 pm

(Sep 4, 2017 03:18 PM)linuxdaddy Wrote: [\[CITE\]](#) I can see that mousepoints 2

What is the installer.exe on D:

(Sep 4, 2017 03:29 PM).Jasper Wrote: [\[CITE\]](#) Just from a quick read I can see

HKU\S-1-5-21-3820243653-2334247829-3564828230-1001\...\MountPoints2:
{3d6e705a-5c6c-11e7-b9e2-806e6f6e6963} - "D:\Installer.exe"

which is uh about as sketchy as it gets not gonna lie

I never use D:/, that's suss as fuck lol. Any way of telling what installed installer.exe because there's no way I would have opened that.

(Sep 4, 2017 03:32 PM)QQ Spitfire Wrote: [\[CITE\]](#) Might be worth you checking the following...

Processors Under task manger
Wireshark checking dodgy connections
Virus/Malware Scan

That should give an outcome to what's going on. If not just backup your files and do a fresh install, if your on Windows 10 there's an option to create a clean install of the OS but keep your files.

Hope this helped!

I don't want to do a fresh install really as like I said earlier, I would probably end up opening it again because there's nothing I can think i have clicked that would have put that there.

EDIT: I'm such a noob. D:/ is my disk drive and it's WoW lol.

Not Your Average Orange - September 4, 2017, 4:19 pm

I couldn't find anything in the FRST logs, but I'm still new to this.

If you're still concerned, try downloading [GlassWire](#), and observing internet connections.

Flaws. - September 4, 2017, 4:21 pm

(Sep 4, 2017 04:00 PM)Effexion Wrote: [\[CITE\]](#) EDIT: I'm such a noob. D:/ is my disk drive and it's WoW lol.

Imao

well then I cant see anything out of the norm really but I only looked over the first list and not Addition.

5chn4pp - September 4, 2017, 11:18 pm

(Sep 4, 2017 02:18 PM)FatSac Wrote: [\[CITE\]](#) Back up all current files to a external harddrive then use a data des on your main/os hard drive then reinstall windows

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

Read the "Ignore users that post dumb recommendations/procedures (IE: format and reinstall)" section.

(Sep 4, 2017 02:29 PM)linuxdaddy Wrote: [\[CITE\]](#) What system are you running?
Windows 10 Home Version 1703

(Sep 4, 2017 03:06 PM)Effexion Wrote: [\[CITE\]](#) FRST.txt: <https://pastebin.com/Xe9RD3Y9>
Addition.txt: <https://pastebin.com/7ZyWrXT2>

Thank you!

FRST logs are clean.

Please download [Junkware Removal Tool](#) to your desktop. Run the tool by double-clicking it. If you are using Windows Vista, 7, or 8; instead of double-clicking, right-mouse click 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.

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.

(Sep 4, 2017 03:18 PM)linuxdaddy Wrote: [\[CITE\]](#) What is the installer.exe on D:
Probably that "WoWDisc3" in his cdrom.

(Sep 4, 2017 04:00 PM)Effexion Wrote: [\[CITE\]](#) EDIT: I'm such a noob. D:/ is my disk drive and it's WoW lol.

This is why we don't want untrained users to look over logs, it took me 5 seconds to look in addition for drives and emulators, "WoWDisc3" is easily identified.

Effexion - September 5, 2017, 2:26 am

(Sep 4, 2017 11:18 PM)Bromo-DragonFLY Wrote: [\[CITE\]](#)
<https://hackforums.net/showthread.php?tid=4557247>

Read the "Ignore users that post dumb recommendations/procedures (IE: format and reinstall)" section.

Windows 10 Home Version 1703

FRST logs are clean.

Please download [Junkware Removal Tool](#) to your desktop. Run the tool by double-clicking it. If you

are using Windows Vista, 7, or 8; instead of double-clicking, right-mouse click 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.

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.

Probably that "WoWDisc3" in his cdrom.

This is why we don't want untrained users to look over logs, it took me 5 seconds to look in addition for drives and emulators, "WoWDisc3" is easily identified.

Thank you:

JRT:

Quote:~

Junkware Removal Tool (JRT) by Malwarebytes

Version: 8.1.4 (07.09.2017)

Operating System: Windows 10 Home x64

Ran by Mikey (Administrator) on 05/09/2017 at 8:50:25.44

~

File System: 5

Successfully deleted:

C:\Users\Mikey\AppData\Roaming\Mozilla\Firefox\Profiles\0uuq1usz.default\extensions\trash
(Folder)

Successfully deleted:
C:\Windows\system32\Tasks\update-S-1-5-21-3820243653-2334247829-3564828230-1001 (Task)
Successfully deleted: C:\Windows\system32\Tasks\update-sys (Task)
Successfully deleted:
C:\Windows\Tasks\update-S-1-5-21-3820243653-2334247829-3564828230-1001.job (Task)
Successfully deleted: C:\Windows\Tasks\update-sys.job (Task)

Registry: 0

~

Scan was completed on 05/09/2017 at 8:54:02.15
End of JRT log

~

Roguekiller:

Quote:RogueKiller V12.11.13.0 (x64) [Sep 4 2017] (Free) by Adlice Software
mail : <http://www.adlice.com/contact/>
Feedback : <https://forum.adlice.com>
Website : <http://www.adlice.com/download/roguekiller/>
Blog : <http://www.adlice.com>

Operating System : Windows 10 (10.0.15063) 64 bits version
Started in : Normal mode
User : Mikey [Administrator]
Started from : C:\Program Files\RogueKiller\RogueKiller64.exe
Mode : Delete -- Date : 09/05/2017 09:24:06 (Duration : 00:51:29)
Switches : -refid

Processes : 0

Registry : 0

Tasks : 0

Files : 1

[Tr.Gen0][File] C:\Users\Mikey\AppData\Roaming\utorrent\updates\3.5.0_43916\utorrentie.exe ->
Deleted

WMI : 0

Hosts File : 0

Antirootkit : 0 (Driver: Loaded)

Web browsers : 0

MBR Check :
+++++ PhysicalDrive0: HGST HTS541010A9E680 +++++
--- User ---
[MBR] aabc97d2ea8ddf7d650ae0838d2b5b8f
[BSP] 3f5fdb6ef98999f2cda82280de35bc7 : Empty MBR Code
Partition table:
0 - [MAN-MOUNT] EFI system partition | Offset (sectors): 2048 | Size: 260 MB
1 - [MAN-MOUNT] Microsoft reserved partition | Offset (sectors): 534528 | Size: 128 MB
2 - Basic data partition | Offset (sectors): 796672 | Size: 931687 MB
3 - [SYSTEM][MAN-MOUNT] | Offset (sectors): 1908893696 | Size: 899 MB
4 - [SYSTEM] Basic data partition | Offset (sectors): 1910734848 | Size: 20890 MB
User = LL1 ... OK
User = LL2 ... OK

5chn4pp - September 5, 2017, 2:31 am

So far, you are clean.

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.

Effexion - September 5, 2017, 3:37 am

(Sep 5, 2017 02:31 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) So far, you are clean.

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.

Can I leave background programs running? I really need Sentry, for now.

5chn4pp - September 5, 2017, 4:49 am

(Sep 5, 2017 03:37 AM)Effexion Wrote: [\[CITE\]](#) Can I leave background programs running? I really need Sentry, for now.

Sure, but I can't guarantee that TDSSKiller won't close Sentry, but it should be unlikely.

Effexion - September 5, 2017, 5:09 am

<https://pastebin.com/YXiddYix>

Thanks for all your help.

virus - September 5, 2017, 2:01 pm

Running a JRT scan might be usefull?

Malwarebytes | Junkware Removal Tool

Download [MalwareBytes JRT](#) 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.

1: Right click to run as administrator. When the tool opens click Yes to disclaimer.

2: "Press any key to continue" speaks for itself.

3: JRT will now create a restore point.

4: Please view the report in JRT.txt Please share this report in a [pastebin](#)

Black Cat - September 5, 2017, 2:06 pm

(Sep 5, 2017 02:01 PM)?arb?thememer Wrote: [\[CITE\]](#) Running a JRT scan might be usefull?

Malwarebytes | Junkware Removal Tool

Download [MalwareBytes JRT](#) 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.

1: Right click to run as administrator. When the tool opens click Yes to disclaimer.

2: "Press any key to continue" speaks for itself.

3: JRT will now create a restore point.

4: Please view the report in JRT.txt Please share this report in a [pastebin](#)
Already was done if you read couple posts back

virus - September 5, 2017, 2:28 pm

(Sep 5, 2017 02:06 PM)Black Cat Wrote: [\[CITE\]](#) Already was done if you read couple posts back
Oh im sorry, dindt read all the posts ?

5chn4pp - September 6, 2017, 3:52 am

I don't see anything malicious, last thing would be to check your system files, open cmd as administrator and execute this command:

Code sfc /scannow

Ranger. - September 6, 2017, 3:58 am

(Sep 4, 2017 02:18 PM)FatSac Wrote: [\[CITE\]](#) Back up all current files to a external harddrive then use a data des on your main/os hard drive then reinstall windows

What is the point of backing up data that contains executables, which could have been infected by said RAT?

Moron..

Effexion - September 6, 2017, 4:02 am

(Sep 6, 2017 03:52 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) I don't see anything malicious, last thing would be to check your system files, open cmd as administrator and execute this command:

Code sfc /scannow

Thanks, man. Will do that now. Would love to know what's wrong with mouse lol. Made a separate thread.

5chn4pp - September 6, 2017, 4:08 am

(Sep 6, 2017 03:34 AM)Effexion Wrote: [\[CITE\]](#) It's a laptop mouse.
Laptop mouse like this one?

If so, make sure you are only touching it at one place, on some designs its very easy to unwillingly move the mouse around because its in an awkward place.

Effexion - September 6, 2017, 4:54 am

(Sep 6, 2017 04:08 AM)Bromo-DragonFLY Wrote: [\[CITE\]](#) Laptop mouse like this one?

If so, make sure you are only touching it at one place, on some designs its very easy to unwillingly move the mouse around because its in an awkward place.

I doubt it's that because it's only a recent issue.