What is HulaToo? How to remove HulaToo?

HulaToo ad software is designed to edit browser settings and can install additional plugins (toolbars, extensions or add-ons) on the web browser to add advertising links. go there. In addition, this program can navigate users 'computers to malicious websites or can install additional malicious programs to compromise security issues on users' computers.

HulaToo ad software is designed to edit browser settings and can install additional plugins (toolbars, extensions or add-ons) on the web browser to " *insert* " links advertise there. In addition, this program can navigate users 'computers to malicious websites or can install additional malicious programs to "compromise" security issues on users' computers.

Part 1: What is HulaToo?

' *HulaToo* ' is a **malicious adware,** if HulaToo is installed on your computer, it will modify the system settings to display advertising popup windows or navigate web browsers to the website contains ads. And if your computer is hacked by HulaToo, the computer screen will display pop-up windows. And this is also one of the **reasons why your computer is getting slower and slower by malicious programs running on the background** .

HulaToo ad software is designed to edit browser settings and can install additional plugins (toolbars, extensions or add-ons) on the web browser to "insert" links advertise there. In addition, this program can navigate users 'computers to malicious websites or can install additional malicious programs to "compromise" security issues on users' computers.

Technically, HulaToo is not a virus that is classified as an unwanted program (PUP - Potentially Unwanted Program) that can contain and install malicious programs on your computer, for example. such as adware (adware), toolbars or viruses. If your computer is infected with adware, then your computer screen will constantly appear pop-up popup windows, banners and sponsored links or in some speed cases. Web browsing of browsers is slow due to malicious programs running in the background.

The HulaToo advertising program is installed on the system without user knowledge, the reason is because these programs are packaged inside other free software and when users download these software to install set, accidentally installed both advertising programs HulaToo advertising.

For this reason, when installing any program on your computer, you should:

1. On the application installation screen, do not click the Next button too fast.
2. Read the terms carefully before clicking Accept.
3. Always select 'Custom' installation - customize the settings.
4. Reject the installation of additional software that you do not want to install.
5. Disregard any of the options that say the homepage and search settings will be edited.

Part 2: Remove HulaToo root

Step 1: Uninstall HulaToo on a Windows computer

The first step is to find and remove the HulaToo program installed on your computer.

1. Access the Uninstall menu.

- On Windows 7 and Windows Vista:

If you use Windows XP, Windows Vista and Windows 7, click the **Start** button, then click **Control Panel** .

- On Windows 10 and Windows 8:

To uninstall a program on a Windows 10 or Windows 8 computer, first right-click the Start button and select **Control Panel** .

2. On the Control Panel window, click on the option to ' *Uninstall a program* ' located in the **Programs** section.

If you are using Classic View on Control Panel, double-click the Programs and Features icon.

3. On the Programs and Features or Uninstall a Program window, scroll down to the list of recently installed programs, then find and uninstall the HulaToo program.

- Also find and uninstall unknown programs.

- To see recently installed programs, click Installed On to arrange applications by date. Then roll down the list and uninstall unwanted programs.

- If you have trouble uninstalling the malicious programs, you can use Revo Uninstaller to completely remove unwanted programs on your computer.

1. Download Revo Uninstaller to your computer and install it here.

Step 2: Remove HulaToo adware on Internet Explorer, Firefox and Chrome with AdwCleaner

AdwCleaner is a free utility that will scan your system and web browsers for finding and removing HulaToo malicious programs, malicious files, and unwanted extensions installed. on the browser without your knowledge.

1. Download AdwCleaner to your device and install it.

Download AdwCleaner to your device and install it here.

2. Before installing AdwCleaner, close all web browsers on your computer, then double-click the AdwCleaner icon.

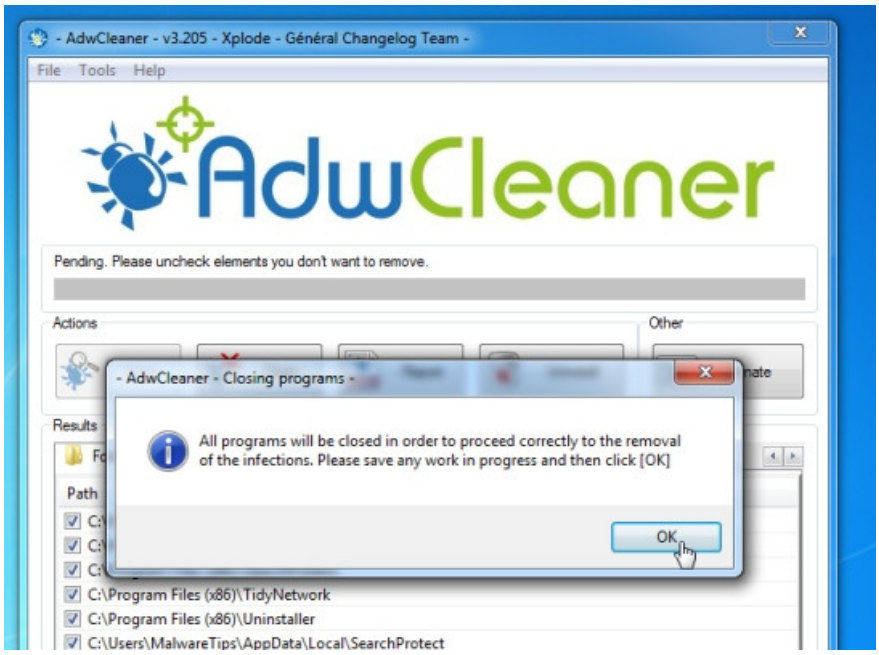
If Windows asks if you want to install AdwCleaner, click **Yes** to allow the program to run.

3. When the program has opened, click the **Scan** button as shown below:

And AdwCleaner will start the scanning process to find and remove adware and other malicious programs.

4. To remove the malicious **Babylon Toolbar files** detected **by AdwCleaner** , click the **Clean** button.

5. AdwCleaner will notify you to save any files or documents that you are opening because the program needs to restart the computer to complete the process of cleaning up the malicious files. Your task is to save the files and documents again, then click **OK** .



Step 3: Clean HulaToo virus with Malwarebytes Anti-Malware Free

Malwarebytes Anti-Malware Free is an on-demand system scan tool that will find and remove all "threats" or malware (malware) from your computer, including worms. , trojian, rootkit, rouge, dialer, spyware (spyware), .

And most importantly, Malwarebytes Anti-Malware will run in parallel with other antivirus software without a conflict.

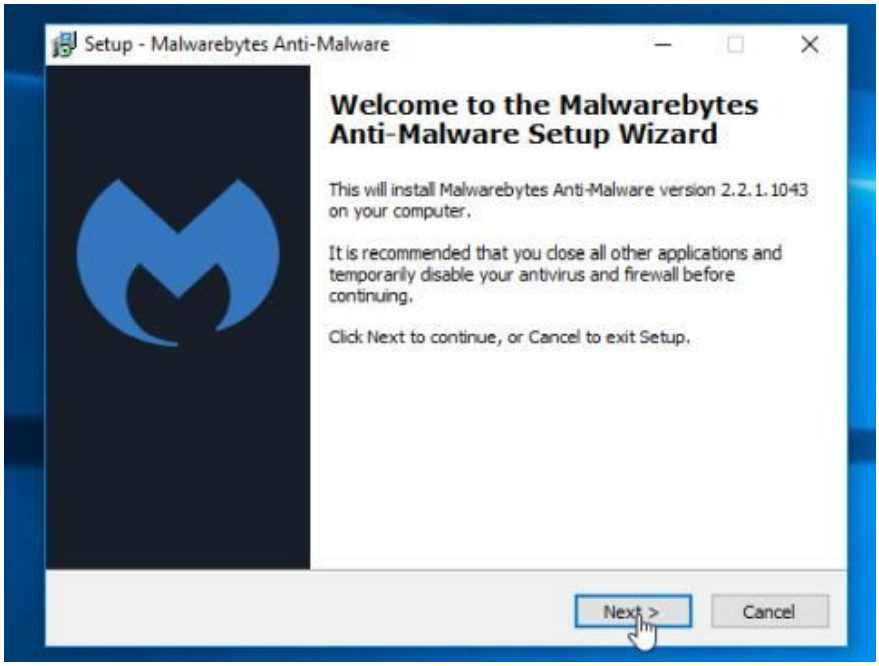
1. Download Malwarebytes Anti-Malware to your computer and install it.

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

2. After downloading Malwarebytes Anti-Malware Free, close all programs, then double-click the icon named **mbam-setup** to start the installation process of Malwarebytes Anti-Malware Free.

The User Account Control dialog box appears now on the screen asking if you want to run the file. Click **Yes** to continue the installation process.

3. Follow the on-screen instructions to install Malwarebytes Anti-Malware Setup Wizard.

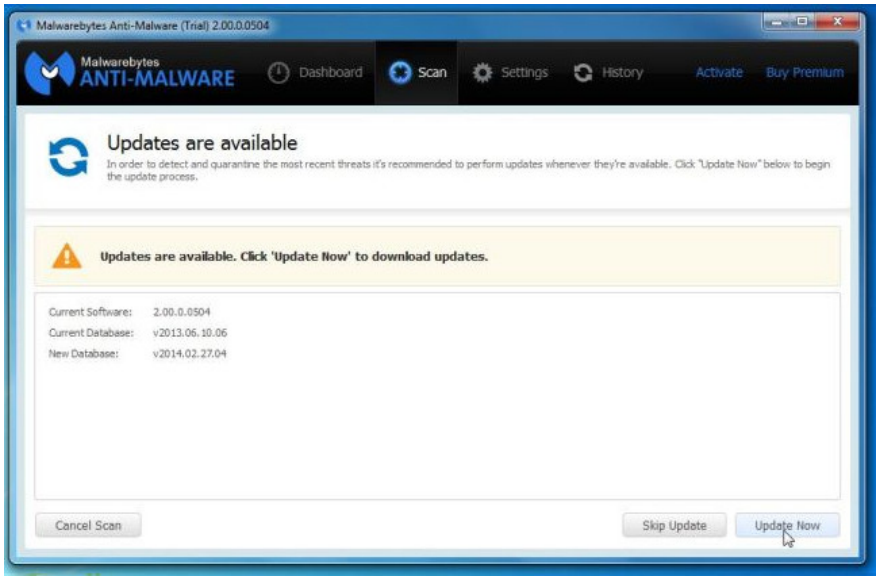


Click **Next** to install Malwarebytes Anti-Malware, until the last window click **Finish** to complete.

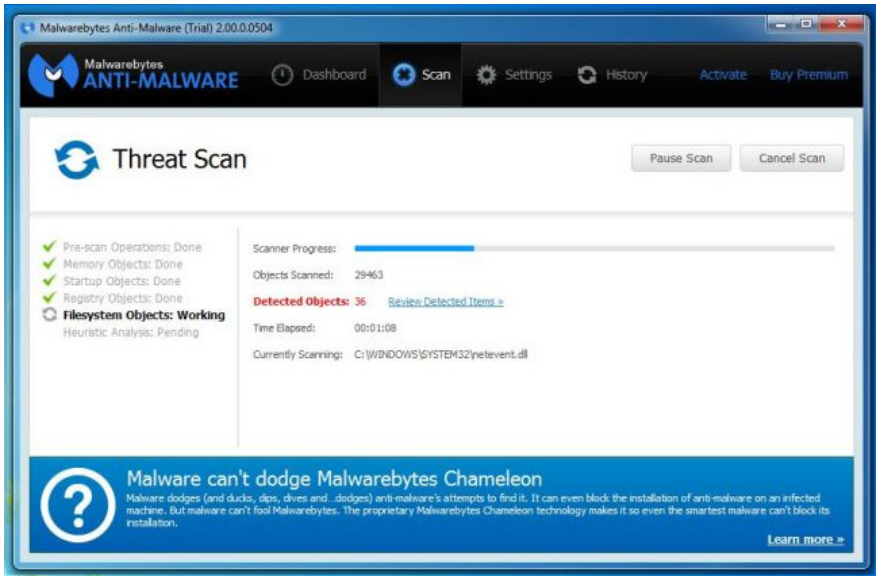
4. After installation is complete, Malwarebytes Anti-Malware will automatically open and update antivirus data. To start the scanning process on the system, click the **Fix Now** button.

Alternatively, you can click the **Scan tab** and select Threat Scan, then click **Scan Now** .

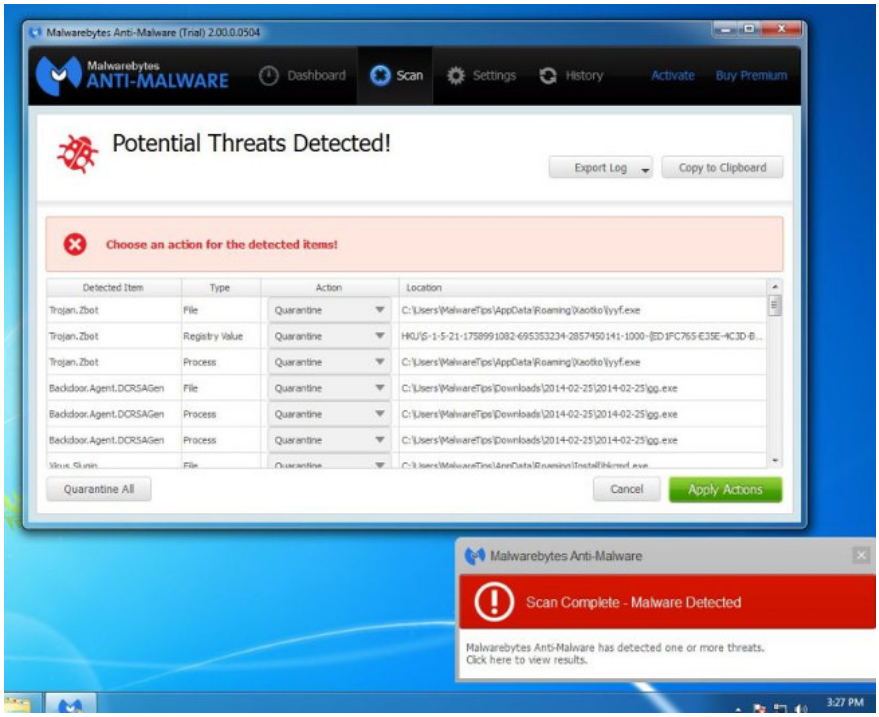
5. Malwarebytes Anti-Malware will start checking for the latest updates. If there are any new updates, click the **Update Now** button.



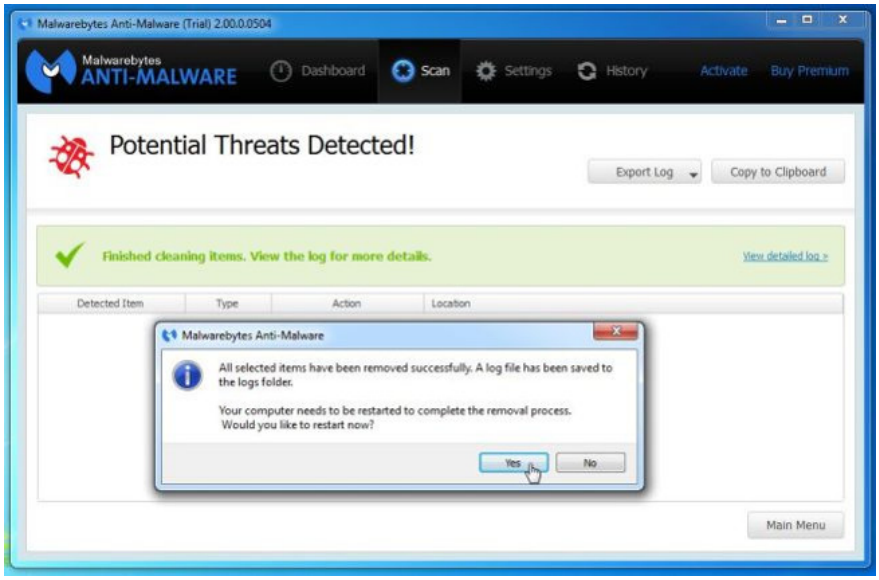
6. Malwarebytes Anti-Malware will start scanning your system to find and remove programs and malware on your system.



7. After the scanning process has finished, a window will appear displaying all the files and malicious programs detected by Malwarebytes Anti-Malware. To remove the malicious programs detected by Malwarebytes Anti-Malware, click the Quarantine All button, then click the **Apply Now** button.



8. Malwarebytes Anti-Malware will remove all the malicious files, programs and registry keys it finds. During the removal of these files, Malwarebytes Anti-Malware may require a reboot of the computer to complete the process.



If a message appears on the screen asking to restart the computer, just restart your computer.

Step 4: Scan the system again with HitmanPro

HitmanPro finds and removes malicious programs (malware), advertising programs (adware), system threats and even viruses. The program is designed to run with antivirus programs and other security tools.

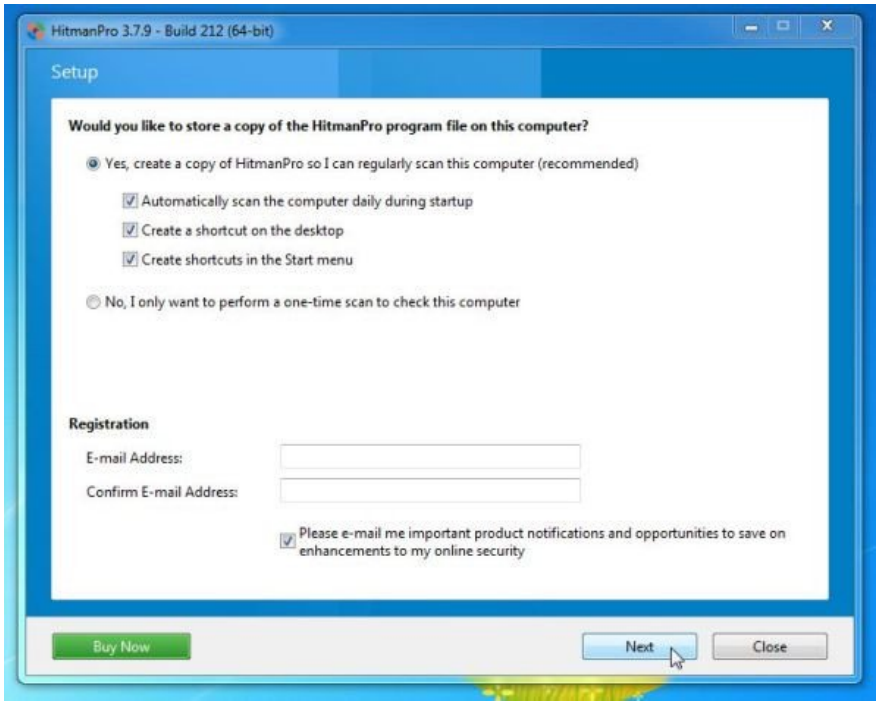
The program will scan your computer at a fairly fast speed (in less than 5 minutes) and never slow down your computer like other antivirus programs.

1. Download HitmanPro to your device and install it.

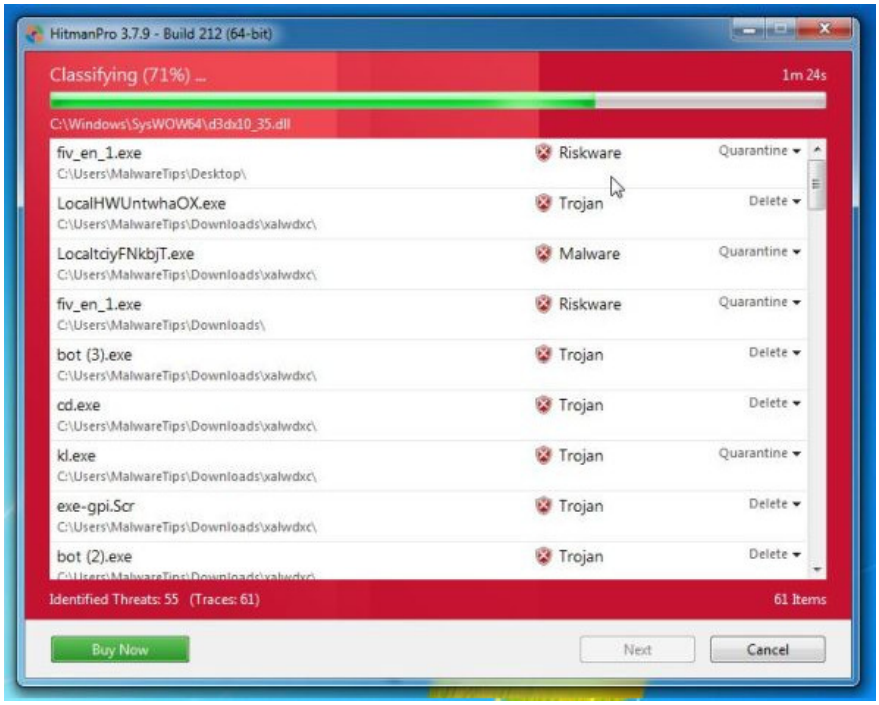
Download HitmanPro to your device and install it here.

2. Double-click the file named 'HitmanPro.exe' (if using a 32-bit version) or double-click the file 'HitmanPro_x64.exe' (if using a 64-bit version). When the program launches, the window will appear as shown below:

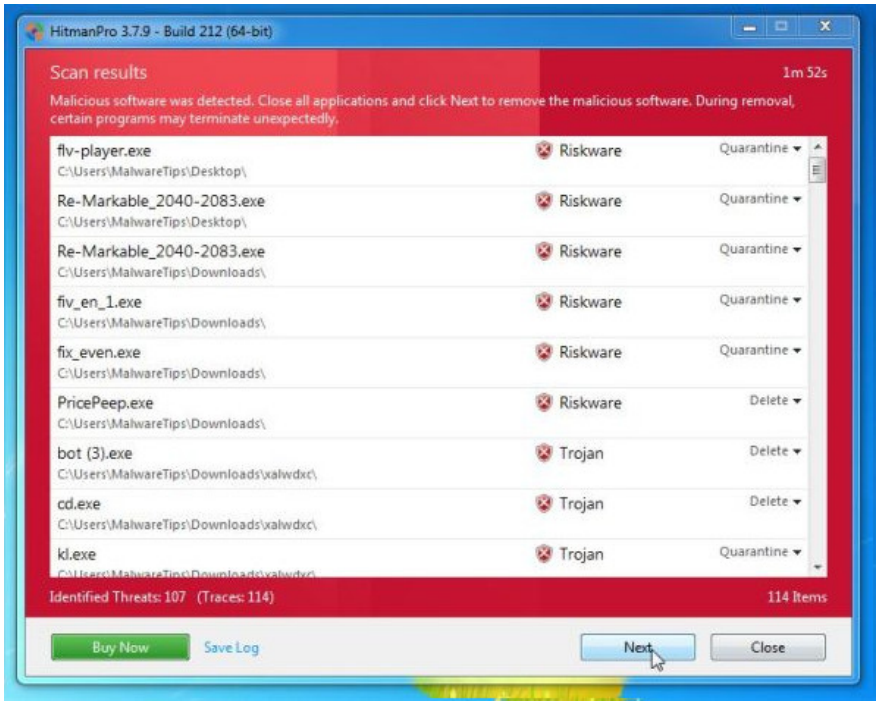
Click **Next** to install HitmanPro on your computer.



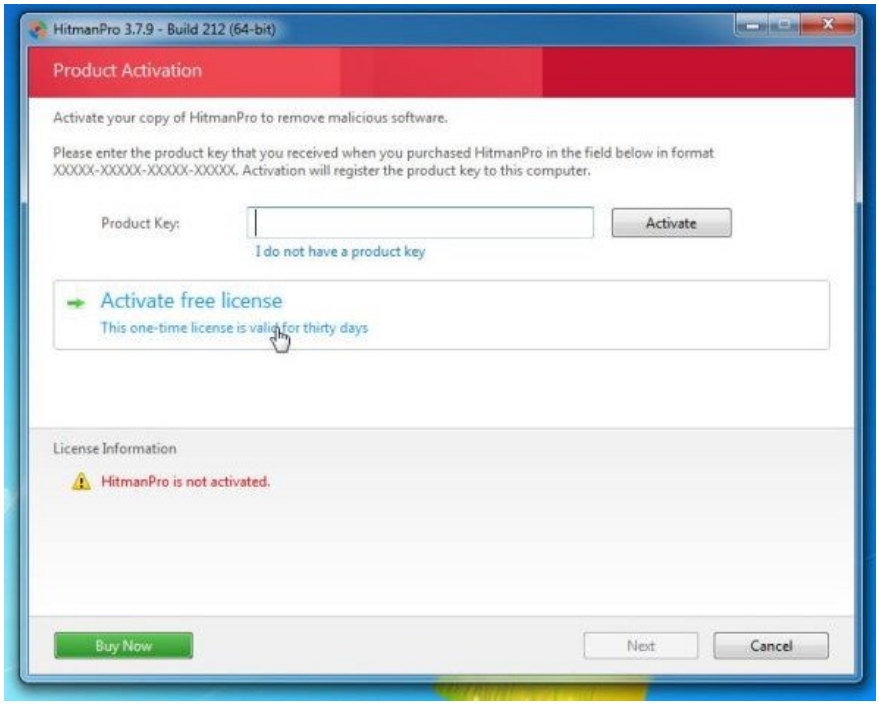
3. And HitmanPro will begin the process of scanning HulaToo malicious files from your computer.



4. After the process finishes, HitmanPro will display the list of malicious programs (malware) that it finds on your system. Click **Next** to remove malicious programs and HulaToo virus.



5. Click the **Activate free license** button to try HitmanPro for 30 days and to remove the malicious files from your system.



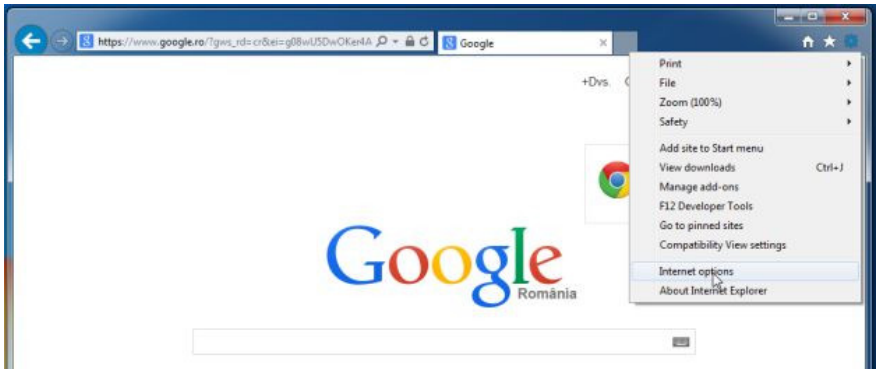
Step 5: Reset Internet Explorer, Firefox and Chrome browsers to the initial default settings

To get rid of HulaToo root from Internet Explorer, Firefox, Google Chrome and Microsoft Edge, you will have to reset the browser to its original default setting.

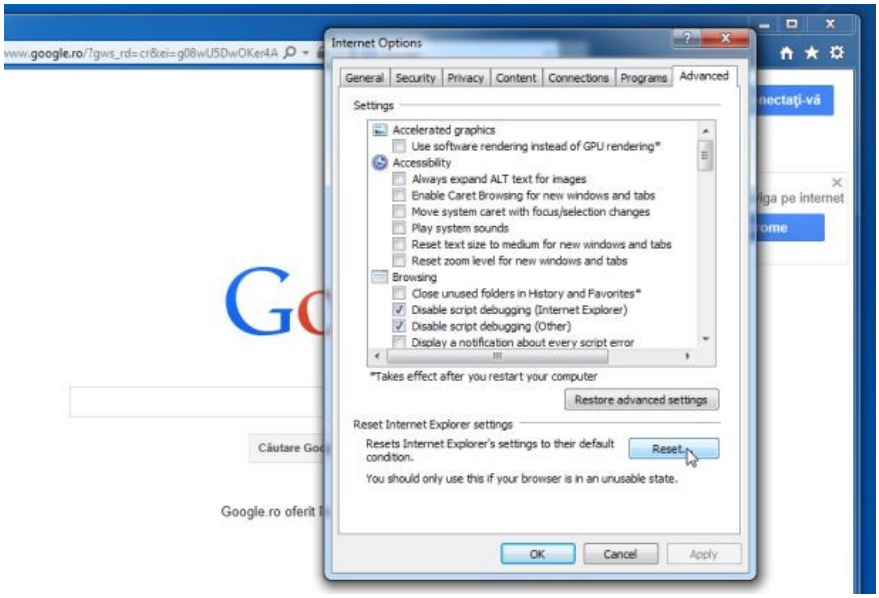
- Internet Explorer browser:

You can reset Internet Explorer to the initial default setting. To do this thing:

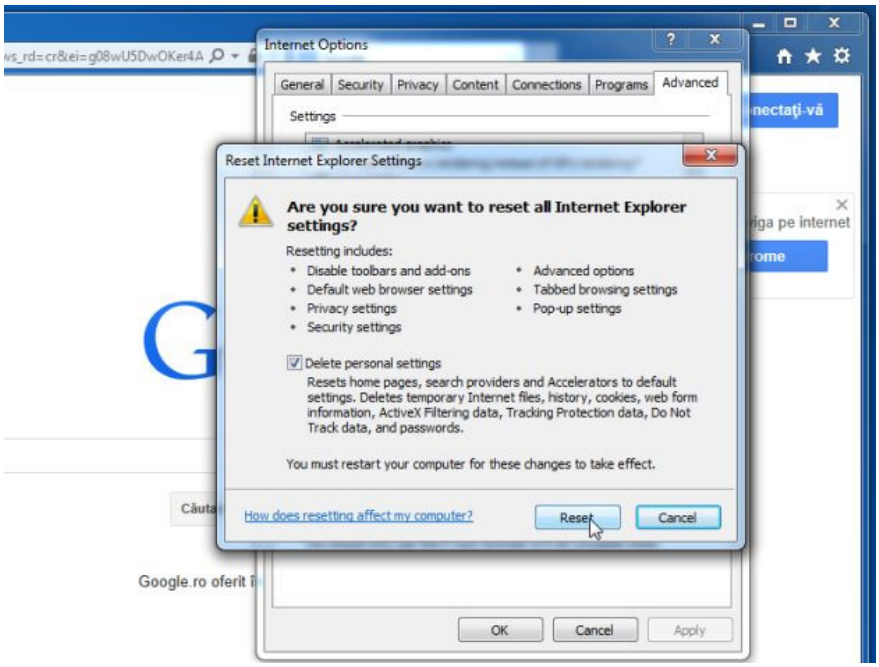
1. Open Internet Explorer on your computer and then click the jagged icon in the top right corner of the screen, select Internet Options.



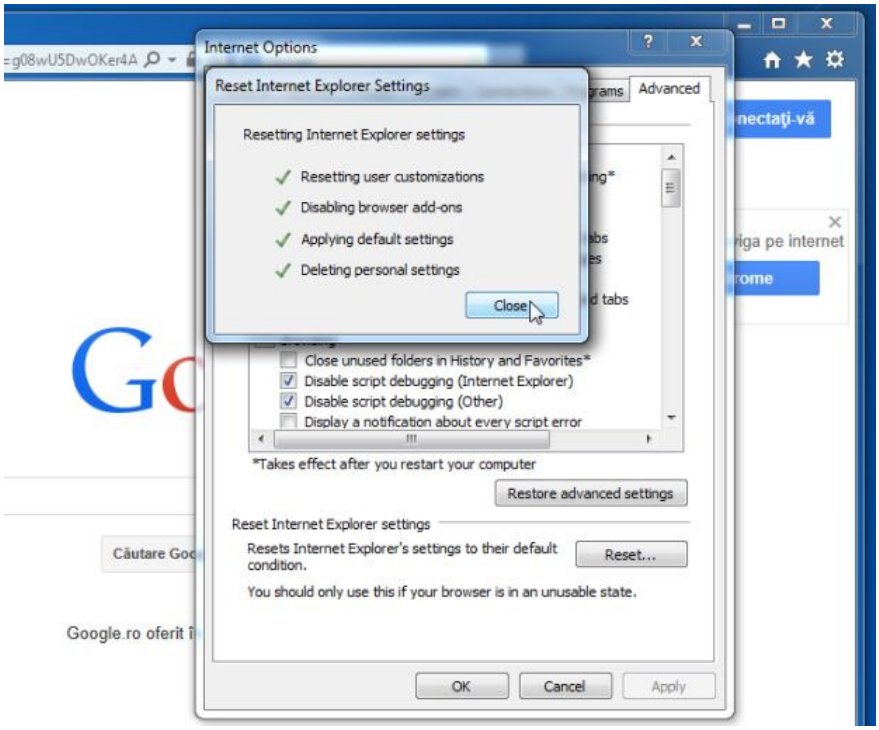
2. On the Internet Options dialog window, click the **Advanced tab** and then click the **Reset** button.



3. Next on the Reset Internet Explorer settings window, select the Delete personal settings button and click the Reset button.



4. After finishing the process, click the **Close** button on the confirmation dialog.

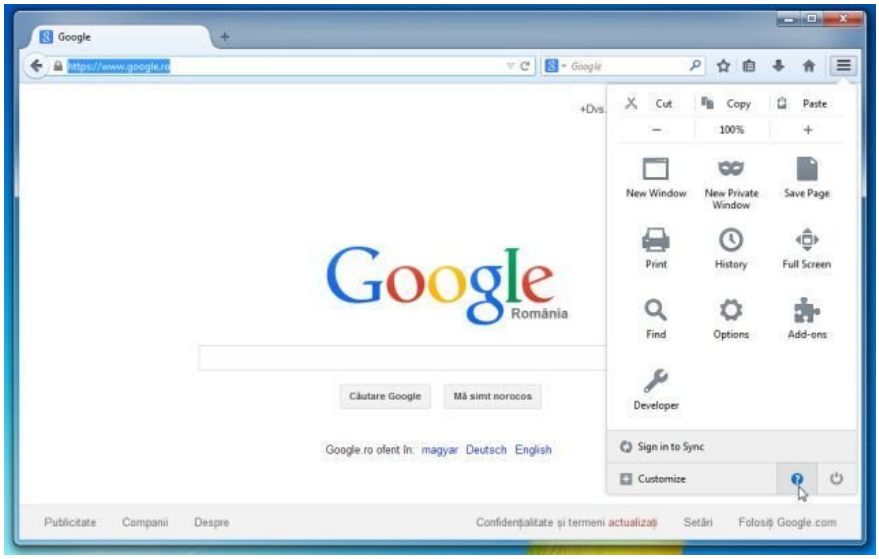


Firefox browser:

The process of resetting Firefox browser will not lose important information that you have saved on the browser such as passwords, bookmarks, auto-fill information, browsing history and opening tabs.

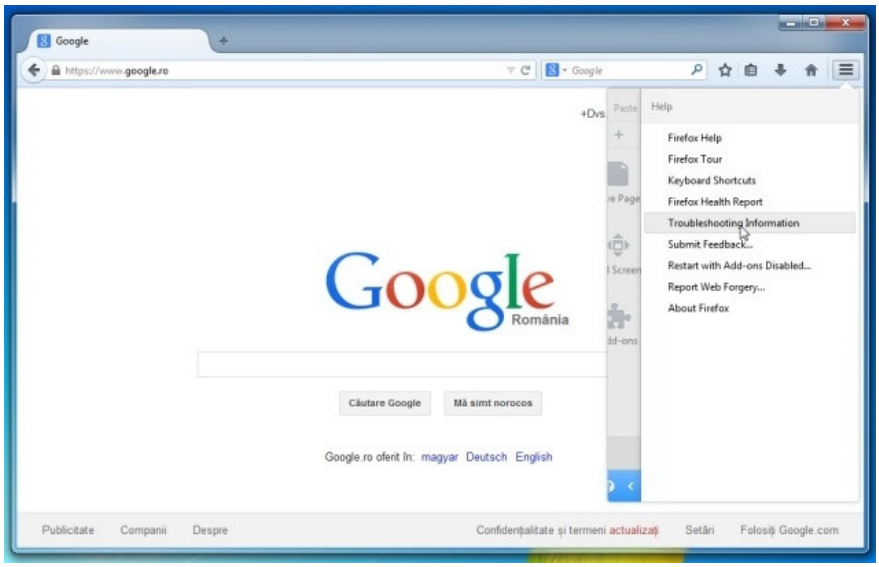
To reset Firefox to its original default state, follow the steps below:

1. Open Firefox on your computer, then click the 3 dash line icon in the top right corner of the screen, click the **Help** button.

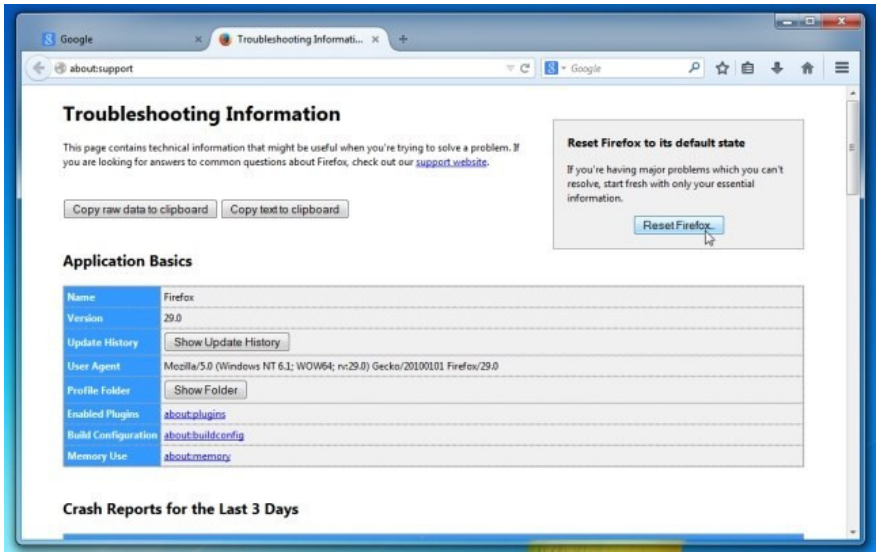


2. From the Help Menu, select **Troubleshooting Information** .

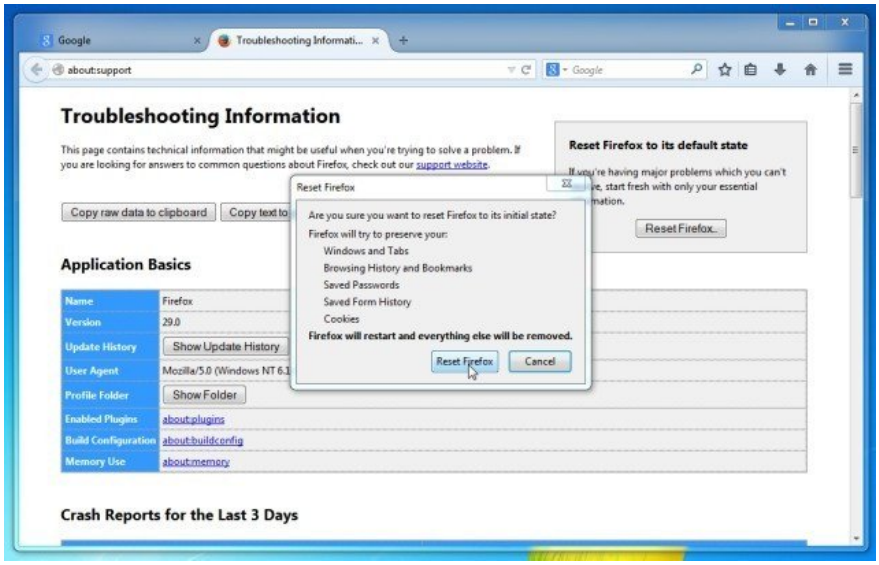
If you cannot access the Menu Help, enter **about: support** in the address bar and press Enter to open the Troubleshooting Information page.



3. Click the **Refresh Firefox** button in the top right corner of the Troubleshooting Information page.



4. To continue, click the **Refresh Firefox** button on the confirmation window.

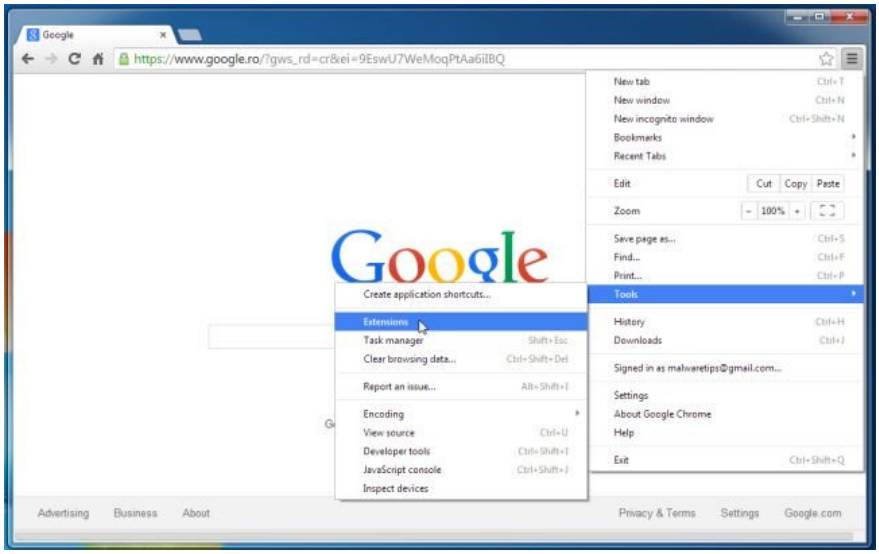


5. Firefox will close itself and revert to the initial default setting. After completing a window displays the converted information appears. Click Finish to finish.

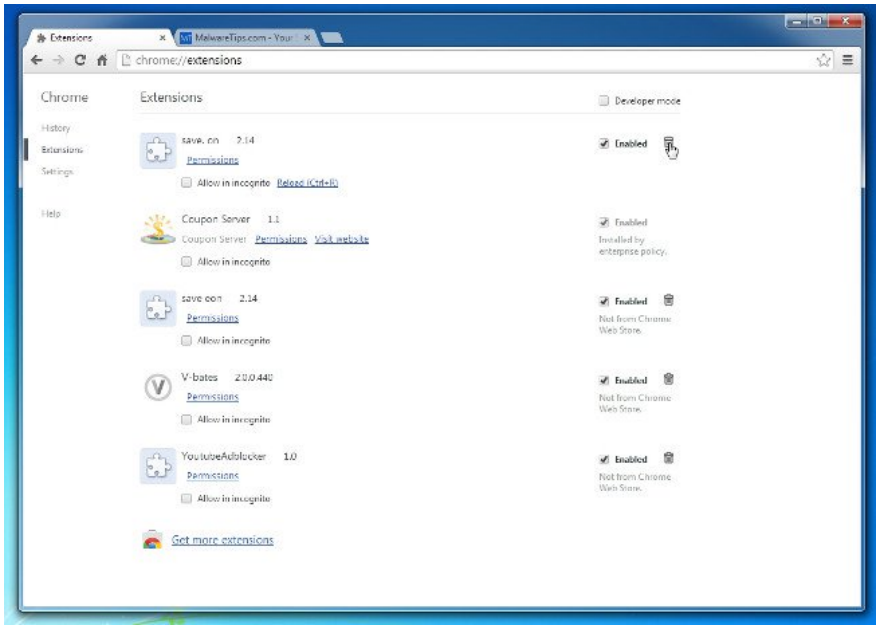
- Chrome browser:

Optional Google Chrome resets the browser to its original default setting. Resetting the browser settings will reset the unwanted changes caused by the installation of other programs on the system. However, the password and bookmarks you save will be erased.

1. On Chrome browser, click the 3 dash line icon or 3 dots at the bottom right corner of the screen, then click **Extensions** .



2. In the **Extensions** window, find and delete the Hula Too extension and unknown sources by clicking the trash can icon.



Refer to some of the following articles:

1. How to set up Private Network on Windows 10?

1. Remove root malware (malware) on Windows 10 computers

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

Good luck!

You finished reading the article "**What is HulaToo? How to remove HulaToo?**" 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.
