Instructions to remove MyStartSearch on all browsers

Technically, MyStartSearch is not a virus but it is an unwanted program (PUP), which can be installed on your computer. If the ad software MyStartSearch attacks the system, whenever accessing and browsing the Internet, the screen will display popup windows, advertising banners.

MyStartSearch is a browser hijacker, changes the default homepage and search settings on popular browsers like Internet Explorer, Google Chrome or Mozilla Firefox to **http://www.mystartsearch.com** No user permission required.In fact, MyStartSearch will edit browser settings to redirect users to ads and make money.

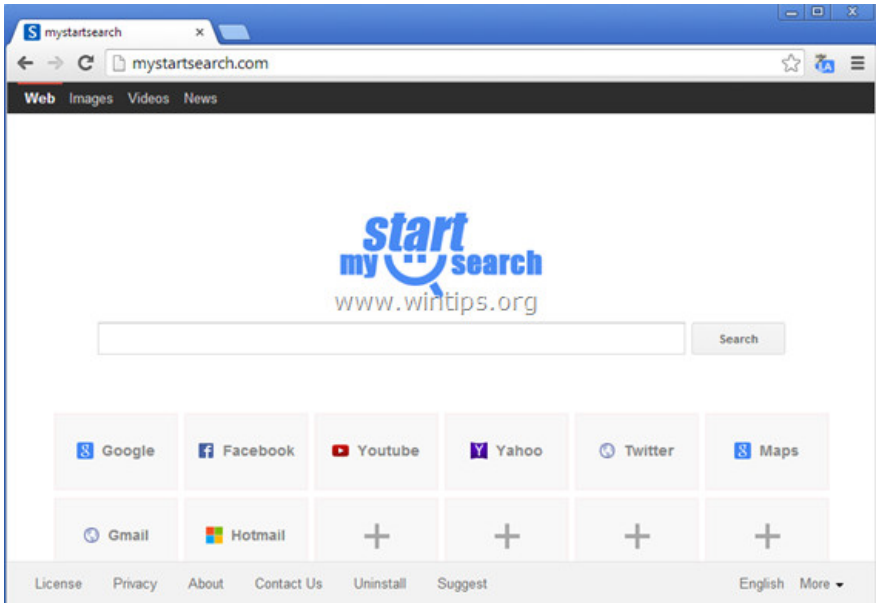
MyStartSearch is designed to edit browser settings and can install additional plugins (toolbars, extensions - extensions or add-ons) on browsers for the convenience of adding links or other ads. on the browser. The attacker of this browser can redirect the user's computer to malicious websites or may install malicious programs to attack the security system on the user's computer.

Technically, MyStartSearch is not a virus but it is an unwanted program (PUP), which can be installed on your computer. If the ad software MyStartSearch attacks the system, whenever accessing and browsing on the Internet, the screen will display popup windows, advertising banners, etc. in some cases that is the cause. making the user's computer slow, browsing speed slowing down.

Therefore when installing any software, certain programs that you download from the Internet or always pay attention to the installation terms of the program because the software installers will contain the installation part Additional soft you don't want.

Simply put, do not install any unrelated software attached to the program or software installer that you want to install. When installing any one program on your computer:

1. On the installation screen, do not click Next continuously without reading the terms.
2. Read the terms carefully before clicking Accept.
3. Always choose Custom installation.
4. Refuse to install additional software that you do not want to install.
5. Disregarding the options says that the browser homepage and search engines will be changed.



Remove MyStartSearch on all browsers

Step 1: Remove MyStartSearch with RogueKiller

RogueKiller is one of the programs against effective malware (malware). The program can detect, prevent and remove malware (malware) in general and both rootkits, rogues, worms, .

1. Download RogueKiller to your device and install it.

Download RogueKiller to your device and install it here.

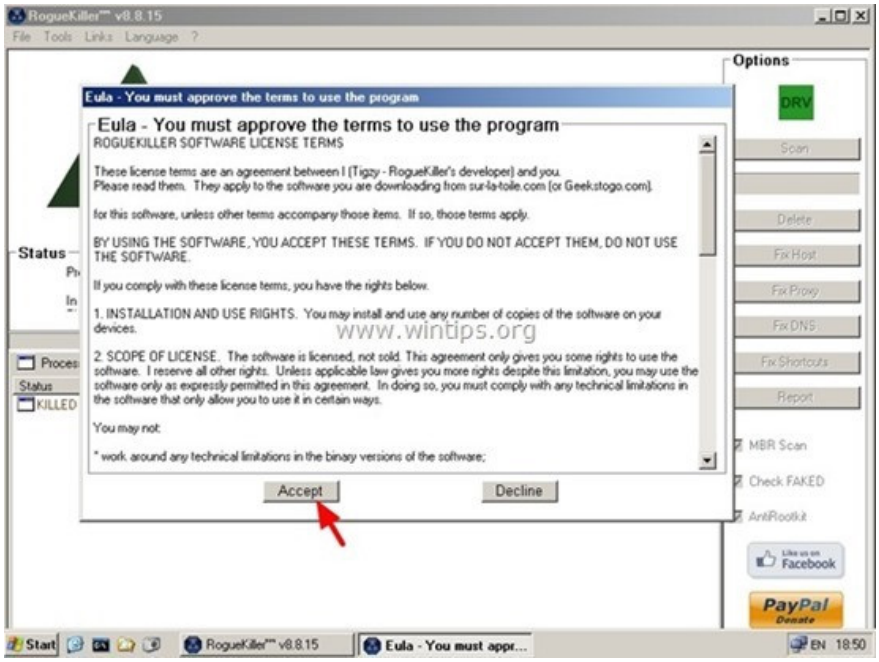
Note:

Download the x86 or x64 version that matches your operating system version. To know the version of the operating system you are using, right-click the **Computer** icon, select **Properties** and search in the **System Type section** .

2. Double click to run RogueKiller.

3. Click **Accept** to agree to the terms, install the program.

4. The next step is to click **Scan** to scan for malware on your computer and on the startup port.



5. Finally, after the scan is complete, click the **Registry** tab, select all the items containing the malware found and click **Delete** to remove all the items.

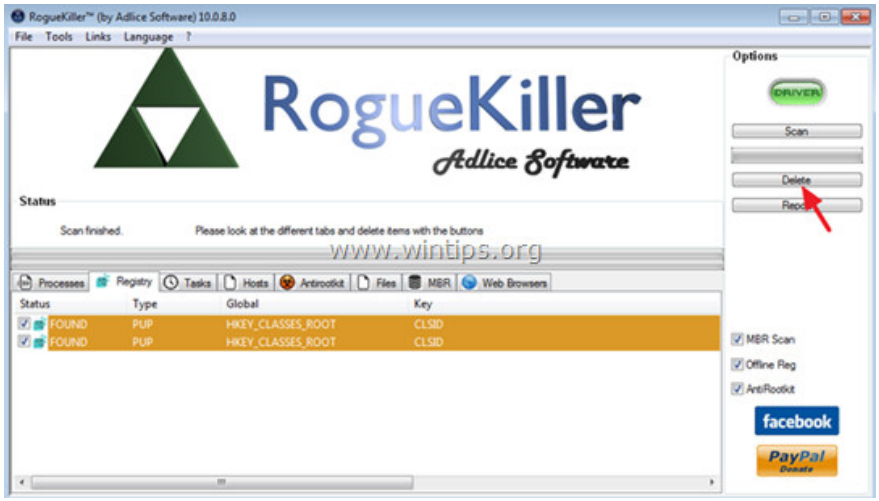
6. Close RogueKiller and proceed to the next step.

Step 2: Uninstall the malware on Control Panel

1. To do this, follow the steps below:

- On Windows 7 and Vista: **Start** => **Control Panel.**

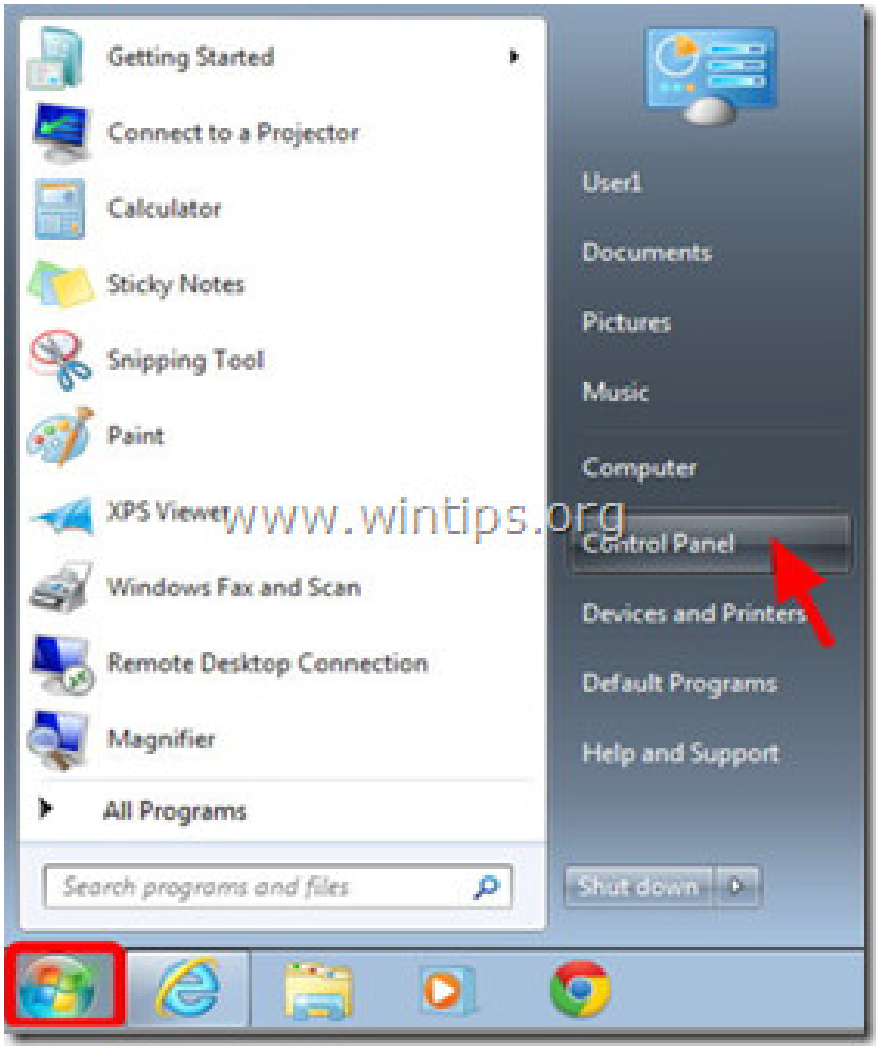
- On Windows XP: **Start** => **Settings** => **Control Panel.**



- On Windows 8 and 8.1:

Press the **Windows + R** key combination to open the Run command window.

Enter **Control Panel** in the Run window and press **Enter.**



2. At the Control Panel window:

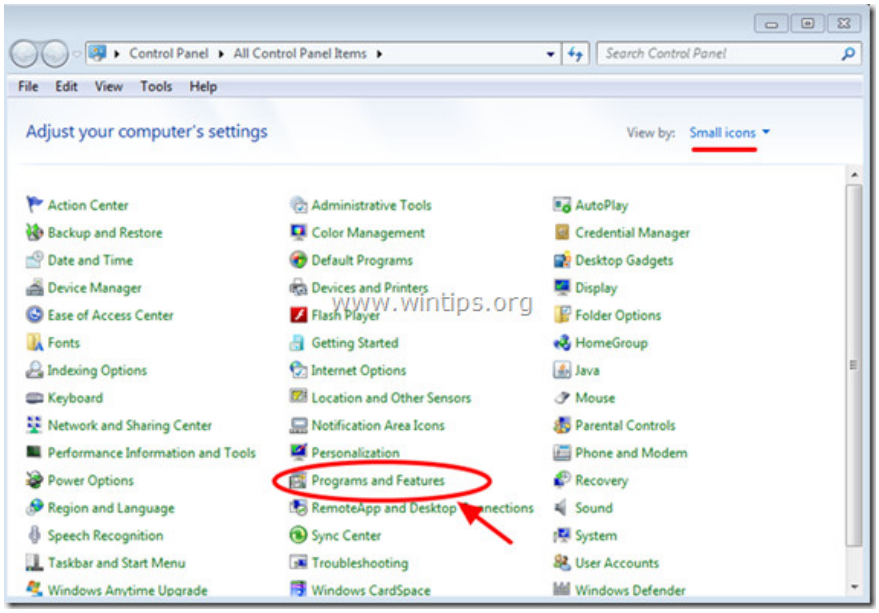
On Windows XP: select **Add or Remove Programs.**

On Windows 7, 8 or Vista: select **Programs and Features** (or Uninstall a Program).

3. In the next window, search for unknown programs in the installation section immediately, then proceed to uninstall those applications from the system.

Also find and remove malicious applications like:

1. MyStartSearch
2. SearchProtect
3. Browser Protect

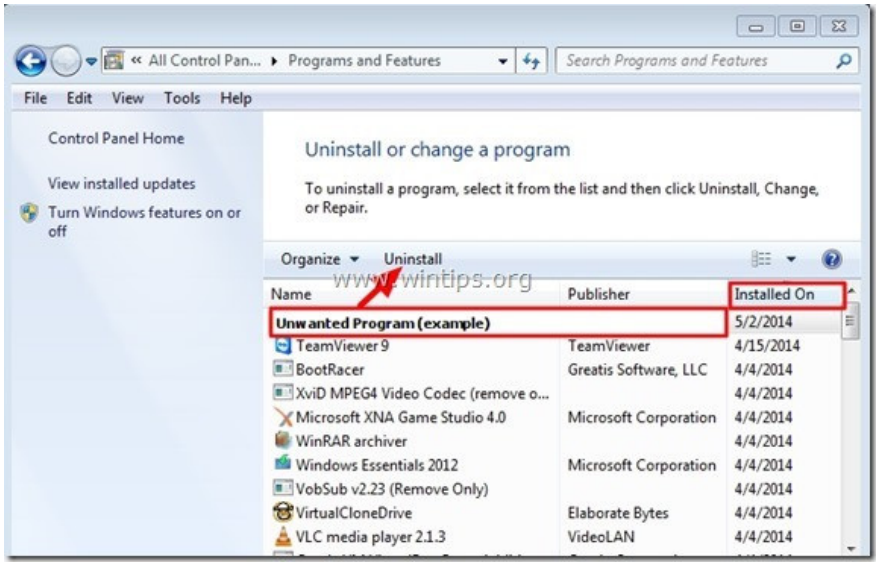


Step 3: Uninstall the 'MyStartSearch' plugin with CCleaner

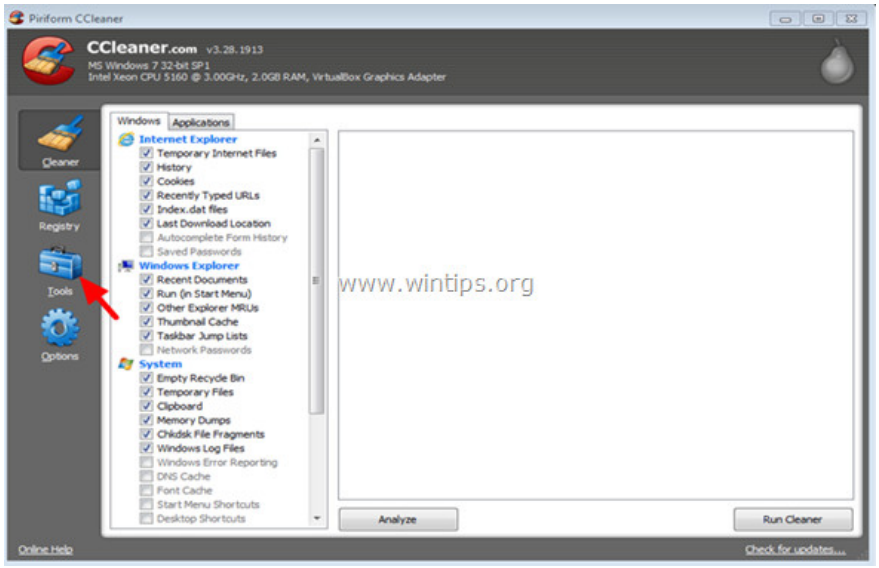
1. Download CCleaner and install it.

Download CCleaner and install it here.

2. Next run CCleaner. On CCleaner main window, select Tools in the left pane.

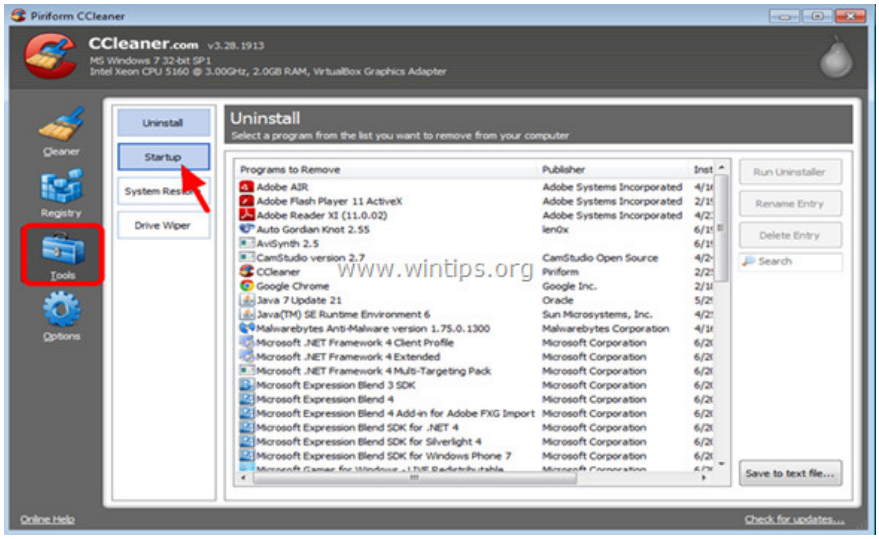


3. At Tools, click **Startup** .



4. Select the "Windows" tab and then select and delete the malware below, if they exist:

MyStartSearch



5. Finally close the CCleaner window and follow the next steps.

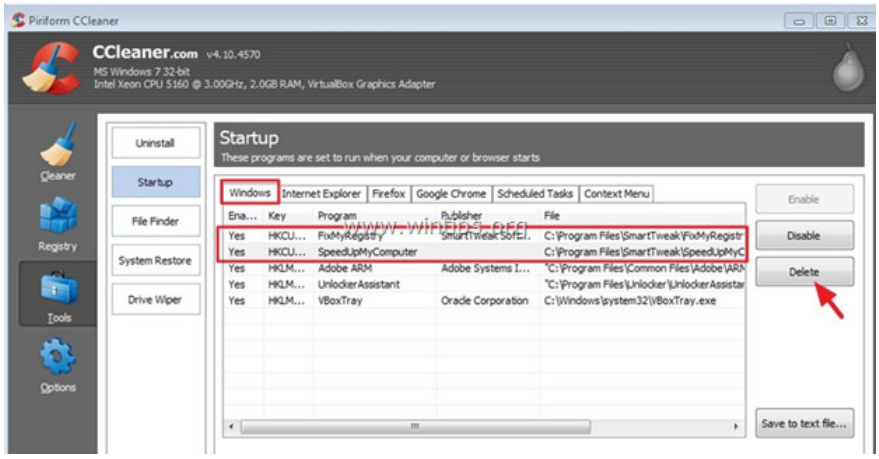
Step 4: Uninstall MyStartSearch.com on the Internet Browser shortcut

1. Right-click the Internet Explorer browser icon, then select **Properties** .

Note:

You must follow the same steps on all Internet Explorer browser shortcuts, including the Program lits list and the Taskbar.

2. On the Shortcut tab, find the Target pane and delete MyStartSearch (such as http://mystartsearch.com/…) that comes with iexplore.exe (with IE shortcut) or firefox.exe (Firefox browser shortcut) or chrome.exe (for Chrome browser shortcut), then select **OK** .



If you receive a notice of 'Provide administrator permission to change these settings', click **Continue.**

3. Follow the next steps.

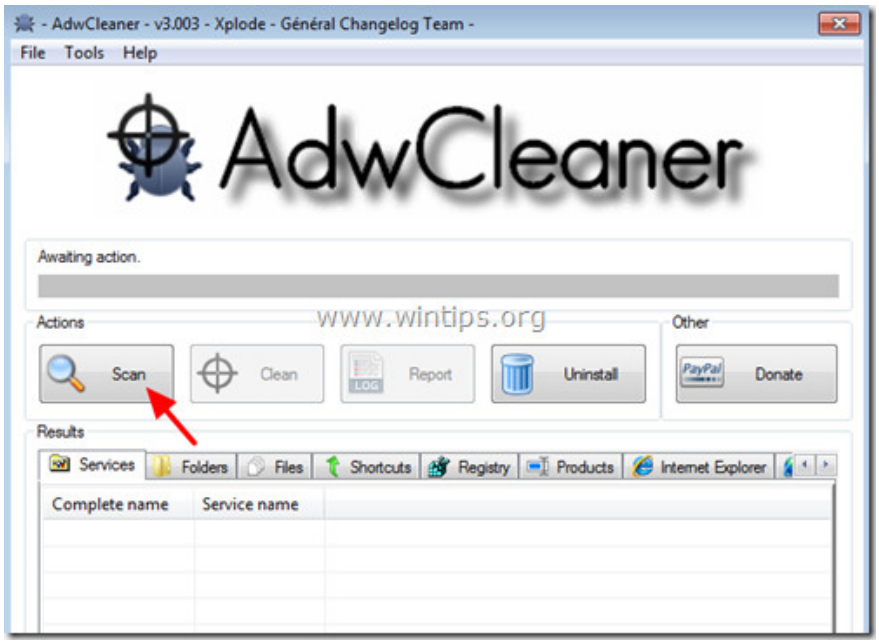
Step 5: Remove MyStartSearch with 'AdwCleaner'

1. Download AdwCleaner to your device and install it.

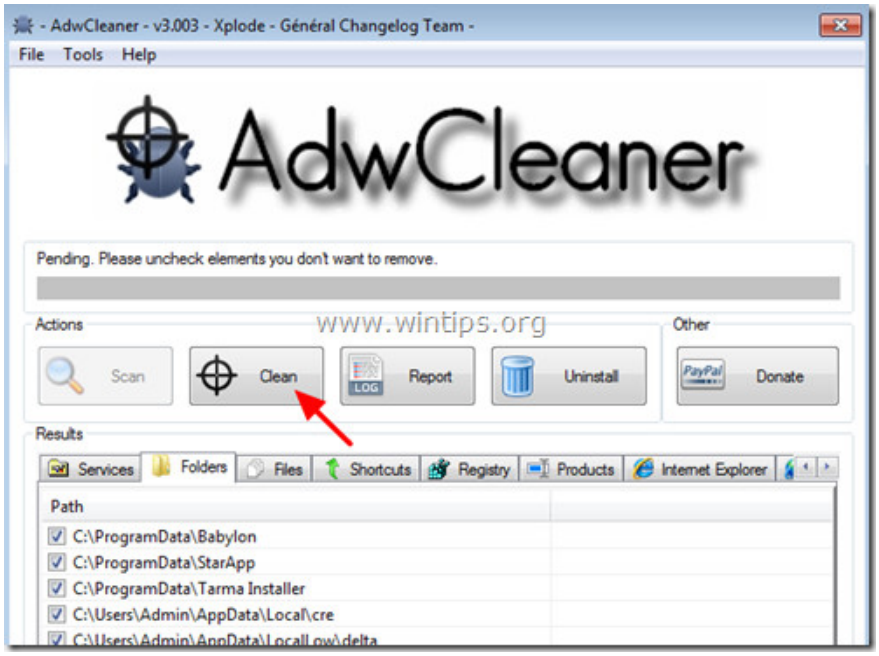
Download AdwCleaner to your device and install it here.

2. Close all open programs on your computer, then double click to open AdwCleaner.

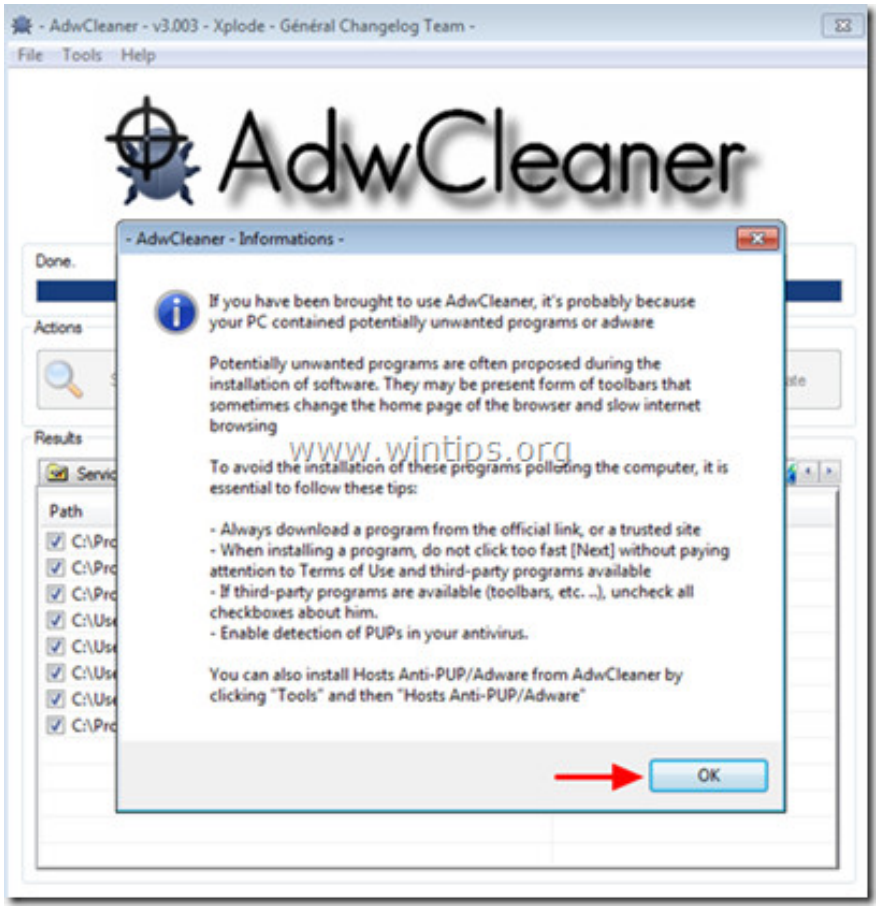
3. After accepting the terms, click the **Scan** button **.**



4. Wait until the scan has finished, click Clean to remove all unwanted malware on your system.



5. On the AdwCleaner - Information window, click **OK** , then select **OK** again to restart your computer.



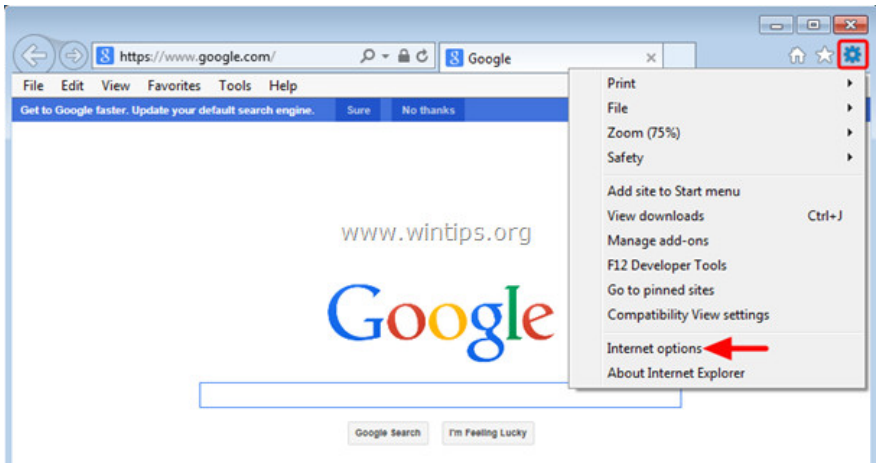
6. When your computer is restarted, close the AdwCleaner "window" and proceed to the next step.

Step 6: Remove MyStartSearch on Internet Explorer, Chrome and Firefox browsers

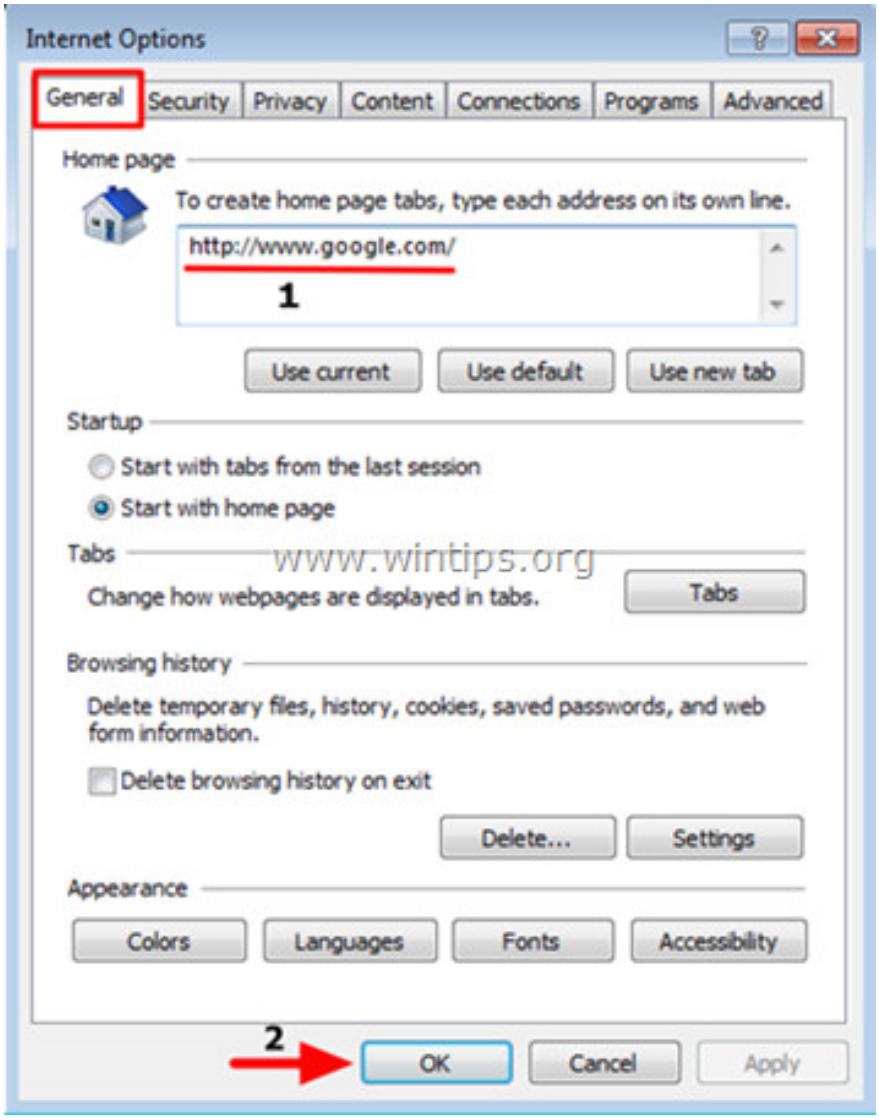
To make sure that 'MyStartSearch.com' has been completely removed from Internet Explorer, Chrome and Firefox, you reset the browser settings to their original default state.

- Internet Explorer browser:

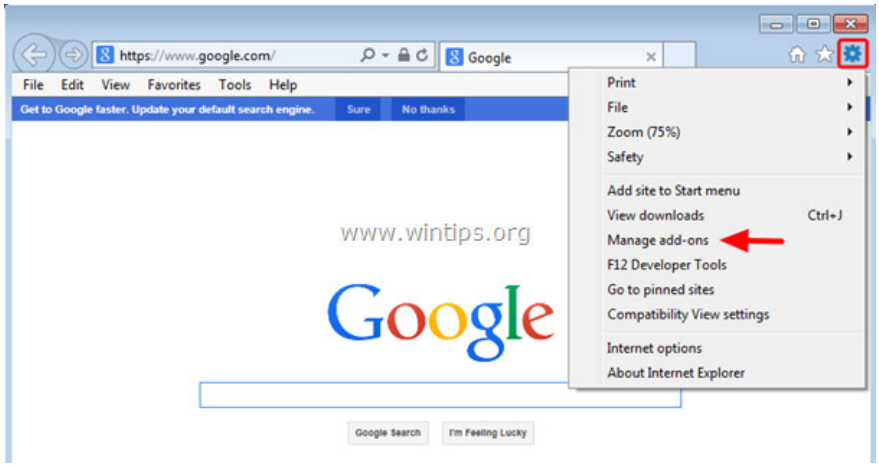
1. In Internet Explorer, click the jagged icon in the top right corner to select Tools and then select **Internet Options** .



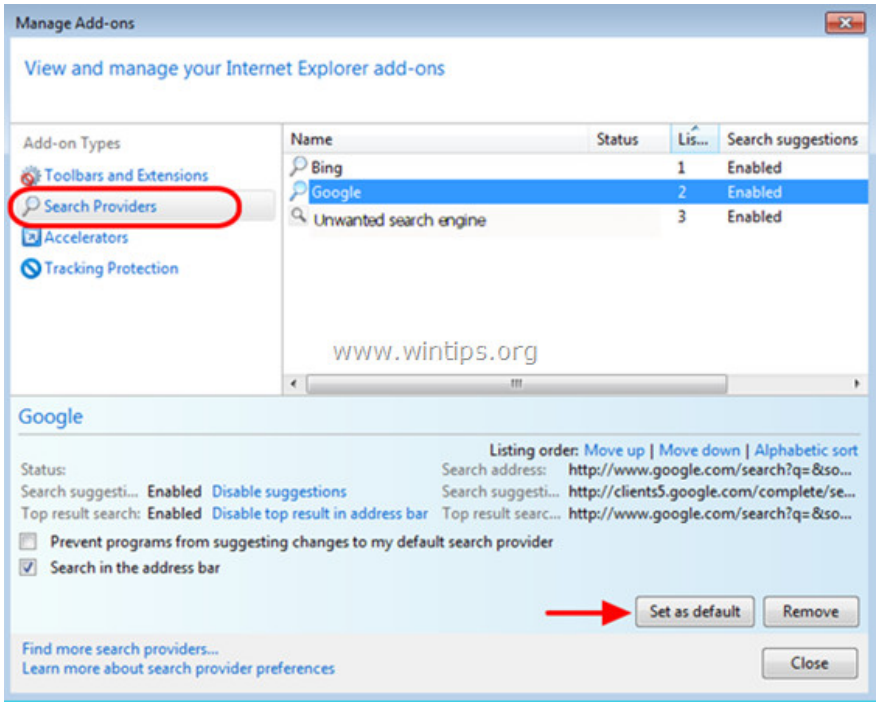
2. On the Internet Optionsn window, click on the **General** tab and delete the unwanted homepage (http://www.mystartsearch.com/…) from the Home page frame and enter the homepage you want (such as www.google .com) and then click **OK** .



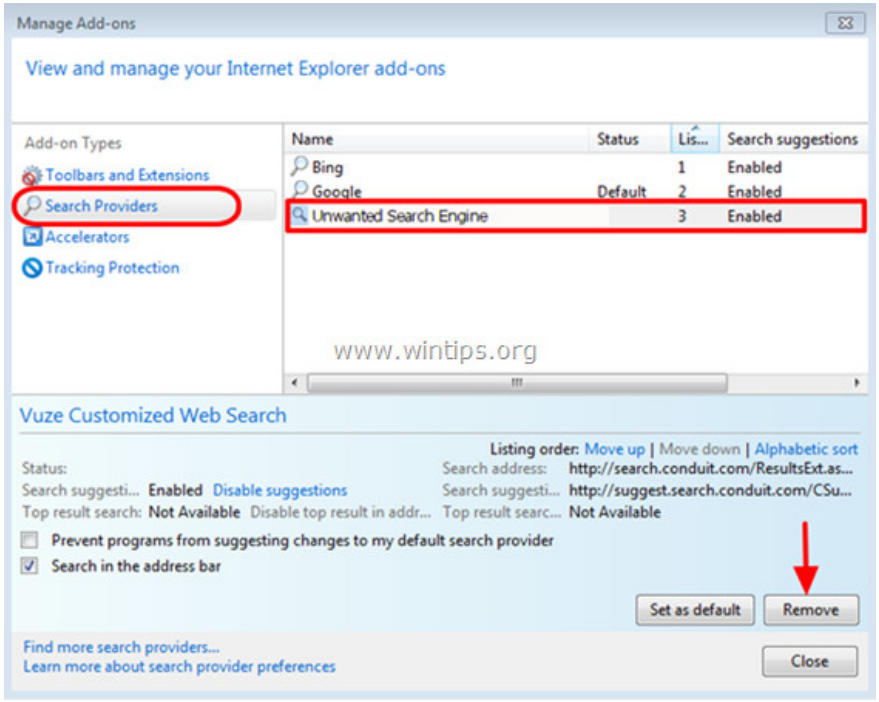
3. From the Menu Tools, select 'Manage Add-ons'.



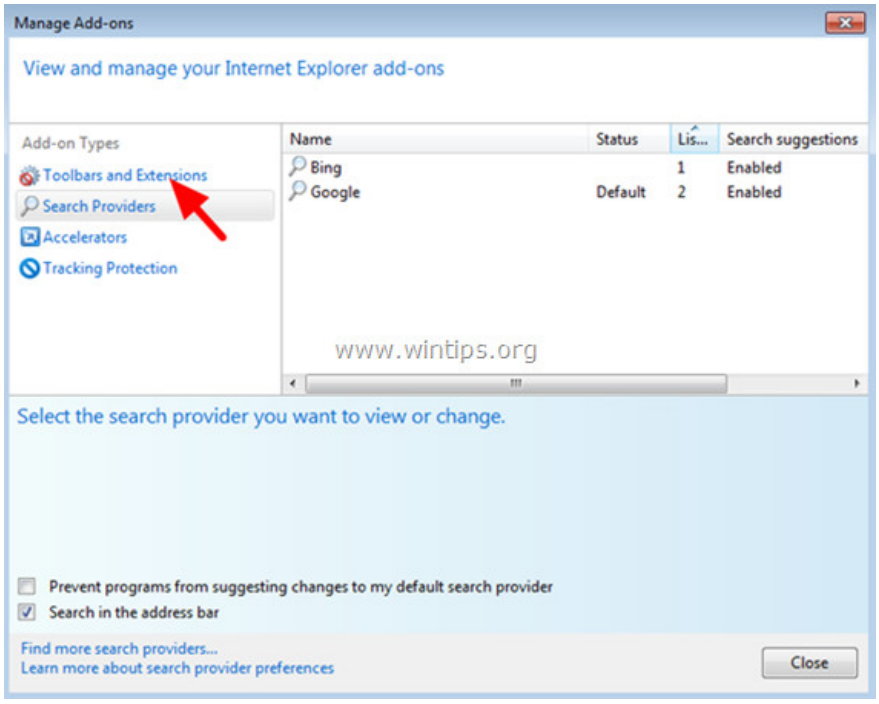
4. On the Manage Add-ons window, in the Search Providers section, select and set a default search tool as Set to replace the MyStartSearch search engine.



5. Next select MyStartSearch and then click **Remove** .



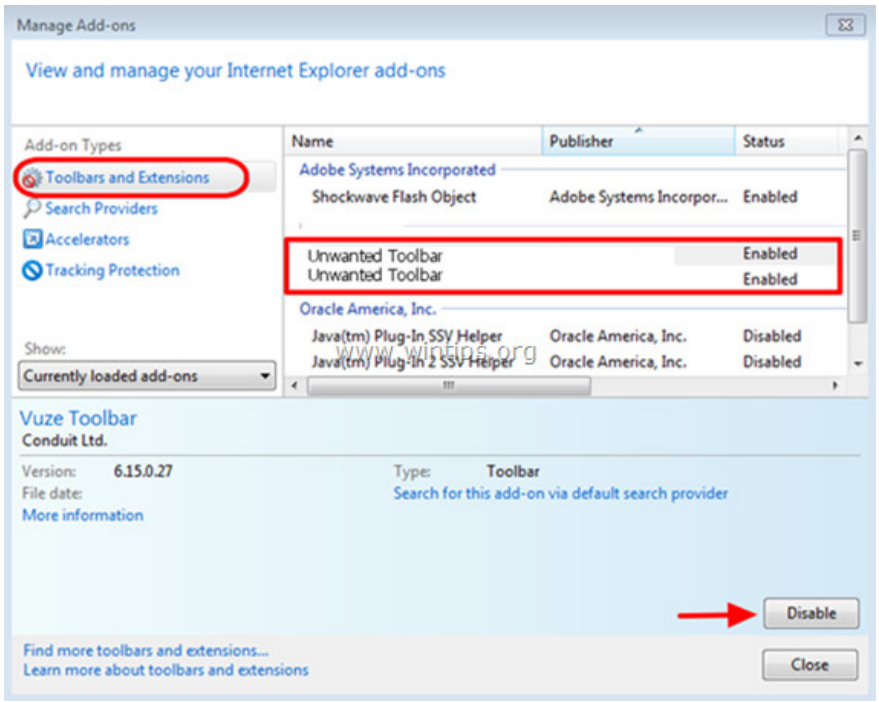
6. Select **Toolbars and Extensions** in the left pane.



7. Disable the unwanted toolbar or extension (My extension) from MyStartSearch.

The extensions should be removed / disabled in this case:

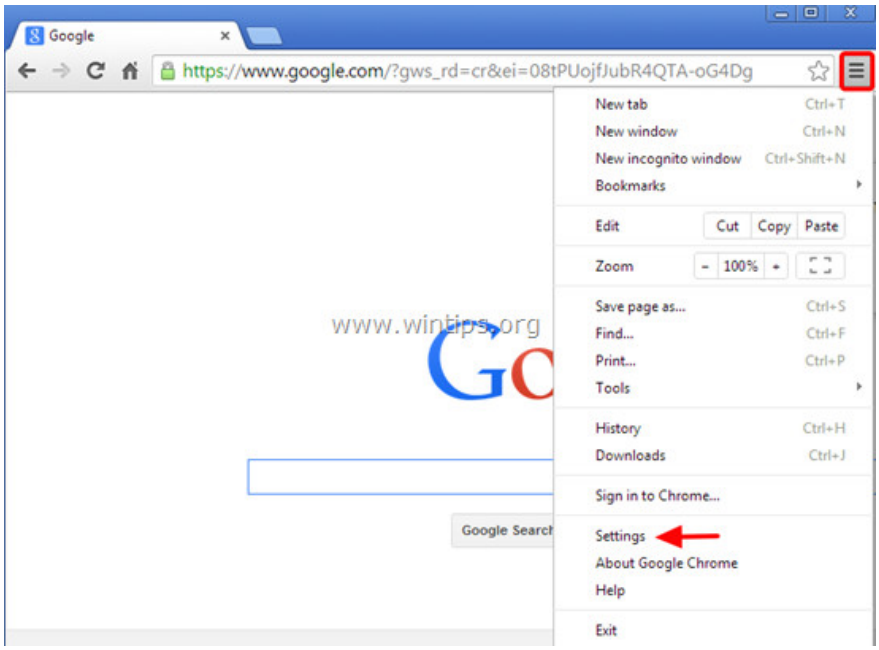
MyStartSearch



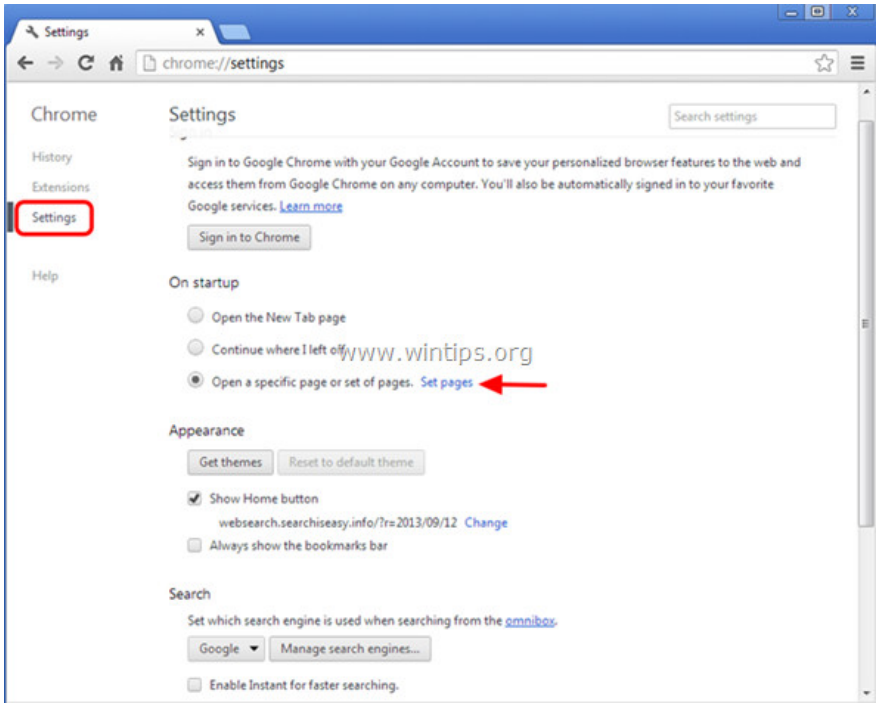
8. Close all Internet Explorer windows and restart the Internet browser.

- On Chrome browser:

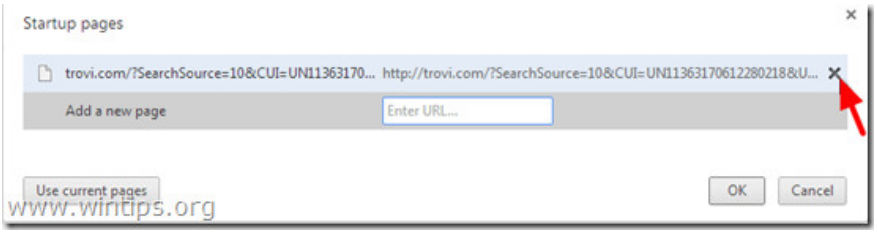
1. Open the Chrome browser on your computer, then click the 3 dash icon icon in the top right corner of the screen, select Settings.



2. On the Settings window, find the On startup section and select **Set Pages** .

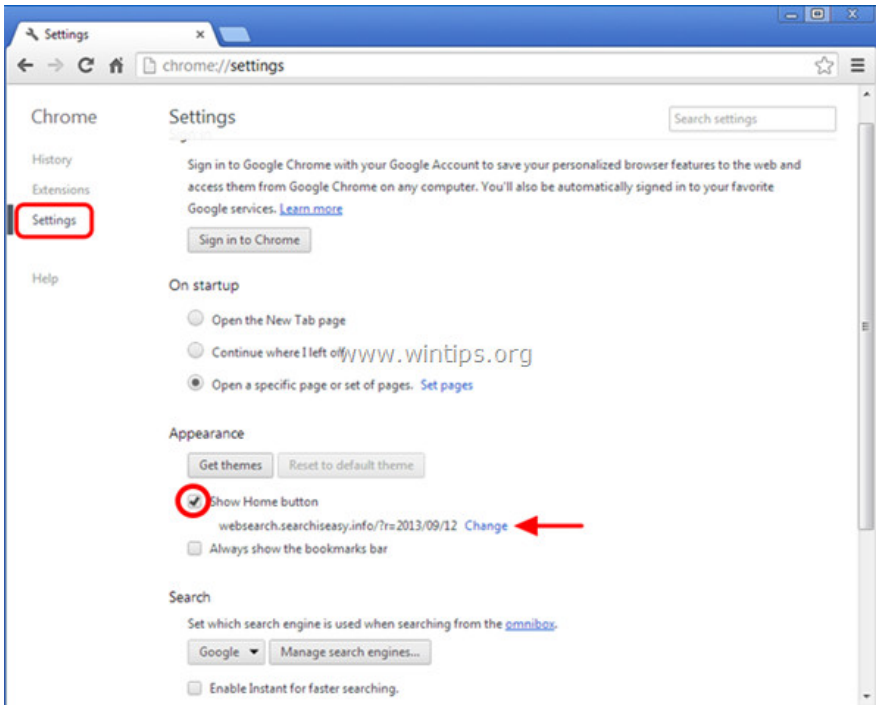


3. Delete http://www.mystartsearch.com in the Startup page section by clicking the x icon in the right pane.

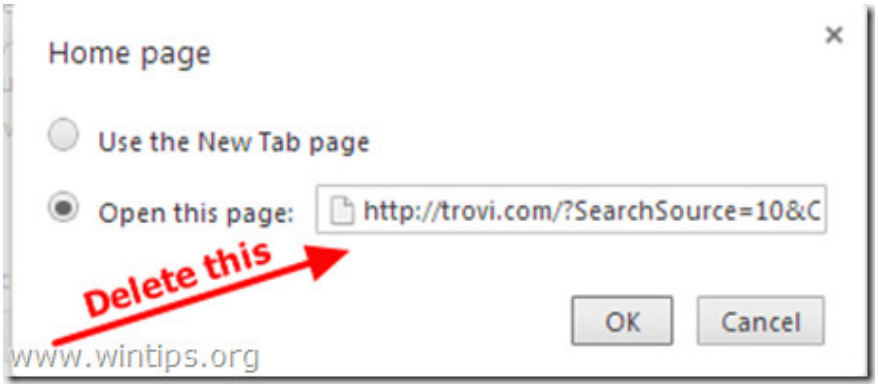


4. Set up the startup page you want (such as http://www.google.com) and then click OK.

5. In Appearance, check the box to activate the **Show Home button** option and click **Change** .

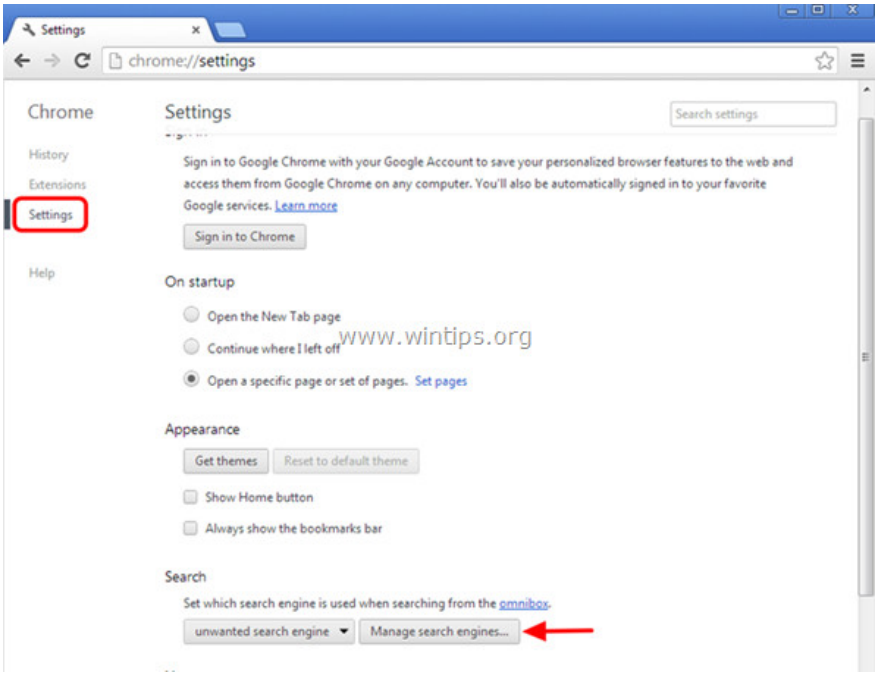


6. Delete 'http://www.mystartsearch.com' on the Open this page frame.

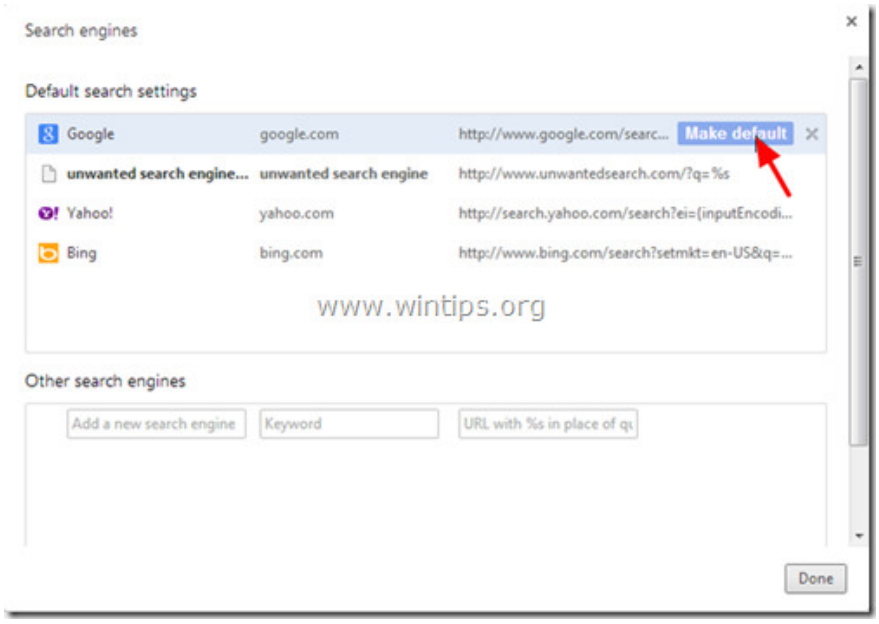


7. Enter the website you want to open when you click the Home page button or leave it blank and click OK.

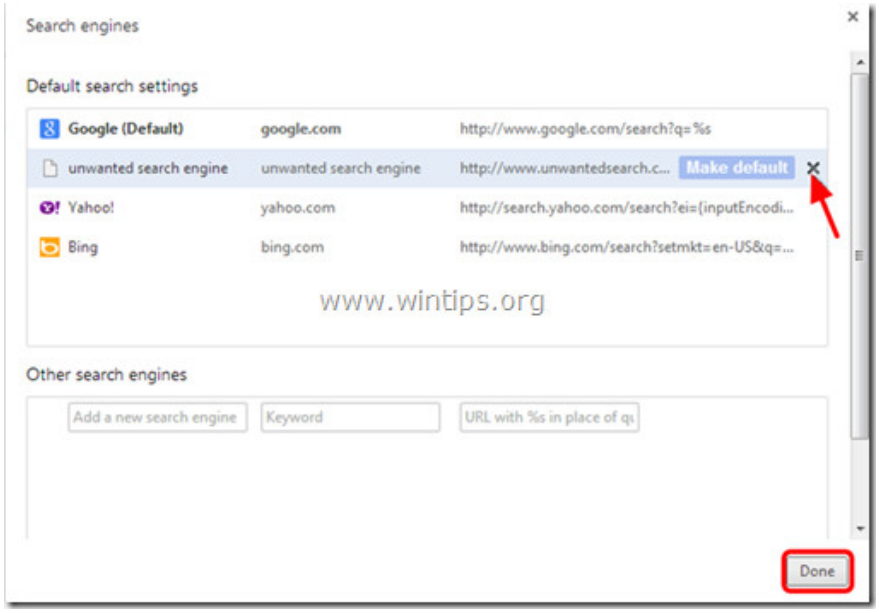
8. Go to Search section and select "Manage search engines".



9. Choose a default search engine that you want (such as Google) and then click Make default.

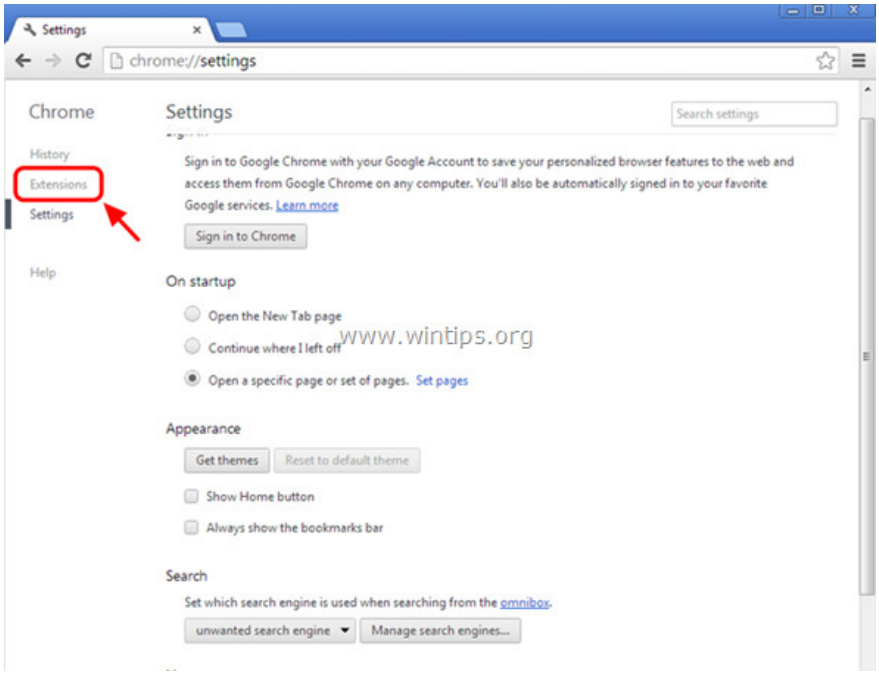


10. Then select the unwanted search engine MyStartSearch (mystartsearch.com) and remove it by clicking the X mark icon in the right corner.

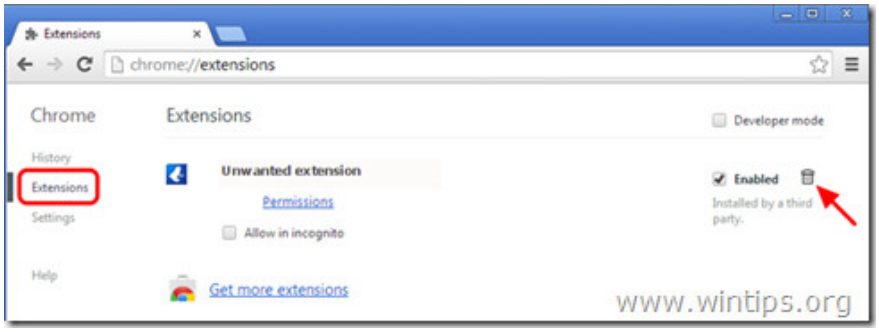


Select Done to close the " *Search engines* " window.

11. Select Extensions in the left pane.



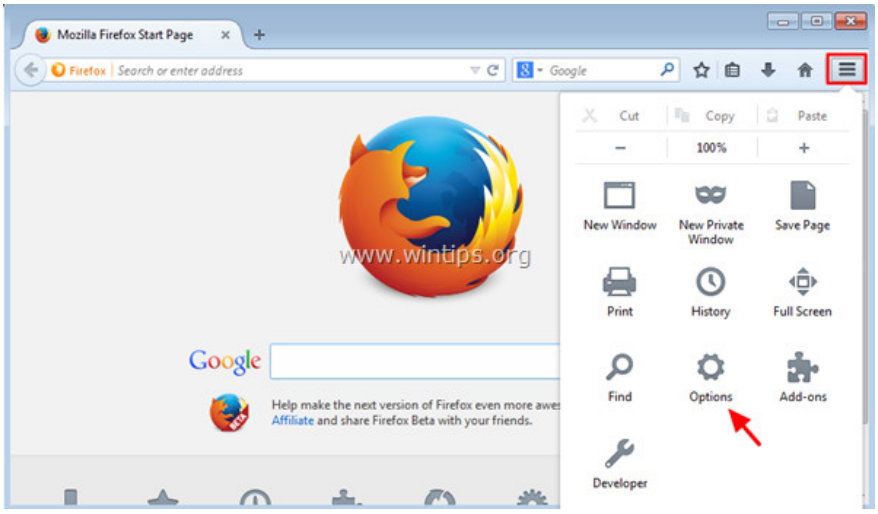
12. In the Extensions window, remove the MyStartSeach extension by clicking the trash can icon in the right pane.



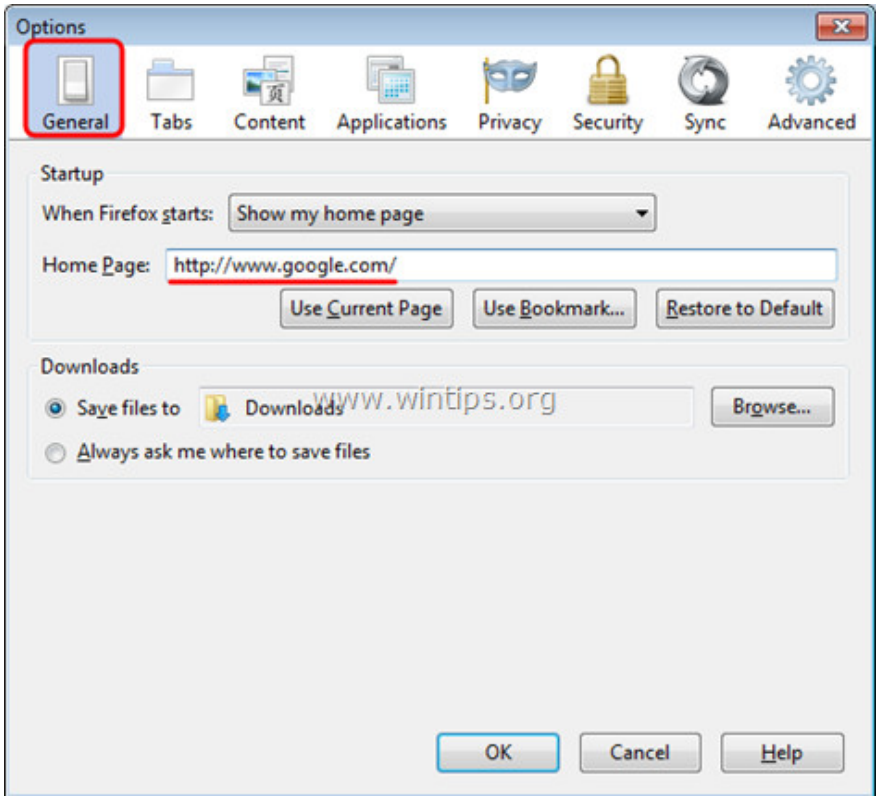
13. Close the Google Chrome window and restart the browser.

- Firefox browser:

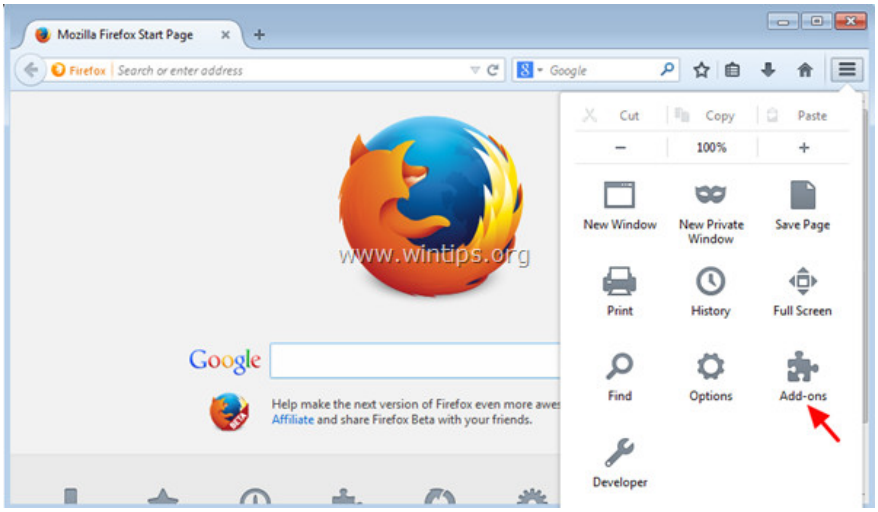
1. Click the 3 dash line icon in the top right corner of the Firefox browser window, then click Options.



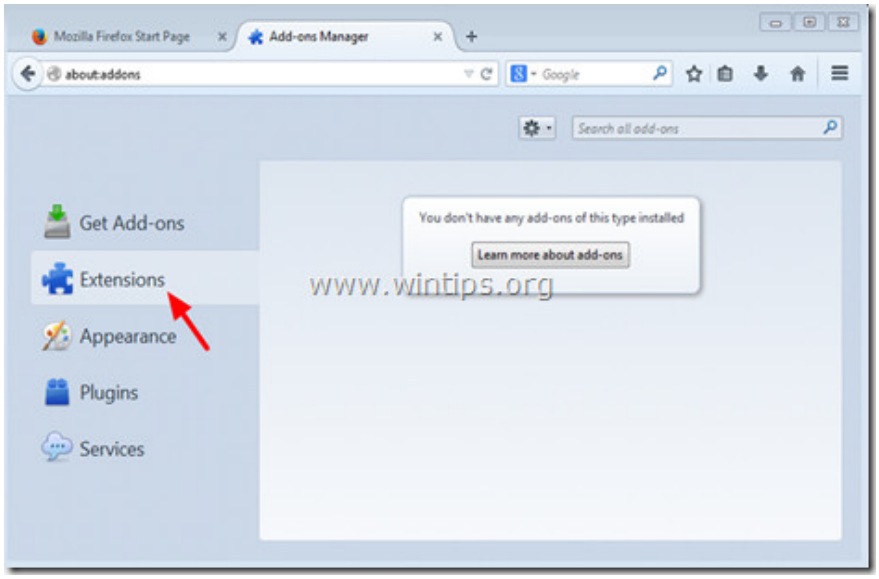
2. On the Options window, at the General tab, at the Homepage, delete 'http:///www.mystartsearch.com .' and add the homepage you like (such as http://www.google.com) then click OK.



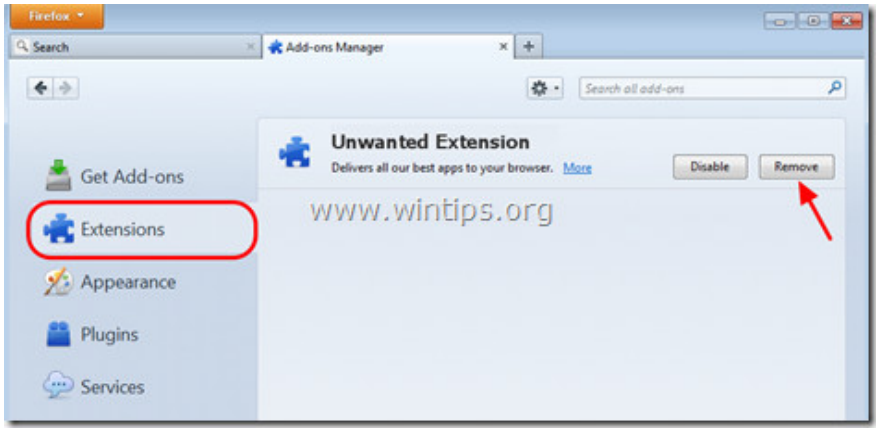
3. From the Firefox Menu, go to **Tools => Manage Add-ons** .



4. Select Extensions in the left pane.



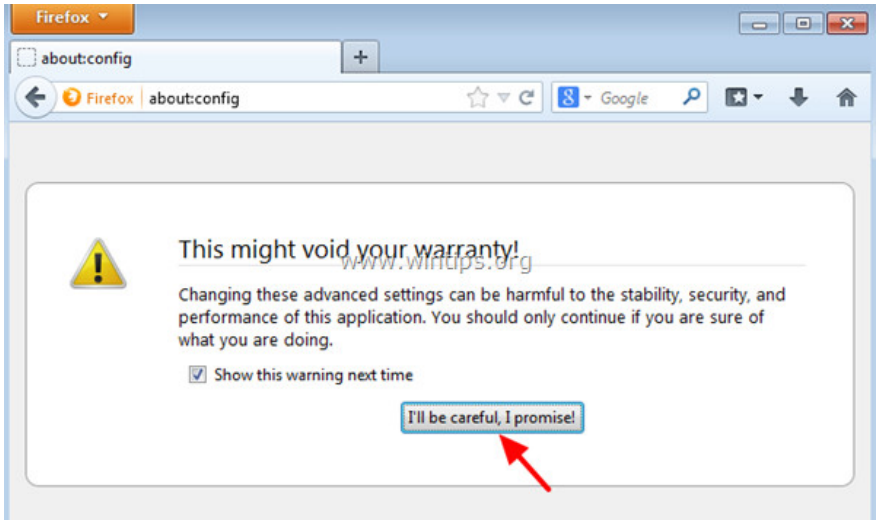
5. Remove all unwanted extensions (eg MyStartSearch) by clicking the Remove button.



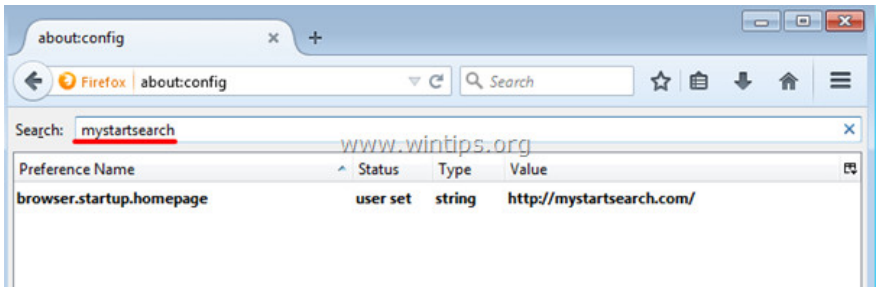
6. Close all Firefox windows and restart the browser.

7. In Firefox browser URL box, enter about: config command there and press Enter.

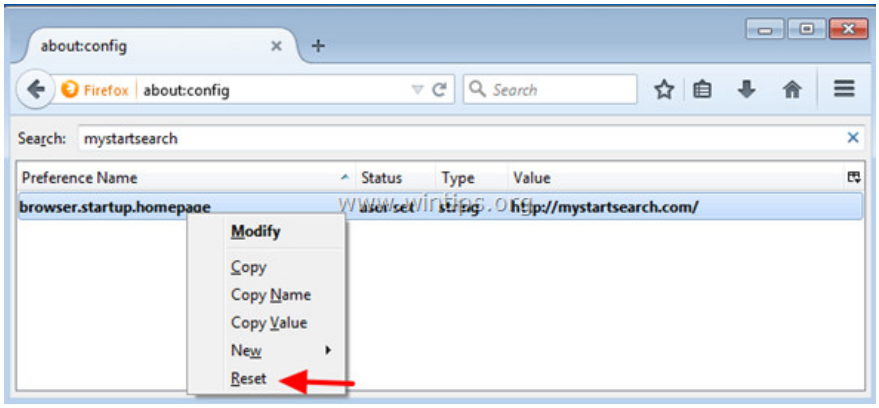
8. Click on ' *I'll be careful, I promise* '.



9. On the Search box, enter mystartsearch there and press Enter.



10. Next right click on the value of mystartsearch and then select Reset.



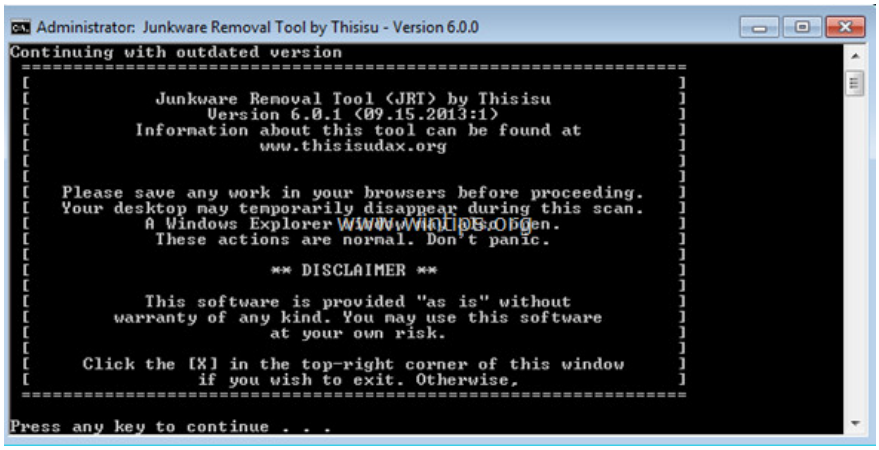
11. Close the Firefox window and restart the browser.

Step 7: Delete Mystart-Search using the Junkware Removal Tool

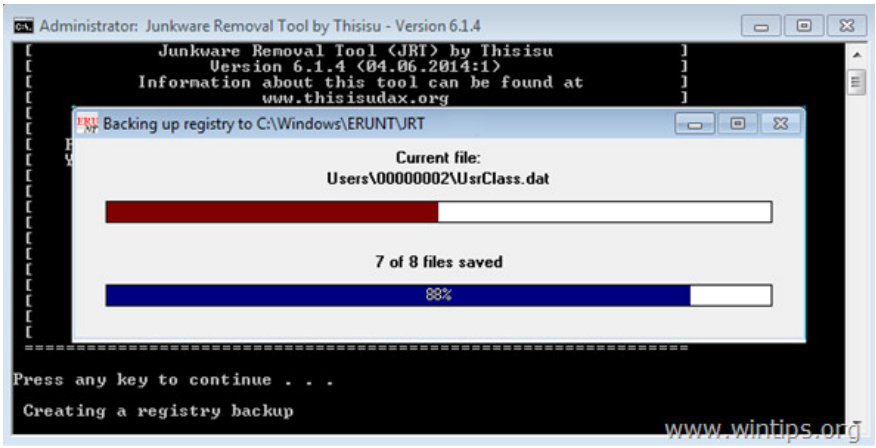
1. Download the Junkware Removal Tool on your device and run the tool.

Download the Junkware Removal Tool on your device and install it here.

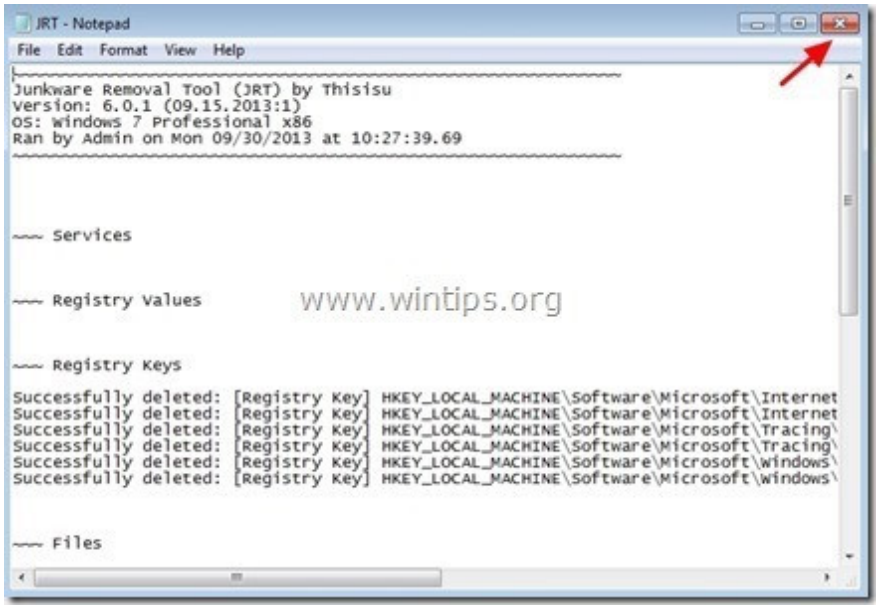
2. Press any key to start scanning your computer using the JRT - Junkware Removal Tool.



3. Wait until the JRT - Junkware Removal Tool scans and "cleans" your system.



4. Close the JRT window and restart your computer.



Step 8: Remove Mystartsearch by Malwarebytes Anti-Malware

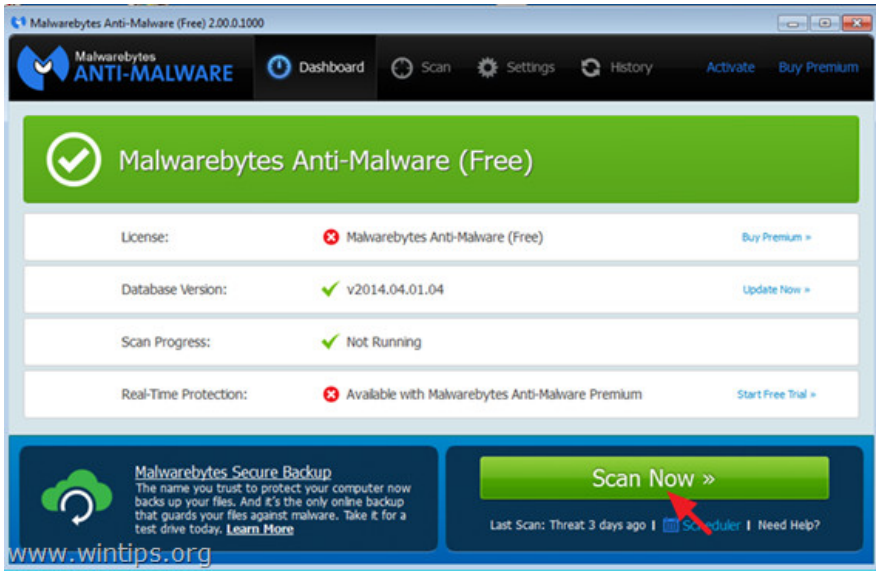
Download Malwarebytes Anti-Malware Premium to your device and install it.

Download Malwarebytes Anti-Malware Premium to your computer and install it here.

Scan and clean your computer with Malwarebytes Anti-Malware:

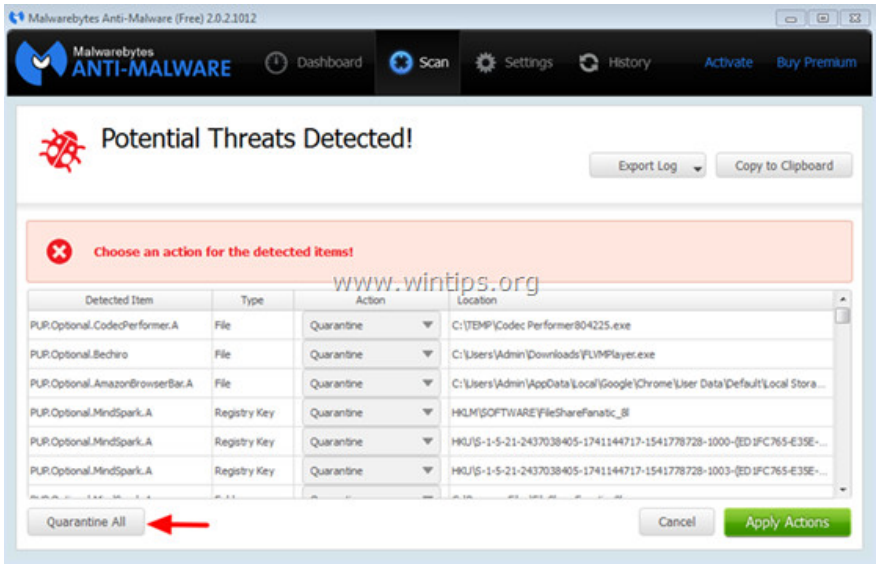
1. Run Malwarebytes Anti-Malware and allow the program to update (update) the latest version (if needed).

2. After the update process finishes, click the **Scan Now** button to start the scan of your system, remove malware and unwanted programs.

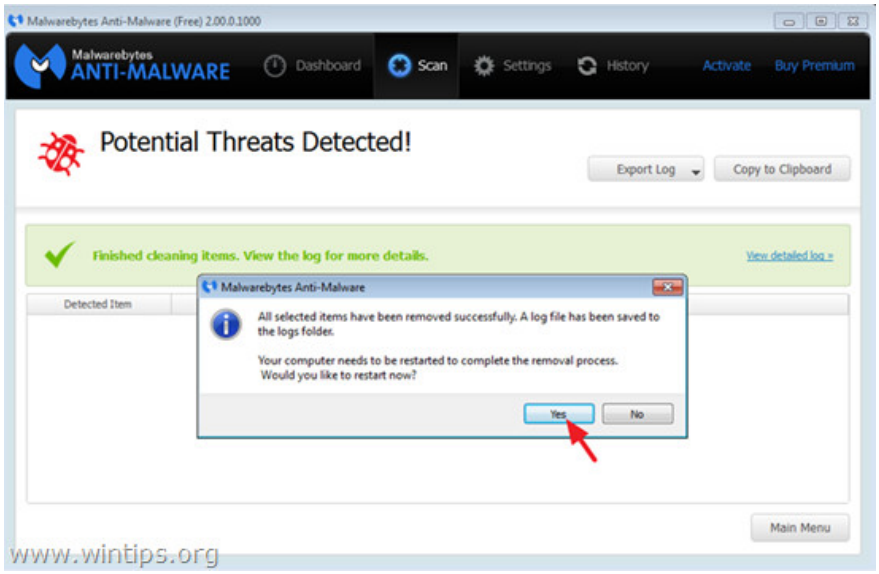


3. Wait until the system scan finishes.

4. Click the **Quarantine All** button to remove all "threats" found on your system.



5. After the process has finished, restart your computer to complete the process.



6. After the computer has finished booting, run Malwarebytes' Anti-Malware again to confirm there are no "threats" on your system.

Step 9: Clean up unwanted files with CCleaner

In addition, you can use CCleaner to clean up the system and temporary internet files and invalid registry entries.

If your computer does not have CCleaner installed, you can download CCleaner and install it here.

Refer to some of the following articles:

1. Chrome browser on Windows computer crashes, this is what you need to do

1. How to remove Trustedsurf.com on Chrome, Firefox and Internet Explorer

1. Rooted Delta Search on Chrome, Firefox and Explorer browsers

Good luck!

You finished reading the article "**Instructions to remove MyStartSearch on all browsers**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
