

Here's how to remove Ask Toolbar and Ask. com Search off Chrome, IE and Firefox browsers

Ask Toolbar and search engine Ask.com are search engines integrated on browser extensions (add-on) Ask.com. Ask Toolbar. And it is considered that the attacker browser by Ask Toolbar & Ask.com modifies the browser search setting to 'search.ask.com' and the browser homepage to 'home.tb.ask.com'.

Ask Toolbar and Ask search tool.com are search engines integrated on browser extensions (add-on) Ask.com. Ask Toolbar. And it is considered the attacker browser by Ask Toolbar and Ask.com edit the browser search setting to 'search.ask.com' and browser homepage to 'home.tb.ask.com'.

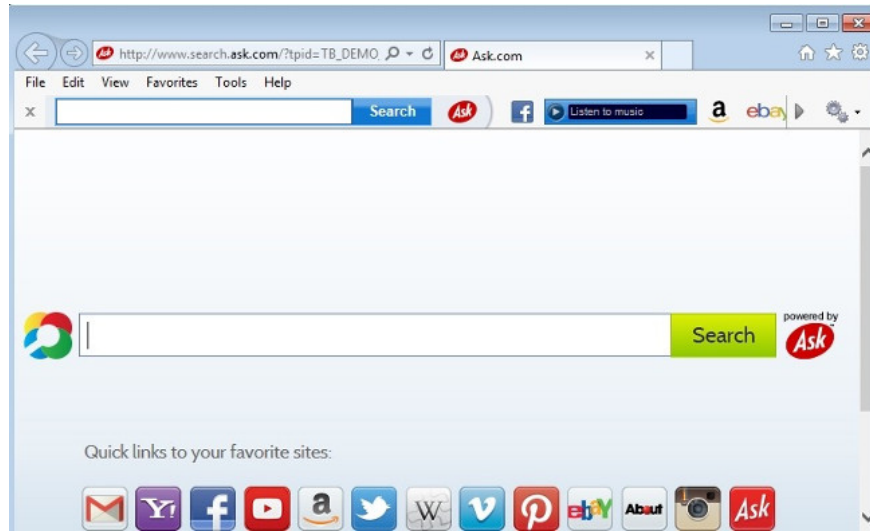
Ask toolbar is installed on the computer without user permission. Then the attacker of this browser will set up and use Ask as the default search engine.



1. What is "Ask Toolbar" and "Ask. Search"?

Ask Toolbar and Ask search tool. com are search engines integrated on browser extensions (add-on) Ask.com. Ask Toolbar. And it is considered the attacker browser by Ask Toolbar and Ask. com edit the browser search setting to 'search.ask.com' and the browser home page to 'home. tb. ask. com'.

For example, if you install JAVA or MINDSPARK, then the search engine and the Ask homepage. com will be installed by default while you install JAVA or MINDSPARK.



2. Why should I remove Ask toolbar?

Ask toolbar is installed on the computer without user permission. Then the attacker of this browser will set up and use Ask as the default search engine.

Often the browser attacker Ask toolbar is integrated on the software, free programs that users download on the network, then when installing the program, the software also accidentally installs according to Ask toolbar without not knowing.

If you want to remove the Ask toolbar installation from the root, follow the steps below.

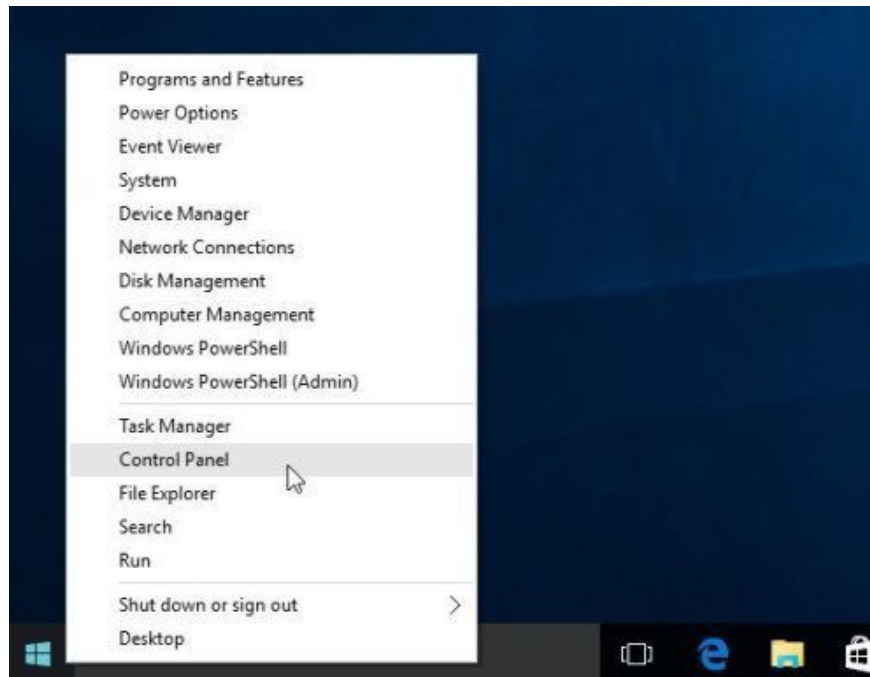
3. Remove Ask Toolbar and Ask.com Search from Chrome, IE and Firefox browsers

Step 1: Remove malicious programs on your Windows computer

1. Access the Uninstall menu.

- On Windows 10 and Windows 8:

1. 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.



- On Windows 7 and Windows Vista:

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



2. On the Control Panel window, find and select the option to ' *Uninstall a program* ' located in the Programs section.

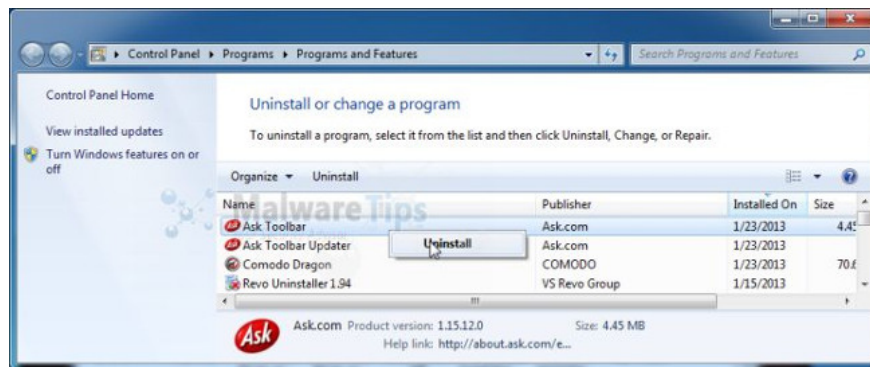


3. On the **Programs and Features** window, scroll down to the list of recently installed applications, programs, and uninstall malicious programs from your computer.

Malicious programs such as Ask Toolbar, Ask Toolbar Updater, Ask Updater and any other programs developed by Ask, Spigot or Mindspark Interactive Network.

1. To see recently installed programs, click Installed On to arrange applications by date. Then roll down the list and uninstall unwanted programs.
2. If you have problems uninstalling the malicious programs, you can use Revo Uninstaller to completely remove unwanted programs on your computer.

Download Revo Uninstaller to your computer and install it here.



Step 2: Use Malwarebytes AdwCleaner to scan the system

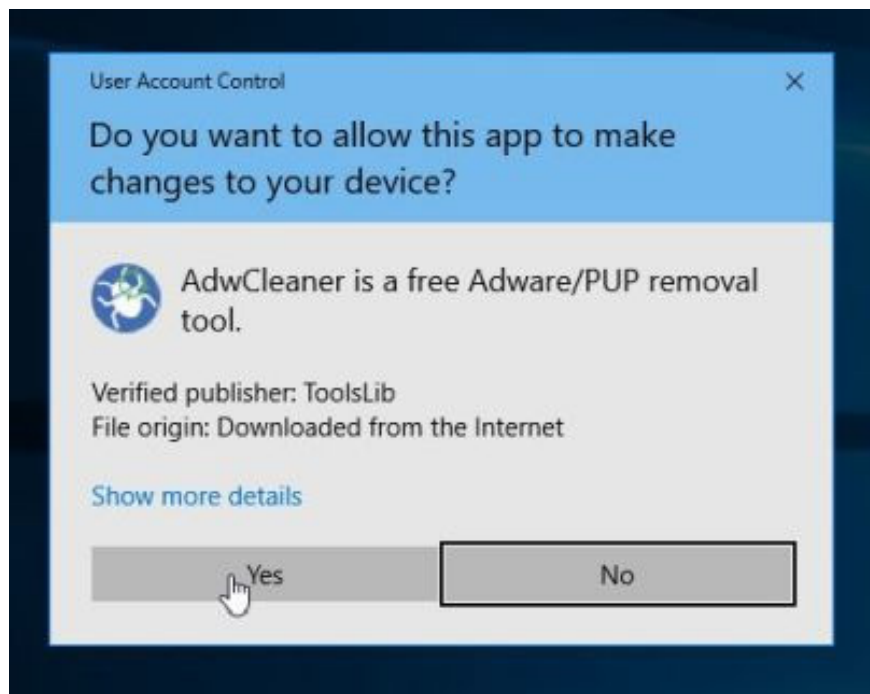
AdwCleaner is a free utility that will scan your system and web browsers to find and remove malware installed on your system.

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.

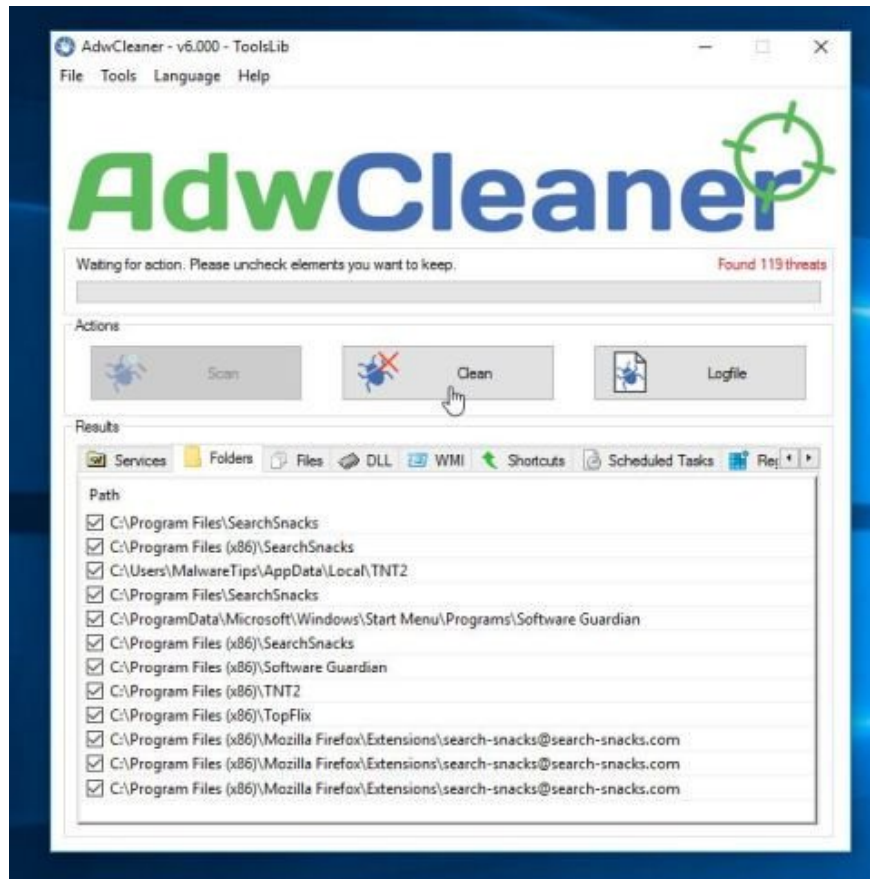


3. When the program has opened, click the **Scan** button as shown below:

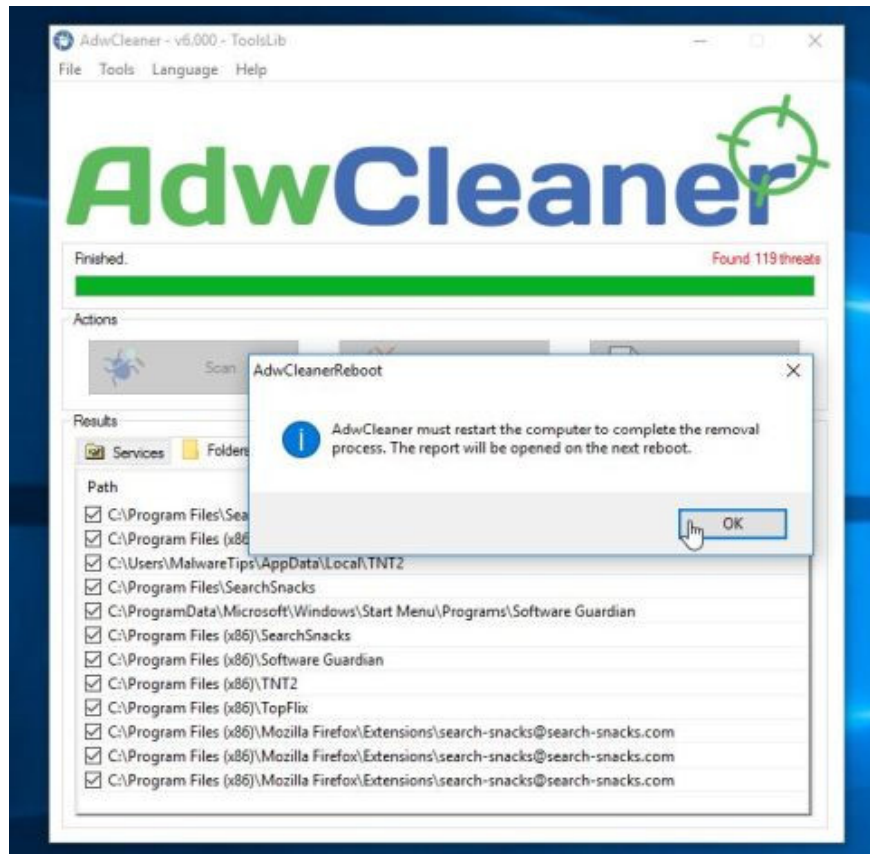


And AdwCleaner will start the scanning process to find and remove other malicious programs and software.

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 3: Use Malwarebytes Anti-Malware to scan the system again

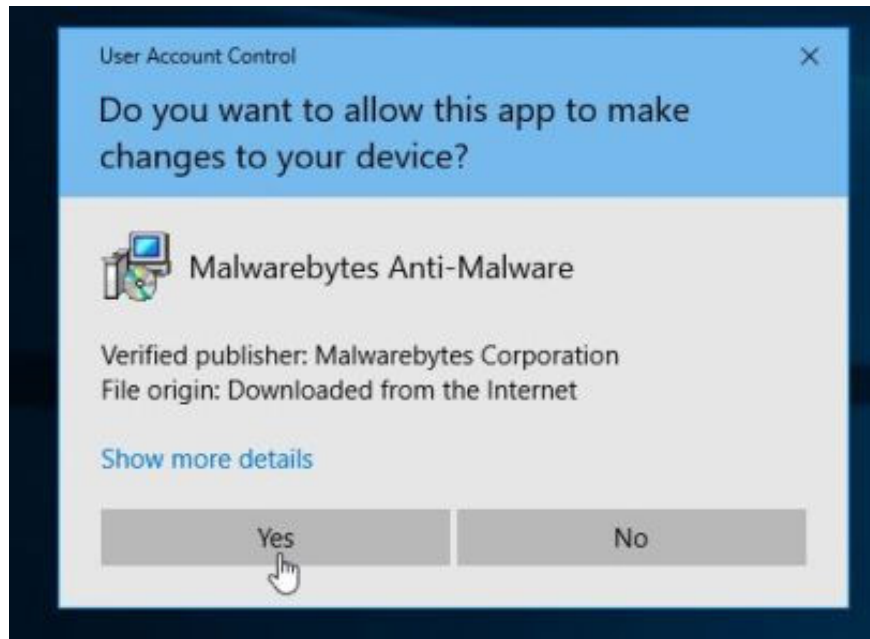
Malwarebytes Anti-Malware is the on-demand system scan tool that will remove all malware (malware), Ask Toolbar and Ask.com out of your Windows computer. The important thing is that Malwarebytes Anti-Malware will run in parallel with other antivirus software without conflict.

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

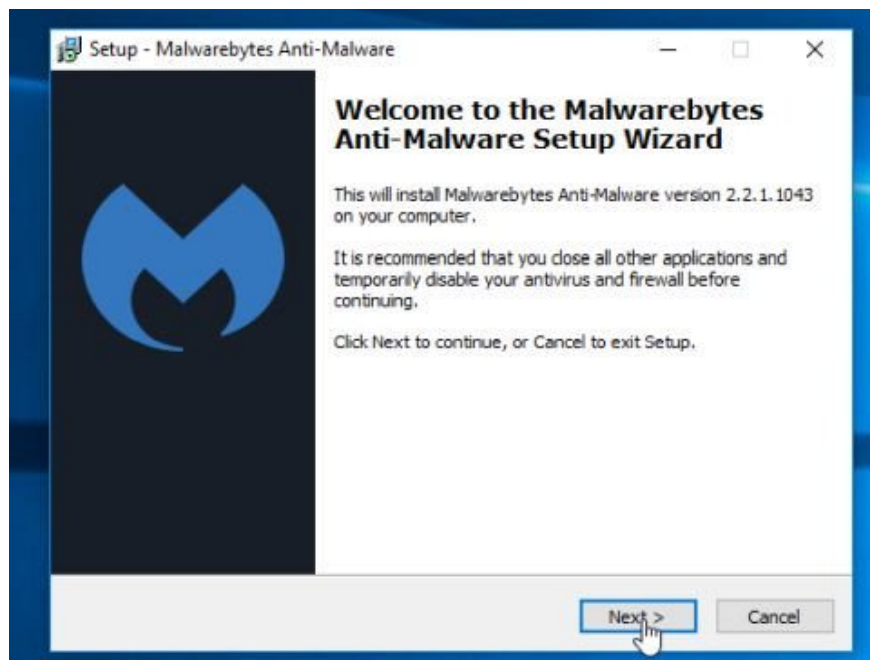
Download Malwarebytes Anti-Malware to your computer and install it here.

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.



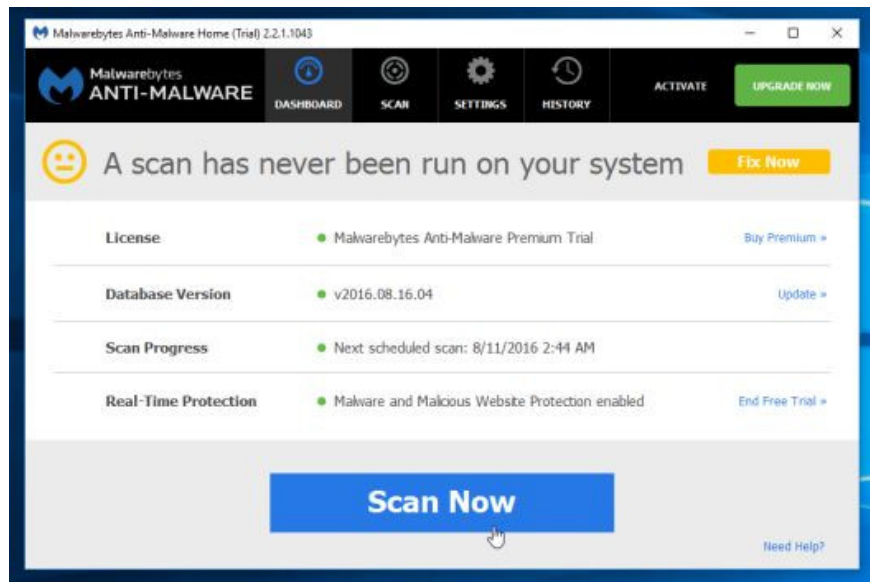
3. Follow the on-screen instructions to install Malwarebytes Anti-Malware Setup Wizard.



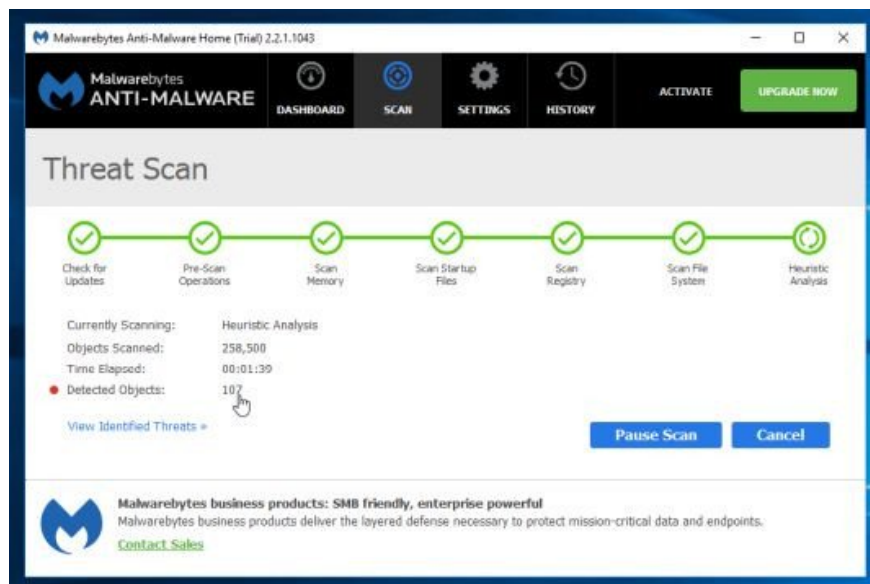
Click **Next** to install Malwarebytes Anti-Malware, until the last window click **Finish** to complete.



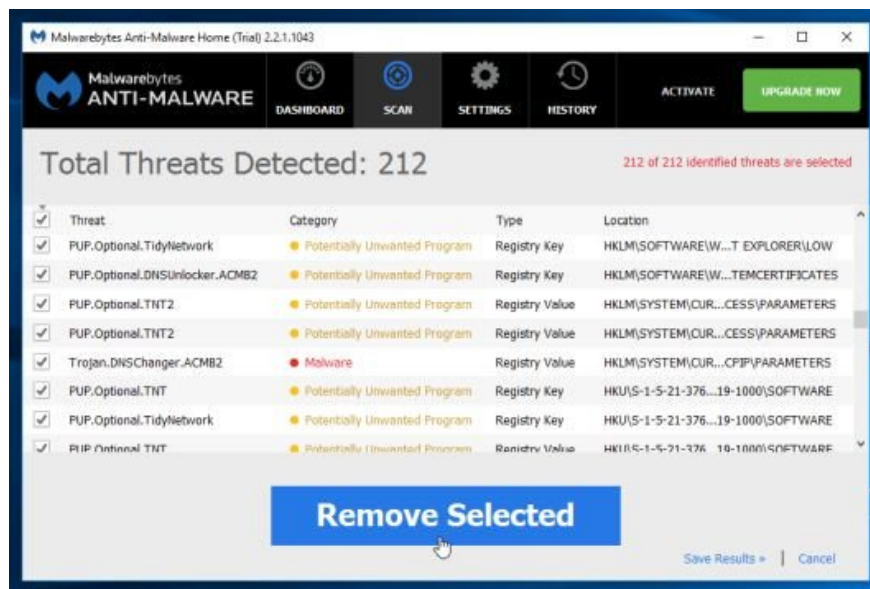
4. After installation is complete, Malwarebytes Anti-Malware will automatically open and **update** antivirus data. To start the scanning process, click the **Scan Now** button.



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 4: Check and 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.

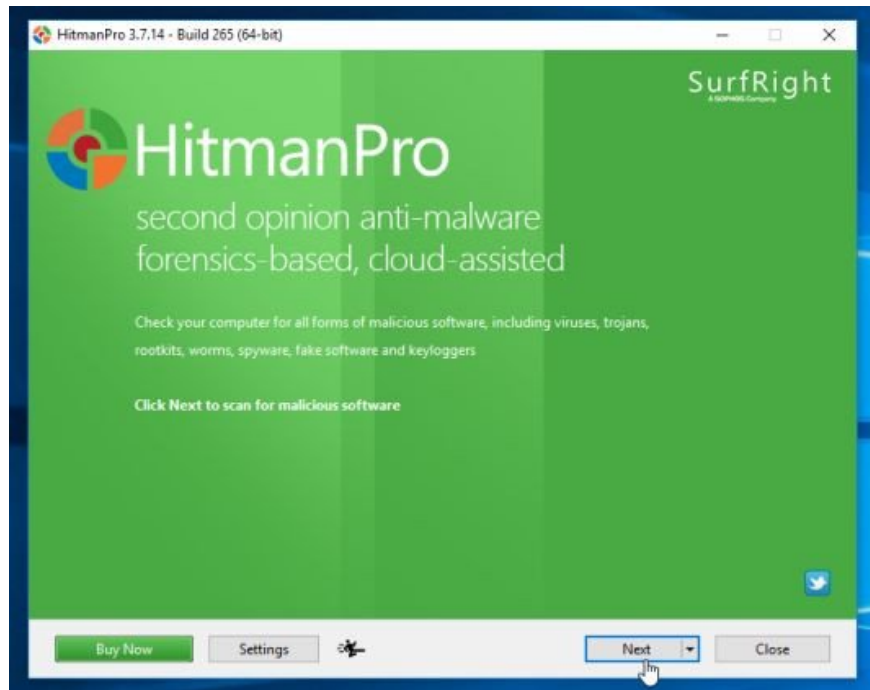
1. Download HitmanPro to your device and install it.

Download HitmanPro to your device and install it here.

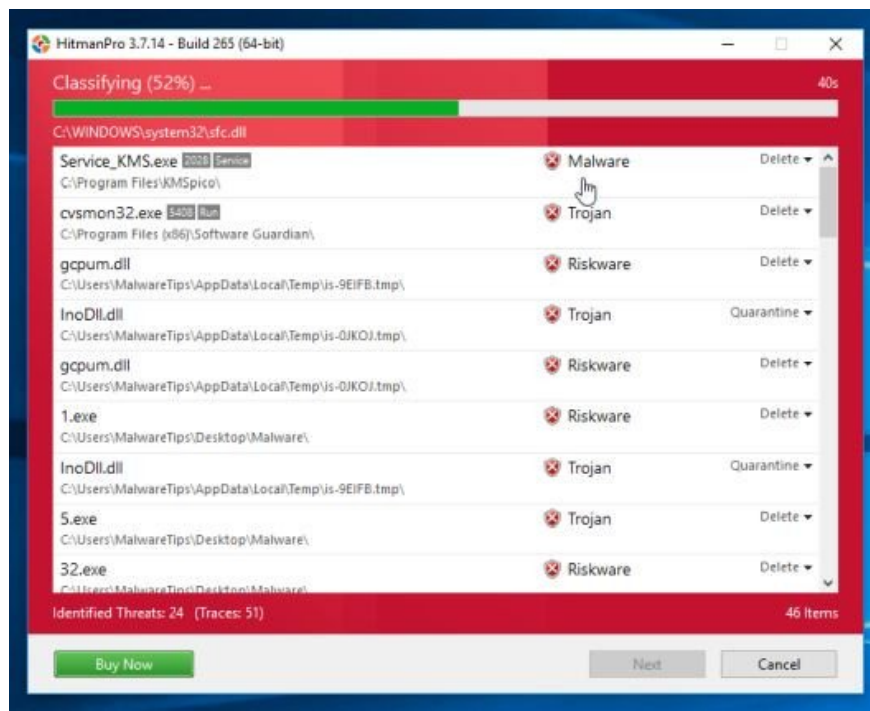
2. Double-click the file named ' *HitmanPro.exe* ' (if using a 32-bit version) or double-click the file ' *HitmanPro_x64.exe* ' (if using a 64-bit version).

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.

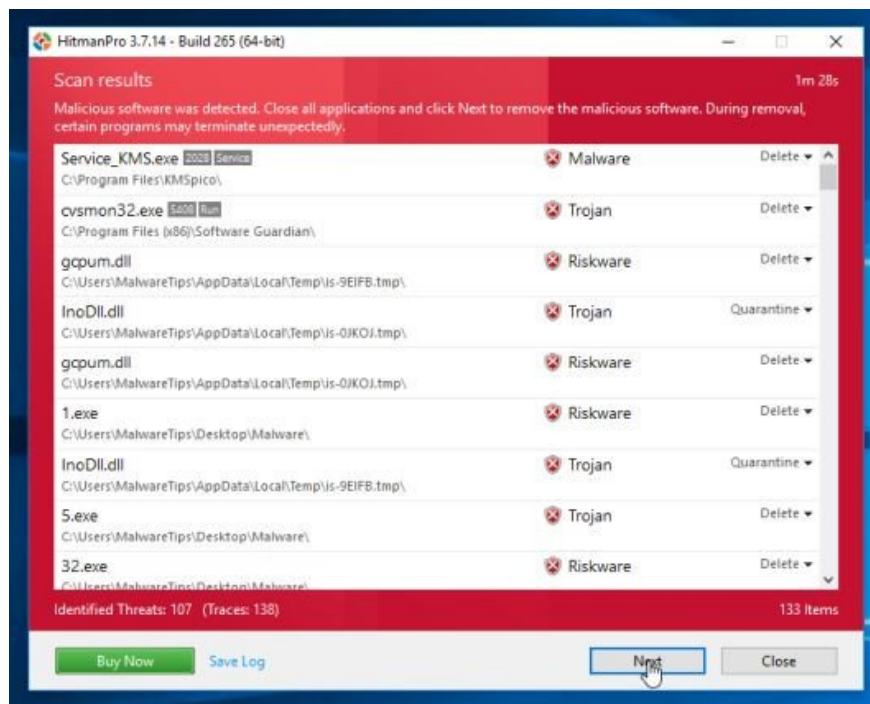
3. Click Next to install HitmanPro on your computer.



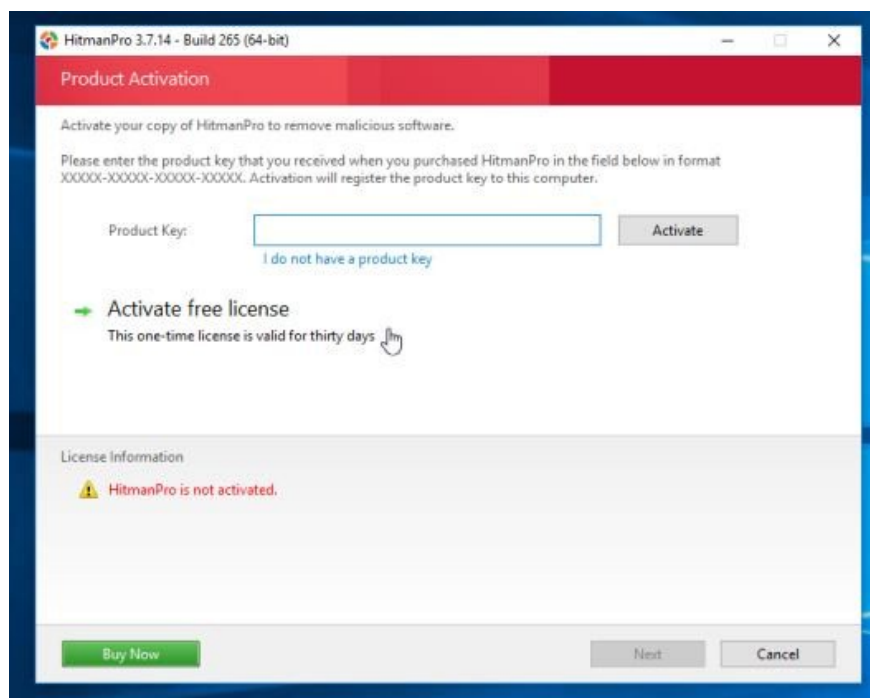
4. And HitmanPro will start the scanning process Malicious programs (malware) on your system.



5. 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.



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



Step 5: Use Zemana AntiMalware to scan the system

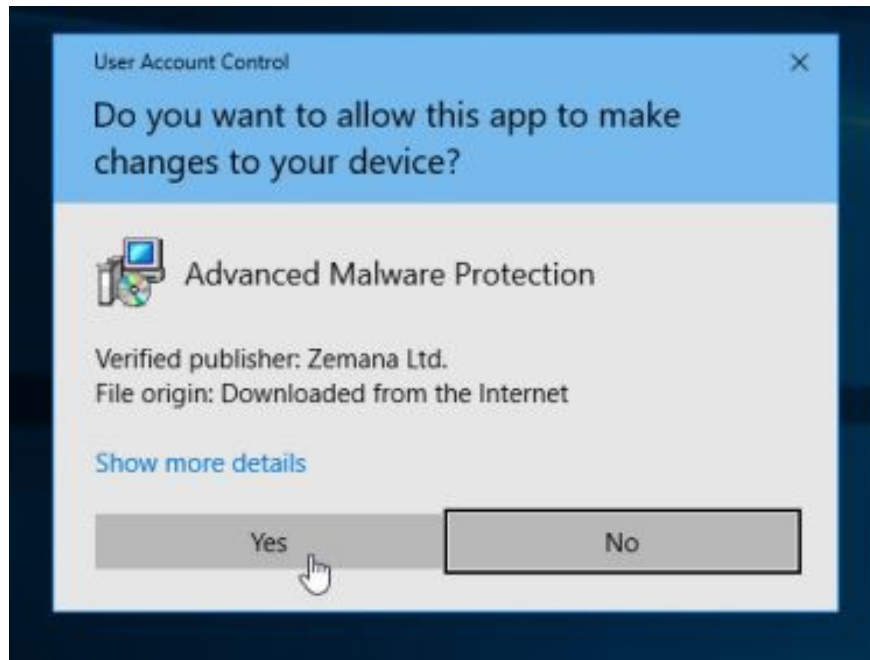
Use Zemana AntiMalware to scan and remove other malicious programs on your computer.

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.

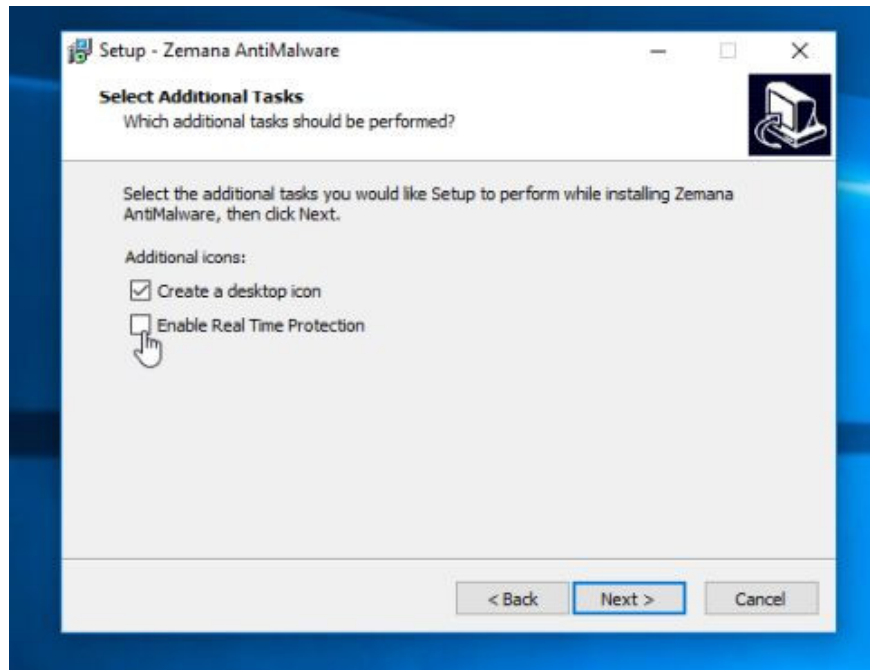
If the User Account Control window appears asking if you want to run the program. Click **Yes** to continue.



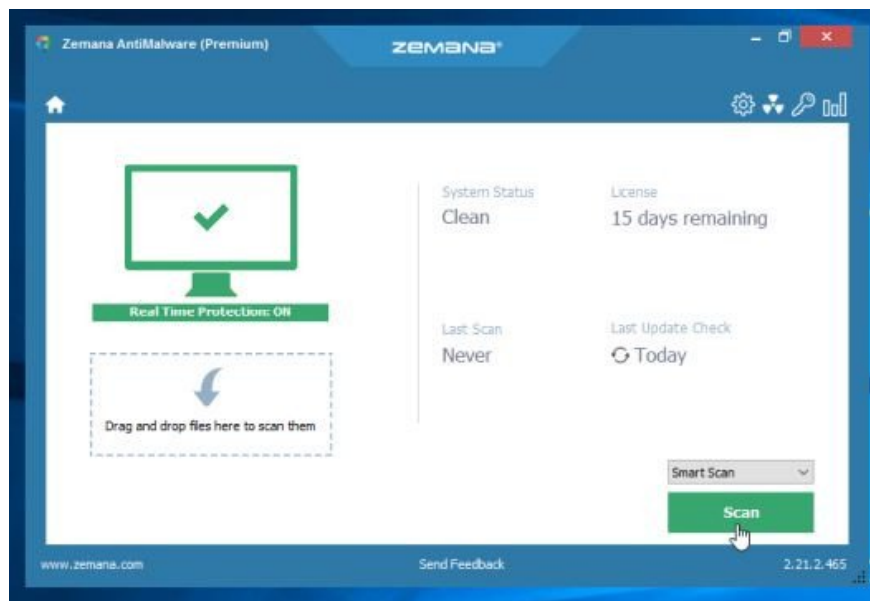
3. Click **Next** and follow the on-screen instructions to install Zemana AntiMalware on your computer.



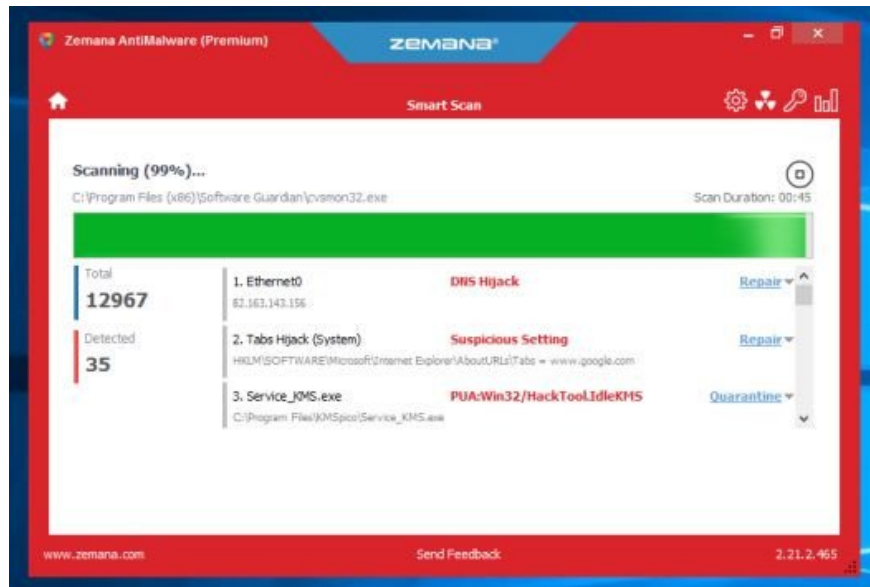
On the ' *Select Additional Tasks* ' screen, you can uncheck the ' *Enable Real Time Protection* ' option and then click Next.



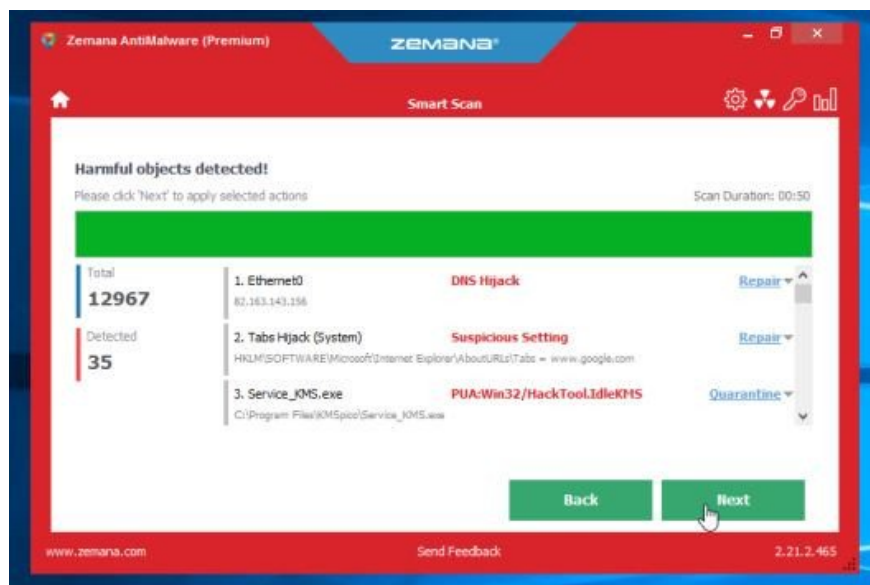
4. When the ZemaNA AntiMalware window opens, click the **Scan** button.



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 select **Next** button to remove all malicious files from your computer.

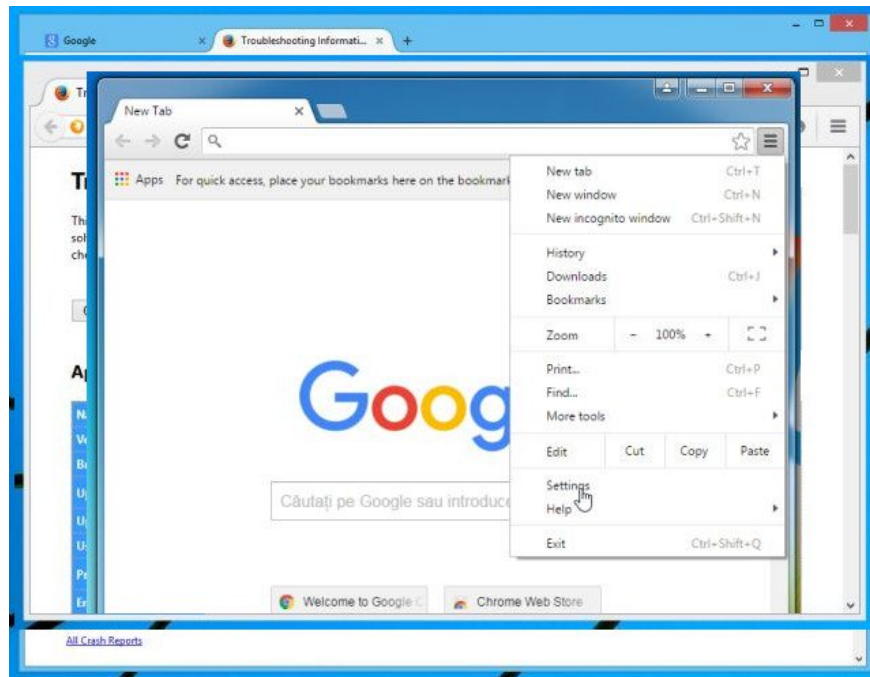


Zemana AntiMalware will remove all malicious files from your computer and will require the system to reboot to remove all malicious programs.

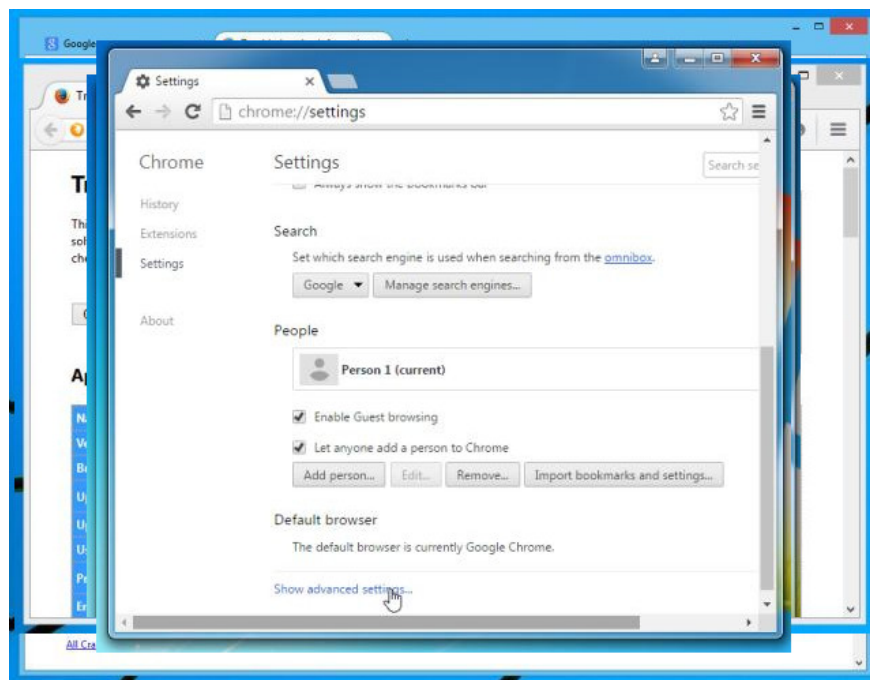
Step 6: Reset your browser to the default setting state

- On Chrome browser:

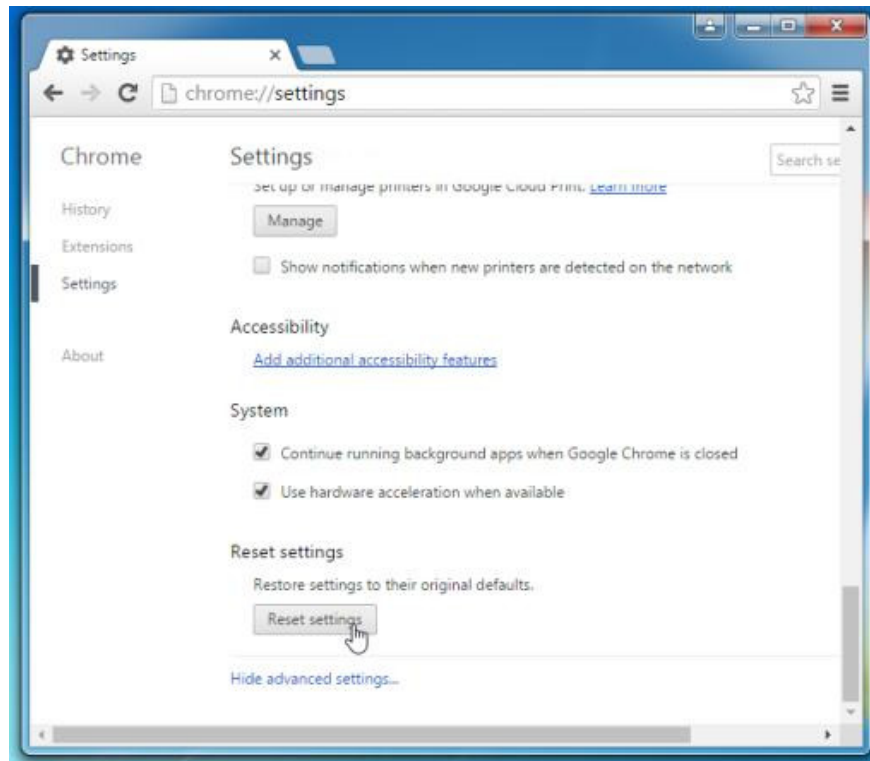
1. Click on the 3 dash line icon in the top corner of the screen, select **Settings** .



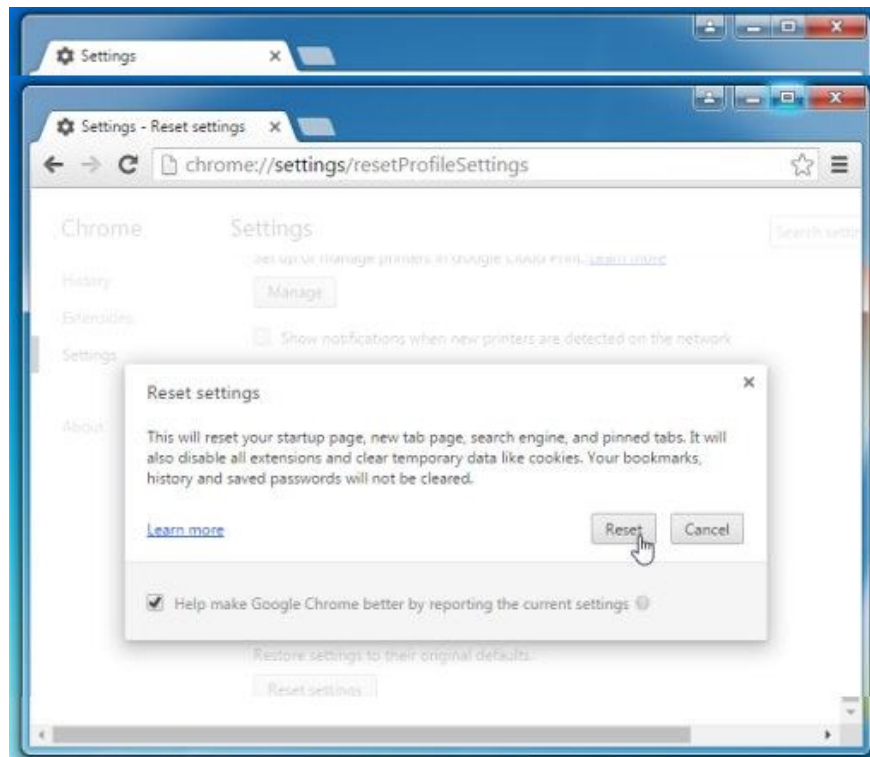
2. Now on the screen appears the Settings window, here you scroll down to find and click **Show advanced settings** (show advanced settings).



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.



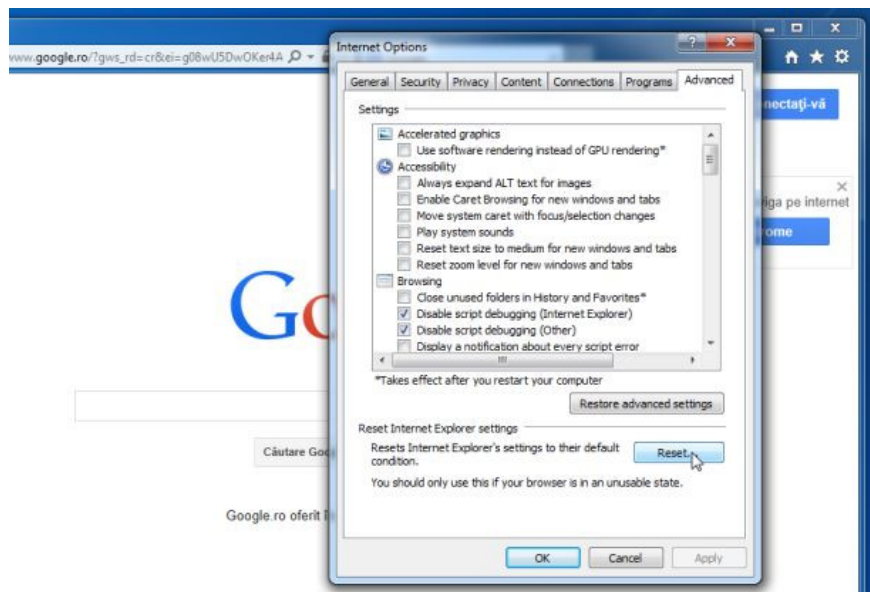
- On Internet Explorer:

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

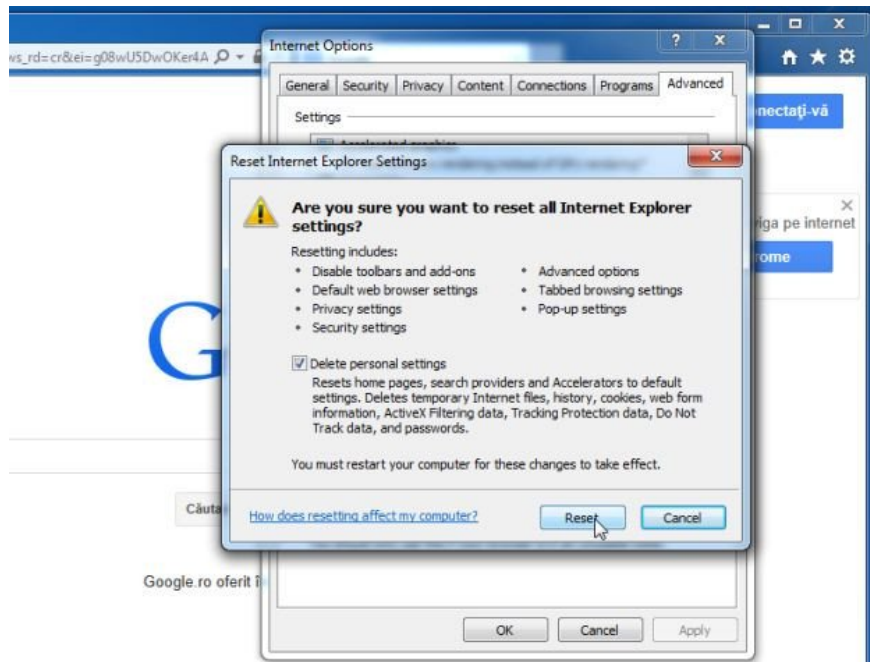
1. Open Internet Explorer, then click the jagged icon in the top right corner of the screen, select **Internet Options** .



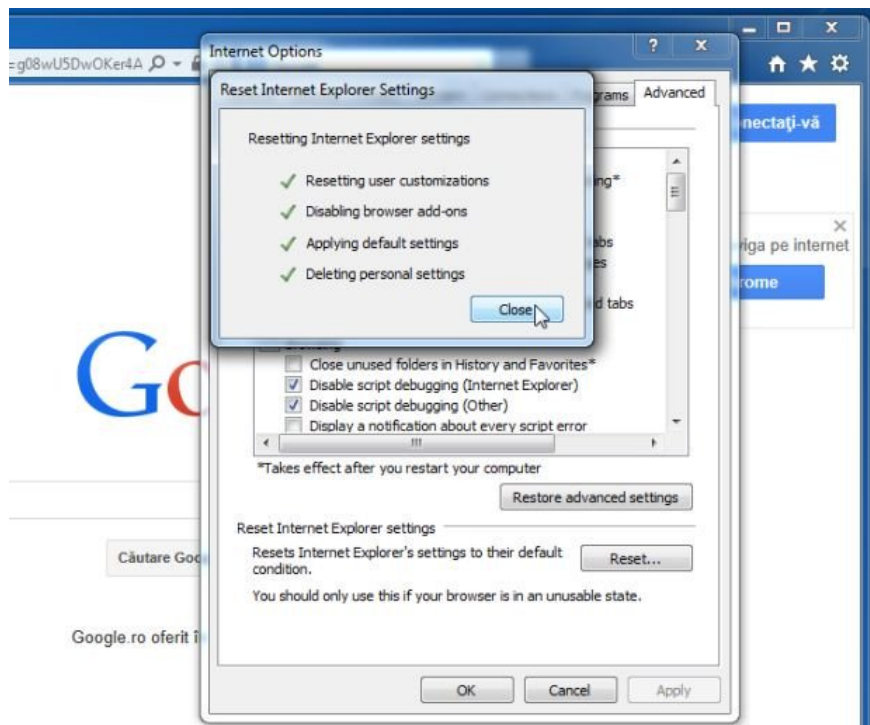
2. At this time, the **Internet Options** window will appear, where you click the **Advanced** tab , then click **Reset** .



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.



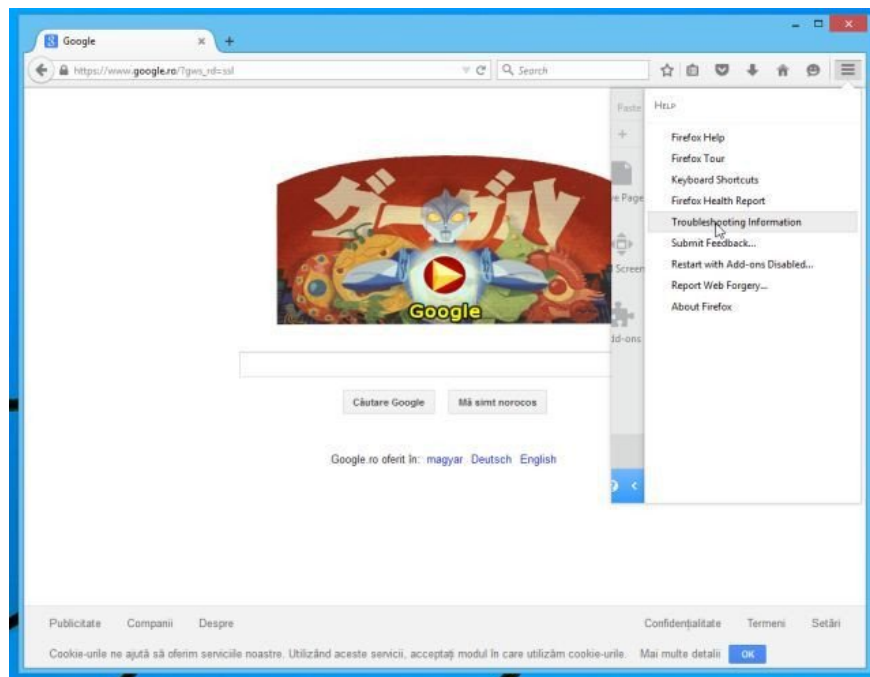
- **On Firefox browser:**

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

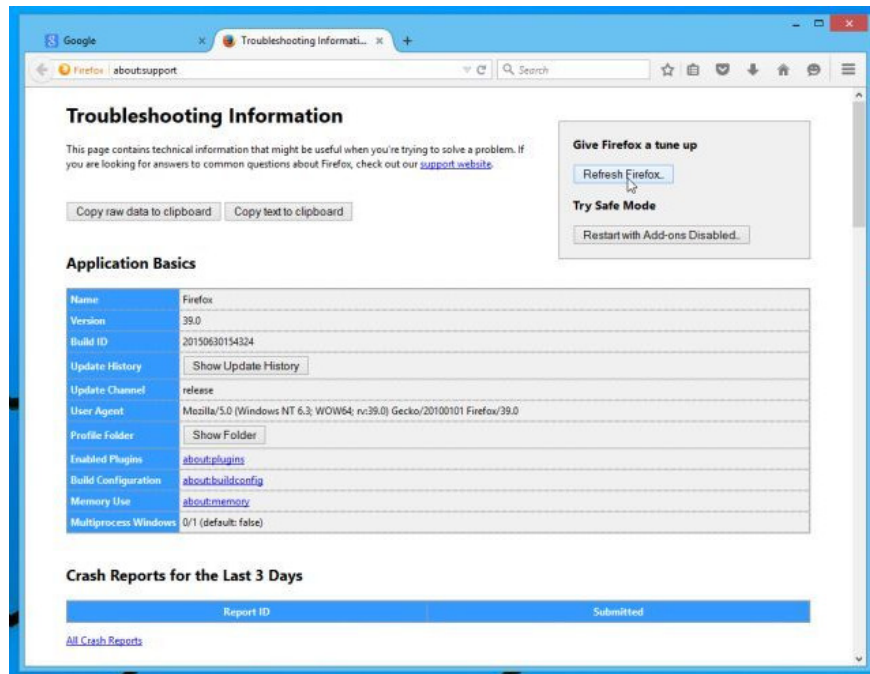


2. On the Help Menu, click Troubleshooting Information

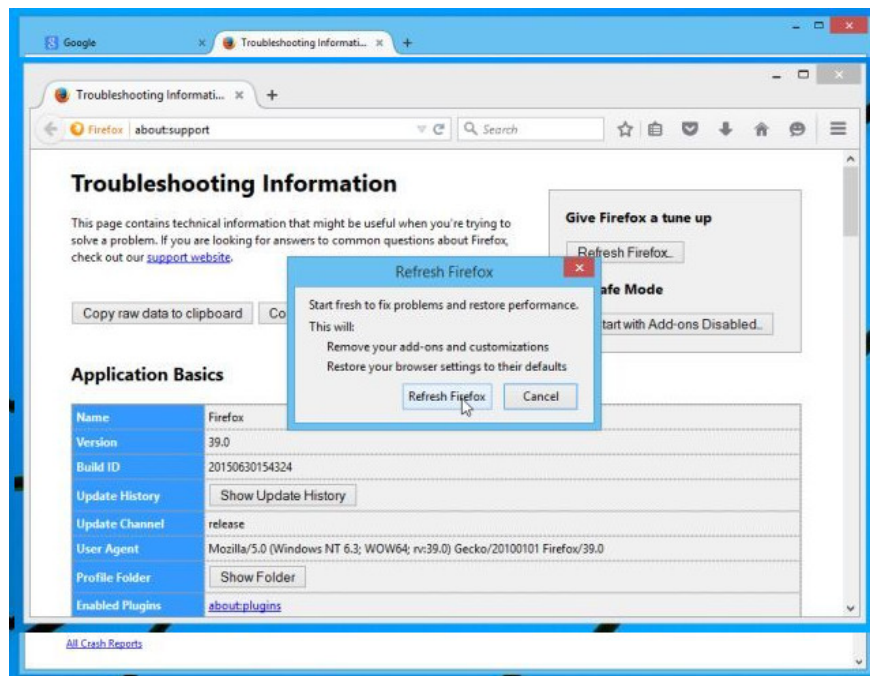
If you cannot access the Help menu, enter **about: support** in the address bar to open the Troubleshooting information page.



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**.

Refer to some of the following articles:

1. How to remove Trustedsurf.com on Chrome, Firefox and Internet Explorer
1. Rooted Delta Search on Chrome, Firefox and Explorer browsers

1. Want to load page speed on Edge browser faster, enable this feature

Good luck!

You finished reading the article "**Here's how to remove Ask Toolbar and Ask.com Search off Chrome, IE and Firefox 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.
