Conduit Removal

Removal of Conduit based popups and search engine redirects.

If you download a program from the internet without extreme care or from an unreliable source, or clicked on a pop-up window, you may get caught by a search engine redirect install or pop up (PUP) generating malware. These are Conduit generated redirects. They will generate, among other aggravations, popups as well as URL redirects from your desired search engine, Internet Explorer, Fire Fox or Google Chrome. They are not viruses but are a real pain, an intrusion into your computer, wasters of your time, slowing down your operating system and attempting to deprive you of money. Some redirects or pop-ups can install rootkits to steal data from your machine and some may direct you to places where you can pick up a virus, Trojan horse or get other nasty item installed in your computer.

Some of the following names are common redirects, but this list below does not contain all of them:
Conduit Search, Link Swift, Optimizer Pro, TidyNetwork, Search Protect, System Requirements Lab, Sweet Packs A8, Price Gong, Smart Bar, PC Health Kit, Quick Share, AVG Secure search, Great Arcade Hits, AVG Toolbar, Lucky Leap, AVG Safeguard Toolbar, My Free Game, Angry Birds, DealPly, Wajam, Scorpion Saver, Level Quality Watcher, and Certified Search bar. Note that some similar names may be legitimate program names so be sure you identify them carefully if they appear on your computer.

For those of you who want to "Cut to the chase." and just get back to normal quickly, here is a link to the suggested removal software. Just click the link below and follow the instructions:

http://general-changelog-team.fr/fr/downloads/finish/20-outils-de-xplode/2-adwcleaner

To know more about Conduit infection and perhaps remove all remaining traces of it from your computer please read on. It is suggested to read it to at least **understand Conduit infections and minimize your future risk**.

SYMPTOMS and REMOVAL:

1) If you keep getting popups or your browser has changed the way it opens, as for instance, your browser shows a home page address that you don't recognize, you may have unknowingly gotten a redirect installed. As soon as the problem is recognized get to removing it. Here is how.

2) For the less experienced user: **Note** that the instructions at Steps 4 thru 18 may be beyond the capability of the newer computer user and in that case a program like **Microsoft free Safety Scanner** at safe link http://www.microsoft.com/security/scanner/en-us/default.aspx where **MSERT.EXE** can be downloaded and run within ten days of the download, after which it expires. **AdwCleaner**, also free program, can be downloaded (though a donation is desired, but not required) and run. Both of these try take care of many, though not necessarily all of the subject problems. **AdwCleaner** and the **Microsoft Safety Scanner** are programs that search for and delete Adware, Toolbars, Potentially Unwanted Programs (PUP), and browser Hijackers from your computer. Using either can remove many of these types of programs. It can be downloaded (carefully) from the French creator (safely at this date) at safe link http://general-changelog-team.fr/fr/downloads/finish/20-outils-de-xplode/2-adwcleaner. They should be run as soon as downloaded as they are constantly updated to reflect new Foistware as they show up. Below is what Bleeping Computer says about **AdwCleaner** and it is equally true of the **Microsoft Safety Scanner** product. . "The types of programs that **AdwCleaner** targets are typically bundled with free programs that you download from the web. In many cases when you download and

install a program, the install will state that some programs will be installed along with the program you downloaded. Unless you perform a Custom install, these unwanted programs will automatically be installed on your computer leaving you with extra browser toolbars, adware, and other unwanted programs. Both products are designed to search for and remove these types of programs.

Instructions:

3) Using either program is straight forward if you follow the on screen instructions. Simply download the program and run it. Follow the instructions to scan the computer for the malware. The Scan button will cause either to search your computer for unwanted programs and then display all the files, folders, and registry entries found on your computer that are used by suspect programs. Clean instructions follow. It is hoped that these programs will remove the worst offenders, but they may not find all of them. They should allow the computer to be returned to near normal operating condition. Next, run **MalwareBytes** or similar program and your **Anti-virus** and **MS Security Essentials** if available. Next, **empty the recycle bin**. This is important. After this shut down the computer and restart it.

4) **For more experienced users**, the following steps allow for a complete removal of all, or any remaining foistware items, though it is a more extensive and therefore time consuming process. If any of the redirects are still remaining in your computer, these steps will take care of it.

5) List any new items that showed up in the download that resulted in the malware or that were not asked for if they are recognized. Check desktop for new icons. In particular, check for those listed above in the second paragraph. Write them down, as you may need those names.

   Before going any further, check your computer's Folder Options. Type "**Folder Options**" in the start menu search box. When **Folder options** is clicked, choose the "**View**" tab and make sure the "**Show hidden files, folders, or drives**" radio button is selected or the folders will be hidden in the next instructions.

6) In **(C)\\Users\Name\AppData** Open each of the folders in **AppData** and look at the date any new unrecognized/unfamiliar apps in any of the sub-folders were installed and note which got installed at or just before the approximate time you noticed infestation. Write these names down as in step 2 if they aren't there already. They will all probably have the same date, the date you got infected.

7) Don't try to delete any of these folders yet. Some may not be able to be deleted until the Registry is cleaned out and the computer restarted later.

8) In **(C) \Program Data** again note the names and date installed. They will all also probably have the same date, the date you got infected.

9) Run **RevoUninstaller** or other uninstall app. If the malware names on your list of steps 2, 4 and 5 are shown as programs, uninstall the malware program or programs. Alternatively, you can use the Windows "**Add Remove Programs**" option to remove them.

10) When you have done the above uninstalls, run **MalwareBytes** or similar program and your **Anti-virus** and **MS Security Essentials** if available. Follow the instructions that appear after a scan is completed.

11) Run a mild registry cleaner like **Auslogics free Registry Cleaner**.

12) Run Regedit as explained after step 19, and search for keys with reference to malware like those noted from **AppData** and **Program Data** and/or those listed above in the second paragraph. Do not remove the keys yet.

13) If you see any keys with the malware names in them, first do a registry backup and then if comfortable, remove any registry entries found. See instructions below step 19.

14) Check your Windows Start Menu and if they are listed delete them from the Start Menu

15) Open your C Drive directory and once more check **(C)\Program Data**, **Program Files** and **Program Files (x86)** and delete those named malware program folders that were found if they still are there.

16) In **(C)\Name\App Data** delete the malware named folders you found earlier if they are still in those folders.

17) **Empty the recycle bin**. This is important. Shut down the computer and restart it.

18) Do one more run of **MalwareBytes** or a similar application. At this point it might be a good idea to recheck the effort of steps 15 and 16. There should no longer be any traces of the foistware.

19) Lastly, remove the link in your browser/search engine, and restore your **Home Page** so that your browser doesn't automatically redirect to any of the malware sites. In **Internet Explorer** go to **TOOLS < INTERNET-OPTIONS < HOME** and make sure that **Home Page** address is what you want not a redirected site. Also double check your **FAVORITES** to verify none of them is a malware site.

Working with the registry:

In the **START** menu, type **REGEDIT,** and click on **REGEDIT.EXE**

1) Allow the program to execute.

2) IMPORTANT, now backup your registry as follows: Open, **FILE** tab, click **EXPORT,** give it a name and **SAVE** to the desktop or to a flash drive or CD.

3) Be sure to go to the top of the left pane and highlight "**Computer**" so as to start the search at the beginning of the registry.

4) Click on the **EDIT** tab then **FIND** and type in the name of one of the **malware items from your list** and click on **FIND NEXT**.

5) When the search finds a Key or entry with the malware name, read carefully to be sure that it correctly identifies the malware not a legitimate program and delete it. Click **DELETE** and **ENTER**

6) Click on **Function key F3** to continue the search and repeat deleting malware keys.

7) When the search notes that the end of the registry has been found, "**Finished searching**…" , repeat step3 through 7 for all the other names of the malware you found.

8) Once you have completed removing all the malware, backup the registry again with a new name as per step 2. (Should you have any problems you will be able to restore the registry as saved or have the ability to compare the two registry backups to help find errors, if required?) Note that the registry can be restored by simply clicking on the icon of the registry backup file you saved shown at the right.

By Fred Wassermann for SCG