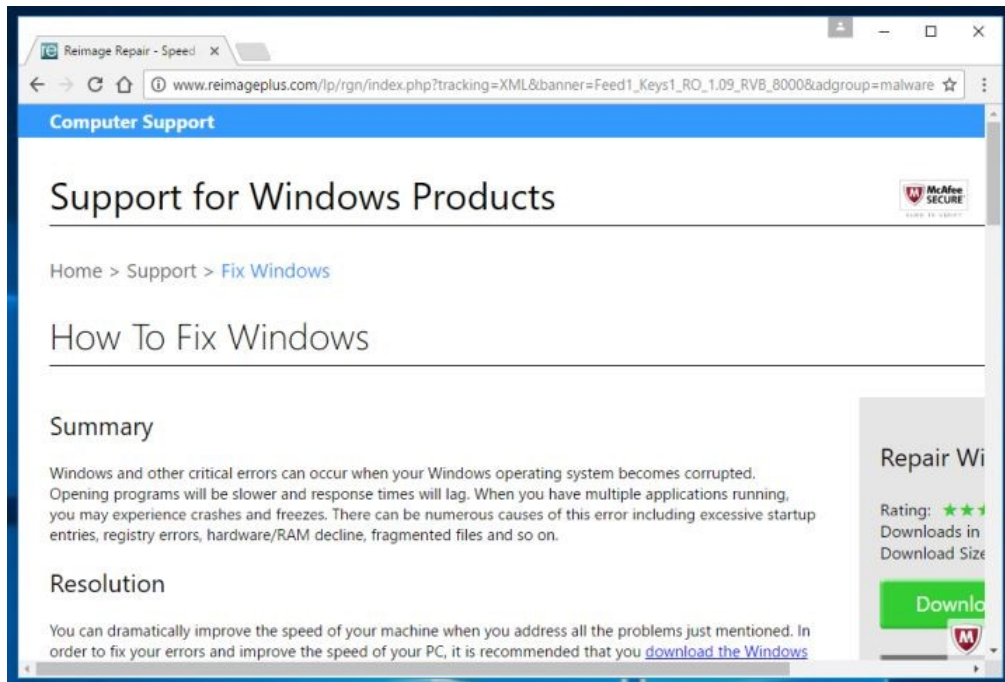


MalwareTips ReimagePlus.com Adware (Virus Removal Guide)

BY STELIAN PILICI (HTTPS://MALWARETIPS.COM/BLOGS/AUTHOR/ADMIN/) ON AUGUST 30, 2017

If your web browser is *constantly* being redirected to the **<http://www.reimageplus.com/lp/sqh/index.php?tracking=RN1&banner=>** site, then it is possible that you have an adware program installed on your computer.



This ReimagePlus.com redirect is usually caused by adware installed on your computer. These adware programs are bundled with other free software that you download off of the Internet. Unfortunately, some free downloads do not adequately disclose that other software will also be installed and you may find that you have installed adware without your knowledge.

Once this malicious program is installed, whenever you will browse the Internet, unwanted advertisements will pop-up on web pages that you visit. These ads are aimed to promote the installation of additional questionable content including web browser toolbars, optimization utilities and other products, all so the adware publisher can generate pay-per-click revenue.

You may also see in the browser status bar the following messages: "Waiting for www.reimageplus.com", "Transferring data from www.reimageplus.com", "Looking up www.reimageplus.com", "Read www.reimageplus.com", "Connected to www.reimageplus.com".

When infected with this adware program, other common symptoms include:

- Advertising banners are injected with the web pages that you are visiting.
- Random web page text is turned into hyperlinks.

You should always pay attention when installing software because often, a software installer includes optional installs. Be very careful what you agree to install.

Always opt for the custom installation and deselect anything that is not familiar, especially optional software that you never wanted to download and install in the first place. It goes without saying that you should not install software that you don't trust.

The below instructions are for Windows users, however we also have an [Android guide \(https://malwaretips.com/blogs/remove-android-virus/\)](https://malwaretips.com/blogs/remove-android-virus/) and a [Mac OS guide \(https://malwaretips.com/blogs/remove-mac-os-x-virus/\)](https://malwaretips.com/blogs/remove-mac-os-x-virus/) which should help clean up your device.

How to remove ReimagePlus.com redirect (Virus Removal Guide)

This malware removal guide may appear overwhelming due to the amount of the steps and numerous programs that are being used. We have only written it this way to provide clear, detailed, and easy to understand instructions that anyone can use to remove malware for free.

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 \(https://malwaretips.com/forums/malware-removal-assistance.10/\)](https://malwaretips.com/forums/malware-removal-assistance.10/).

To remove the ReimagePlus.com Adware, follow these steps:

STEP 1: Uninstall the malicious programs from Windows

STEP 2: Use AdwCleaner to remove the ReimagePlus.com Redirect

STEP 3: Use Malwarebytes to scan for Malware and Unwanted Programs

STEP 4: Double-check for malicious programs with HitmanPro

(OPTIONAL) STEP 5: Reset your browser to default settings

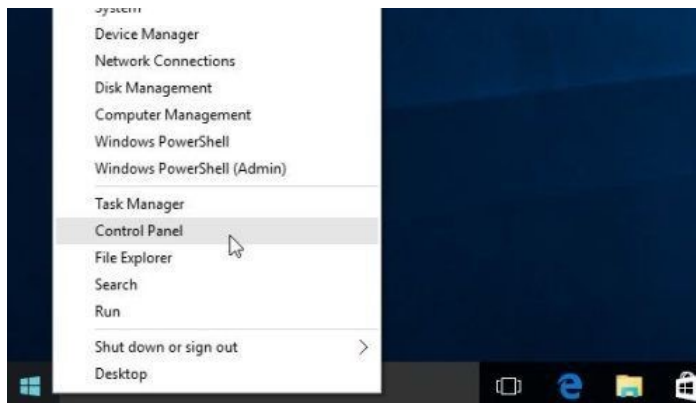
STEP 1 : Uninstall the malicious programs from Windows

In this first step, we will try to identify and remove any malicious program that might be installed on your computer.

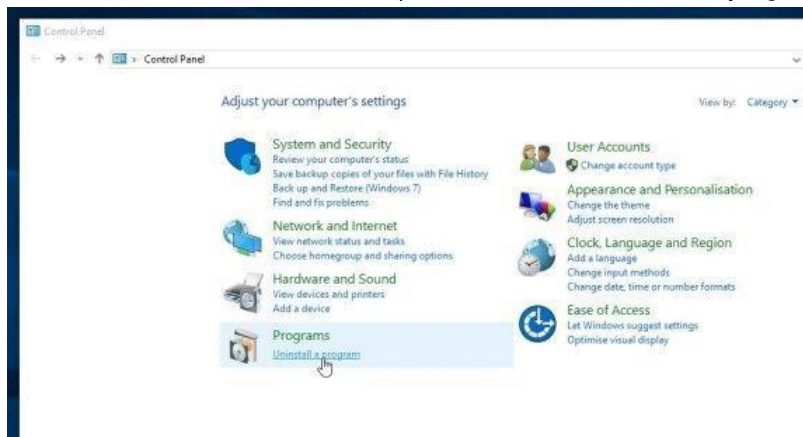
1. Go to the uninstall menu.

Windows 10 or Windows 8.1

1. To uninstall a program on **Windows 10** or **Windows 8**, right-click on the **Windows Start button** and choose **"Control Panel"** from the pop-up menu.



2. When the “Control Panel” window opens click on the “Uninstall a program” option under “Programs” category.



Windows 7

1. If you are using Windows XP, Windows Vista or Windows 7, click the “Start” button, then click on the “Control Panel” menu option.



2. When the “Control Panel” window opens click on the “Uninstall a program” option under “Programs” category.



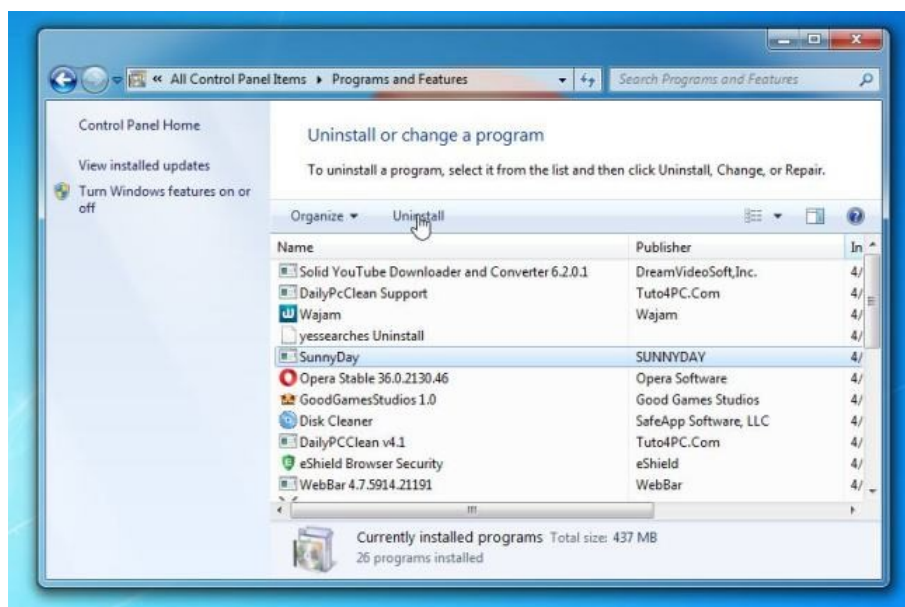
2. When the “**Programs and Features**” screen is displayed, scroll through the list of currently installed programs and uninstall all the unwanted or suspicious programs.

Known malicious programs: Wajam, 1.0.0.1, DNS Unlocker, Cinema Plus, Price Minus, SalesPlus, New Player, MediaVideosPlayers, Browsers_Apps_Pro, PriceLEess, Pic Enhance, Sm23mS, Salus, Network System Driver, SS8, Save Daily Deals, Word Proser, Desktop Temperature Monitor, CloudScout Parental Control, Savefier, Savepass, HostSecurePlugin, CheckMeUp and HD-V2.2.

The malicious program may have a different name on 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 through the list, and uninstall any unwanted or unknown programs.

If you cannot find any unwanted programs on your computer, you can proceed with the next step.

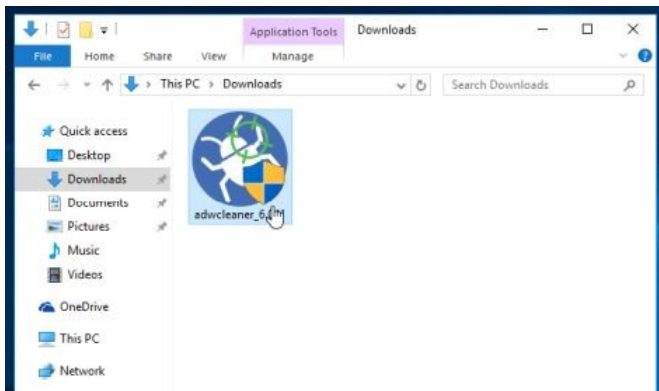
If you are having issues while trying to uninstall a program, you can use [Revo Uninstaller \(https://malwaretips.com/download-revouninstaller\)](https://malwaretips.com/download-revouninstaller) to completely remove this unwanted program from your machine.



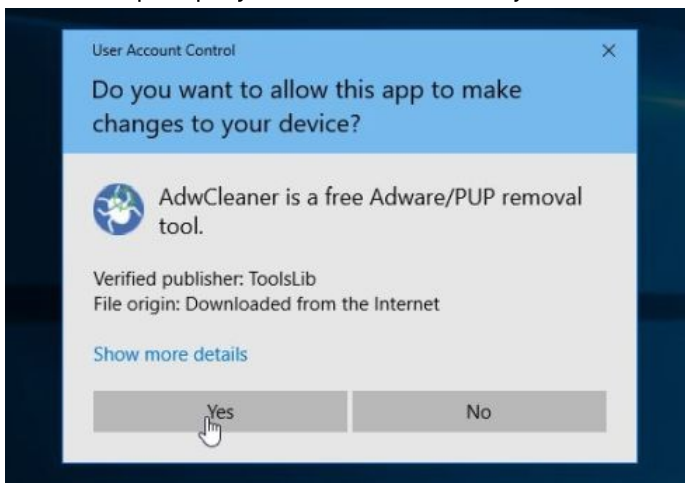
1. You can download **Malwarebytes AdwCleaner** from the below link.

MALWAREBYTES ADWCLEANER DOWNLOAD LINK (<https://toolslib.net/downloads/finish/1/>) (This link will start the download of "Malwarebytes AdwCleaner" on your computer)

2. When Malwarebytes AdwCleaner has finished downloading, please double-click on the AdwCleaner icon to perform a system scan with this program.



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



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



Malwarebytes AdwCleaner will now start to search for the ReimagePlus.com adware and other malicious programs.

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



5. Malwarebytes AdwCleaner will prompt you to save any open files or documents, as the program will need to reboot the computer to complete the cleaning process. Please do so, and then click on the “OK” button.



When your computer reboots and you are logged in, Malwarebytes AdwCleaner will automatically *open a log file* that contains the files, registry keys, and programs that were removed from your computer. Please review this log file and then close the notepad window.

You can now continue with the rest of the instructions.

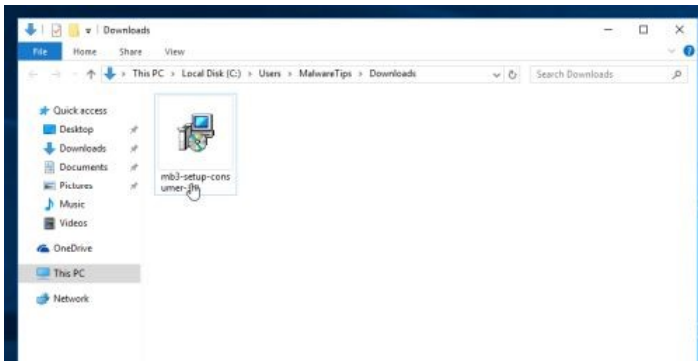
STEP 2: Use Malwarebytes to scan for Malware and Unwanted Programs

Malwarebytes is a powerful on-demand scanner which will scan your PC for malware and other unwanted programs that may

1. You can download **download Malwarebytes** from the below link.

MALWAREBYTES DOWNLOAD LINK (<https://malwaretips.com/download-malwarebytes>) (This link open a new page from where you can download "Malwarebytes")

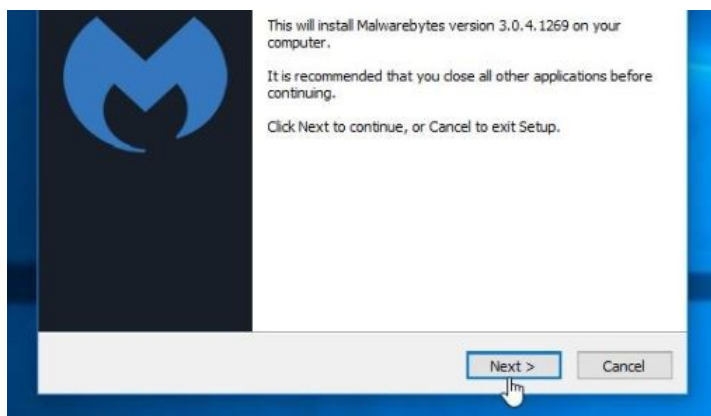
2. When Malwarebytes has finished downloading, double-click on the "mb3-setup-consumer" file to install Malwarebytes on your computer.



You may be presented with an *User Account Control* pop-up asking if you want to allow Malwarebytes to make changes to your device. If this happens, you should click "Yes" to continue with the installation.



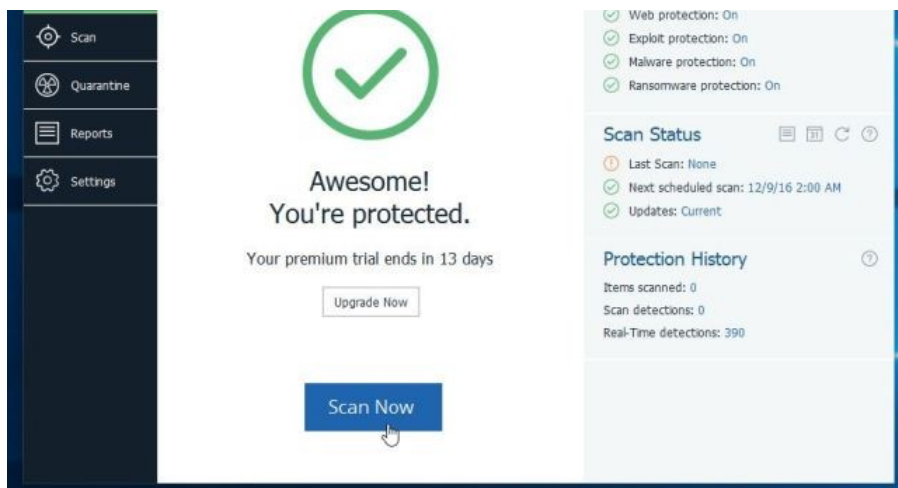
3. When the Malwarebytes installation begins, you will see the *Malwarebytes Setup Wizard* which will guide you through the installation process.



To install Malwarebytes on your machine, **keep following the prompts** by clicking the **“Next”** button.

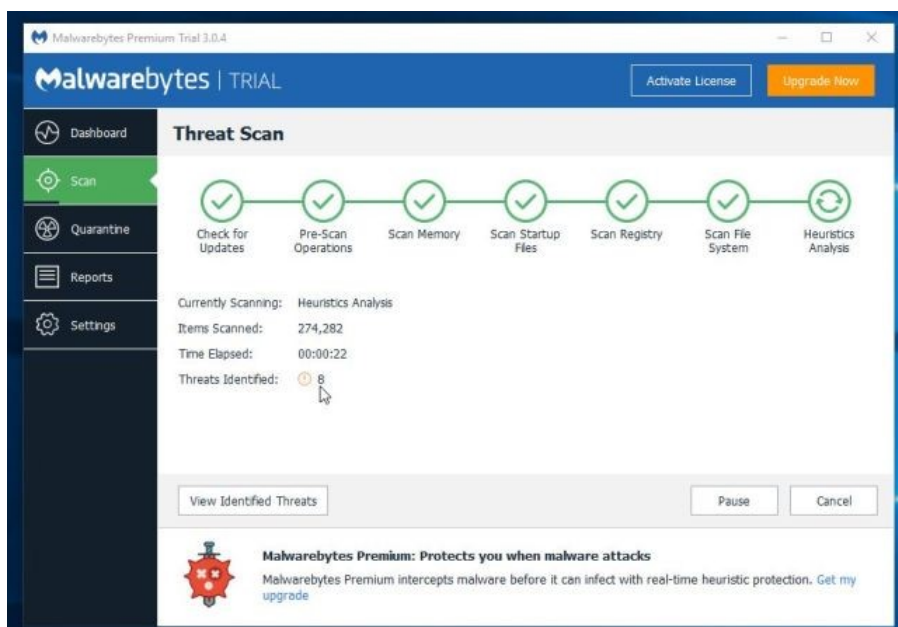


44. Once installed, Malwarebytes will automatically start and update the antivirus database. To start a system scan you can click on the **“Scan Now”** button.



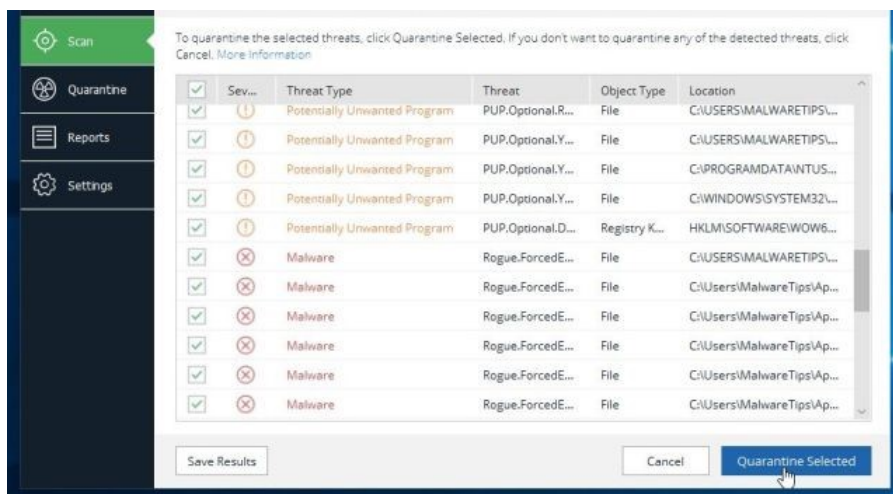
55. Malwarebytes will now start scanning your computer for malicious programs.

This process can take a few minutes, so we suggest you do something else and periodically check on the status of the scan to see when it is finished.

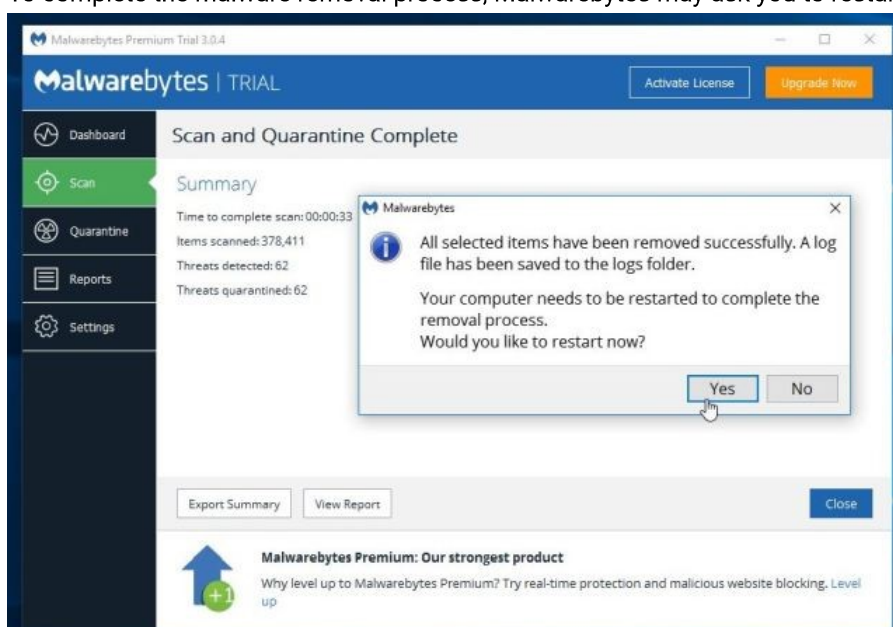


56. When the scan has completed, you will be presented with a screen showing the malware infections that Malwarebytes has detected.

To remove the malicious programs that Malwarebytes has found, click on the **"Quarantine Selected"** button.



7. Malwarebytes will now quarantine all the malicious files and registry keys that it has found.
To complete the malware removal process, Malwarebytes may ask you to restart your computer.



When the malware removal process is complete, you can close Malwarebytes and continue with the rest of the instructions.

STEP 4: Double-check for malicious programs for HitmanPro

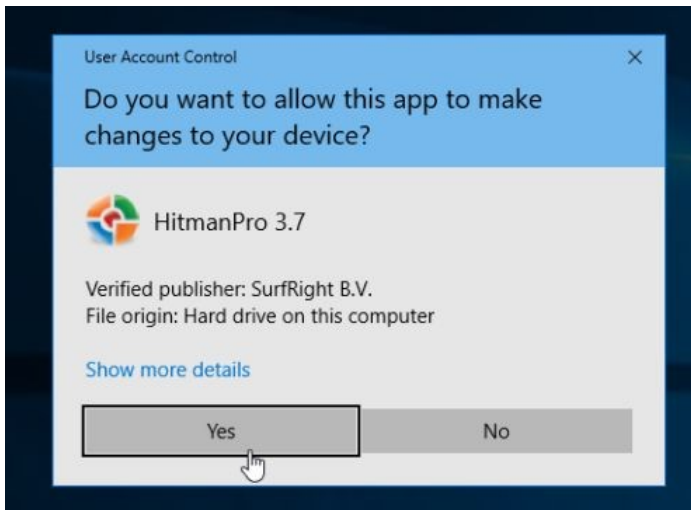
HitmanPro can find and remove malware, adware, bots, and other threats that even the best antivirus suite can oftentimes miss. HitmanPro is designed to run alongside your antivirus suite, firewall, and other security tools.

11. You can download **HitmanPro** from the below link:

HITMANPRO DOWNLOAD LINK (<https://malwaretips.com/download-hitman-pro>) (This link will open a new web page from where you can download "HitmanPro")



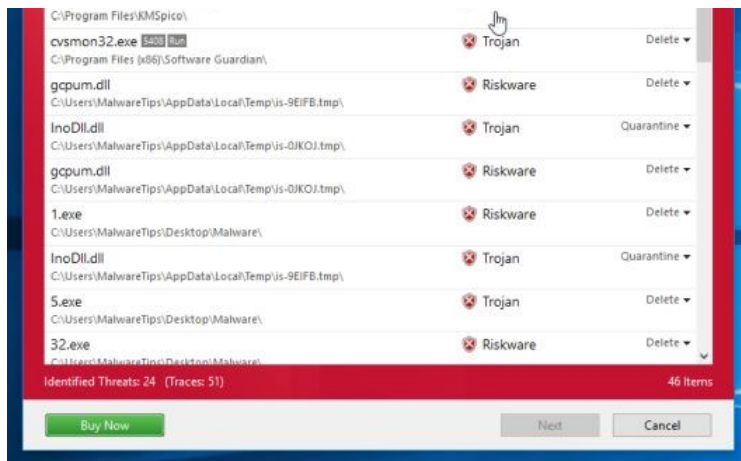
You may be presented with an *User Account Control* pop-up asking if you want to allow HitmanPro to make changes to your device. If this happens, you should click “Yes” to continue with the installation.



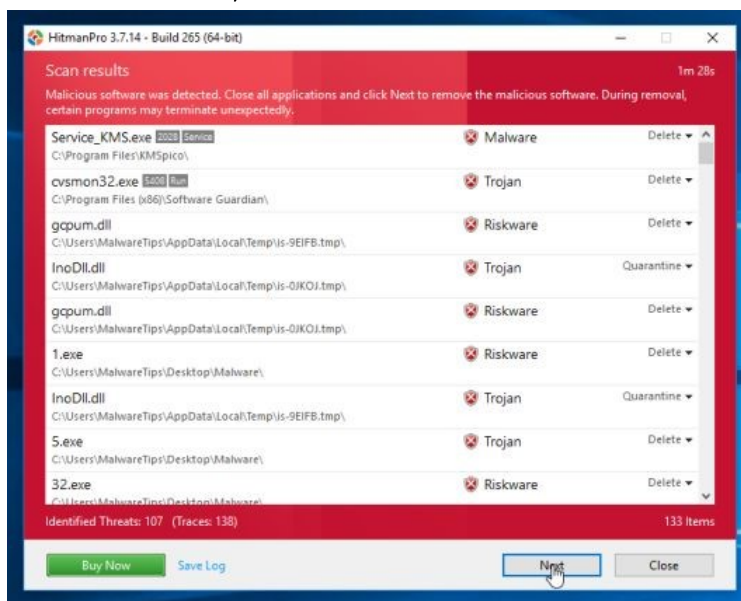
3. When the program starts you will be presented with the start screen as shown below. Now click on the **Next** button to continue with the scan process.



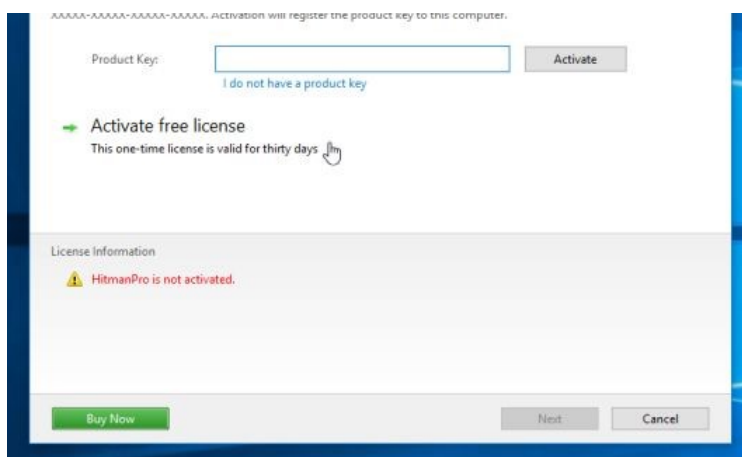
4. HitmanPro will now begin to scan your computer for malware.



55. 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 malware.



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



When the process is complete, you can close HitmanPro and continue with the rest of the instructions.

(OPTIONAL) STEP 5: Reset your browser to default settings

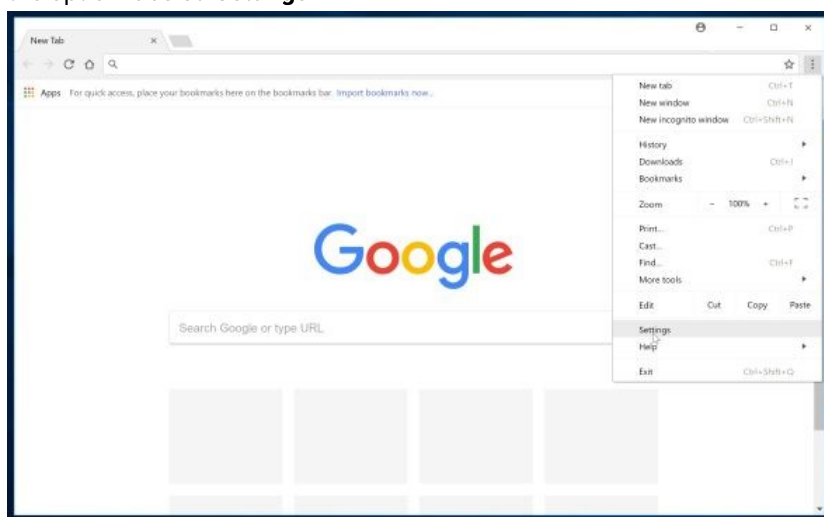
If you are still experiencing issues with the ReimagePlus.com redirect within Internet Explorer, Firefox or Chrome, we will need to reset your browser to its default settings.

This step should be performed only if your issues have not been solved by the previous steps.

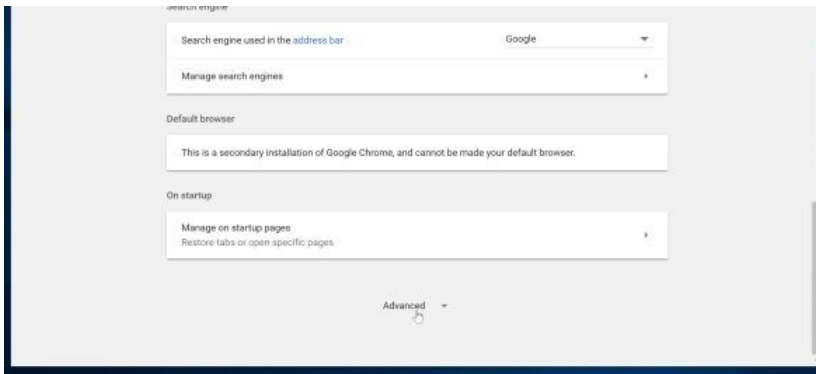
Google Chrome

Google Chrome has an option that will reset itself to its default settings. Resetting your browser settings will reset the unwanted changes caused by installing other programs. However, your saved bookmarks and passwords will not be cleared or changed.

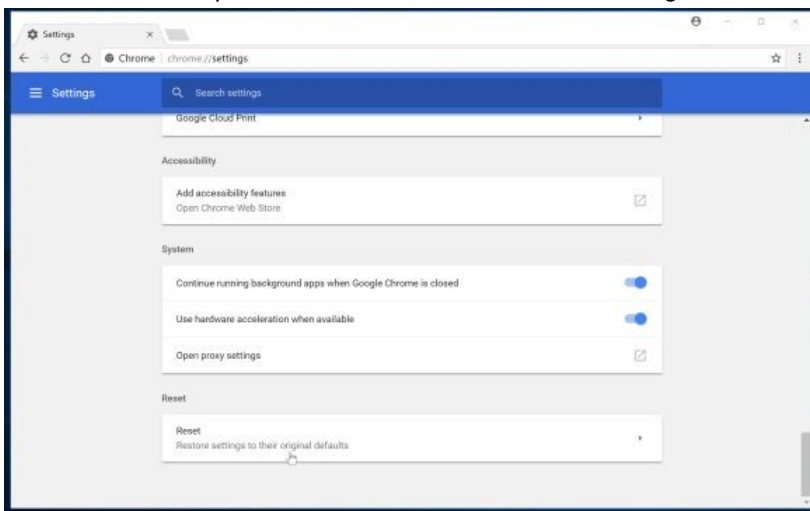
1. Click on Chrome's main menu button, represented by three horizontal lines. When the drop-down menu appears, select the option labeled **Settings**.



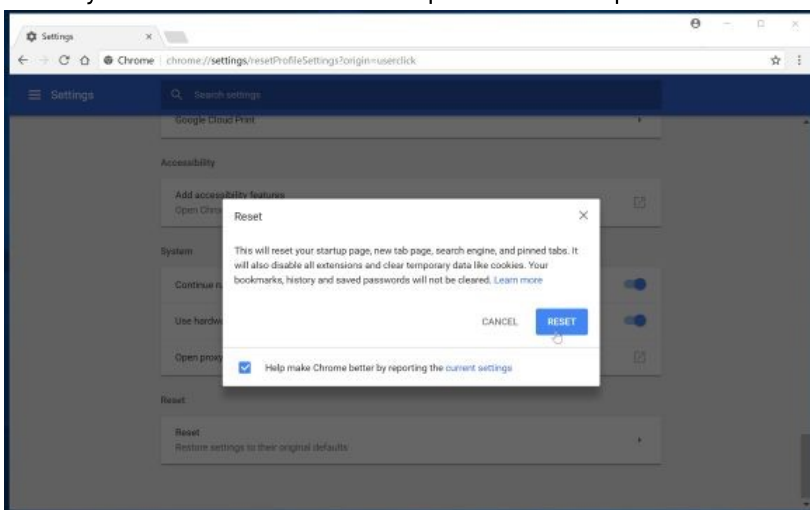
2. Chrome's Settings should now be displayed in a new tab or window, depending on your configuration. Next, scroll to the bottom of the page and click on the **Advanced** link (as seen in the below example).



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** 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.

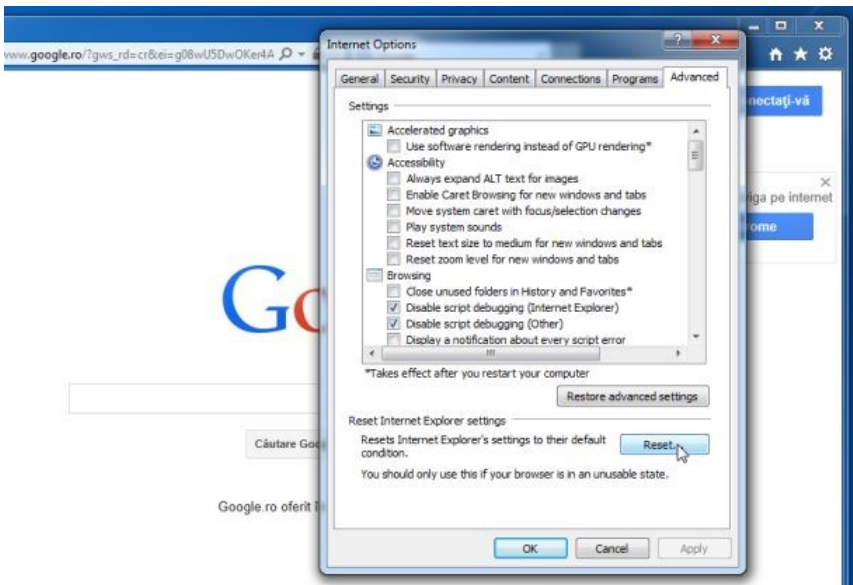


Internet Explorer

1. Open Internet Explorer, click on the **"gear icon"** in the upper right part of your browser, then click again on **Internet Options**.



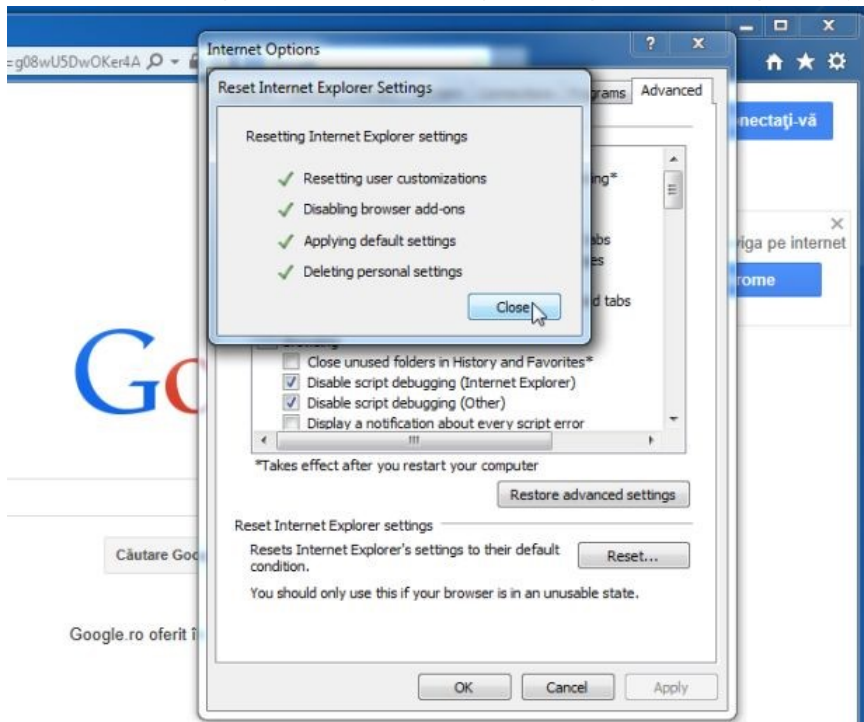
2. In the *"Internet Options"* dialog box, click on the **"Advanced"** tab, then click on the **"Reset"** button.



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.



Mozilla Firefox

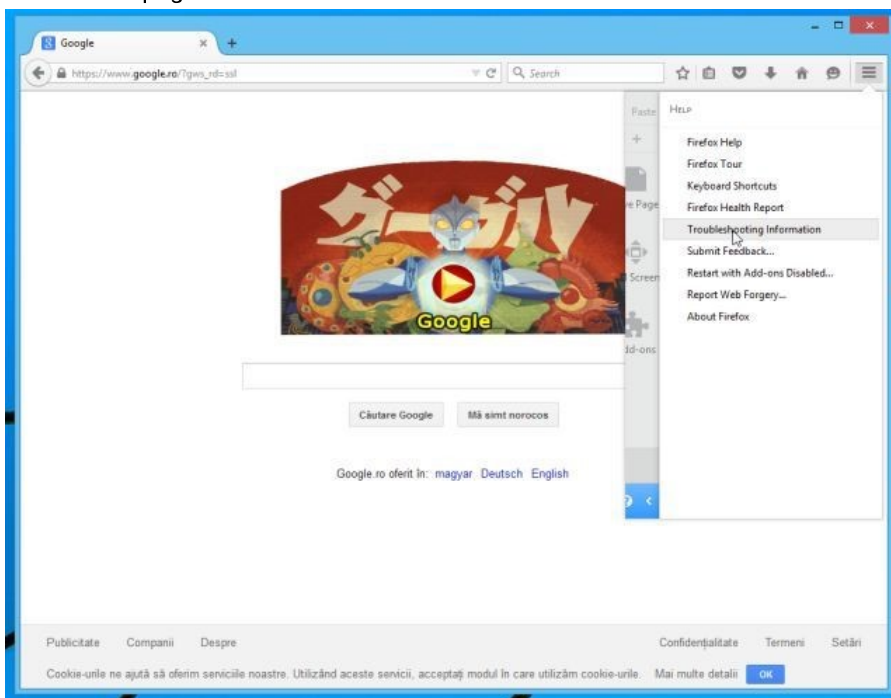
If you're having problems with Firefox, resetting it can help. The reset feature fixes many issues by restoring Firefox to its factory default state while saving your essential information like bookmarks, passwords, web form auto-fill information, browsing history and open tabs.

1. In the upper-right corner of the Firefox window, click the **Firefox menu button**, then click on the **“Help”** button.

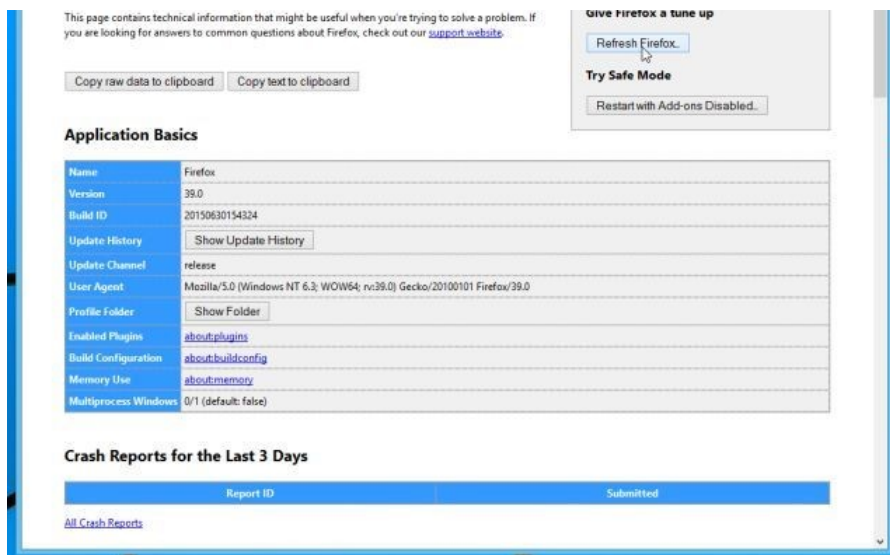


2. From the *Help* menu, choose **Troubleshooting Information**.

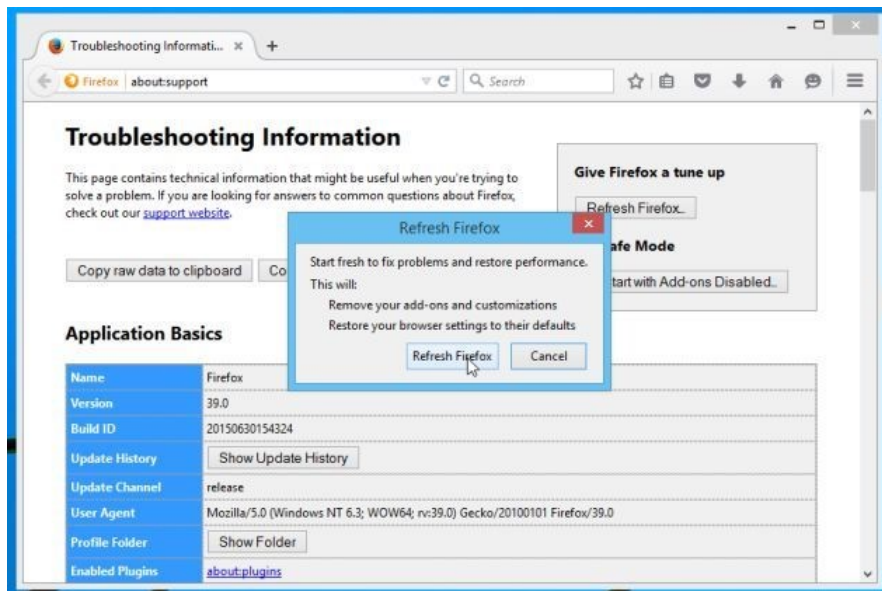
If you're unable to access the Help menu, type `about:support` in your address bar to bring up the Troubleshooting information page.



3. Click the **"Refresh Firefox"** button in the upper-right corner of the *"Troubleshooting Information"* page.



4. To continue, click on the **“Refresh 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”**.

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.

Your PC should now be free of the ReimagePlus.com adware. If you are still experiencing problems while trying to remove ReimagePlus.coma redirect from your web browser, please do one of the following:

- Run a system scan with **Zemana AntiMalware** (<https://malwaretips.com/blogs/run-a-scan-with-zemana-antimalware/>)
- Ask for help in our **Malware Removal Assistance For Windows** (<https://malwaretips.com/forums/malware-removal-assistance->

WE LOVE MALWAREBYTES AND HITMANPRO!

We really like the free versions of Malwarebytes and HitmanPro, and we love the **Malwarebytes Anti-Malware Premium** and **HitmanPro.Alert** features.



Malwarebytes Anti-Malware Premium sits beside your traditional antivirus, filling in any gaps in its defenses, providing extra protection against sneakier security threats.

MALWAREBYTES ANTI-MALWARE PREMIUM FEATURES ([HTTPS://MALWARETIPS.COM/MALWAREBYTES-PRO](https://malwaretips.com/malwarebytes-pro))



HitmanPro.Alert prevents good programs from being exploited, stops ransomware from running, and detects a host of different intruders by analyzing their behavior. HitmanPro.Alert will run alongside your current antivirus without any issues.

HITMANPRO.ALERT FEATURES ([HTTPS://MALWARETIPS.COM/DOWNLOAD-HITMANPROALERT](https://malwaretips.com/download-hitmanproalert))

« [HOW TO REMOVE SPOUTLY ADWARE \(VIRUS REMOVAL GUIDE\)](https://malwaretips.com/blogs/remove-spoofly-ads/) ([HTTPS://MALWARETIPS.COM/BLOGS/REMOVE-SPOUTLY-ADS/](https://malwaretips.com/blogs/remove-spoofly-ads/))
[REMOVE FUNDONALD EXTENSION BY WELOACK.COM \(CHROME SCAM\)](https://malwaretips.com/blogs/remove-fundonald-by-weioack-com/) » ([HTTPS://MALWARETIPS.COM/BLOGS/REMOVE-FUNDONALD-BY-WELOACK.COM/](https://malwaretips.com/blogs/remove-fundonald-by-weioack-com/))

NEED HELP?

If you would like help with any of these fixes, you can ask for free malware removal support in the [Malware Removal Assistance](https://malwaretips.com/forums/malware-removal-assistance-for-windows.10/) (<https://malwaretips.com/forums/malware-removal-assistance-for-windows.10/>) forum. In this support forum, a trained staff member will help you clean-up your device by using advanced tools. Never used a forum? [Learn how](https://malwaretips.com/help/welcome-guide/) (<https://malwaretips.com/help/welcome-guide/>).

ASK FOR HELP NOW ([HTTPS://MALWARETIPS.COM/FORUMS/MALWARE-REMOVAL-ASSISTANCE-FOR-WINDOWS.10/](https://malwaretips.com/forums/malware-removal-assistance-for-windows.10/))

HELPFUL LINKS

[Contact Us](https://malwaretips.com/misc/contact) (<https://malwaretips.com/misc/contact>)

COMMUNITY

[Meet the Staff Team](https://malwaretips.com/members/?type=staff)
(<https://malwaretips.com/members/?type=staff>)

TIP

Without meaning to, you may click a link that installs malware on your computer. To keep your computer safe, only click links

[Terms and Rules \(https://malwaretips.com/help/terms\)](https://malwaretips.com/help/terms)

[We Use Cookies \(https://malwaretips.com/help/cookies\)](https://malwaretips.com/help/cookies)

[Privacy Policy \(https://malwaretips.com/help/privacy-policy/\)](https://malwaretips.com/help/privacy-policy/)

[Our Community Guidelines \(https://malwaretips.com/help/rules/\)](https://malwaretips.com/help/rules/)

[Welcome Guide \(https://malwaretips.com/help/welcome-guide/\)](https://malwaretips.com/help/welcome-guide/)

and downloads from sites that you trust.
Don't open any unknown file types, or
download programs from pop-ups that
appear in your browser.

MalwareTips.com is an Independent Website. All trademarks mentioned on this page are the property of their respective owners. We can not be held responsible for any issues that may occur by using this information.