Remove root malware (malware) on Windows 10 computers

If pop-up windows are displayed on your Windows 10 computer screen or your computer is redirected to advertising windows, it is likely that your computer has adware or chapters. Unexpected process of attack.

If pop-up windows are displayed on your Windows 10 computer screen or your computer is redirected to advertising windows, it is likely that your computer has adware or chapters. Unexpected process of attack.

These pop up ads are usually caused by advertising support programs, distributed through various platforms during the program installation process.

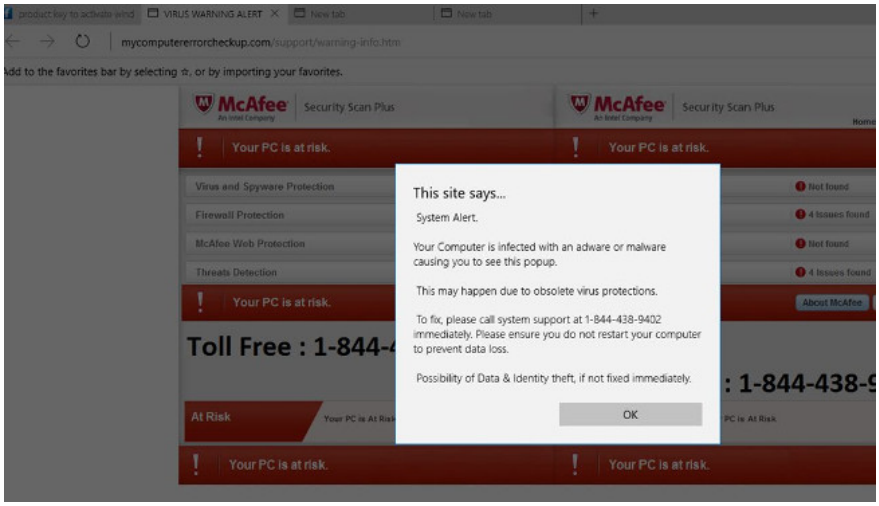
Malicious programs often infiltrate the system when you install some free software that includes the installation of these advertising programs.

When an adware program is installed on your computer, in the process of using a web browser (Google Chrome, Firefox, Microsoft Edge or Internet Explorer), you will see different popup popup windows. . Which includes:

1. Banner ads on the website you visit.
2. Content of random web pages is converted to hyperlink.
3. The browser displays popup windows that suggest you to update or install fake software.
4. Unwanted adware programs are installed on the system without users knowing.

In addition to displaying ads and collecting data, ads on Windows 10 are often 'hidden' so that users are unaware. Usually, there is no trace on the system tray, even in the list of programs installed on your system.

Adware can slow down your computer. In addition, it is also the cause of slow internet connection on the system by downloading ads. Sometimes the process of programming the adware is faulty can cause your computer to be unstable. In addition, you have to click to close each popup window.



Remove root malware (malware) on Windows 10 computers

Step 1: Scan the system with Malwarebytes AdwCleaner

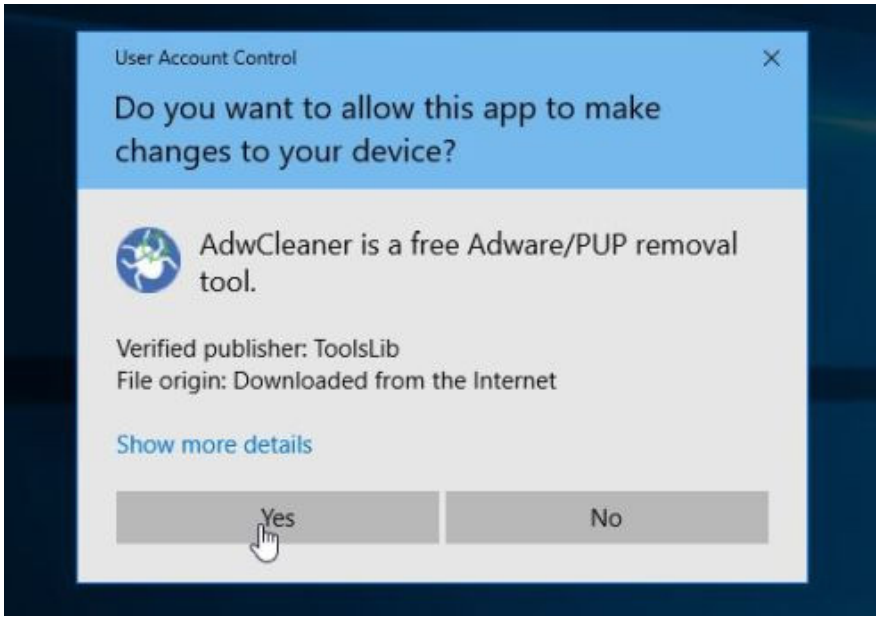
AdwCleaner is a free utility that will scan your system and web browsers to find and remove software installed on your system without your knowledge.

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 malware (malware) as well as adware.

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

5. AdwCleaner will notify you to save any files or documents that you are reopening 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** .

After your computer has finished booting and you are **logged in** again, AdwCleaner will automatically open a **Log file** containing the files, **registry keys** and programs that have been removed from your computer. You can review this log file and close the **Notepad** window again.

Step 2: Use Malwarebytes Anti-Malware to scan the system again

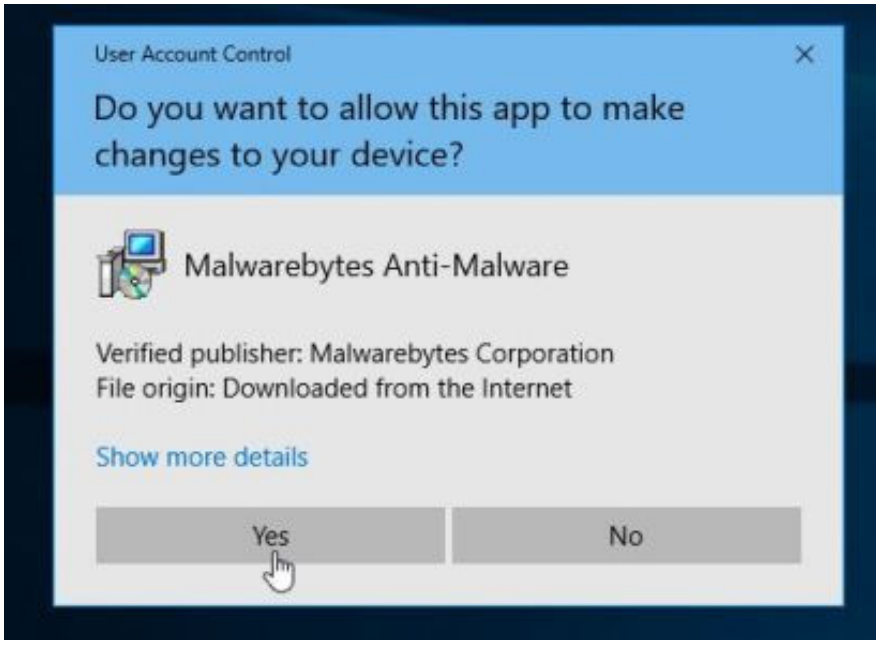
Malwarebytes Anti-Malware is an on-demand system scan tool that will remove all malware (malware) from your Windows 10 computer. The important thing is that Malwarebytes Anti-Malware will run in parallel with other antivirus software without conflict.

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

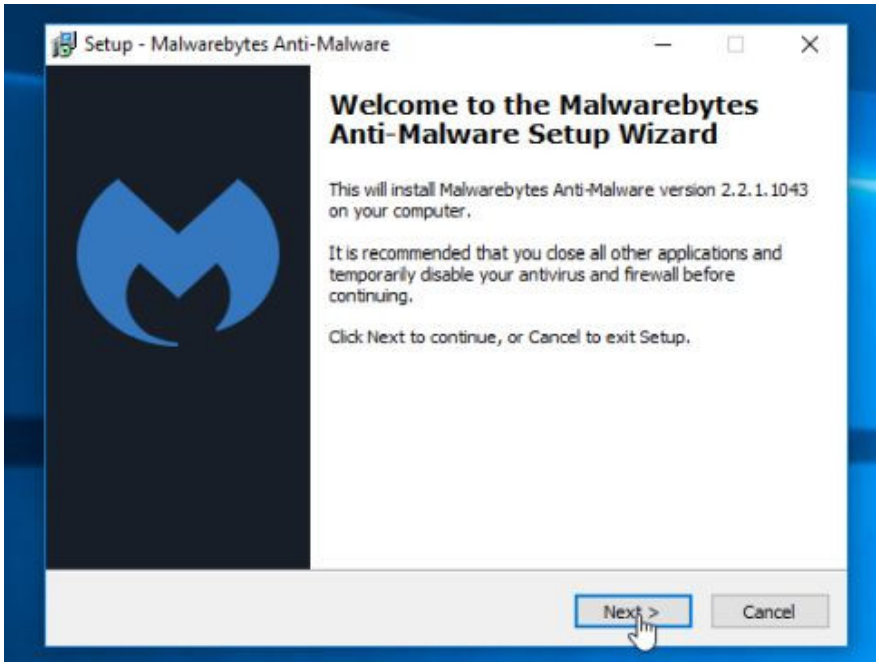
Download Malwarebytes Anti-Malware to your computer and install it here.

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

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.

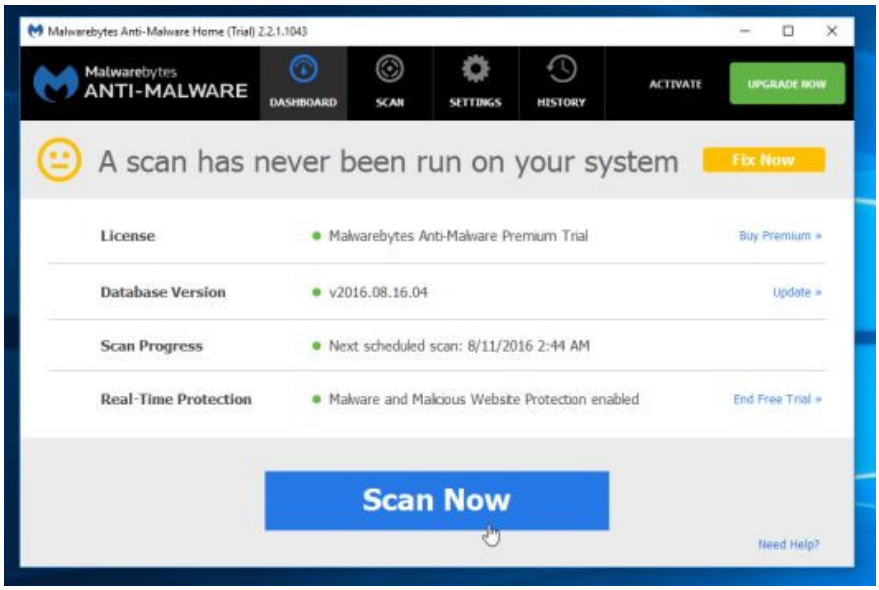


3. Follow the on-screen instructions to install Malwarebytes Anti-Malware Setup Wizard.

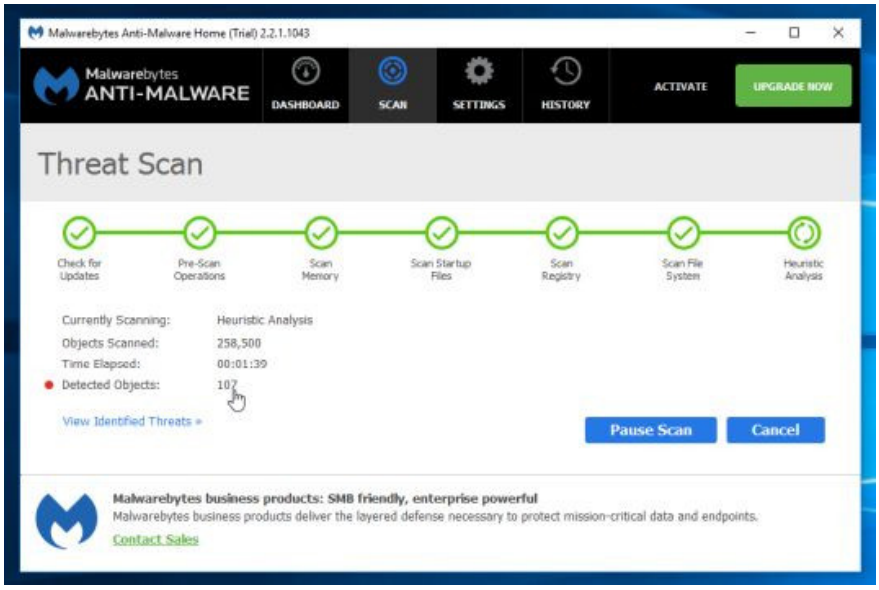


Click **Next** to install Malwarebytes Anti-Malware, until the last window click **Finish** to complete.

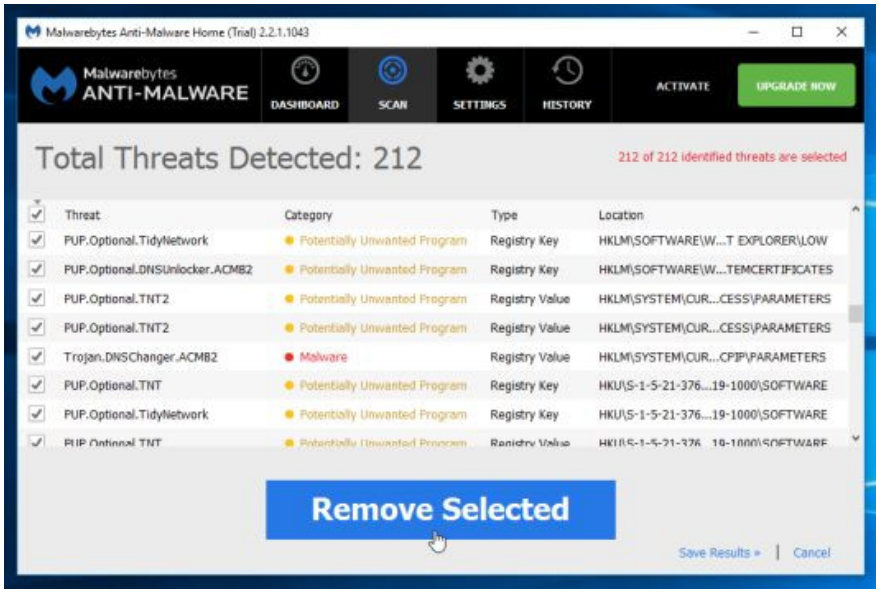
4. After installation is complete, Malwarebytes Anti-Malware will automatically open and **update** antivirus data. To start the scanning process, click the **Scan Now** button.



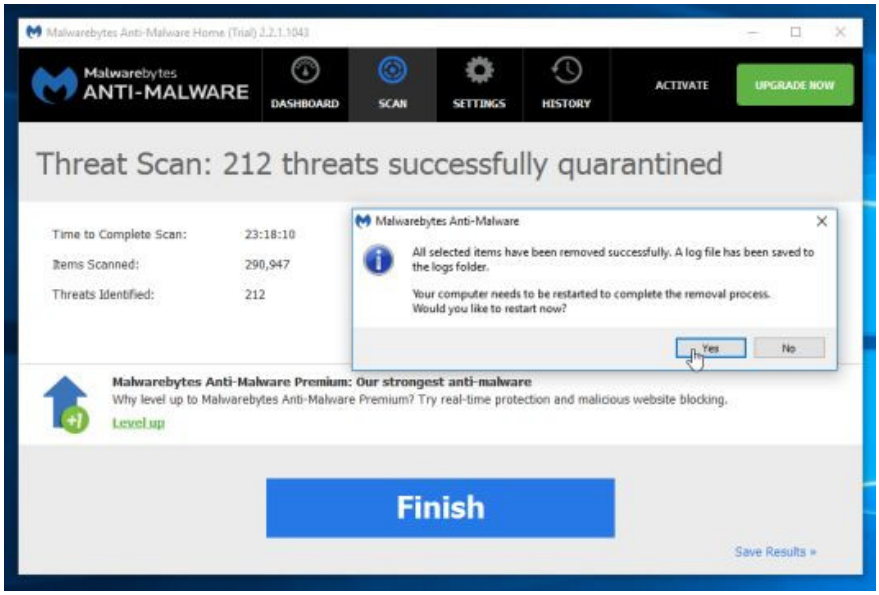
5. Malwarebytes Anti-Malware will start scanning your system to find and remove malware.



6. 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 Remove Selected button.



7. 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.



Step 3: Use HitmanPro to scan and test the system

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.

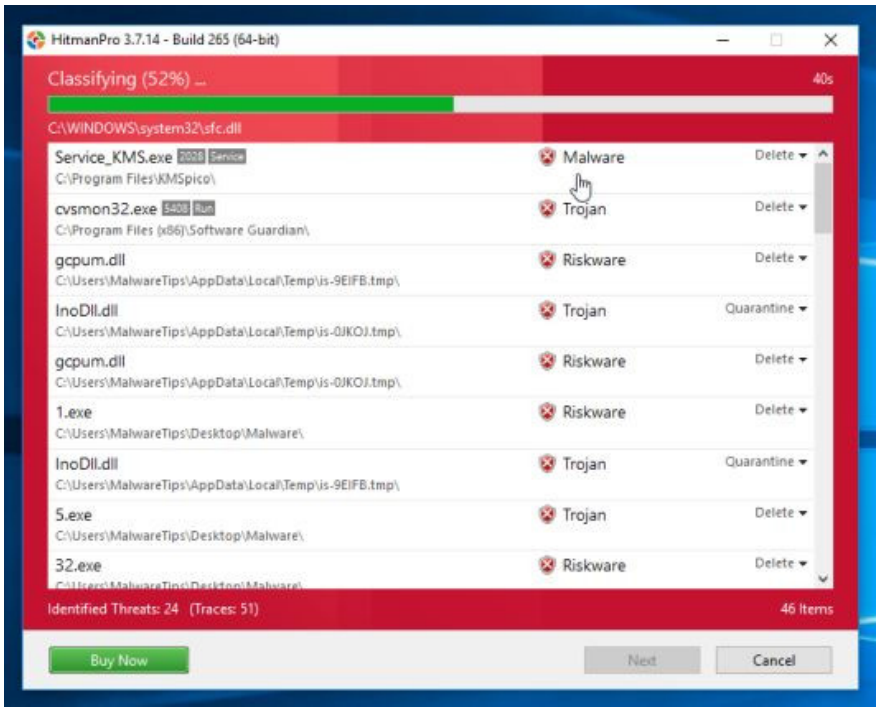
1. Download HitmanPro to your device and install it.

Download HitmanPro to your device and install it here.

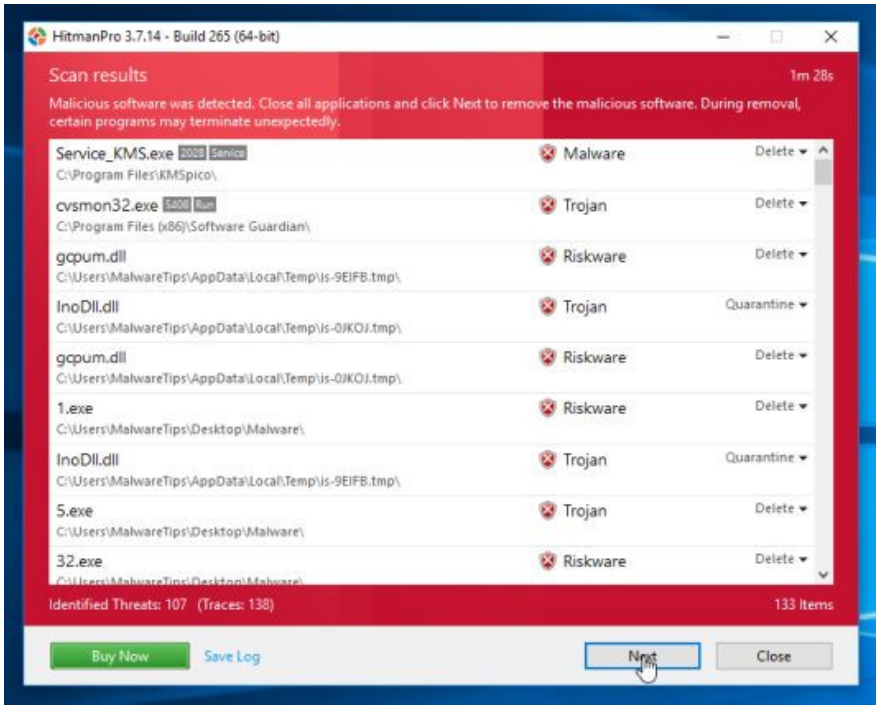
2. Double-click the file named ' *HitmanPro.exe* ' (if using a 32-bit version) or double-click the file ' *HitmanPro_x64.exe* ' (if using a 64-bit version).

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

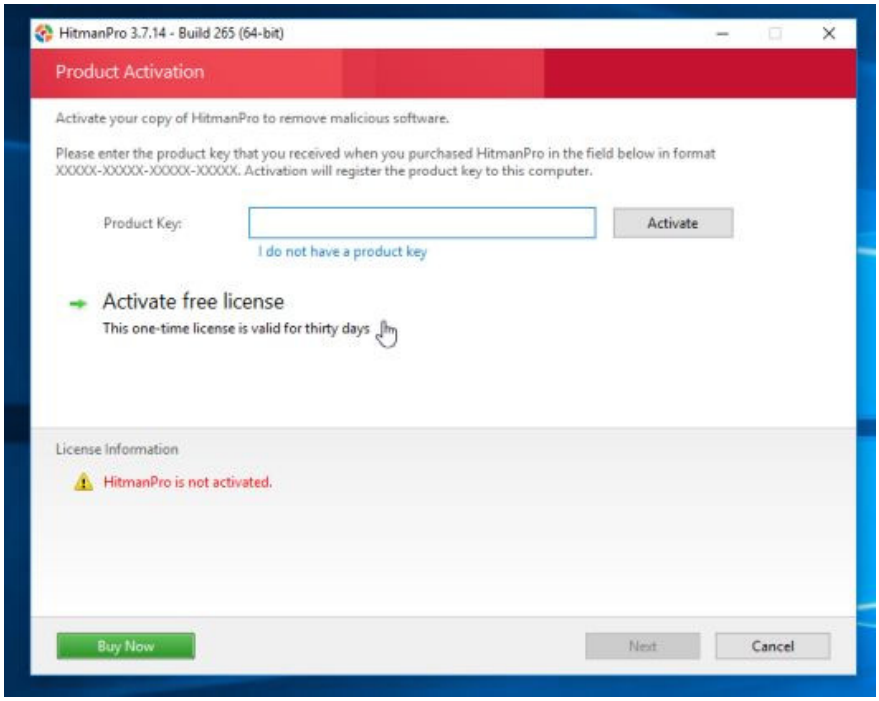
3. And HitmanPro will start the process of scanning **malicious programs** (malware) on your system.



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



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



Step 4: Use Zemana AntiMalware to scan the system

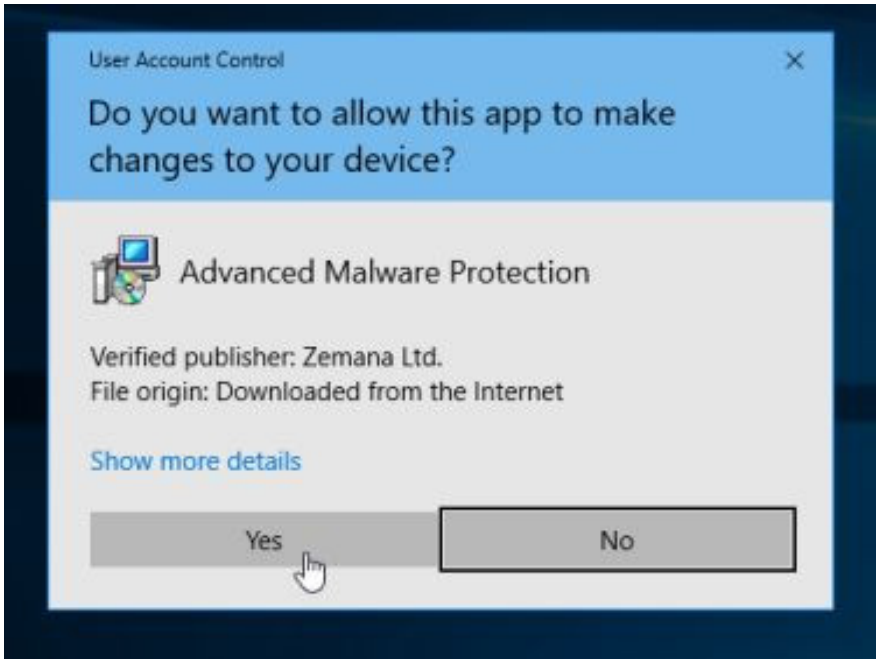
Use Zemana AntiMalware to remove the Youndoo.com extension on your browser and other malicious programs on your computer.

1. Download Zemana AntiMalware to your device and install it.

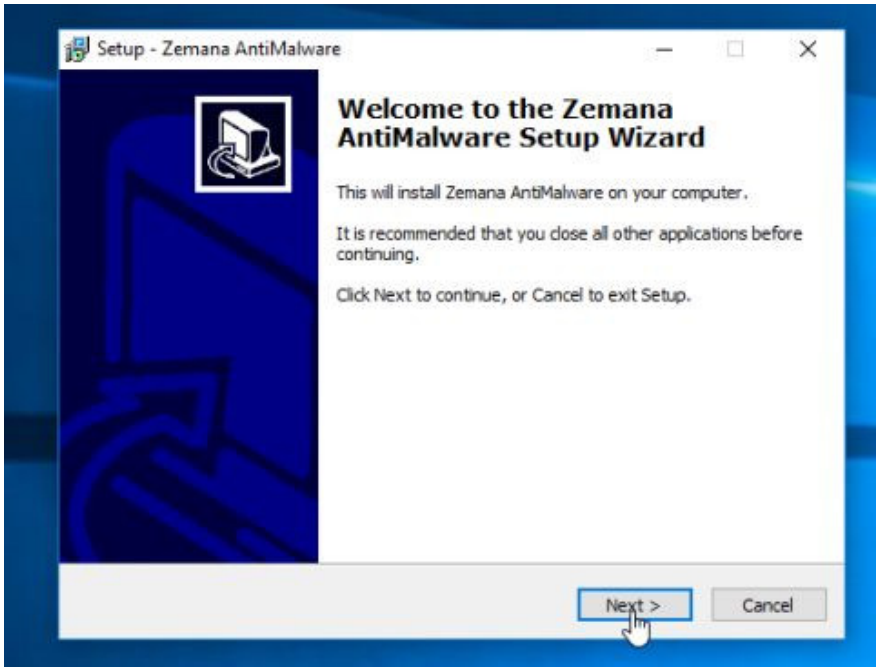
Download Zemana AntiMalware and install it here.

2. Double-click the file named **'Zemana.AntiMalware.Setup.exe'** to install Zemana AntiMalware on your computer.

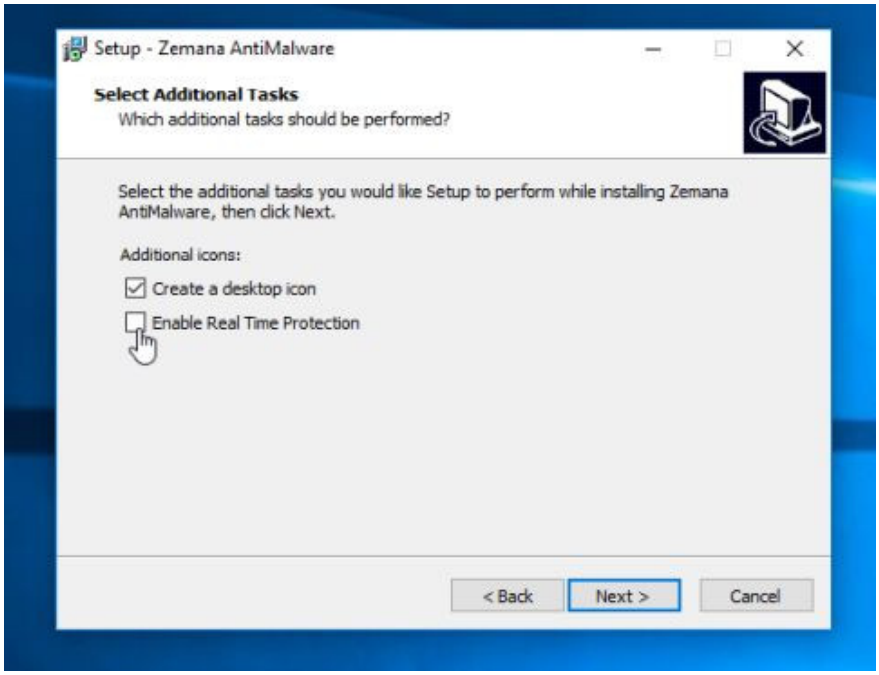
The **User Account Control** dialog box appears now on the screen asking if you want to run the file. Click **Yes** to continue the installation process.



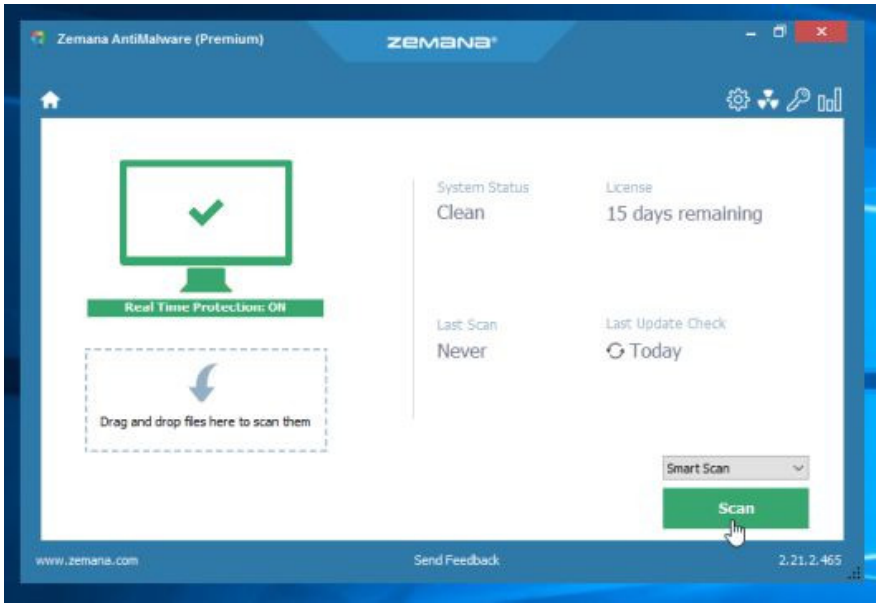
3. Click **Next** and follow the on-screen instructions to install Zemana AntiMalware on your computer.



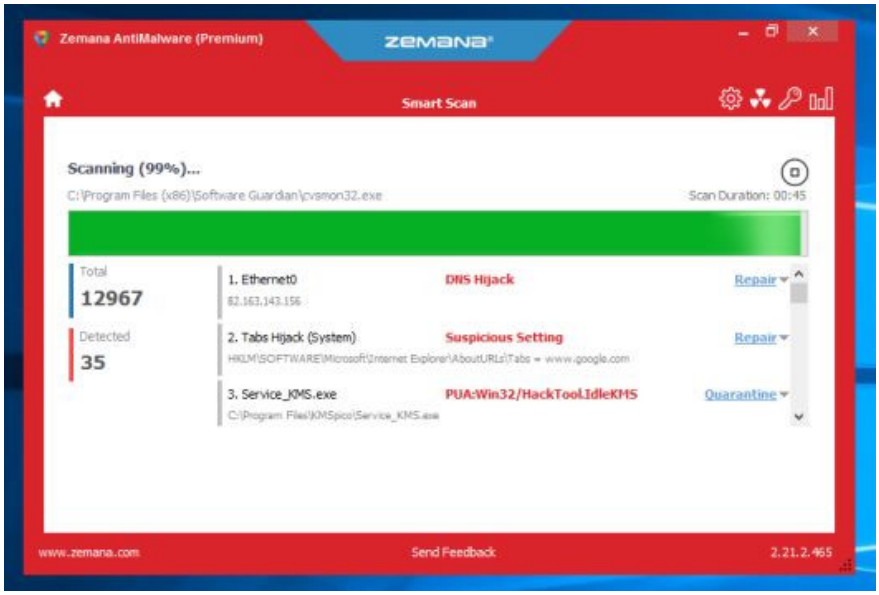
Go to the Select Additional Task window, you can uncheck the **Enable Real Time Protection** option and click Next.



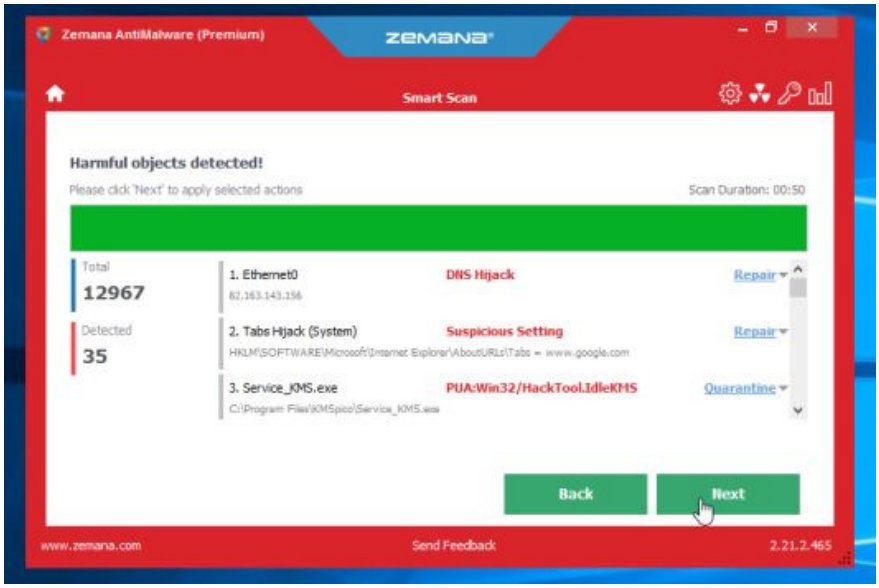
4. When the Zemana AntiMalware window opens, click **the Scan button** .



5. Zemana AntiMalware will start scanning your computer for malicious files. Scanning may take up to 10 minutes.



6. At the end of the scanning process, Zemana AntiMalware will display a list of all detected malicious programs. Click **the Next button** to remove all malicious files from your computer.



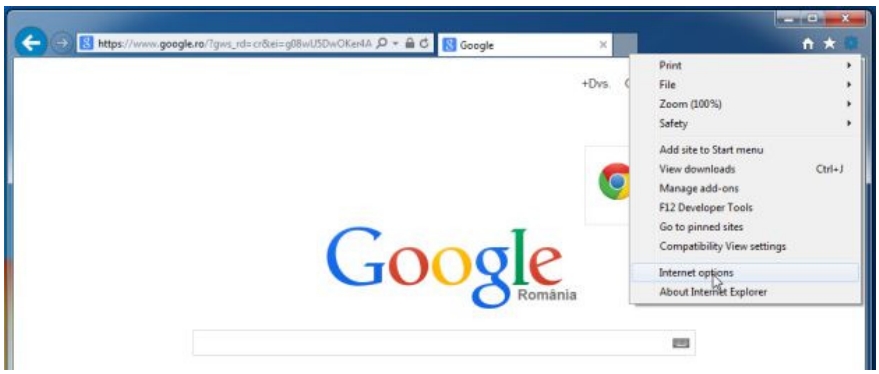
Zemana AntiMalware will remove all malicious files from your computer and will require the system to reboot to remove all malicious programs.

Step 5: Reset your browser to the default setting state

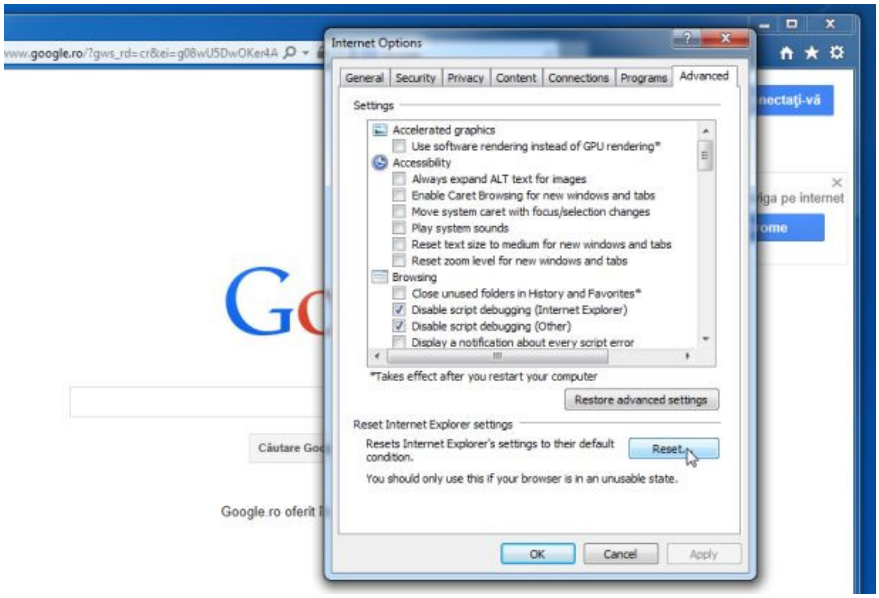
- On Internet Explorer:

To reset Internet Explorer to the default setting, follow the steps below:

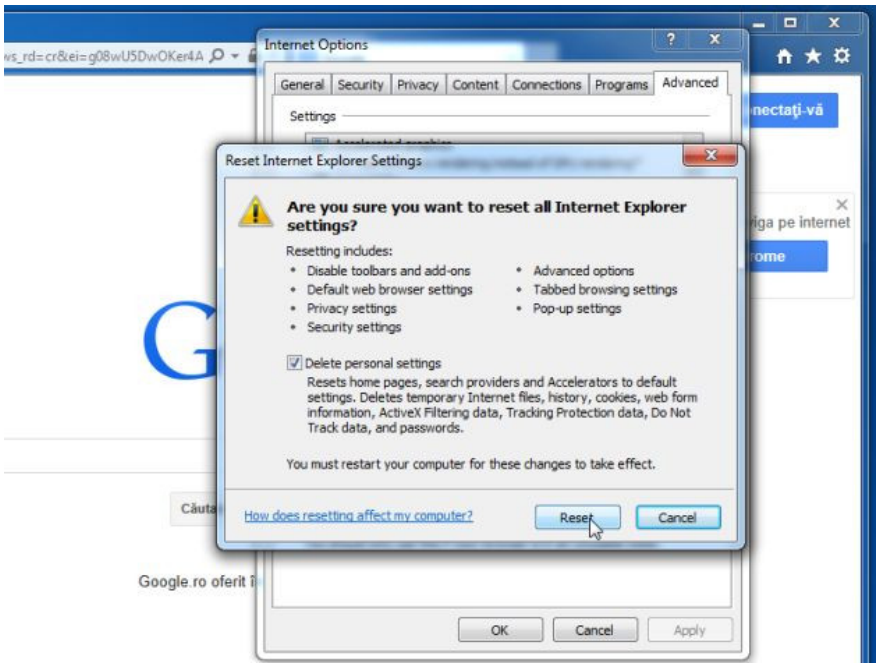
1. Open Internet Explorer, then click the jagged icon in the top right corner of the screen, select Internet Options.



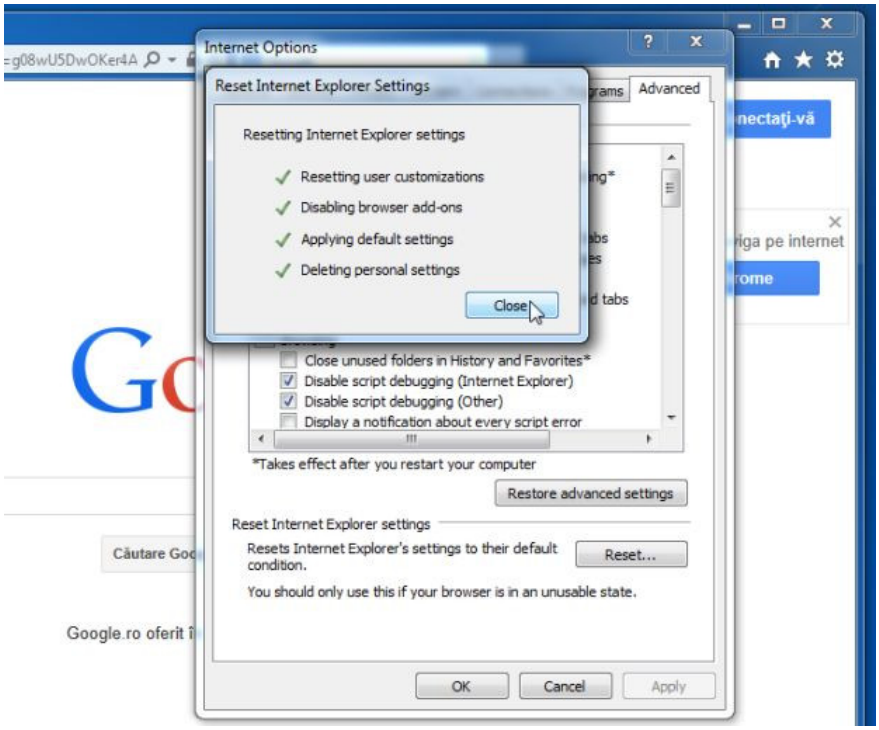
2. At this time, the **Internet Options** window will appear, where you click the **Advanced tab** , then click **Reset** .



3. On the **'Reset Internet Explorer settings' window** , select **'Delete personal settings'** and click the **Reset** button **.**

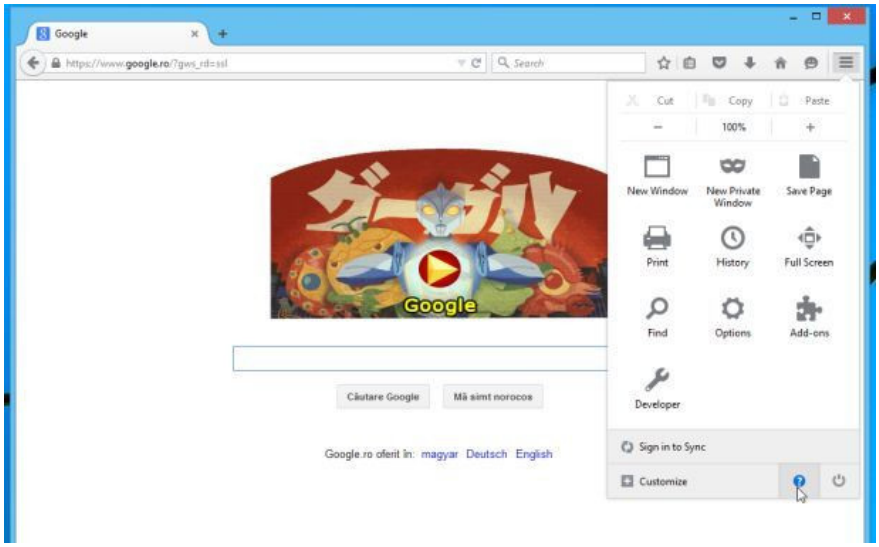


4. After the reset process finishes, click the Close button to close the confirmation dialog window. Finally restart your Internet Explorer again.



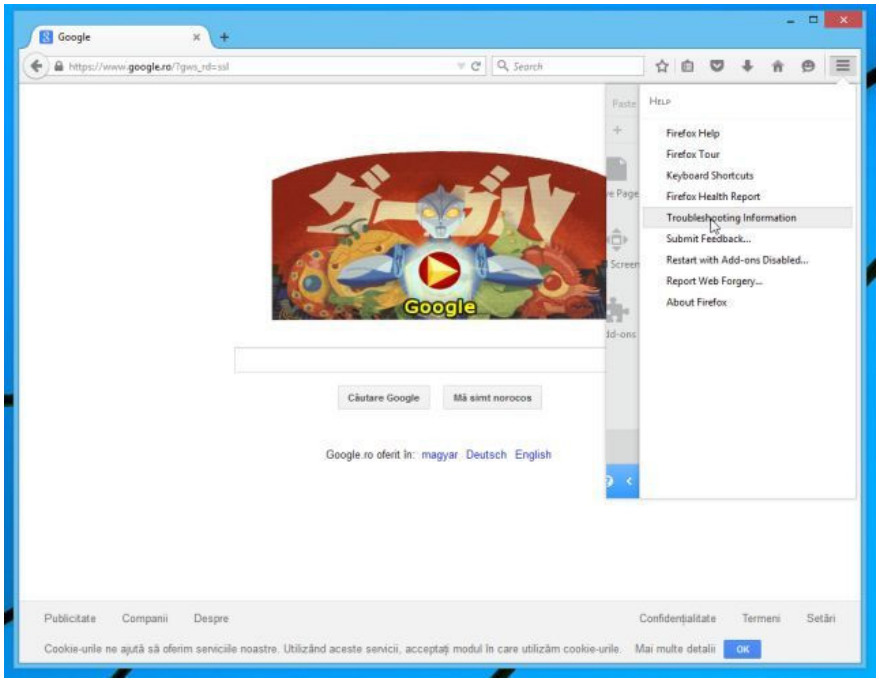
- On Firefox browser:

1. Click the 3 dash line icon in the top right corner of the screen, then select **Help.**

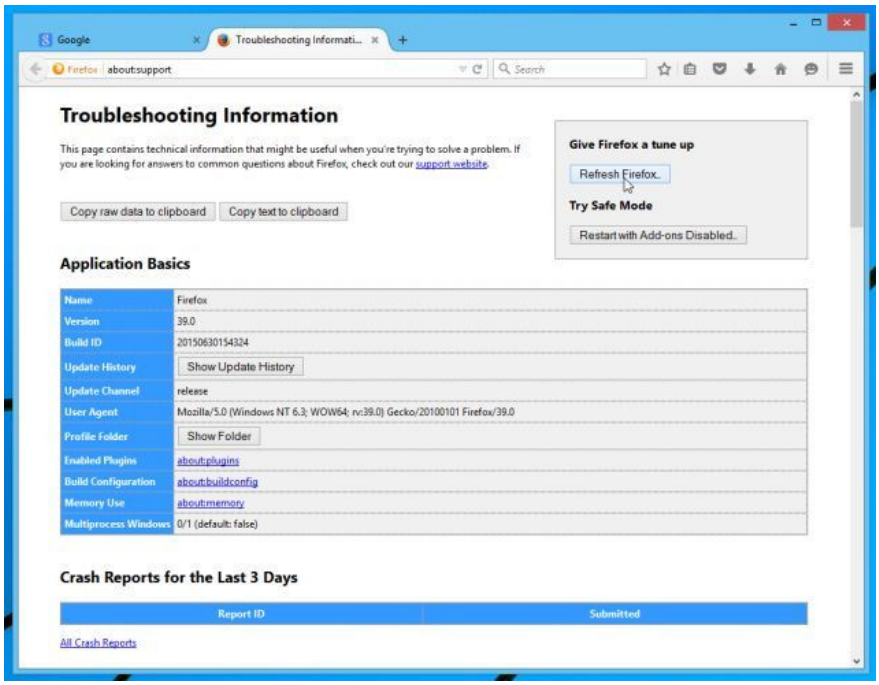


2. On the Help Menu, click Troubleshooting Information.

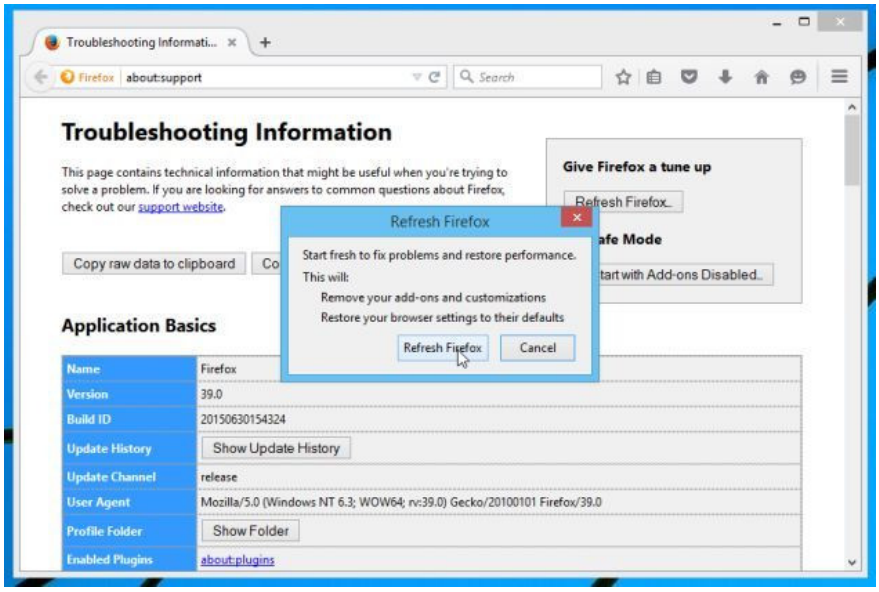
If you cannot access the Help menu, enter **about: support** in the address bar to open the Troubleshooting information page.



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



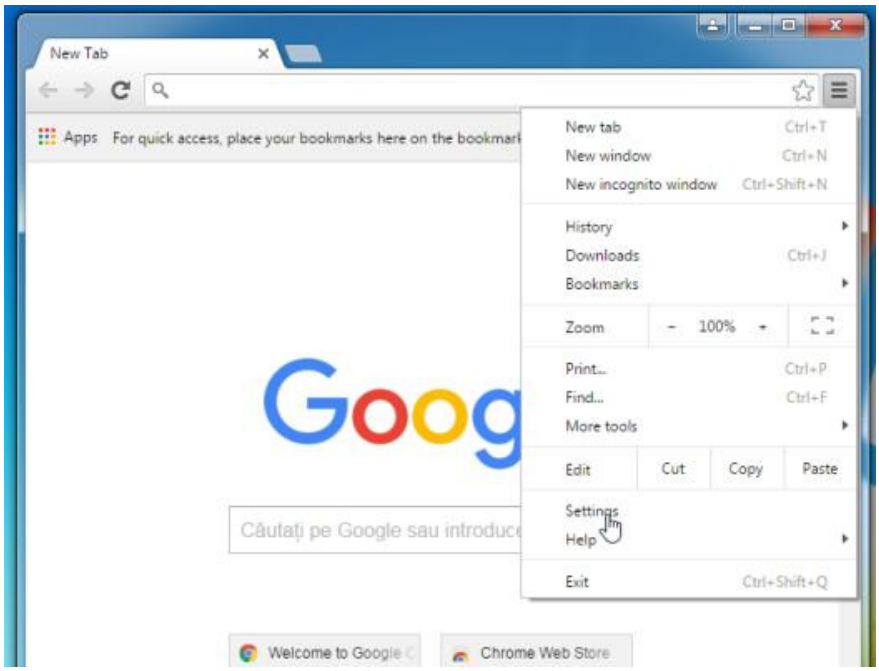
4. Continue to click the **Refresh** button **Firefox** on the confirmation window.



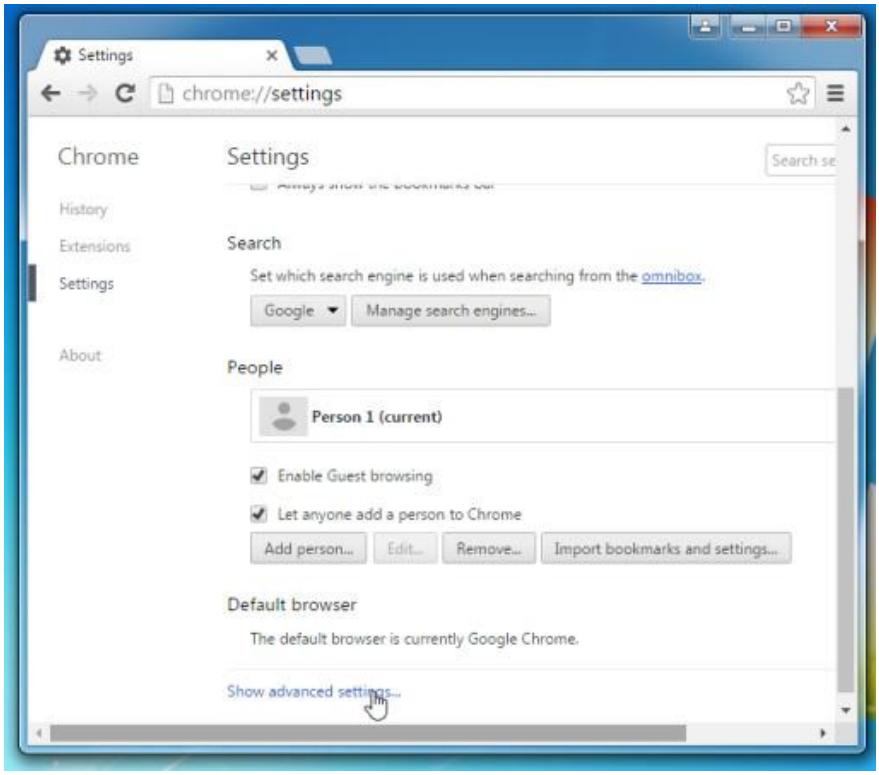
5. Firefox will automatically close the window and return to the original default installation state. Once completed, a window displaying the information will appear. Click **Finish.**

- On Chrome browser:

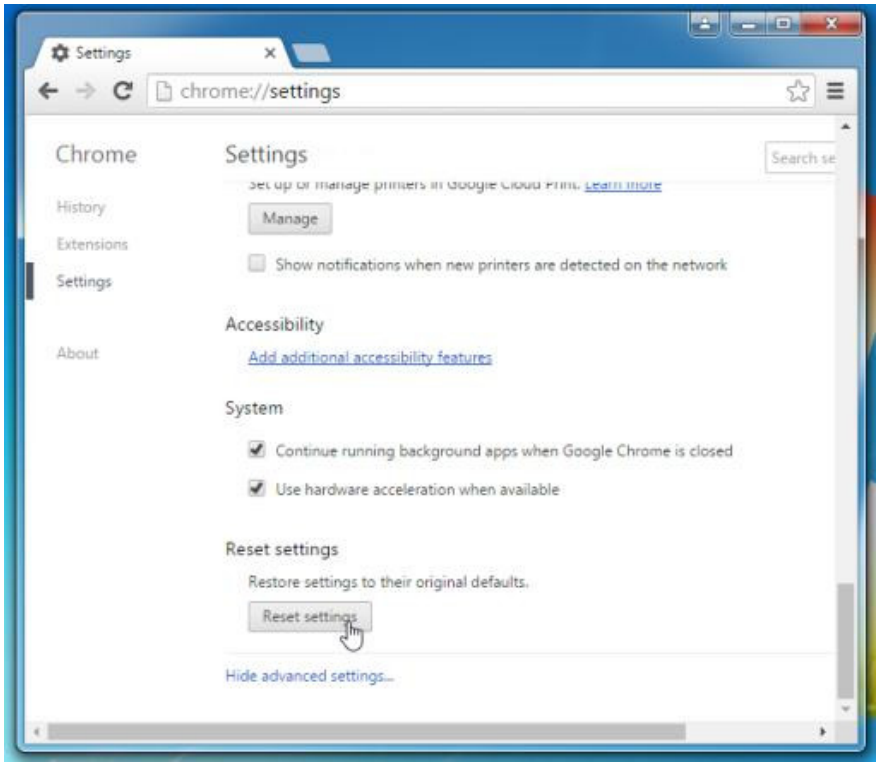
1. Click on the 3 dash line icon in the top corner of the screen, select **Settings** .



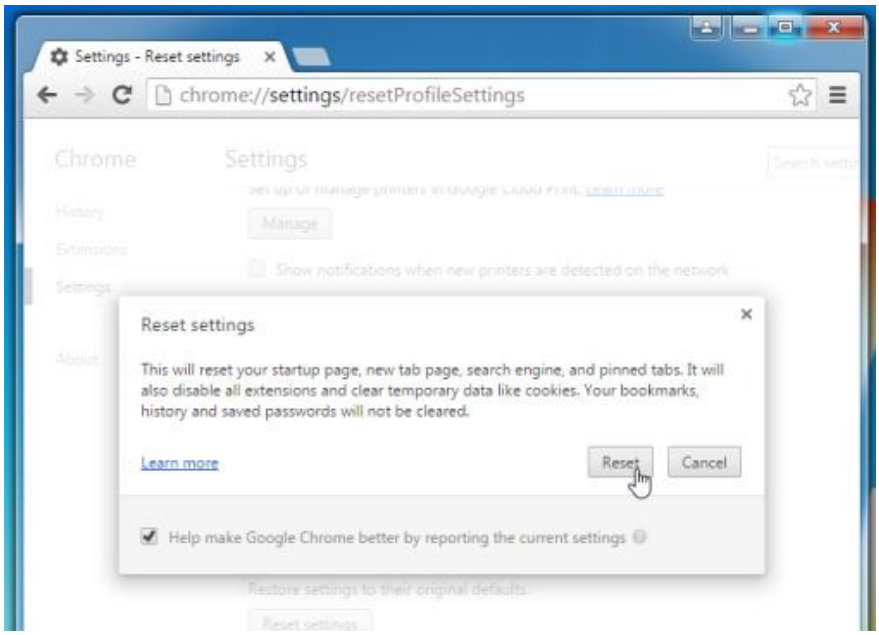
2. Now on the screen appears the Settings window, here you scroll down to find and click **Show advanced settings** (show **advanced settings**).



3. On the screen, an advanced installation window of the Chrome browser will appear, here you scroll down to find **Reset browser settings** . Next click on **Reset browser** button.

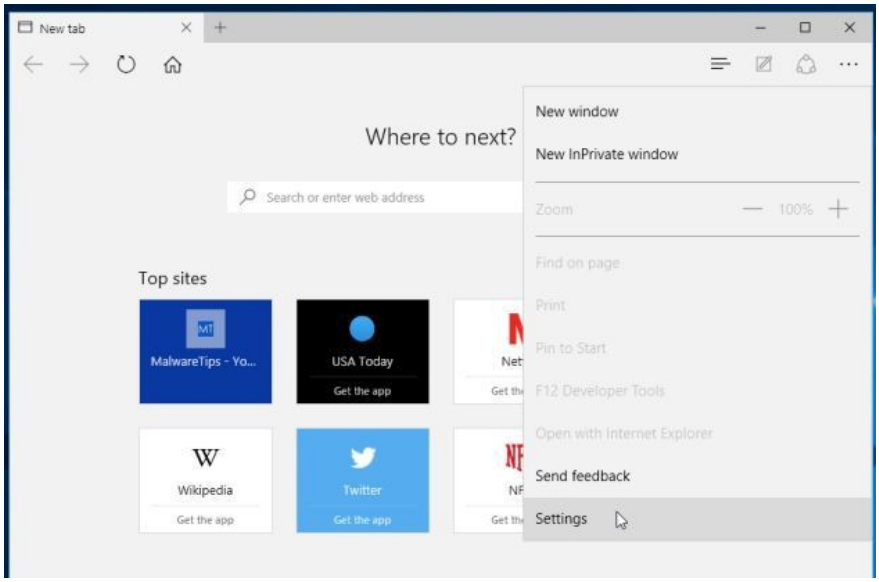


4. A confirmation window will appear on the screen, your task is to click the Reset button to confirm.

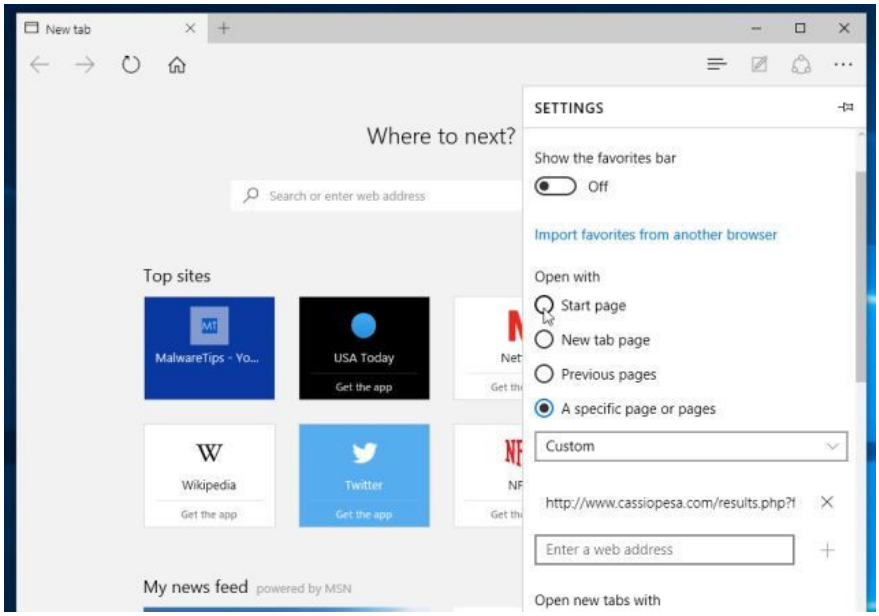


- On Microsoft Edge browser:

1. On Microsoft Edge browser, click on More actions icon (3 dots icon), then click **Settings** .



2. Next under **Open with** , select the **Start page** option.



Refer to some of the following articles:

1. When the network speed is slow, turn this feature off to browse the Web on browsers faster

1. Fix Err-Connection-Refused and Err_Connection_Closed errors on Chrome browser

1. Instructions to remove Social Search toolbar in Chrome, Firefox and Internet Explorer browsers

Good luck!

You finished reading the article "**Remove root malware (malware) on Windows 10 computers**" 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.
