

Forum: [Hack Forums](#)

Thread: [Majorly Infected](#)

Gokus_Dog - October 3, 2013, 8:48 pm

AdwCleaner Log - <http://privatepaste.com/cbeba3ed99>

ESET Scan Log - <http://privatepaste.com/deb8ac9106>

Malwarebytes Anti-Malware Scan Log - <http://privatepaste.com/f60edc799d>

OTL.txt - <http://privatepaste.com/7bb610514f>

Extras.txt - <http://privatepaste.com/5418690edf>

SecurityCheck Log - <http://privatepaste.com/b9ce7d17c5>

Paradoxum - October 5, 2013, 9:15 am

Before anything else, open the legitimate Google Chrome and [set it as your default browser](#).

Greetings,

I will analyse your logs given that you agree to my terms, which I will elaborate below. Feel free to inform me right after this post if you do not agree and I will swiftly close your thread. Continuing with the process will be deemed as compliance.

You are to finish the entire process. If you decide to reformat or discontinue, I ask to be informed. Fail to do so and there will be no guarantee that I will help you in the future.

You are not to create any new threads regarding the similar topic. Post your responses on this thread alone.

You are not to install any new software in your system until I declare you clean, as it may hinder our process thus making this futile.

You are not to modify the logs in any way. Failure to do so will instantly deprive you of this service.

You are not to PM me regarding anything about your thread. I do not forget--my schedule, however, gets tight at times.

You are to post the logs on the thread unless I say otherwise.

Provided that you will continue with this service, you hereby agree that I have the right to discontinue the analysis at any time, upon a violation of a single rule.

Thank you. Step 1

You currently have the outdated version(s) of the program(s) below. These programs, if left outdated, are vulnerable and will be targets of malware. It is essential that you update them before we begin:

Java

Mozilla Firefox

Take care not to install any bundled software that might come with any of the above. An example would be Adobe Flash Player giving you the option to install a scanner. Please opt-out.

Step 2

I notice there are signs of one or more P2P (Person to Person) File Sharing Programs on your computer. Your system is at risk. Even if you are using a safe P2P program, it is only the program that is safe. You will be sharing files from uncertified sources, and these are often infected. The bad guys use P2P filesharing as a major conduit to spread their wares.

I strongly recommend that you uninstall the following program(s) present in your system through Add or Remove Programs for Windows XP and Programs and Features for Vista and Windows 7:

µTorrent

Note: If you choose not to remove the program(s), please do not use them until this computer is clean.

Step 3

I noticed that you do not have an anti-virus installed in your system presently. Do understand that you are making yourself defenseless against malware. Though it is plausible that caution can somehow prevent infection, it is still advisable to install an anti-virus. An anti-virus is crucial to your system's security. Without one, reinfection is imminent after a clean. Here are lists of well-known and proven software.

Freeavast! Free Antivirus Visit the official site ['here'](#) for its features and download link.

Avira Free Antivirus Visit the official site ['here'](#) for its features and download link.

Microsoft Security Essentials Visit the official site ['here'](#) for its features and download link.

Paid Avira Antivirus Premium 2013 Visit the official site ['here'](#) for its features and download link.

ESET NOD32 Antivirus Visit the official site ['here'](#) for its features and download link.

Kaspersky Anti-Virus 2013 Visit the official site ['here'](#) for its features and download link.

From the list above, choose one, click on the name of the program that suites you best, download it and proceed to the installation. You can either choose the free version or purchase a full version. Regardless, having one is truly an aid to your computer's defense capability.

Step 4

Run OTL.exe.

Copy and paste the following text written inside of the code box into the Custom Scans & Fixes box located at the bottom of OTL.

Code :OTL

```
[2013/10/03 21:27:46 | 000,002,103 | ---- | C] () -- C:\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\Quick Launch\Fast Browser.lnk
[2013/10/03 21:27:46 | 000,002,079 | ---- | C] () -- C:\Users\Public\Desktop\Fast Browser.lnk
[2013/10/03 21:14:54 | 000,001,000 | ---- | C] () --
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MyPC Backup.lnk
[2013/10/03 21:14:54 | 000,000,990 | ---- | C] () -- C:\Users\Administrator\Desktop\MyPC Backup.lnk
[2013/10/03 21:14:04 | 000,001,078 | ---- | C] () -- C:\Users\Public\Desktop\Advanced System Protector.lnk
[2013/10/03 21:12:38 | 000,000,000 | ---D | C] --
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\BitGuard
[2013/10/03 21:12:27 | 000,000,000 | ---D | C] -- C:\ProgramData\BitGuard
[2013/10/03 21:12:12 | 000,000,000 | ---D | C] -- C:\Program Files (x86)\Delta
[2013/10/03 21:11:50 | 000,000,000 | ---D | C] -- C:\ProgramData\DSearchLink
[2013/10/03 21:11:45 | 000,000,000 | ---D | C] --
C:\Users\Administrator\AppData\Roaming\Systweak
[2013/10/03 21:11:43 | 000,000,000 | ---D | C] -- C:\Program Files (x86)\RegClean Pro
[2013/10/03 21:11:16 | 000,000,000 | ---D | C] -- C:\ProgramData\Babylon
[2013/10/03 21:27:56 | 000,000,000 | ---D | C] -- C:\Users\Administrator\AppData\Local\Fast Browser
[2013/10/03 21:27:46 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Fast Browser
[2013/10/03 21:27:42 | 000,000,000 | ---D | C] -- C:\Program Files (x86)\Fast Browser
[2013/10/03 21:21:58 | 000,000,000 | ---D | C] -- C:\Users\Administrator\AppData\Local\Systweak
[2013/10/03 21:14:54 | 000,000,000 | ---D | C] --
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\MyPC Backup
[2013/10/03 21:14:54 | 000,000,000 | ---D | C] -- C:\Program Files (x86)\MyPC Backup
[2013/10/03 21:14:04 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Advanced System Protector
[2013/10/03 21:14:04 | 000,000,000 | ---D | C] -- C:\Program Files (x86)\Advanced System Protector
[2013/10/03 21:14:01 | 000,000,000 | ---D | C] -- C:\ProgramData\Systweak
O4 - Startup: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MyPC Backup.lnk = C:\Program Files (x86)\MyPC Backup\MyPC Backup.exe (MyPCBackup.com)
O4 - HKCU..Run: [GoogleChromeAutoLaunch_FD61B43EF6A3E51EEC71EC221939BB92] C:\Program Files (x86)\Fast Browser\Application\chrome.exe (Fast Browser)
O4 - HKCU..Run: [SearchProtection] C:\Users\Administrator\AppData\Roaming\Search Protection\SearchProtection.EXE (Spigot, Inc.)
```

[2013/10/03 21:12:12 | 000,000,000 | ---D | M] (No name found) -- C:\Program Files (x86)\Mozilla Firefox\extensions\ffxtlbr@babylon.com

[2013/10/03 21:12:13 | 000,000,000 | ---D | M] (Delta Toolbar) -- C:\Users\Administrator\AppData\Roaming\Mozilla\Firefox\Profiles\yvqliq1q.default\extensions\ffxtlbr@delta.com

IE - HKCU\..\SearchScopes\{0ECDF796-C2DC-4d79-A620-CCE0C0A66CC9}: "URL" = http://www.delta-search.com/?q={searchTerms}&babsrc=SP_ss&mntrId=105A6CF049049FD2&afflD=122786&tsp=5025

SRV - (BackupStack) -- C:\Program Files (x86)\MyPC Backup\BackupStack.exe (Just Develop It)

SRV - (DSUDiskOptimizer) -- C:\Program Files (x86)\Disk Speedup\DSUDefragSrv64.exe (Systweak Inc., (www.systweak.com))

PRC - C:\Users\Administrator\AppData\Roaming\Search Protection\SearchProtection.exe (Spigot, Inc.)

PRC - C:\ProgramData\BitGuard\2.6.1694.246\{c16c1ccb-1111-4e5c-a2f3-533ad2fec8e8}\BitGuard.exe ()

[2013/10/03 21:35:45 | 000,000,000 | ---D | M] -- C:\Users\Administrator\AppData\Roaming\Systweak

[2013/08/22 21:18:11 | 000,000,000 | ---D | M] -- C:\Users\Administrator\AppData\Roaming\Search Protection

[2013/10/03 21:13:59 | 000,001,196 | ---- | C] () -- C:\Users\Public\Desktop\Disk Speedup.lnk

[2013/10/03 21:11:50 | 000,001,765 | ---- | C] () -- C:\Users\Administrator\Desktop\Search.lnk

[2013/10/03 21:13:59 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Disk Speedup

[2013/10/03 21:13:58 | 000,000,000 | ---D | C] -- C:\Program Files (x86)\Disk Speedup

:Files

C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extensions\eooncjejnppfjklapaamhcdmjbilmde

C:\ProgramData\BitGuard

:Commands

[emptytemp]

Then click the Run Fix button at the top.

Let the program run unhindered; it will reboot when it is done. If it does not, please reboot your system.

You will need to post the log that you will see upon rebooting your system.

Step 5

Double-click OTL.exe to run it.

Make sure all other windows are closed to let it run uninterrupted.

When the window appears, make sure that you set the following specifications: Under Extra Registry choose Use SafeList.

Check the LOP Check and Purity Check boxes.

Click the Run Scan button. The scan won't take long.

When the scan completes, it will open two Notepad windows:OTL.txt

Extras.txt

Please copy (Right-click > Select All > Copy) the contents of these files and post them on '[Private Paste](#)'.

In your next post, please provide the following:

OTL Log(s)OTL Fix Log

OTL.txt

Extras.txt

Gokus_Dog - October 5, 2013, 10:20 am

OTL Fix Log - <http://privatepaste.com/a3939261a6>

OTL.txt - <http://privatepaste.com/5f3045f8a6>

Extras.txt - <http://privatepaste.com/ecb502b3a1>

Thanks for the help and swift reply

Paradoxum - October 6, 2013, 8:41 am

Step 1

Download Junkware Removal Tool from '[here](#)' and save it to your desktop.

Make sure all other windows are closed and to let it run uninterrupted.

Run the file. Windows Vista and Windows 7 users should run it as an administrator.

Press any key to continue.

It will undergo processes--your desktop will momentarily disappear. This is normal.

A log file will automatically pop-up after the process.

Copy and paste the contents of the log into your next reply. You can also locate the log at your desktop as JRT.txt.

Step 2

Download AdwCleaner from ['here'](#) and save it to your desktop.

Make sure all other windows are closed and to let it run uninterrupted.

Run the file. Windows Vista and Windows 7 users should run it as an administrator.

Click Scan and wait for it to finish.

Once done, click Clean.

Confirm the following prompts with OK.

Your system will be rebooted automatically.

A log file will automatically pop-up after the reboot. Copy and paste the contents of the log into your next reply. You can also locate the log at C:\AdwCleaner[S*].txt.

Step 3

Double-click OTL.exe to run it.

Make sure all other windows are closed to let it run uninterrupted.

When the window appears, make sure that you set the following specifications: Under Extra Registry choose Use SafeList.

Check the LOP Check and Purity Check boxes.

Click the Run Scan button. The scan won't take long.

When the scan completes, it will open two Notepad windows: OTL.txt

Extras.txt

Please copy (Right-click > Select All > Copy) the contents of these files and post them on ['Private Paste'](#).

In your next post, please provide the following:

AdwCleaner Log

Junkware Removal Tool Log

OTL Log(s)OTL.txt

Extras.txt

Gokus_Dog - *October 6, 2013, 9:54 am*

AdwCleaner Log - <http://privatepaste.com/b207390cc5>

Junkware Removal Tool Log - <http://privatepaste.com/bf7b3f2213>

OTL.txt - <http://privatepaste.com/6a775da789>

Extras.txt - <http://privatepaste.com/1cf573e727>

Paradoxum - *October 6, 2013, 10:00 am*

How is everything running?

Step 1

Looking at your log, I have seen that you have the program(s) below installed. I highly suggest a removal through Add or Remove Programs or Programs and Features. I am asking you this for I have seen negative feedback from users. Should the program(s) in question be utterly clean, no such comment should be seen. Take this as a pre-cautionary measure. Better safe than sorry.

The list below shows the program(s) with poor or flawed reputation that you currently have installed in your system:

Fast Browser

Search Protection

Please respond back if you encounter difficulties uninstalling the program(s). If Windows says the file has already been uninstalled or that it cannot be found, simply proceed to allow its removal from the list.

Step 2

Run OTL.exe.

Copy and paste the following text written inside of the code box into the Custom Scans & Fixes box located at the bottom of OTL.

Code :OTL

[2013/07/14 02:55:21 | 000,000,000 | ---D | M] -- C:\Users\Administrator\AppData\Roaming\System

Then click the Run Fix button at the top.

A log will pop-up shortly. Post that log.

Step 3

Download TDSSKiller from '[here](#)' and save it to your desktop.

Make sure all other windows are closed and to let it run uninterrupted.

Run the file. Windows Vista and Windows 7 users should run it as an administrator.

Then select Start Scan.If an infected file is detected, the default action will be Cure, click on Continue.

If a suspicious file is detected, the default action will be Skip, click on Continue.

It may ask you to reboot the computer to complete the process. Click on Reboot Now.

Once done, simply click Close.

Click the Report button and copy and paste the contents of the log into your next reply. A log file will be created in the C:\ directory as well.

In your next post, please provide the following:

OTL Log(s)OTL Fix Log

TDSSKiller Log

Gokus_Dog - October 6, 2013, 11:27 am

OTL Fix Log - <http://privatepaste.com/f0a9dcfabf>

TDSSKiller Log - <http://privatepaste.com/5ef0e6f17f>

Thanks for the help I really appreciate it and I removed those two programs that you suggested.

Paradoxum - October 7, 2013, 8:19 am

Are you still experiencing any issues thus far?

Gokus_Dog - October 7, 2013, 4:32 pm

(Oct 7, 2013 08:19 AM)Paradoxum Wrote: [\[CITE\]](#) Are you still experiencing any issues thus far? Nope I think it's all good for now I really appreciate your help with this!

Paradoxum - October 8, 2013, 2:11 am

I see no infections present in your log anymore. If you are not having any further problems, I declare you ALL CLEAN.

Update Internet Explorer

I ask that you do not disregard this step whether you are using Internet Explorer or not as your main browser. Please be advised that though you don't seem to be using this, I can assure you that most of your everyday applications use this browser's technology to update thereby solidifying the necessity to update it.

Please download the latest version (version 10.00) from ['here'](#) and install it.

Open Internet Explorer once you have successfully installed it.

At Internet Explorer's interface navigate to Tools (ALT + X) > Internet Options.

Click once on Security > Internet > Custom Level....

Choose Medium-High if that is not your default setting already.

Click OK > Apply > OK.

Update Java

You must make sure your Java is up-to-date. Older versions have vulnerabilities that can be exploited. Follow the steps below to update Java.

To get the latest version of Java please go ['here'](#).

Proceed to uninstalling the older versions: Windows XP: Start > Control Panel > Add or Remove Programs.

Windows Vista and Windows 7: Start > Control Panel > Programs and Features.

Search the list for all previously installed versions of Java: All versions before Java 7 Update 40

All versions before Java SE Development Kit 7 Update 40

Choose Uninstall.

Now install the version(s) you downloaded earlier.

Uninstall AdwCleaner

This will uninstall AdwCleaner and remove all of the logs it has produced. Run AdwCleaner.exe.

Windows Vista and Windows 7 users should run it as an administrator.

Click the Uninstall button.

Clean-Up with OldTimer's List-It

This will remove all temporary files stored in your computer and as well as the files generated by the specialised tools I instructed you to use. Run OTL.exe. Windows Vista and Windows 7 users should run it as an administrator.

Click the CleanUp button.

Once done, it will ask you to reboot.

Allow it by pressing Yes when prompted.

Set A Clean System Restore Point

System Restore maintains a backup of your programs however it may also backup infections therefore constant flushing is required to create a clean restore point.

For Windows XP:

On the desktop, right-click My Computer > Properties > System Restore tab.

Check Turn off System Restore.

Click Apply > Yes.

Please wait a few moments to let it clear.

After doing so, remove the check from Turn off System Restore.

Click Apply > OK.

System Restore will be working again and will have a new restore point.

For Windows Vista: On the desktop, click Start > Control Panel > System and Maintenance > System.

Click on System Protection in the left-hand task list.

Under the Create restore points automatically on the selected disks header, uncheck the boxes.

Click Turn System Protection Off > OK.

Please wait a few moments to let it clear.

After doing so, place a check on the boxes under Create restore points automatically on the selected disks which had a check to begin with.

Click Apply > OK.

System Restore will be working again and will have a new restore point.

For Windows 7:

On the Start Menu, right-click Computer > Properties > System Protection.

Click Configure.

Click Delete > Continue > Close > OK.

You are now back at the System Protection Tab.

Click Create > <Any Title Here> > Create.

A prompt should tell you that it was successful. Click Close.

Click OK.

System Restore will be working again and will have a new restore point.

A Quick Summary To Prevent Reinfection

1. Install an anti-virus and keep it updated. Run complete system scans.

You have to make sure you have an anti-virus installed. Update your anti-virus every day to make sure it has the latest signatures. Yes, updating is essential in maintaining your computer. The latest updates will ensure the integrity of your chosen program. Some paid anti-viruses even offer hourly updates and the reason for this is clear--malware gets advanced and new variants are detected in a short span of time. In addition to updating, perform a complete scan monthly. You might think you don't need it however you do. Don't rely on your instincts that your system is clean.

2. Keep Windows updated.

You may currently have an outdated Windows operating system. It is highly recommended you install the latest updates as these are extremely important which contain fixes for several bugs and security issues that attackers exploit. Always make sure that you are protected on all sides.

Microsoft offers these updates free of charge. I present to you the option to perform the update.

Go to the '[Official Microsoft Windows Update](#)' site using the latest version of Internet Explorer. On the Tools menu in Internet Explorer, click Internet Options.

Click the Security tab.

Click the Trusted Sites icon, and then click Sites....

Uncheck the Require Server Verification checkbox.

Make sure the following URLs are listed in the Web Sites list box:

http://*.windowsupdate.microsoft.com

http://*.windowsupdate.com

A pop-up will automatically open.

If the pop-up failed to open, click the Start button, click All Programs, and then click Windows Update.

Install the Important Updates and reboot as required.

3. Prevention is better than any cure.

Constant vigilance is your number one tool. Aside from keeping in mind safe surfing habits, specific tools are there to further enhance your security. The good thing is that they are free, reliable and low on system resources. Even having them running together won't slow down your system. To download, simply click on the name of each software.

[CCleaner](#)

CCleaner is a freeware system optimization, privacy and cleaning tool. CCleaner is the number one tool for cleaning your Windows PC. It protects your privacy online and makes your computer faster and more secure. Easy to use and a small, fast download. Run CCleaner regularly, suggestively after you are done browsing or using your system for the day as it cleans temporary files such as cookies that may prove harmful. Open CCleaner.

On the CCleaner tab, select Analyze and wait for the analysis.

Click on the Run Cleaner button

On the Registry tab, select Scan For Issues and wait until it finishes.

Select Fix Selected Issues > No > Fix All Selected Issues > Close.

[MVPS Hosts](#)

MVPS Hosts helps to protect your Privacy and Security by blocking sites that may track your viewing habits. In many cases using a well designed HOSTS file can speed the loading of web pages by not having to wait for these ads, annoying banners, hit counters, etc. to load. Make sure to check the MVPS Hosts ['site'](#) for updates monthly.