How to remove Adware and pop-up ads (Removal Guide)

This page is a comprehensive guide, which will remove Pop-up Ads from Internet Explorer, Firefox and Google Chrome.
Please perform all the steps in the correct order. If you have any questions or doubt at any point, **STOP** and ask for our assistance.
STEP 1: Uninstall Pop-up Ads malicious programs from your computer
STEP 2: Remove Pop-up Ads from Internet Explorer, Firefox and Chrome
STEP 3: Remove Pop-up Ads adware with AdwCleaner
STEP 4: Remove Pop-up Ads browser hijackers with Junkware Removal Tool
STEP 5: Remove Pop-up Ads virus with Malwarebytes Anti-Malware Free
STEP 6: Double-check for the Pop-up Ads infection with HitmanPro

STEP 1 : Uninstall Pop-up Ads program from your computer

Most Pop-up Adss will install a program on your computer, while this is not a general rule, we will need to check for any malicious programs.
In this first step, we will try to identify and remove any malicious program that might be installed on your computer.

1. To uninstall the program that has installed is responsible for the pop-up ads, click the **Start** button, then click on the **Control Panel** menu option.

If you are using **Windows 8**, simply drag your mouse pointer to the right edge of the screen, select **Search** from the list and search for "*control panel*" .Or you can **right-click on a bottom left hot corner** (formerly known as the Start button) and select **Control**

Panel from there.

2. When the *Control Panel* window opens click on the **Uninstall a program** option under *Programs* category. This option is shown by the arrow in the image below. If you are using the *Classic View* of the Control Panel, then you would double-click on the **Programs and Features** icon instead.

3. When the **Programs and Features** or the **Uninstall a Program** screen is displayed, scroll through the list of currently installed programs and uninstall **AlllCheapPeruiCe 5.2**, **YoubeAdBlocker 1.2**, **TheBlooccker 1.3**, **Video Player**, **Plus-HD 1.3**, **BetterSurf**, **CouponMeApp**, **TubeAdblOCkER**, **BLoCkTheADApp 3.2**, **WatchItAdBlocake**, **Media Player 1.1**, **Savings Bull**, **Start Savin**, **Websteroids**, **ScorpionSaver**, **HD-Plus 3.5**, **Media Watch**, **Re-Markit**, **Remarkable, SupTab, Key-Find uninstaller, Feven Pro 1.2, HD-Plus, HD-Professional-HQ, Quick Share** and any other recently installed unknown program from your computer.
To view the most recently installed programs, you can click on the "*Installed On*" column to sort your program by the installation date. Scroll though the list, and uninstall any unwanted or unknown programs
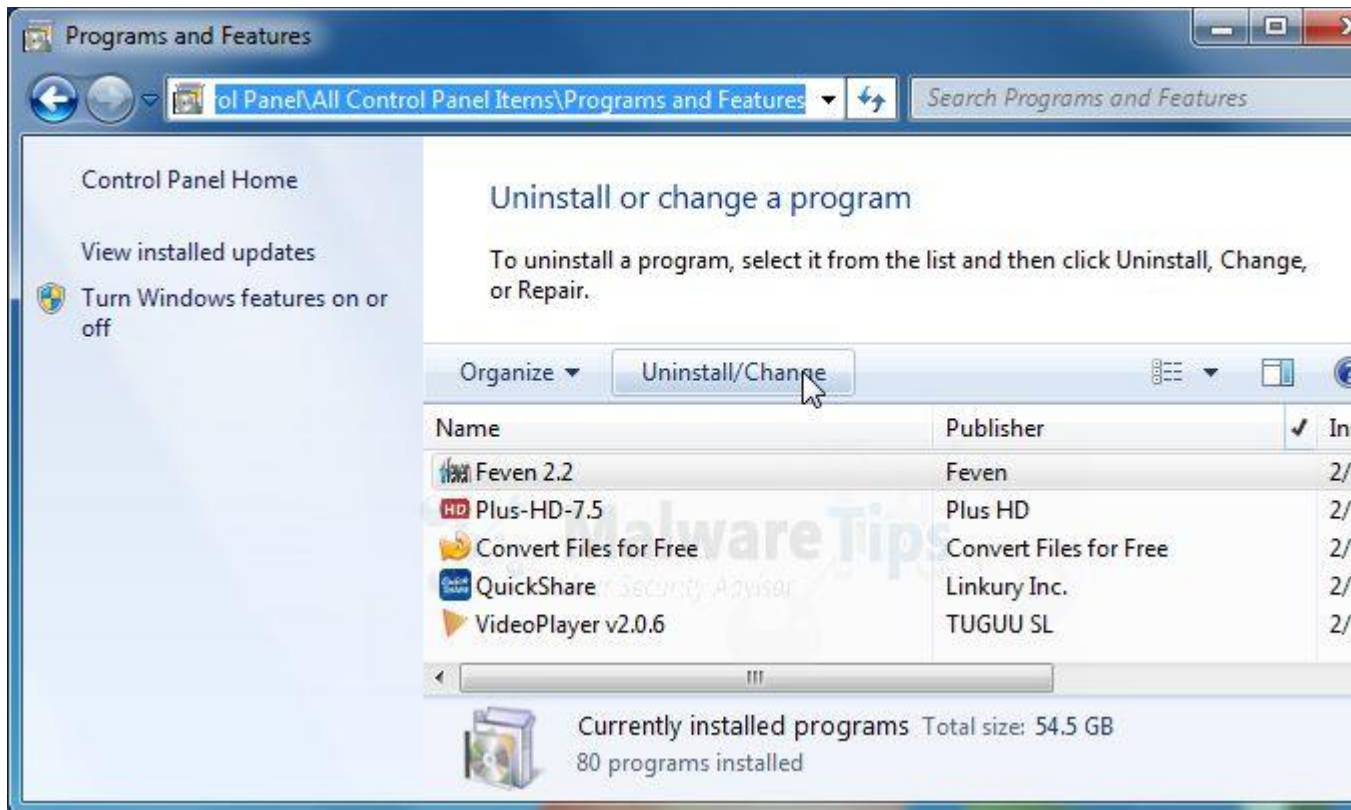
Depending on what program has installed the adware infection, the above program may have a different name or not be installed on your computer. If you cannot find any unwanted or unknown programs on your machine, then you can proceed with the next step.

# STEP 2 : Remove Pop-up Ads from Internet Explorer, Firefox and Chrome

Remove Pop-up Ads from Internet Explorer

You can reset Internet Explorer settings to return them to the state they were in when Internet Explorer was first installed on your PC.

1. Open Internet Explorer, click on the "**gear icon**" ⚙ in the upper right part of your browser, then click again on **Internet Options**.
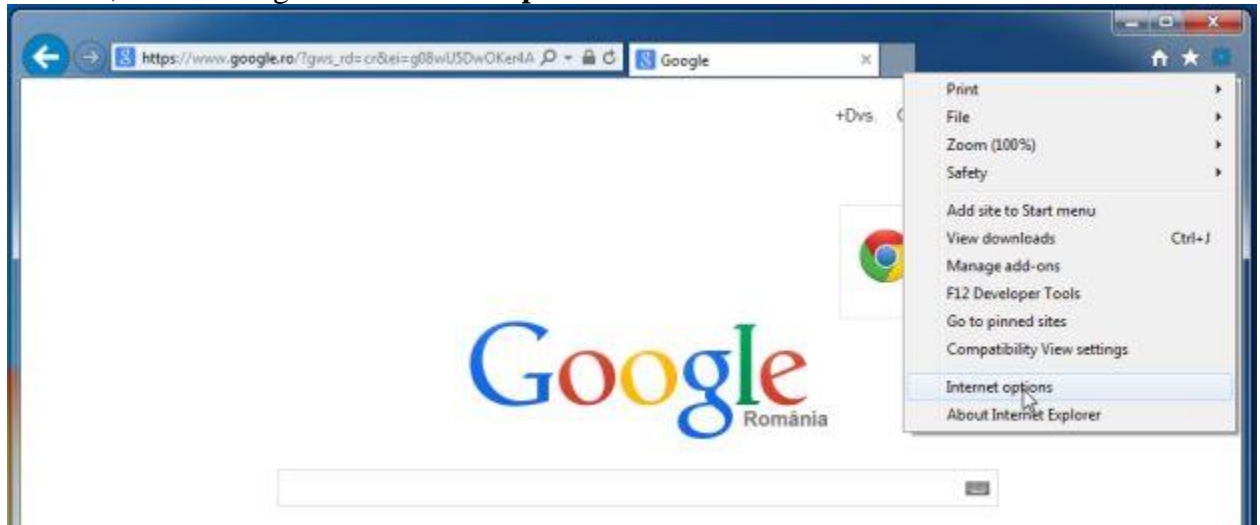
2. In the "*Internet Options*" dialog box, click on the "**Advanced**" tab, then click on the "**Reset**" button.
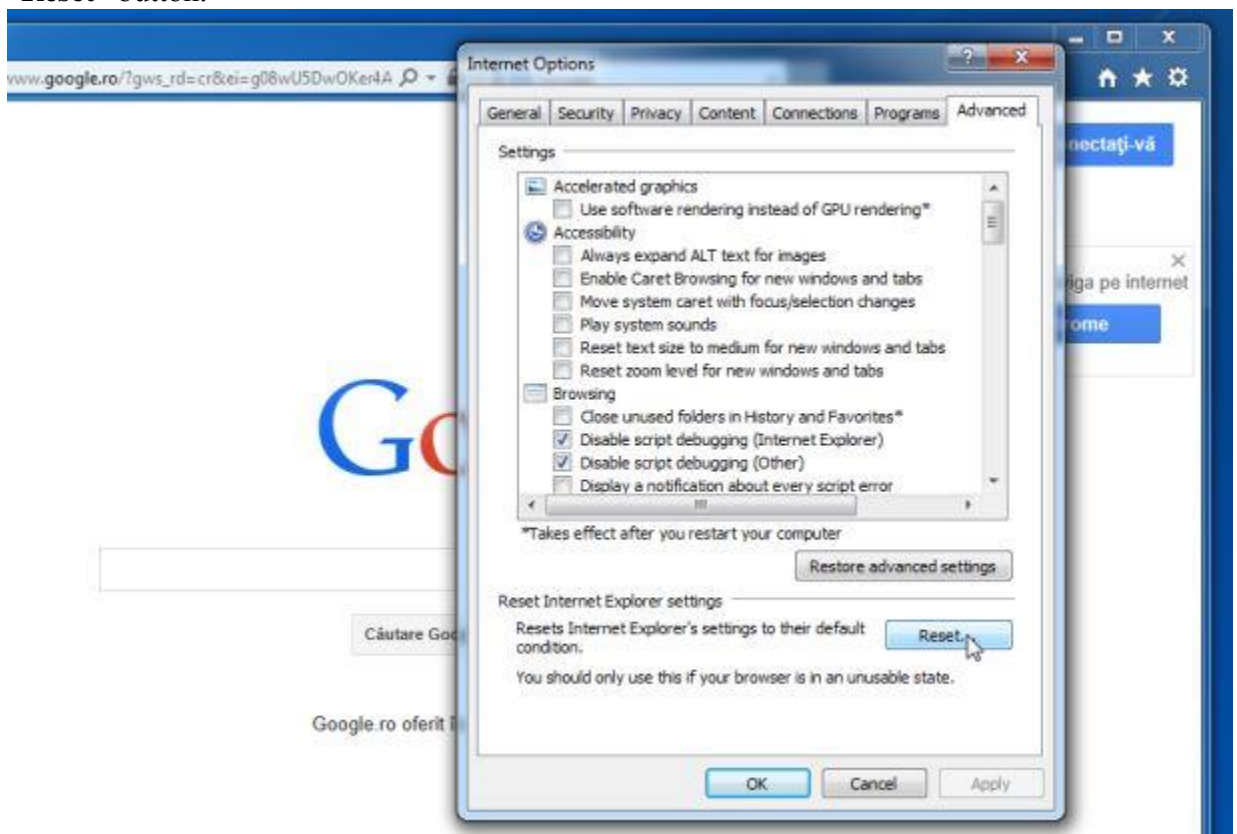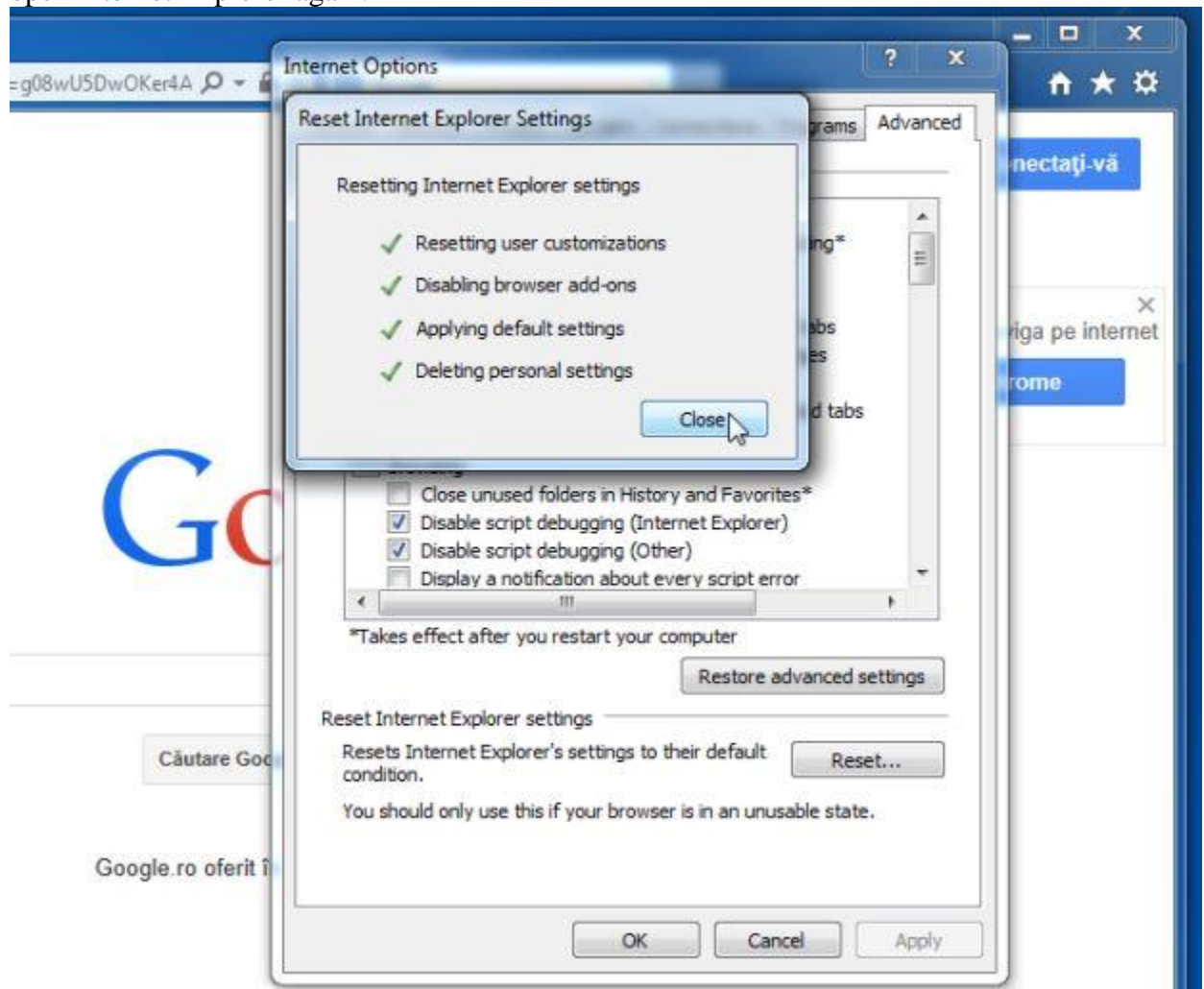
3. In the "*Reset Internet Explorer settings*" section, select the "**Delete personal settings**" check box, then click on "**Reset**" button.
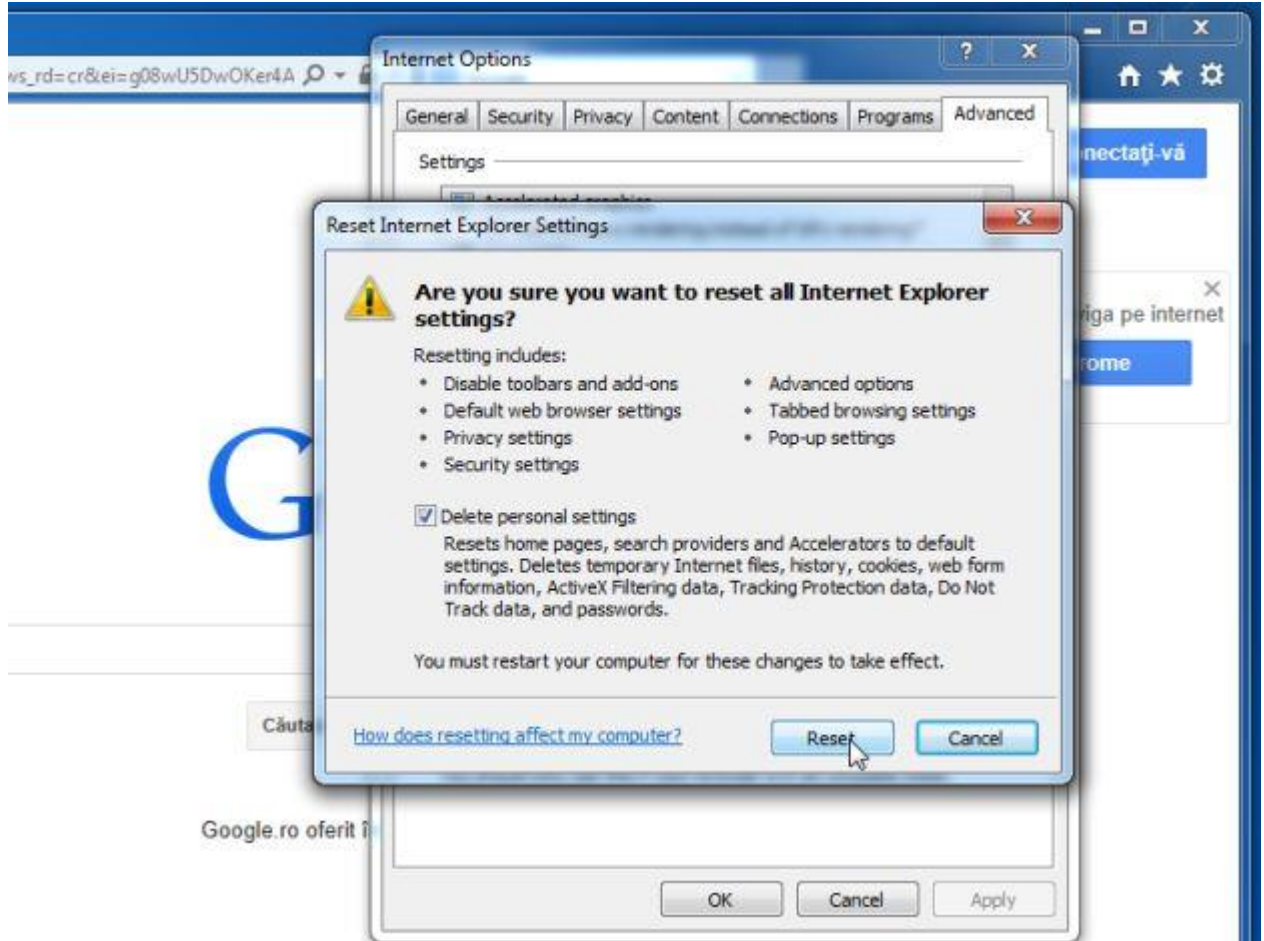
4. When Internet Explorer has completed its task, click on the "**Close**" button in the confirmation dialogue box. You will now need to close your browser, and then you can

open Internet Explorer again.

## Remove Pop-up Ads from Mozilla Firefox

If you're having problems with Firefox, resetting it can help. The reset feature fixes many issues by restoring Firefox to its factory default state while saving your essential information like bookmarks, passwords, web form auto-fill information, browsing history and open tabs.

1. In the upper-right corner of the Firefox window, click the **Firefox menu button** (≡), the click on the "**Help**" (❓) button.
   If you're unable to access the *Help* menu, type *about:support* in your address bar to bring

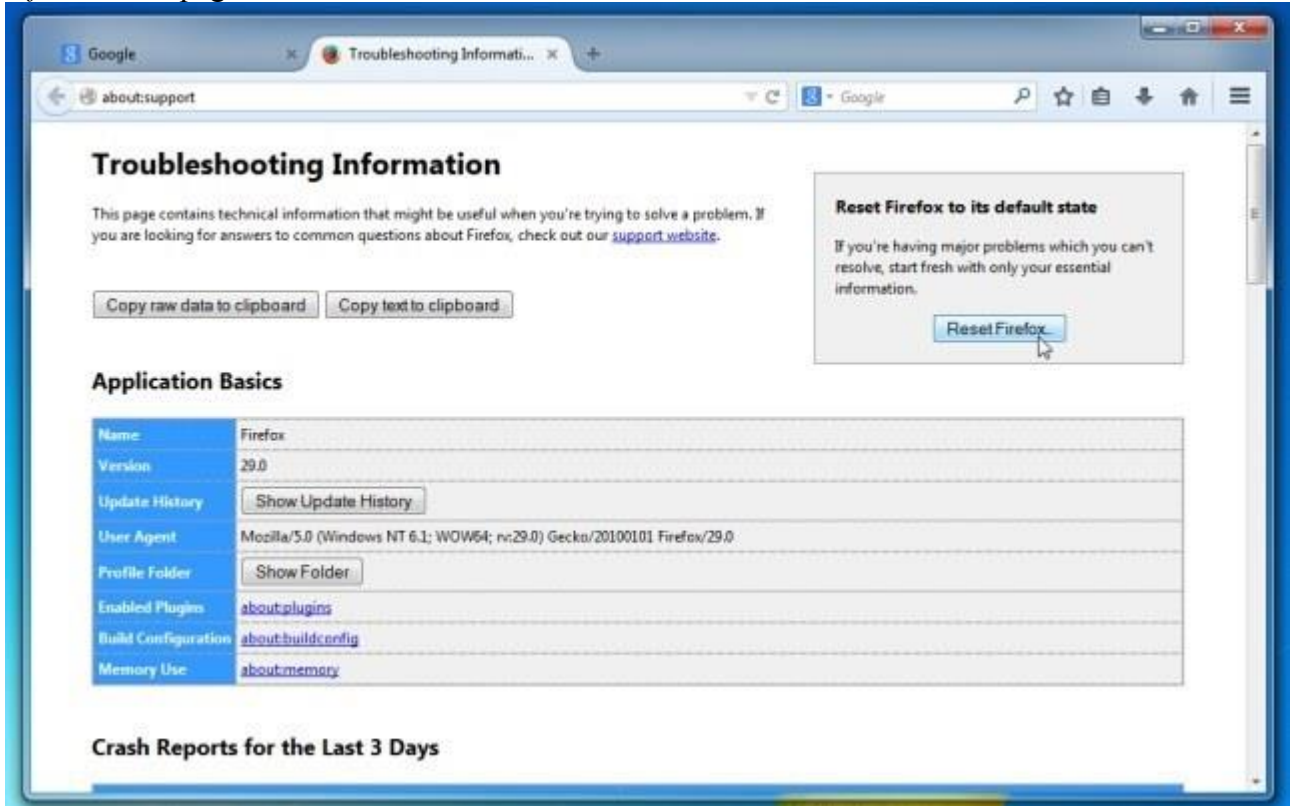up the Troubleshooting information page.
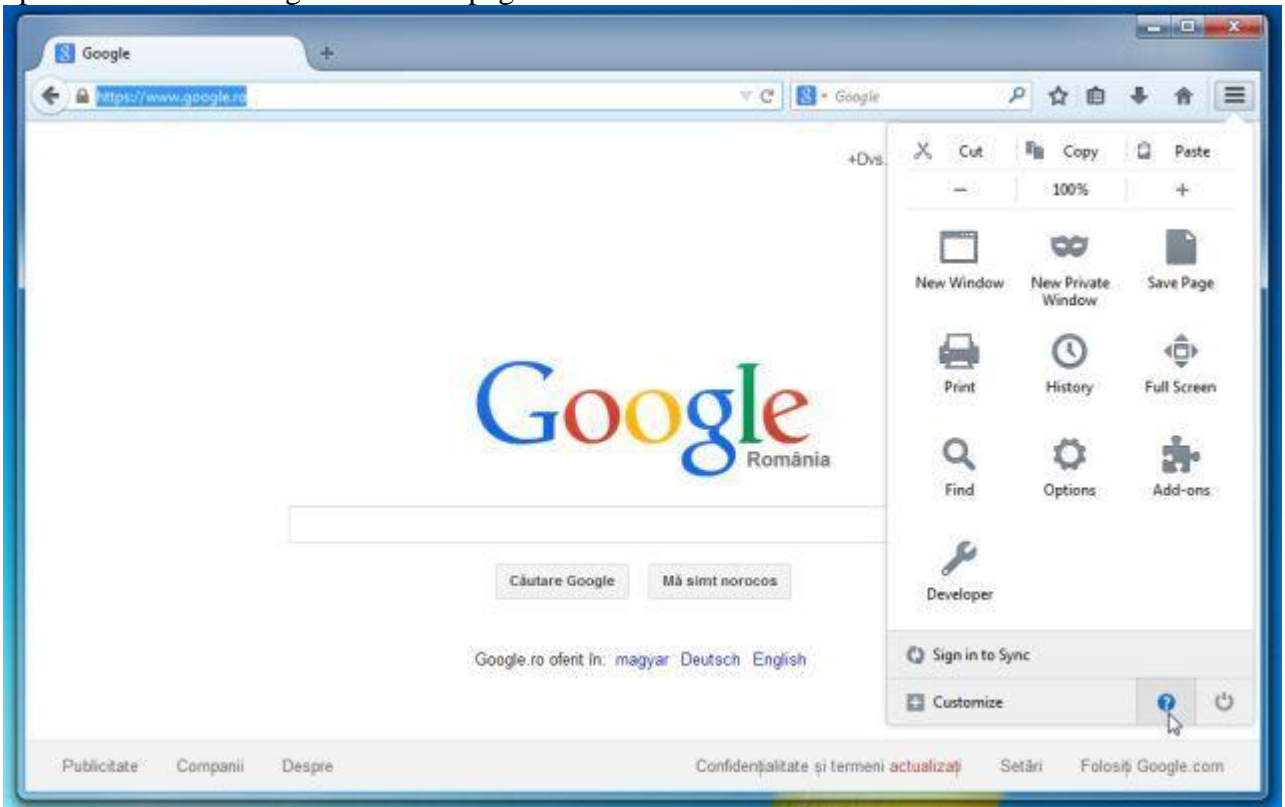
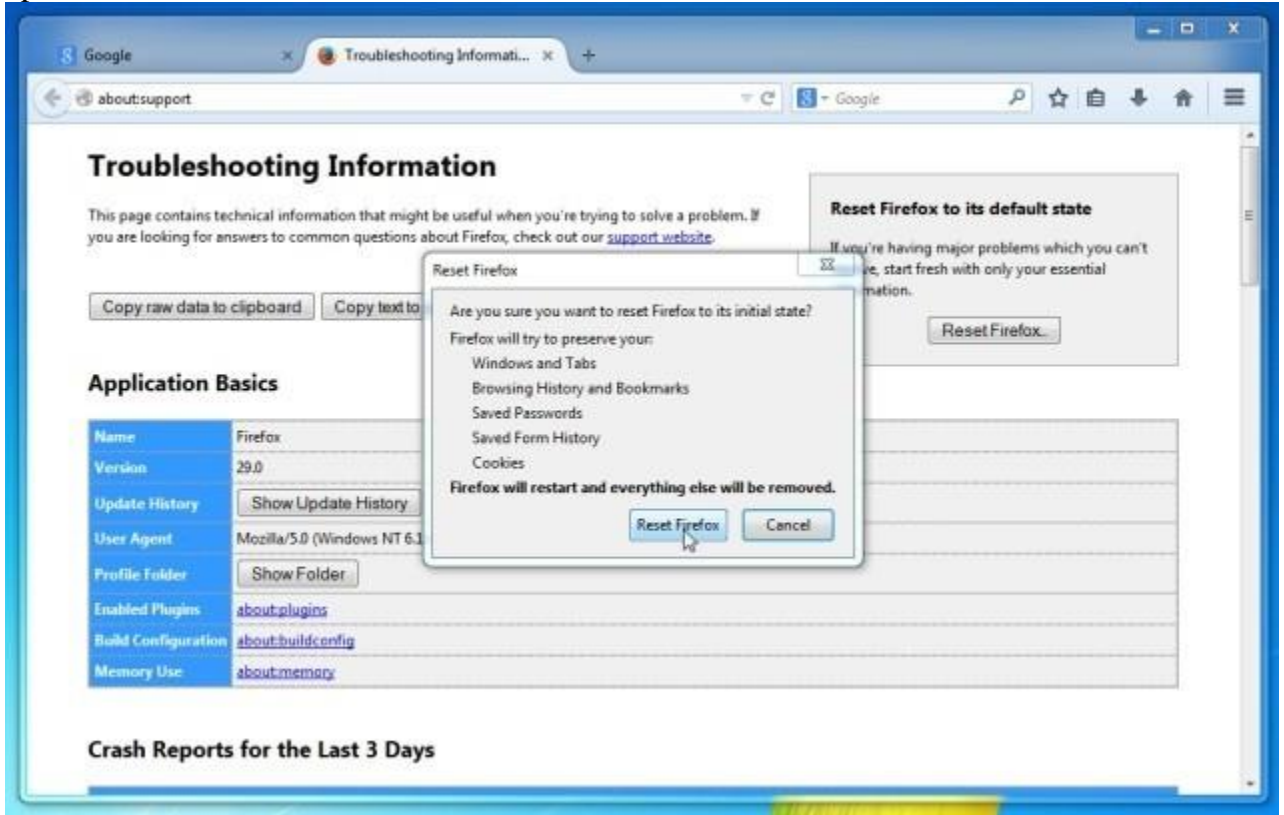2. From the *Help* menu choose **Troubleshooting Information**.
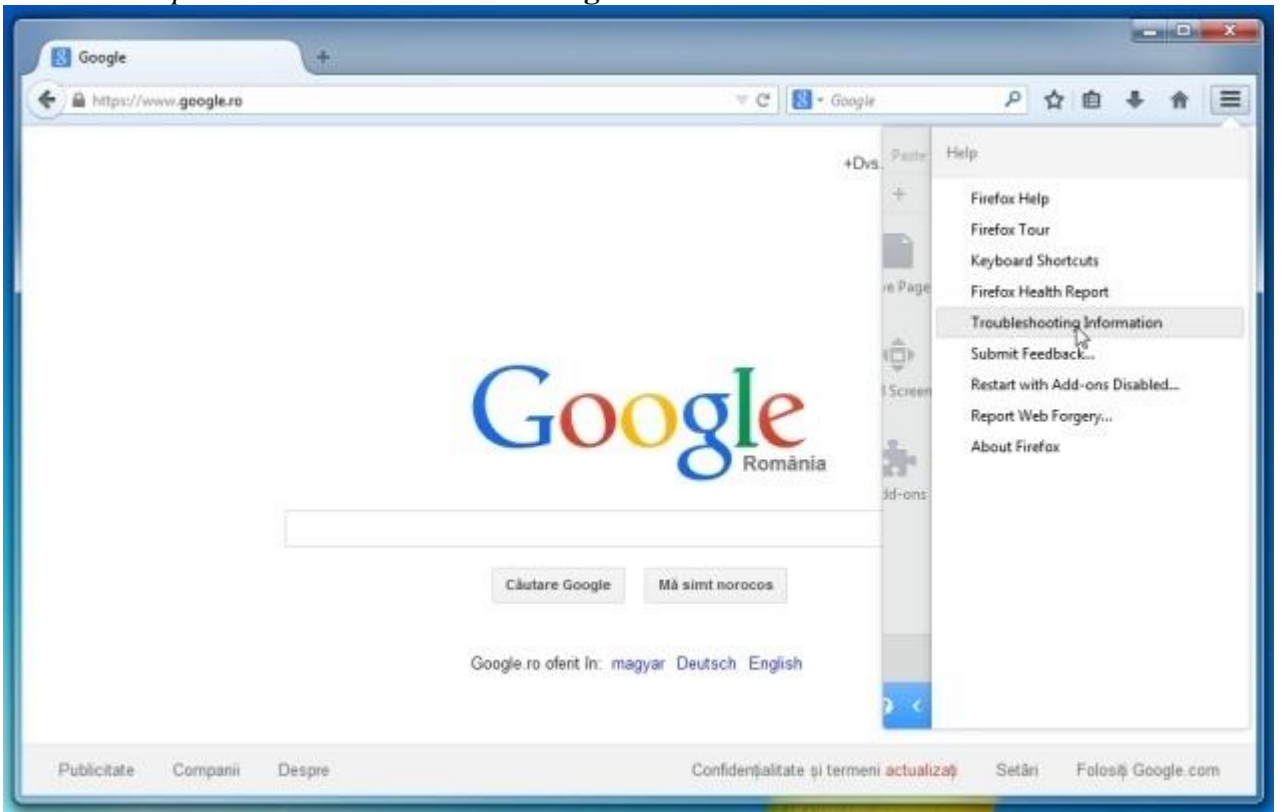
3. Click the "**Reset Firefox**" button in the upper-right corner of the "*Troubleshooting Information*" page.

4. To continue, click on the "**Reset Firefox**" button in the new confirmation window that opens.

5. Firefox will close itself and will revert to its default settings. When it's done, a window will list the information that was imported. Click on the "**Finish**".

Note: Your old Firefox profile will be placed on your desktop in a folder named "*Old Firefox Data*". If the reset didn't fix your problem you can restore some of the information not saved by copying files to the new profile that was created. If you don't need this folder any longer, you should delete it as it contains sensitive information.

Remove pop-up ads from Google Chrome

1. Click on Chrome's main menu button, represented by three horizontal lines (☰) .When the drop-down menu appears, select the option labeled **Settings**.
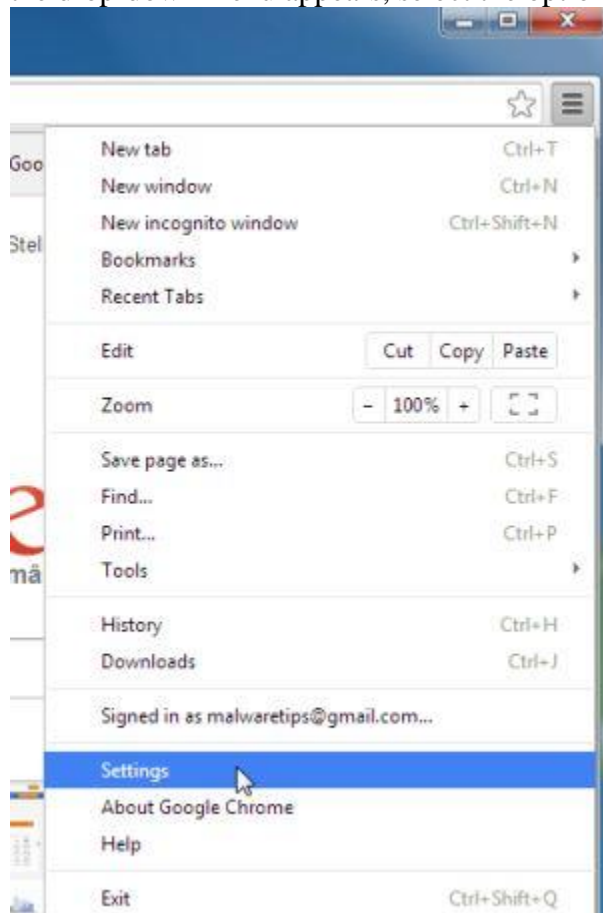

2. Chrome's Settings should now be displayed in a new tab or window, depending on your configuration. Next, scroll to the bottom of the page and click on the **Show advanced**

settings link (as seen in the below example).
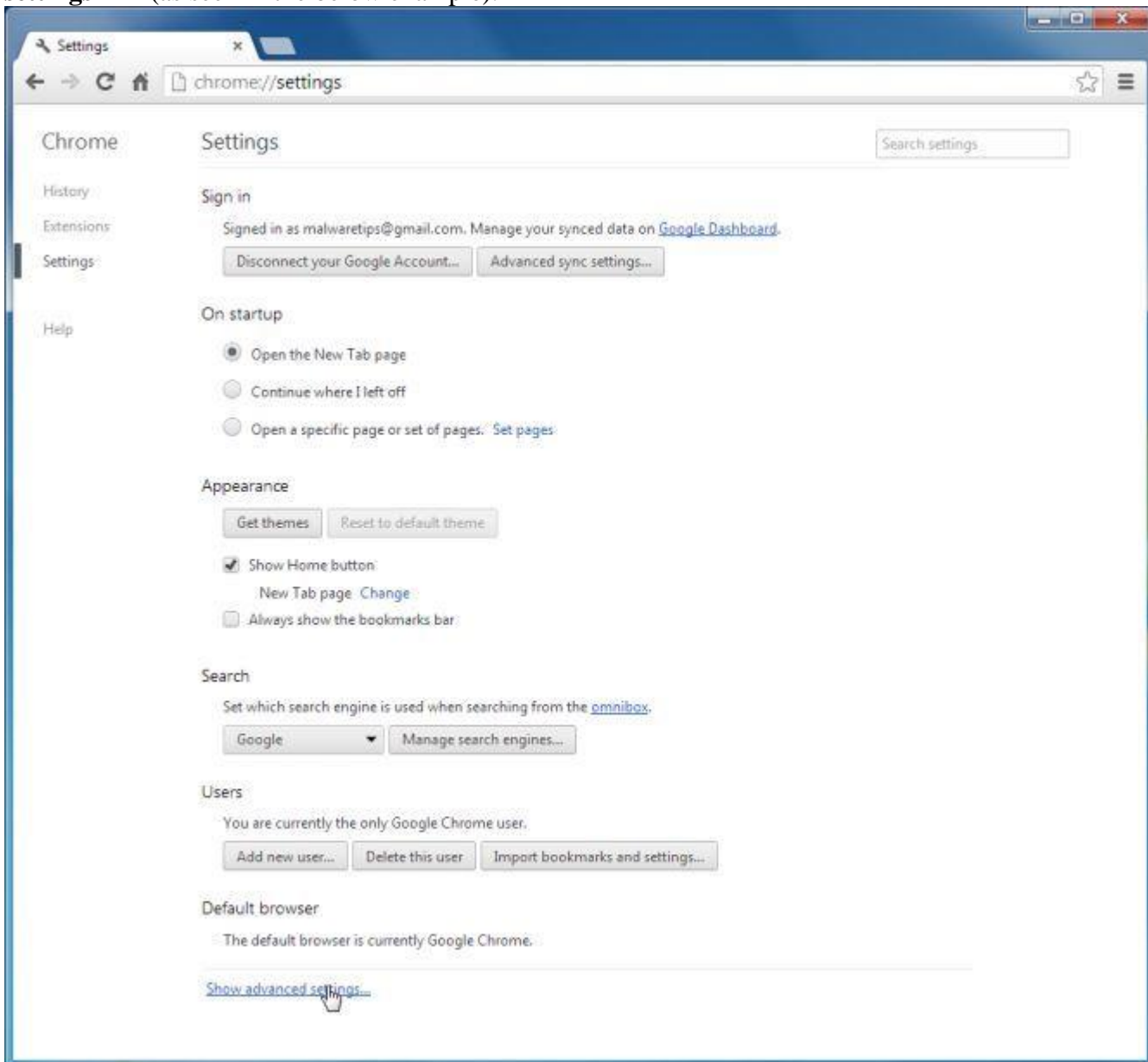
3. Chrome's advanced Settings should now be displayed. Scroll down until the *Reset browser settings* section is visible, as shown in the example below. Next, click on the
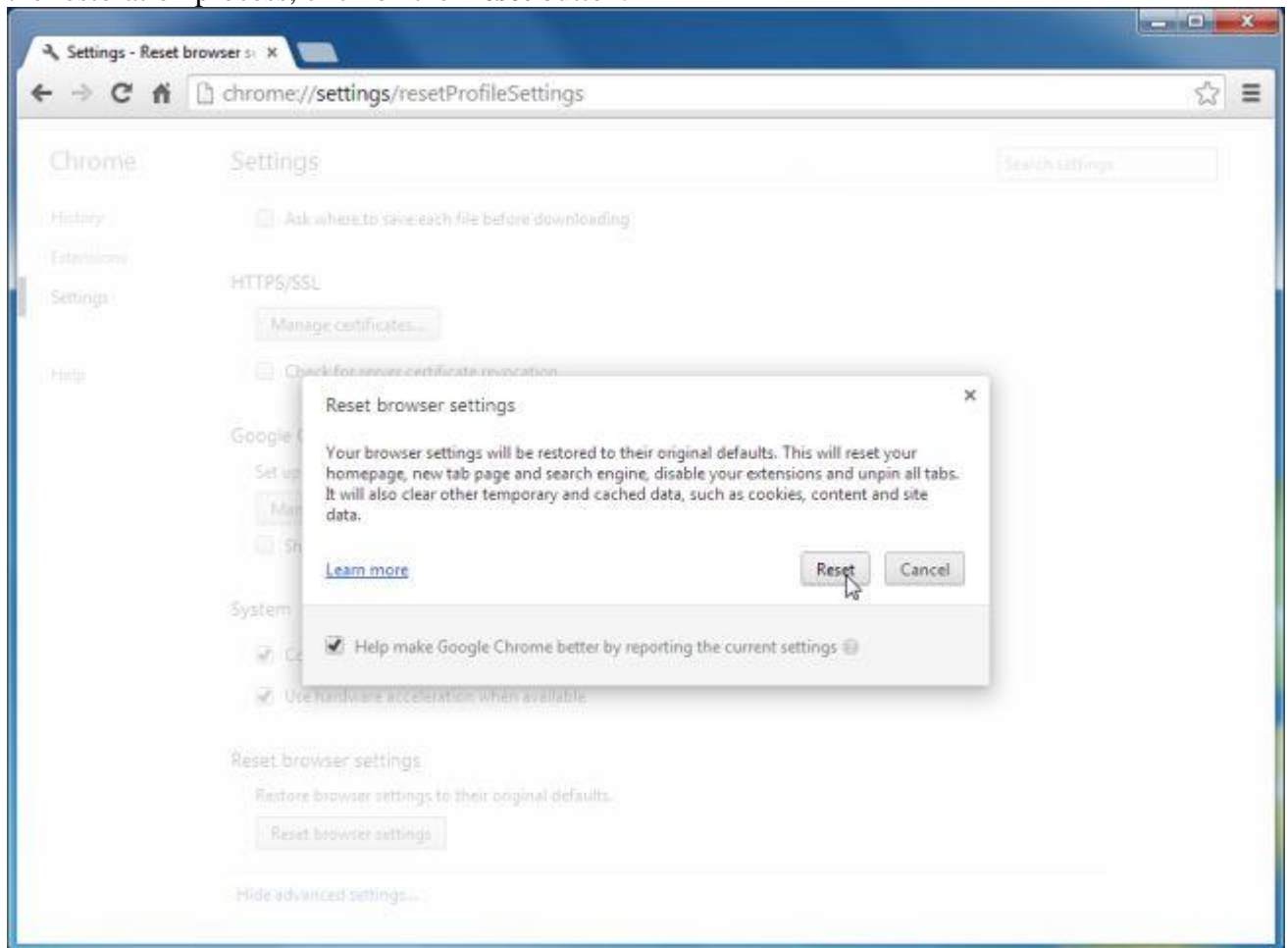
Reset browser settings button.
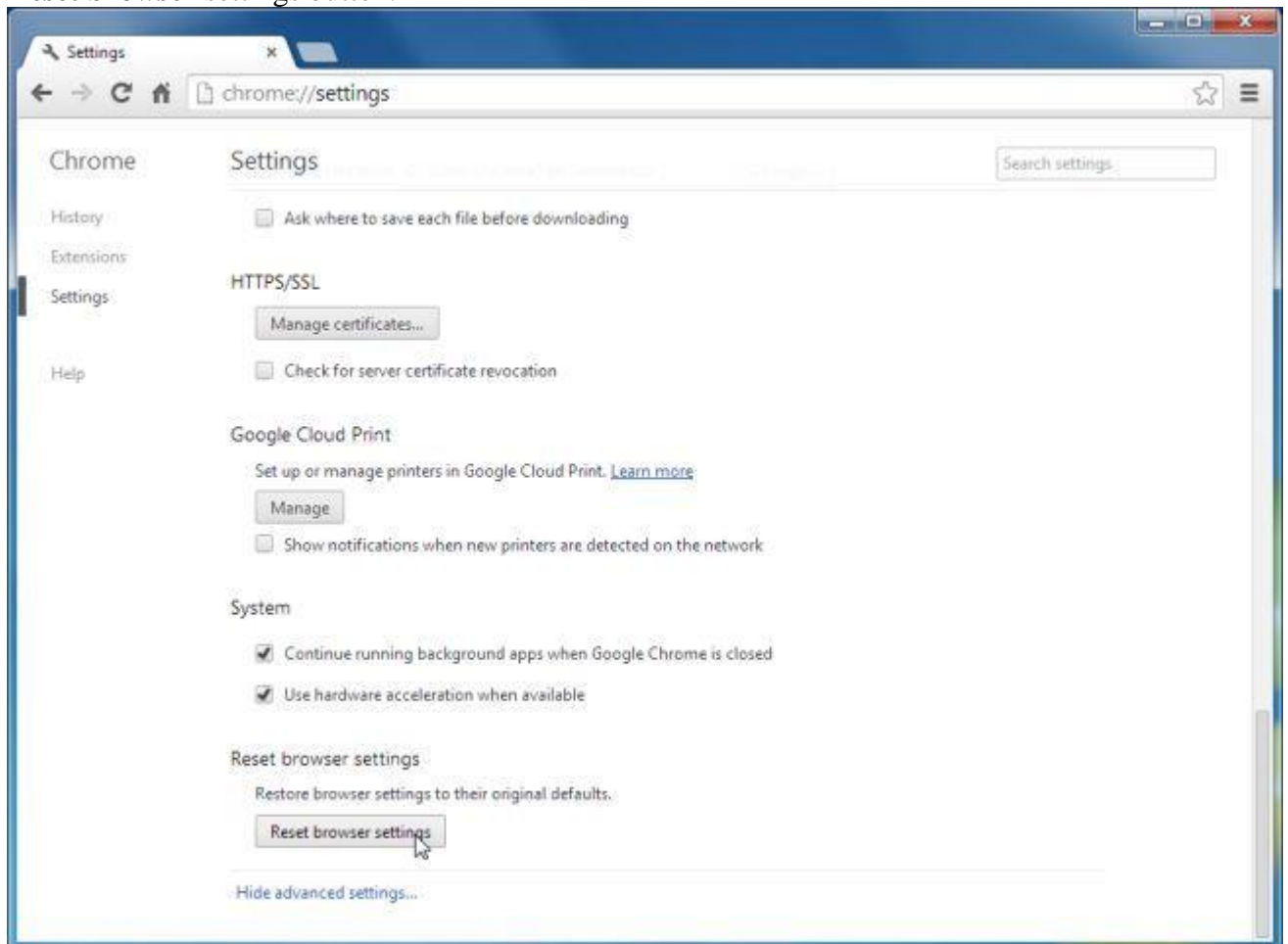
4. A confirmation dialog should now be displayed, detailing the components that will be restored to their default state should you continue on with the reset process. To complete

the restoration process, click on the **Reset** button.

STEP 3: Remove Pop-up Ads adware from your computer with AdwCleaner.

The AdwCleaner utility will scan your computer and web browser for malicious files, adware browser extensions and registry keys, that may have been installed on your computer without your knowledge.

1. You can **download AdwCleaner** utility from the below link.
   ADWCLEANER DOWNLOAD LINK (*This link will automatically download AdwCleaner on your computer*)
2. Before starting AdwCleaner, **close all open programs and internet browsers**, then **double-click on the AdwCleaner icon**.

If Windows prompts you as to whether or not you wish to run AdwCleaner, please allow it to run.

3. When the AdwCleaner program will open, click on the "**Scan**" button as shown below.

AdwCleaner will now start to search for the any malicious files that may be installed on your computer.

4. To remove the malicious files that were detected in the previous step, please click on the "**Clean**" button.

5. AdwCleaner will now prompt you to **save any open files or documents,** as the program will need to reboot the computer. Please do so and then click on the **OK** button.

STEP 4: Remove Pop-up Ads browser hijacker with Junkware Removal Tool

Junkware Removal Tool is a powerful utility, which will remove Pop-up Ads redirect from Internet Explorer, Firefox or Google Chrome.

1. You can download the **Junkware Removal Tool utility** from the below link:
   JUNKWARE REMOVAL TOOL DOWNLOAD LINK *(This link will automatically download the Junkware Removal Tool utility on your computer)*
2. Once Junkware Removal Tool has finished downloading, please **double-click on the JRT.exe** icon as seen below.

If Windows prompts you as to whether or not you wish to run Junkware Removal Tool, please allow it to run.

3. Junkware Removal Tool will now start, and at the Command Prompt, you'll need to *press any key* to perform a scan for the Pop-up Ads hijacker.
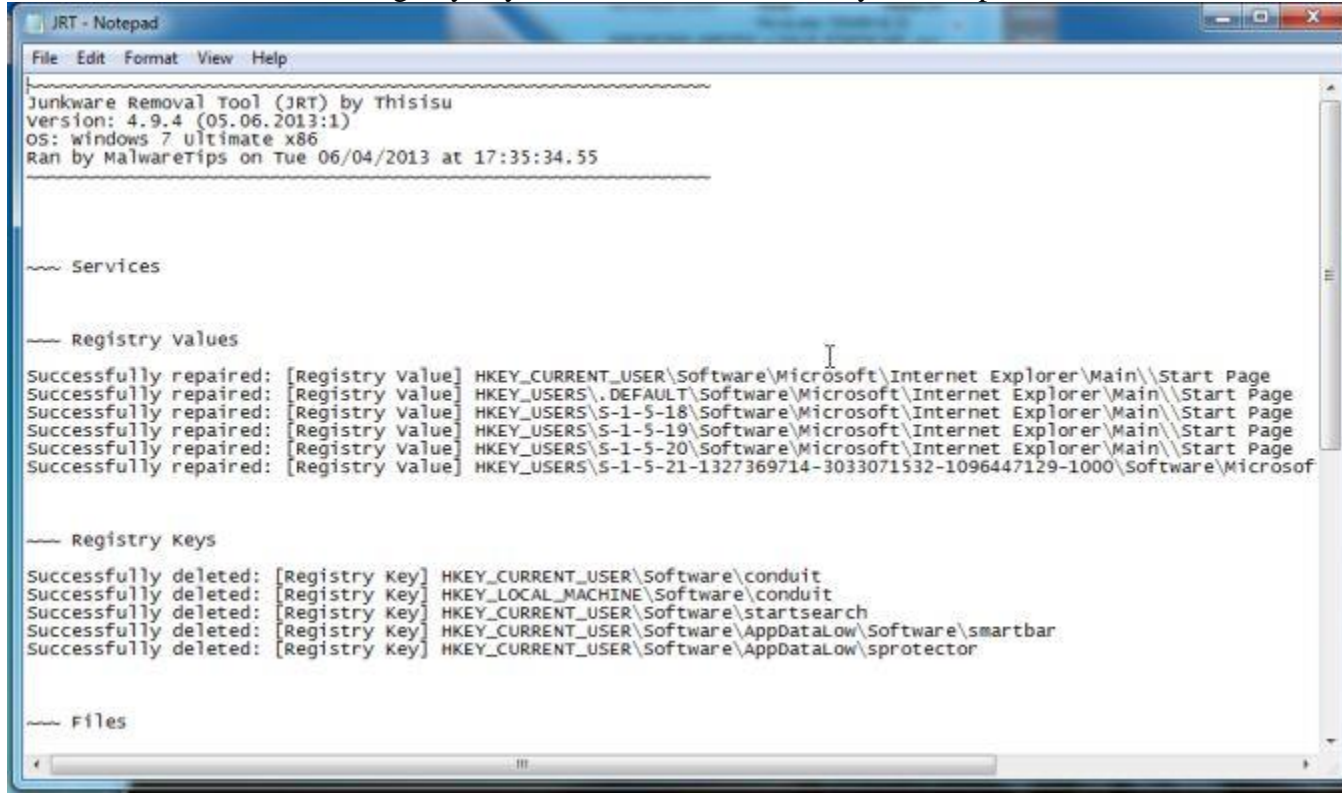

Please be patient as this can take a while to complete (up to 10 minutes) depending on your system's specifications.

4. When the scan Junkware Removal Tool will be completed, this utility will display a log with the malicious files and registry keys that were removed from your computer.

STEP 5: Remove Pop-up Ads virus with Malwarebytes Anti-Malware FREE

Malwarebytes Anti-Malware Free uses industry-leading technology to detect and remove all traces of malware, including worms, Trojans, rootkits, rogues, dialers, spyware, and more.
It is important to note that Malwarebytes Anti-Malware works well and should run alongside antivirus software without conflicts.

1. You can download **download Malwarebytes Anti-Malware** from the below link.
MALWAREBYTES ANTI-MALWARE DOWNLOAD LINK *(This link will open a new web page from where you can download Malwarebytes Anti-Malware Free)*
2. Once downloaded, close all programs, then double-click on the icon on your desktop named "*mbam-setup-consumer-2.00.xx*" to start the installation of Malwarebytes Anti-Malware.

🛡️You may be presented with a User Account Control dialog asking you if you want to run this file. If this happens, you should click "*Yes*" to continue with the installation.

3. When the installation begins, you will see the *Malwarebytes Anti-Malware Setup Wizard* which will guide you through the installation process.

To install Malwarebytes Anti-Malware on your machine, *keep following the prompts* by

clicking the "**Next**" button.

4. Once installed, Malwarebytes Anti-Malware will automatically start and you will see a message stating that you should update the program, and that a scan has never been run on your system. To start a system scan you can click on the "**Fix Now**" button.

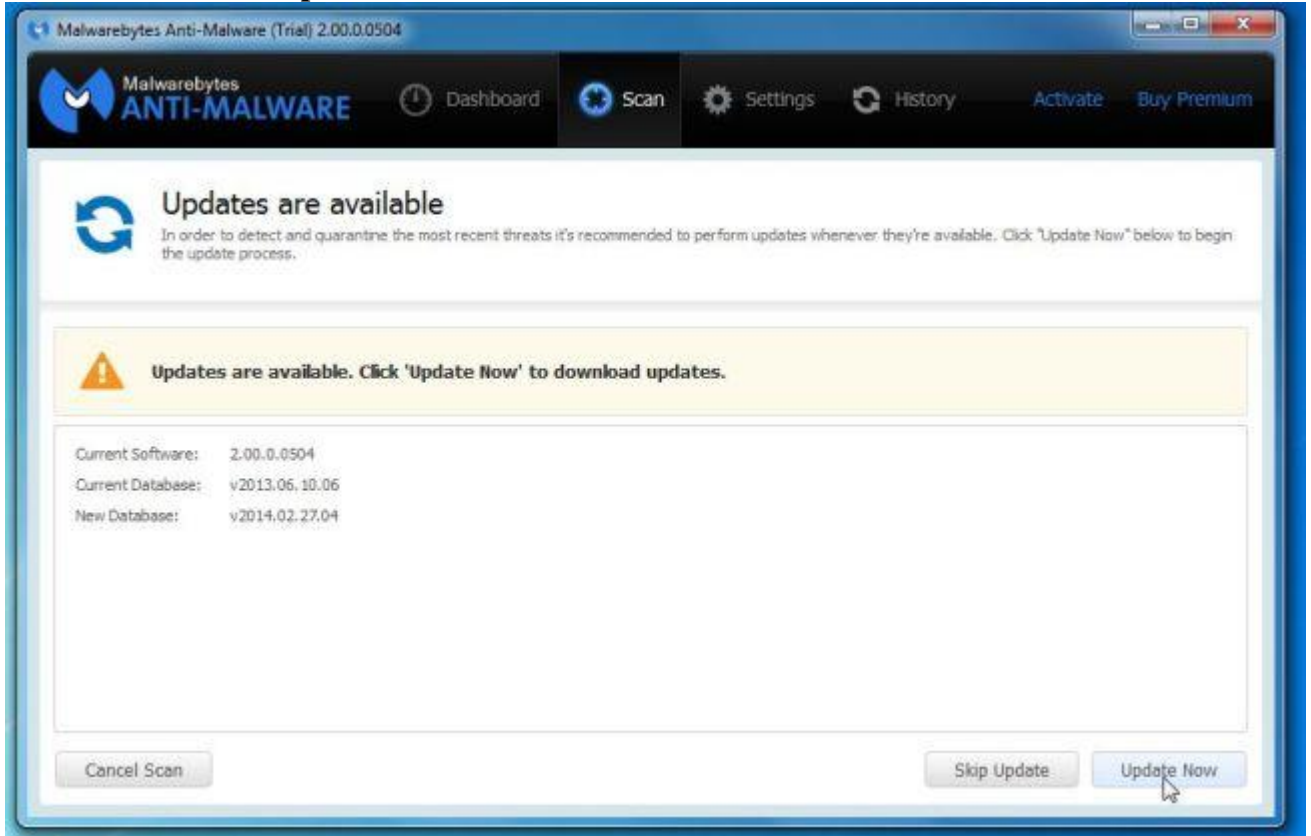Alternatively, you can click on the "**Scan**" tab and select "*Threat Scan*", then click on the
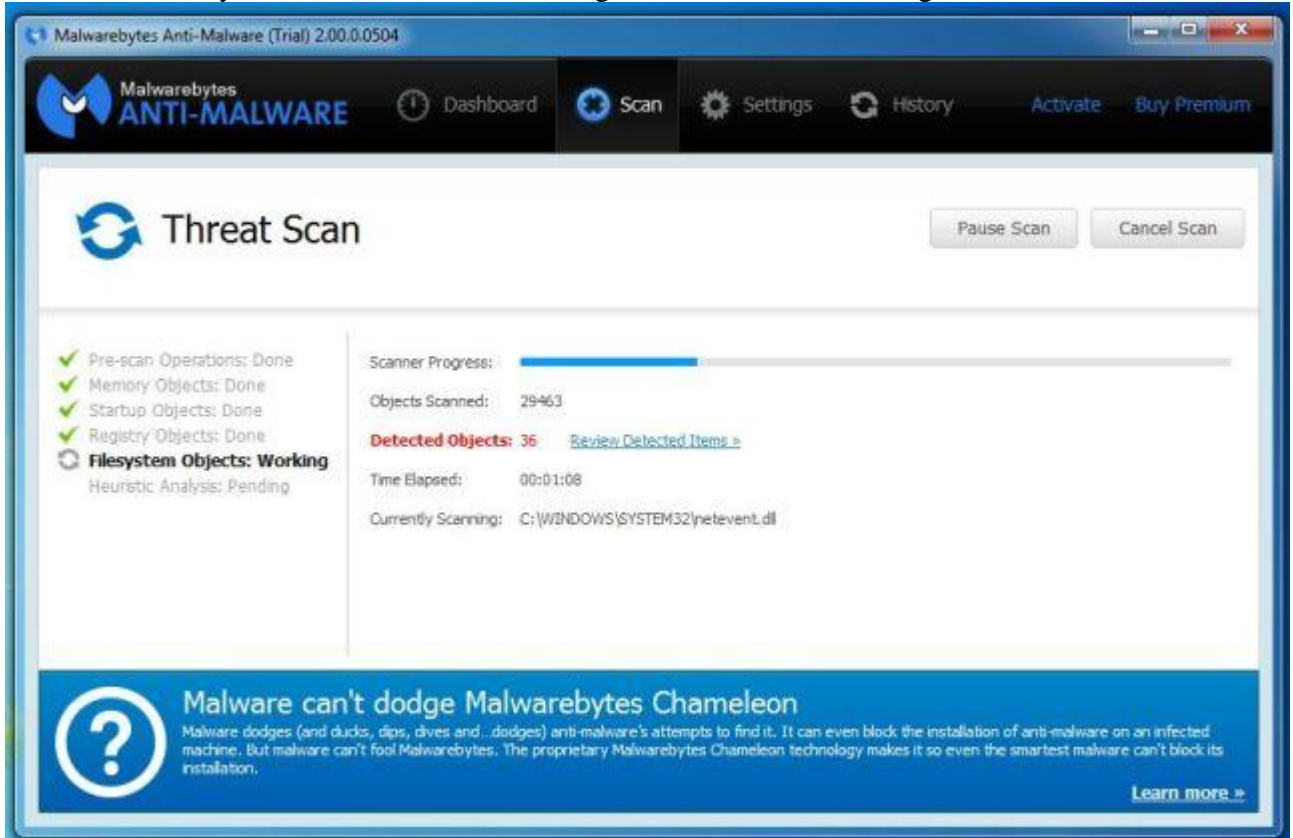
"Scan Now" button.
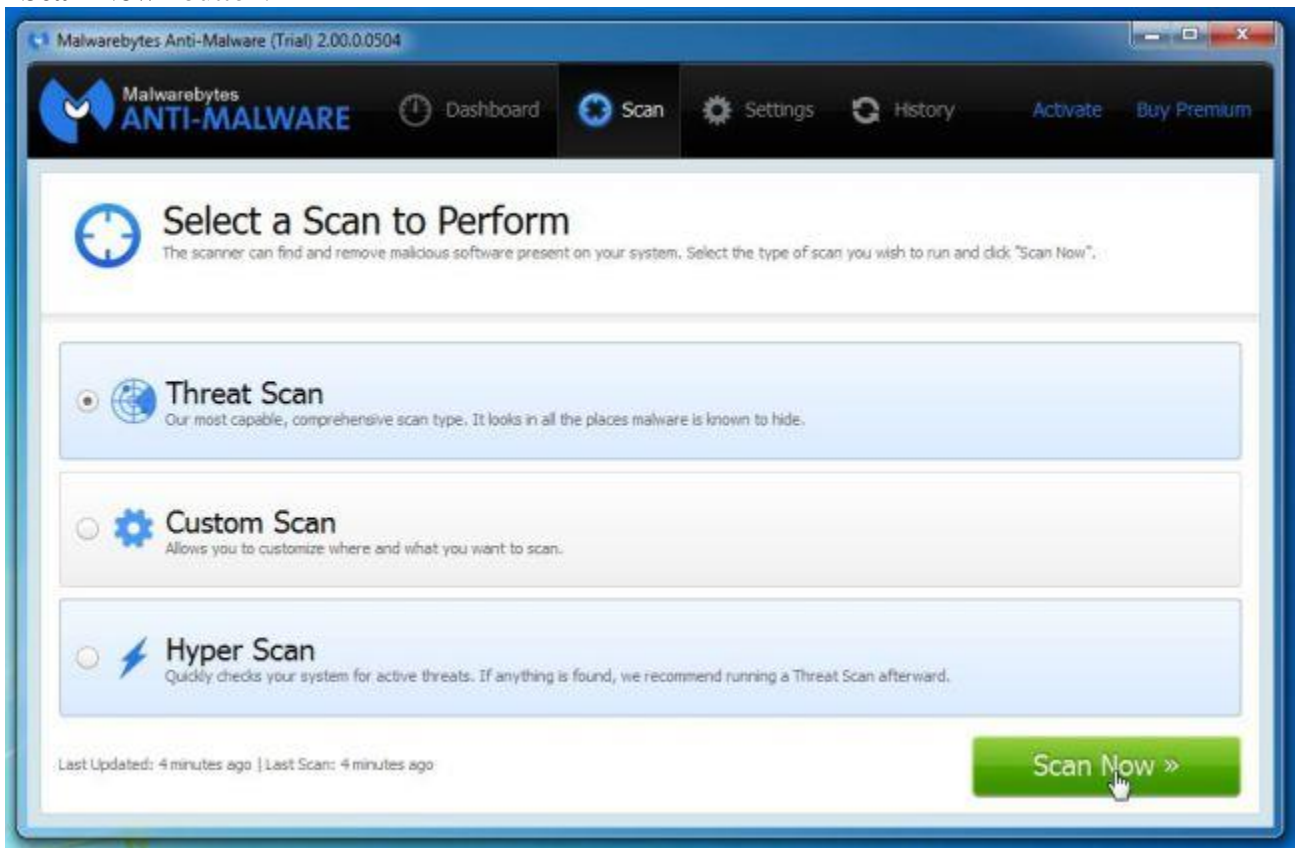
5. Malwarebytes Anti-Malware will now check for updates, and if there are any, you will need to click on the "**Update Now**" button.

6. Malwarebytes Anti-Malware will now start scanning your computer for the pop-up virus. When Malwarebytes Anti-Malware is scanning it will look like the image below.

7. When the scan has completed, you will now be presented with a screen showing you the malware infections that Malwarebytes' Anti-Malware has detected. To remove the malicious programs that Malwarebytes Anti-malware has found, click on the "**Quarantine All**" button, and then click on the "**Apply Now**" button.
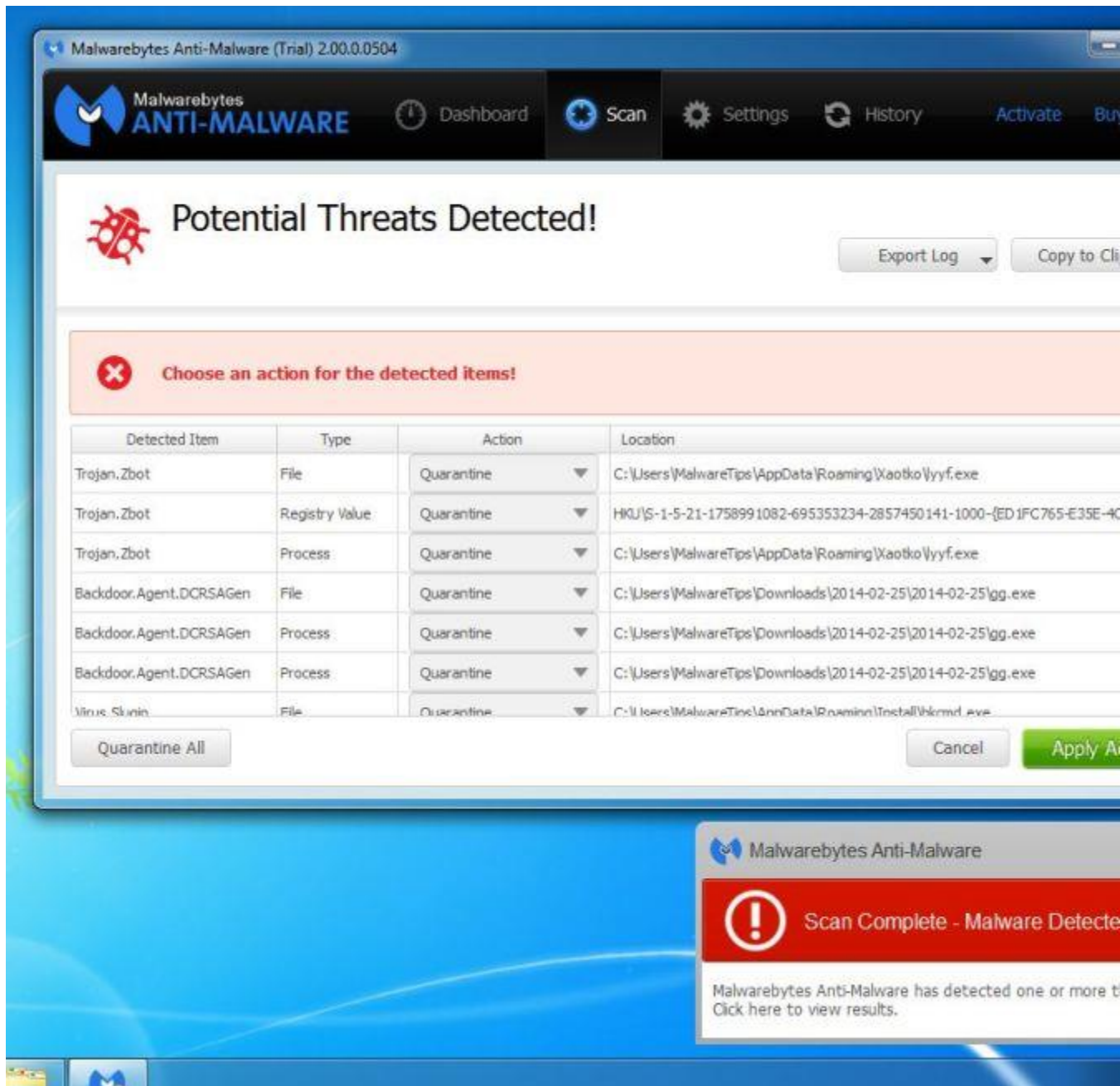
Please note that the infections found may be different than what is shown in the image.

8. Malwarebytes Anti-Malware will now quarantine all the malicious files and registry keys that it has found. When removing the files, Malwarebytes Anti-Malware may require a reboot in order to remove some of them. If it displays a message stating that it needs to reboot your computer, please allow it to do so.
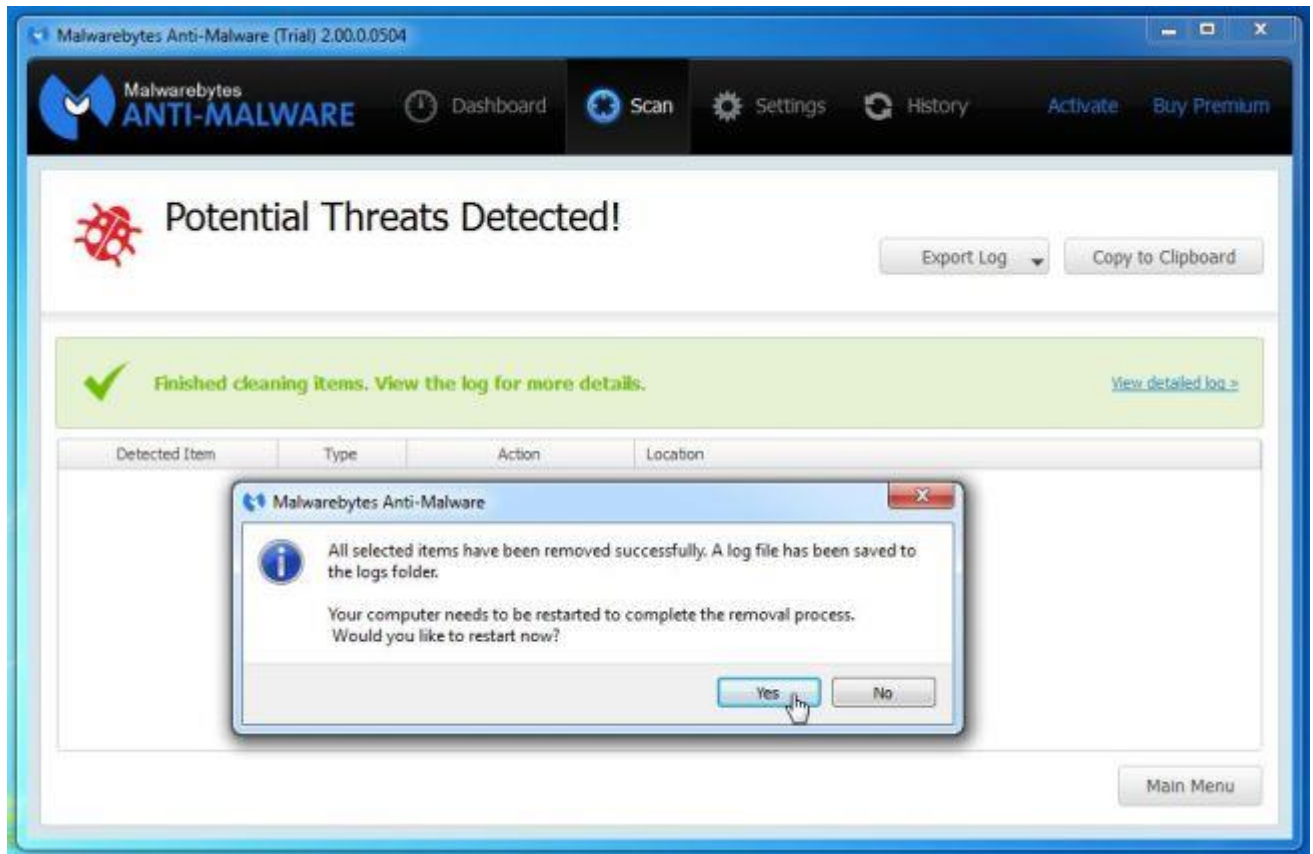
After your computer will restart, you should open Malwarebytes Anti-Malware and perform another "Threat Scan" scan to verify that there are no remaining threats

---

STEP 6: Double-check for the Pop-up Ads infection with HitmanPro

HitmanPro is a second opinion scanner, designed to rescue your computer from malware (viruses, trojans, rootkits, etc.) that have infected your computer despite all the security measures you have taken (such as anti virus software, firewalls, etc.). HitmanPro is designed to work alongside existing security programs without any conflicts. It scans the computer quickly (less than 5 minutes) and does not slow down the computer.

1. You can download **HitmanPro** from the below link:
   HITMANPRO DOWNLOAD LINK *(This link will open a new web page from where you can download HitmanPro)*
2. Double-click on the file named "**HitmanPro.exe**" (for 32-bit versions of Windows) or "**HitmanPro_x64.exe**" (for 64-bit versions of Windows). When the program starts you will be presented with the start screen as shown below.

Click on the "**Next**" button, to install HitmanPro on your computer.

HitmanPro 3.7.9 - Build 212 (64-bit)
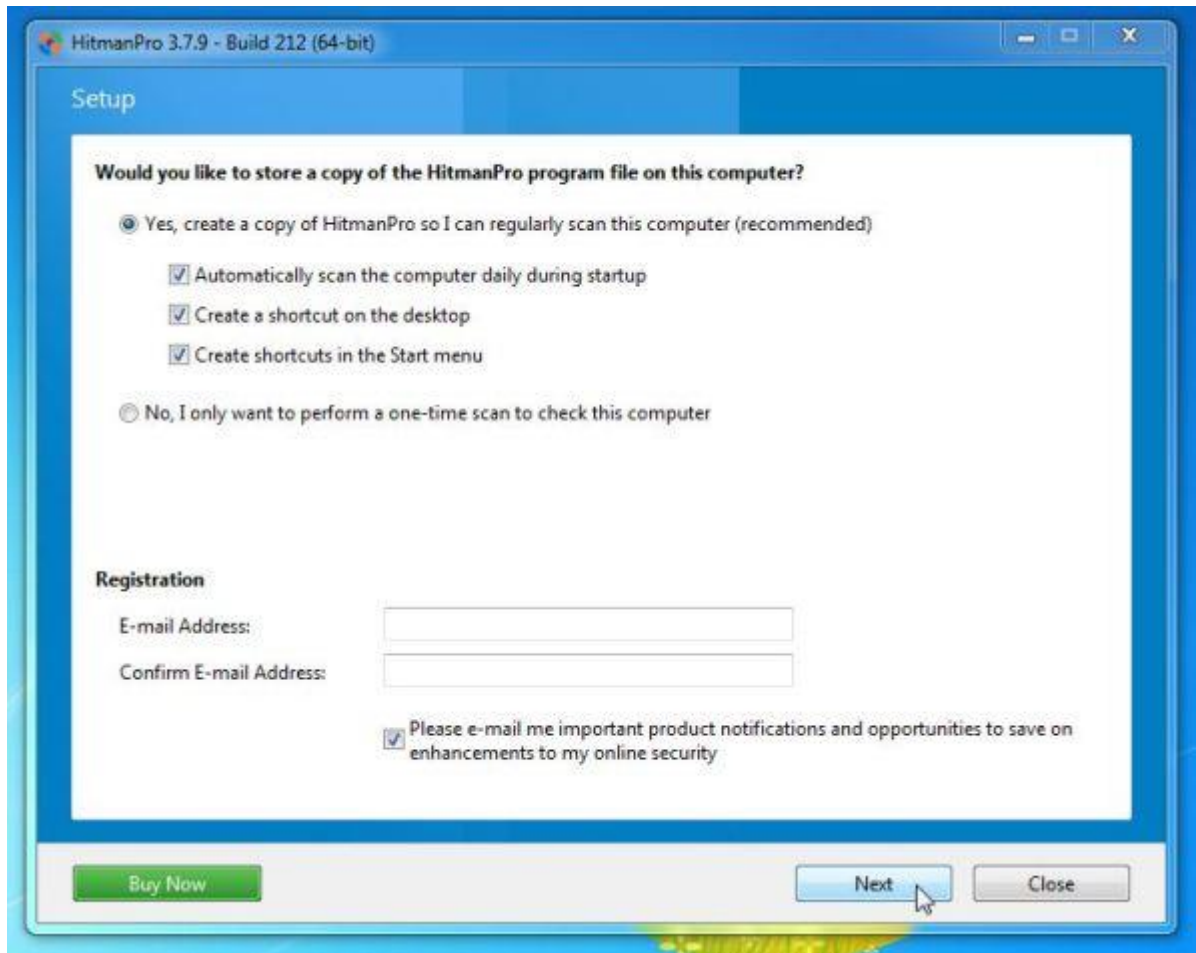
Setup

Would you like to store a copy of the HitmanPro program file on this computer?

◉ Yes, create a copy of HitmanPro so I can regularly scan this computer (recommended)

☑ Automatically scan the computer daily during startup
☑ Create a shortcut on the desktop
☑ Create shortcuts in the Start menu

○ No, I only want to perform a one-time scan to check this computer

Registration

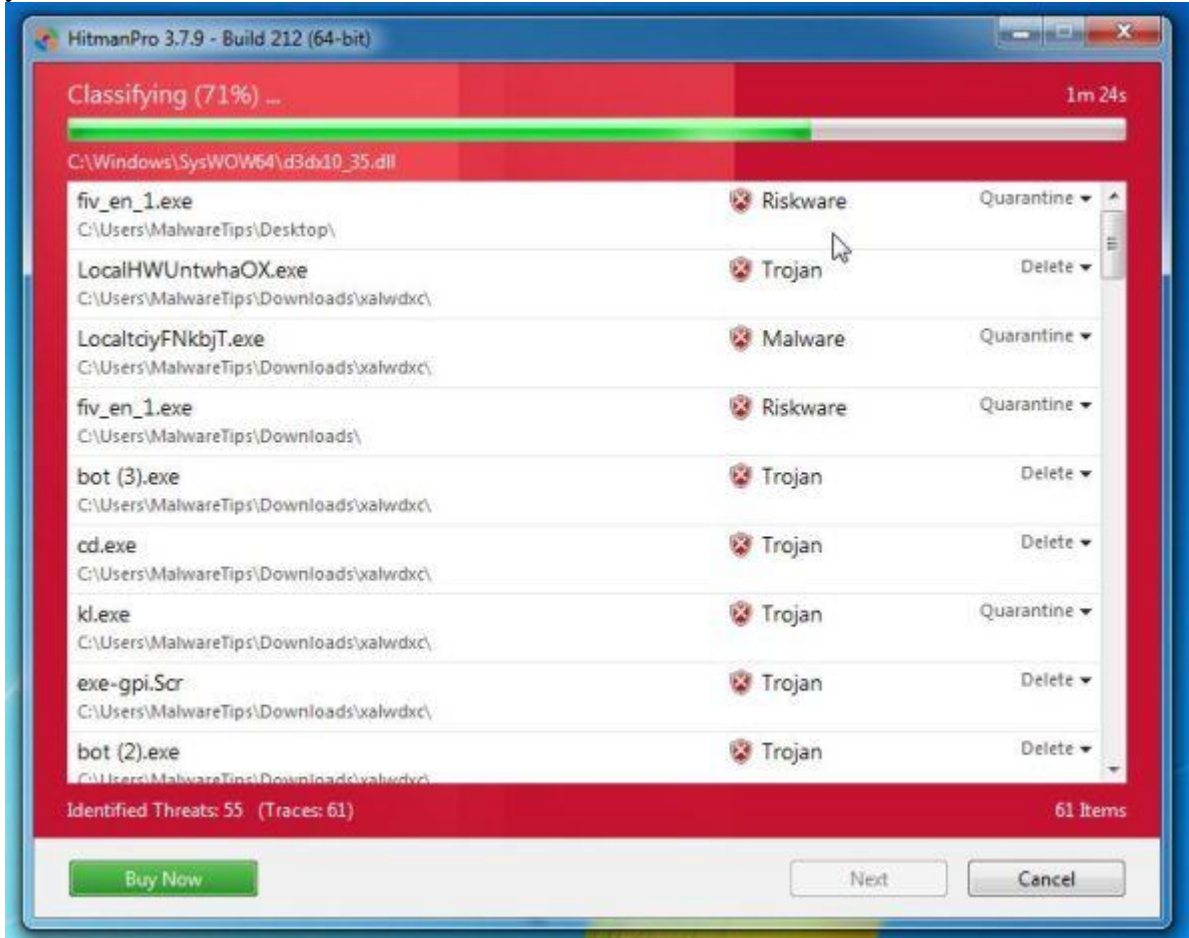E-mail Address:

Confirm E-mail Address:

☑ Please e-mail me important product notifications and opportunities to save on enhancements to my online security
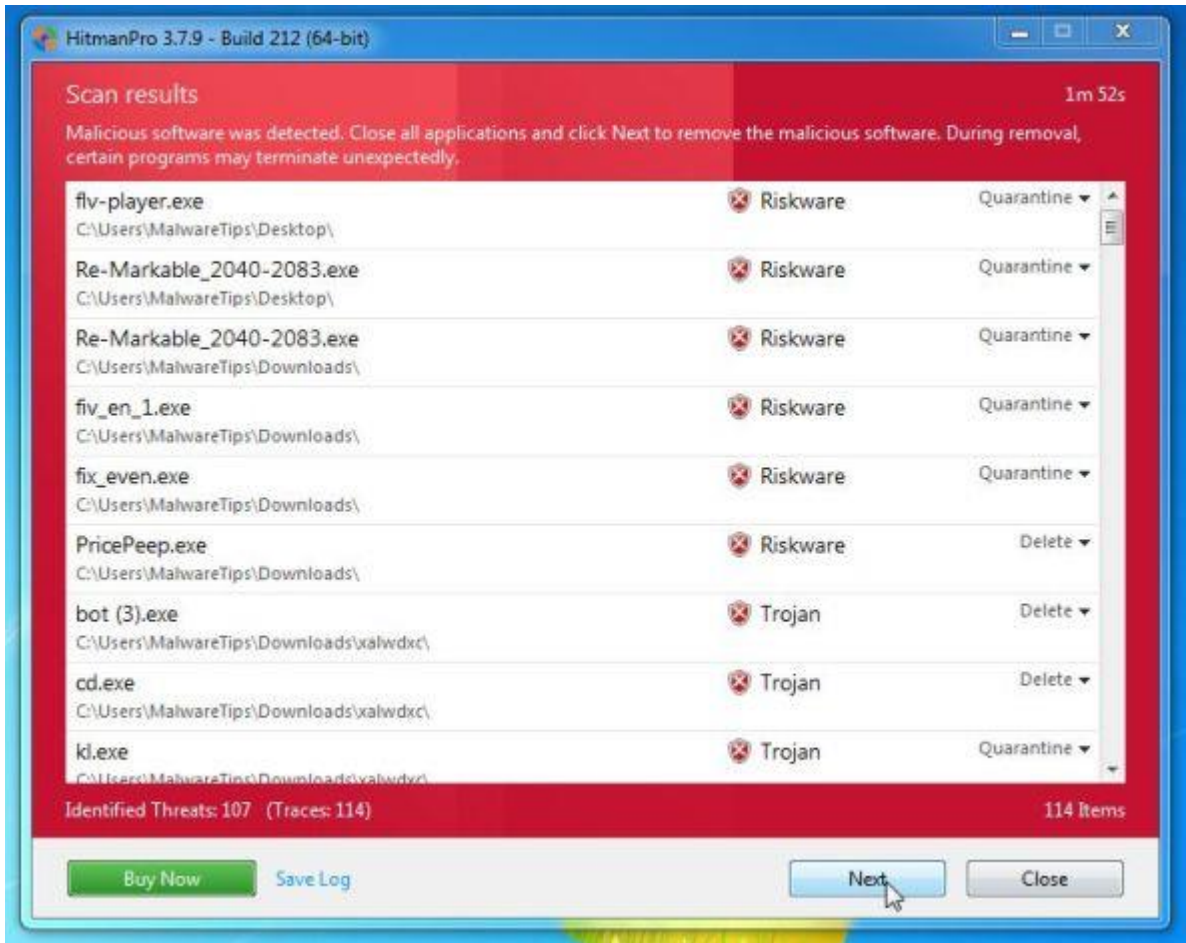
Buy Now   Next   Close

3. HitmanPro will now begin to scan your computer for any malicious files that may be on your machine.

4. When it has finished it will display a list of all the malware that the program found as shown in the image below. Click on the "**Next**" button, to remove any virus that has been

found.

5. Click on the "**Activate free license**" button to begin the **free 30 days trial**, and remove all the malicious files from your computer.