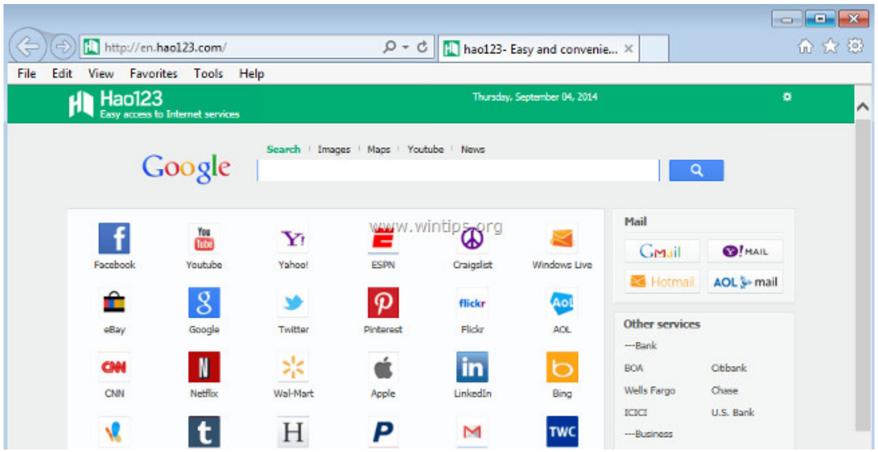
Steps to remove page Hao123. com

Hao123 is designed to edit your browser settings and can install some plugins (toolbar, extensions - extensions or add-ons) on your web browser to integrate more advertising links. . And the attacker of the browser can redirect users 'computers to malicious websites or can install' malicious 'programs to' compromise 'users' computers with security problems. security.

Hao123 is a browser hijacker, usually bundled with free software that you download from unreliable sources. When installed on Hao123 will set the default browser and search engine homepage to hao123.com without your permission. This is not harmful in itself, because many safety programs also change these settings. However, Hao123 has many suspicious behaviors, as well as arbitrarily adding the URL hao123.com parameter to the shortcut on Windows desktop and Start menu.



Hao123 is designed to edit your browser settings and can install some plugins (toolbar, extensions - extensions or add-ons) on your web browser to integrate more advertising links. . Hao123 can redirect users 'computers to malicious websites or may install' malicious 'programs to' compromise 'users' computers with security issues.

Hao123 has many different languages, depending on your location, such as' *en.hao123. com ', br.hao.123.com* ', ' *tw.hao.123.com* ', '' *ar.hao.123.com* ',' *sa.hao.123.com* ',' *id.hao.123.com* ',' *th.hao.123.com* ',' *jp.hao.123.com* ',' *ar.hao.123.com* ',' *ae.hao.123.com* 'or' *vn.hao.123.com* ''.

Technically, 'hao123. com 'is **not a virus** and it is classified as an unwanted program (PUP - Potentially Unwanted Program) that can contain and install malicious programs on your computer, such as adware (the adware), toolbars or viruses. If your computer is infected with adware 'hao123. com ', then on your computer screen will constantly appear popup windows, banners and sponsored links or in some cases the browsing speed of the browser is slow due to the chapters program running on background.

Hao123.com 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 it accidentally install hao123.com.

Therefore, 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.

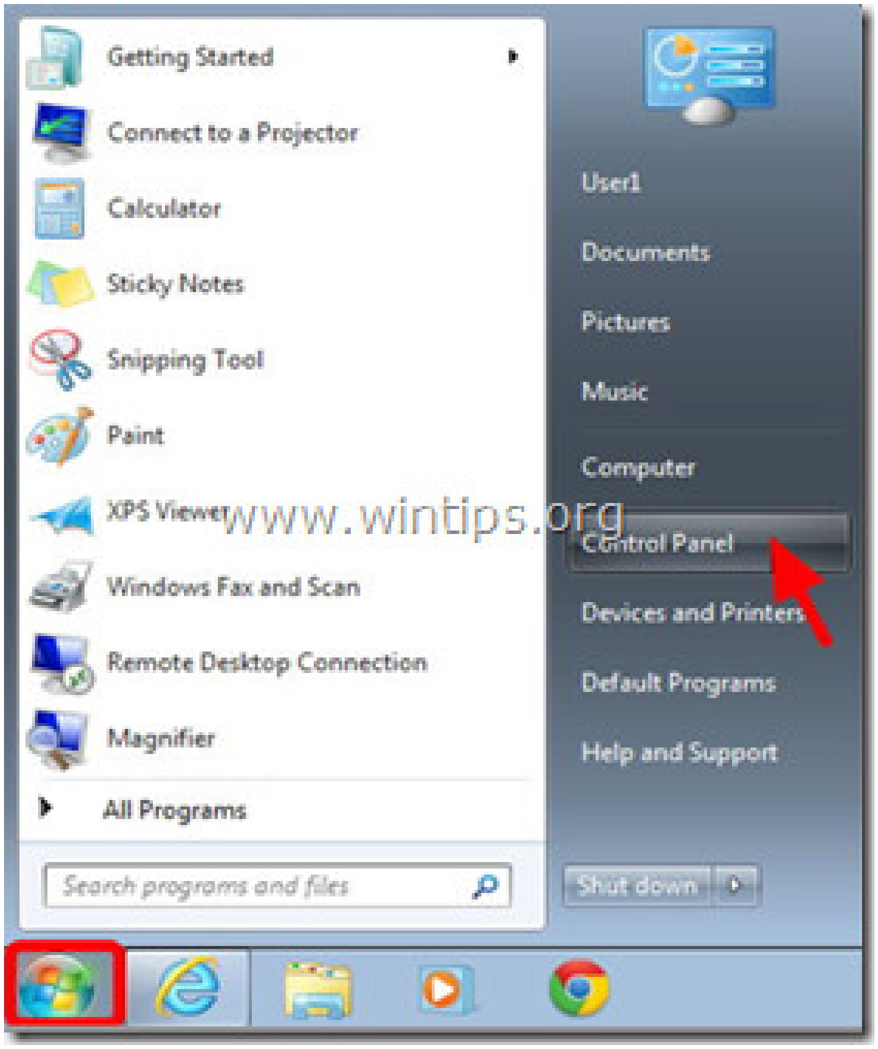
Remove the original page of Hao123. com on Windows computers

Step 1: Uninstall the malware on Control Panel

1. Try to remember when the first time you saw Hao123 on your computer, what software did you download and installed earlier on your computer? When you remember, remove the software immediately from your computer. If you can't remember, open Control Panel and check if any strange software is installed on the machine.

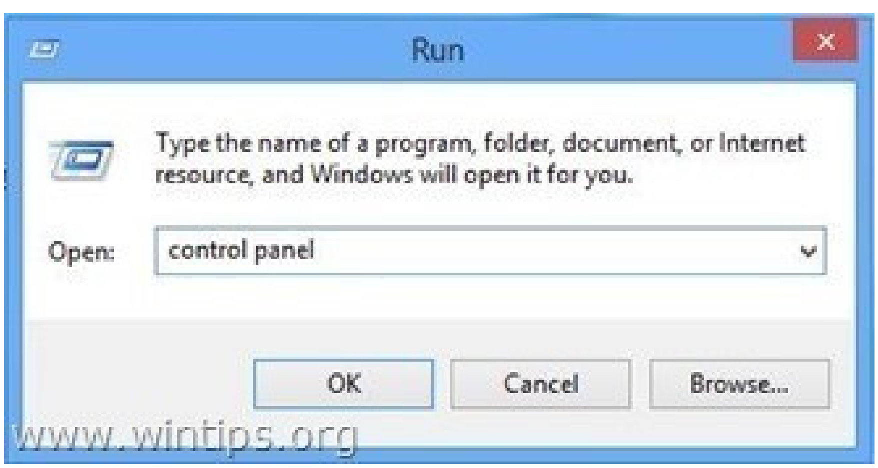
- On Windows 10, 7, Vista: **Go to Start => Control Panel** .

- On Windows XP: **Go to Start => Settings => Control Panel** .



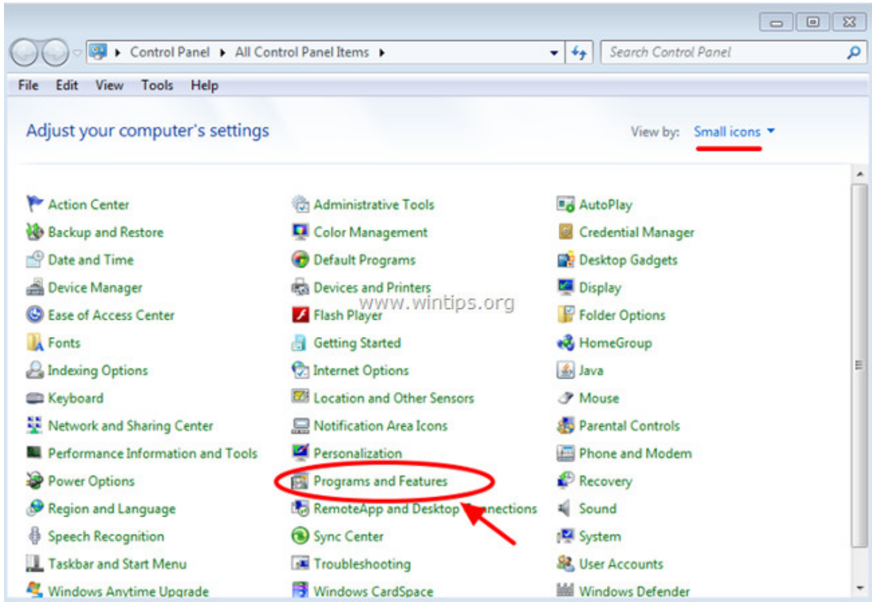
- On Windows 8 and Windows 8.1:

1. Press the Windows + R key combination to open the Run command window.
2. Enter "control panel" in the Run command window and press Enter.



2. On the Control Panel window, double click to open:

1. **Add or Remove Programs** : if using Windows XP.
2. **Programs and Features** (or 'Uninstall a Program') if using Windows 8, 7 or Vista.

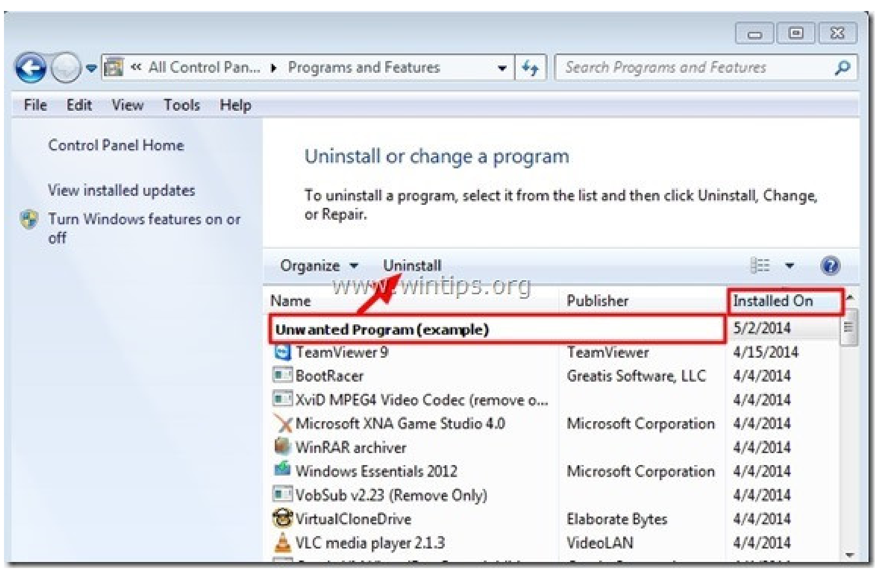


3. On the screen, a list of installed programs will be displayed:

- Arrange the programs displayed by the installation date (Installed On), then uninstall new unknown programs installed on your system.

- Also you should remove dangerous programs like:

1. Hao123 SmartBar

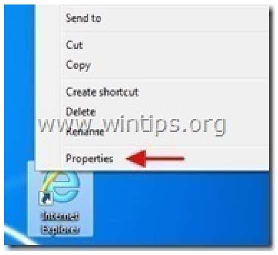


Step 2: Remove Hao123. com from Internet browser shortcut

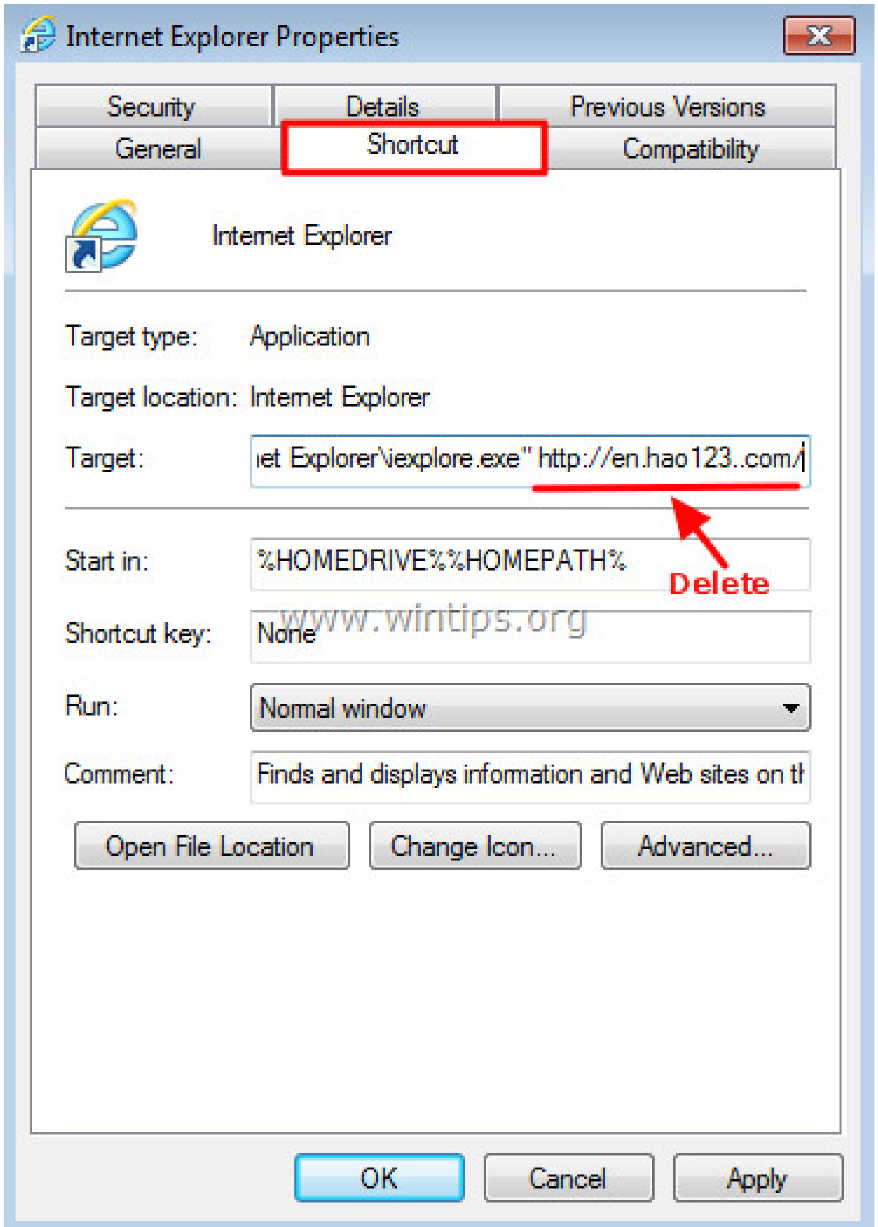
1. Right-click the Internet browser icon, select Properties.

Note:

You must follow the same steps for all Internet browser shortcuts, including Program lists and Taskbar.



2. On the Internet Explorer Properties window, click the 'Shortcut' tab, then find the Target frame and delete the Hao123 value (eg 'http:///en.hao123.com/…'), then enter 'iexplore .exe '(for Shortcut IE) or' firefox.exe '(for the Firefox shortcut), or' chrome.exe '(for the Chrome shortcut) and then click OK.



Click **Continue** when the 'Provide administrator permission to change these settings' window appears.

3. Follow the steps below.

Step 3: Scan the system with Malwarebytes AdwCleaner

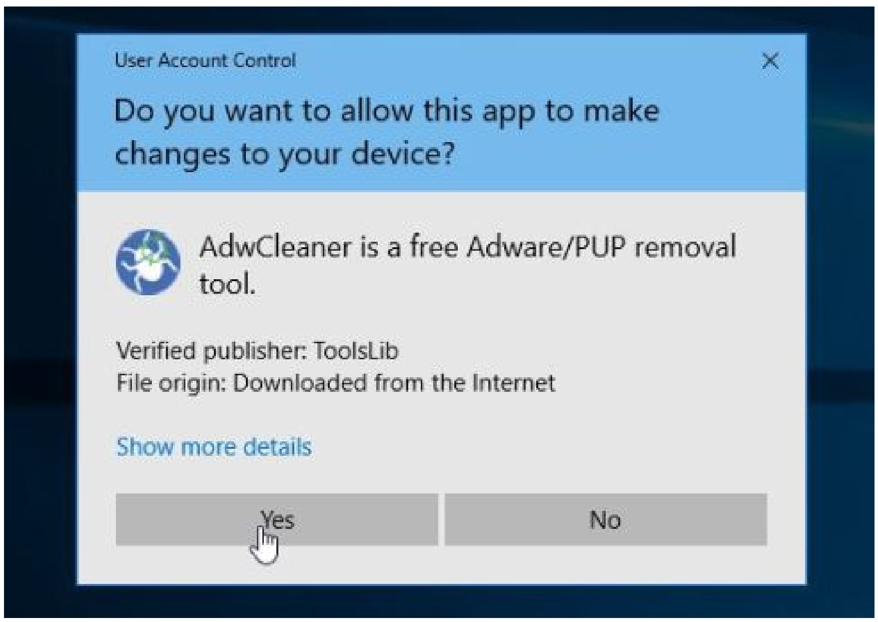
AdwCleaner is a free utility that will scan your system and web browsers to find and remove software installed on your system without your knowledge.

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.

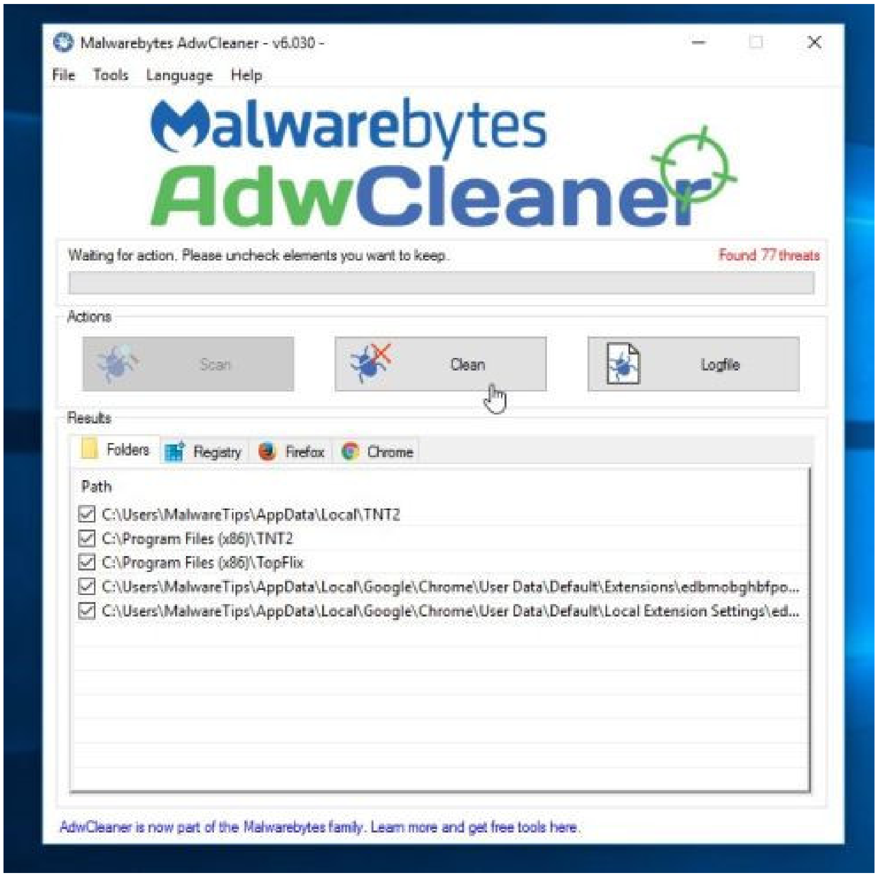
If Windows asks if you want to install AdwCleaner, click **Yes** to allow the program to run.



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

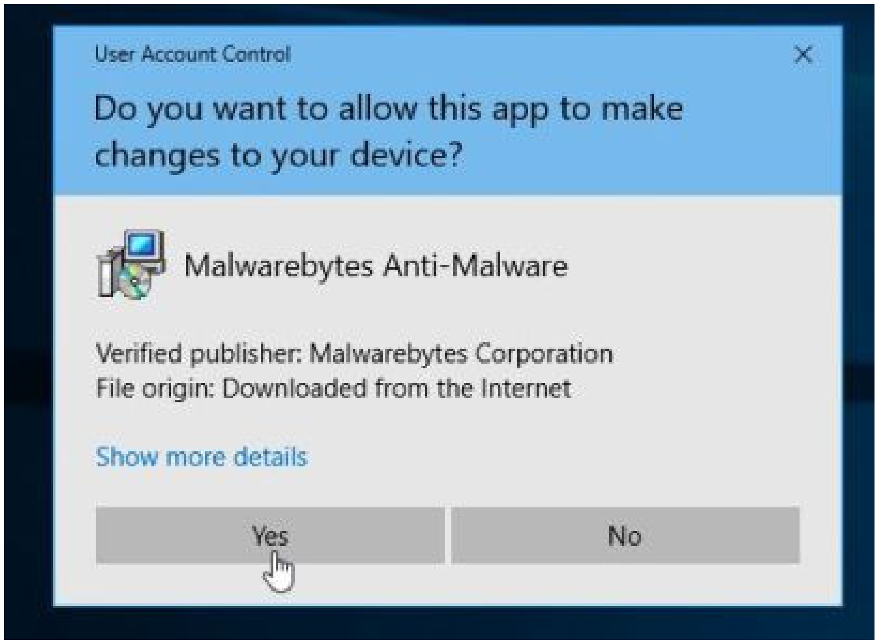
Malwarebytes Anti-Malware is an on-demand system scan tool that will remove all malware (malware) as well as Hao123 page. com out of your Windows computer. The important thing is that Malwarebytes Anti-Malware will run in parallel with other antivirus software without conflict.

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

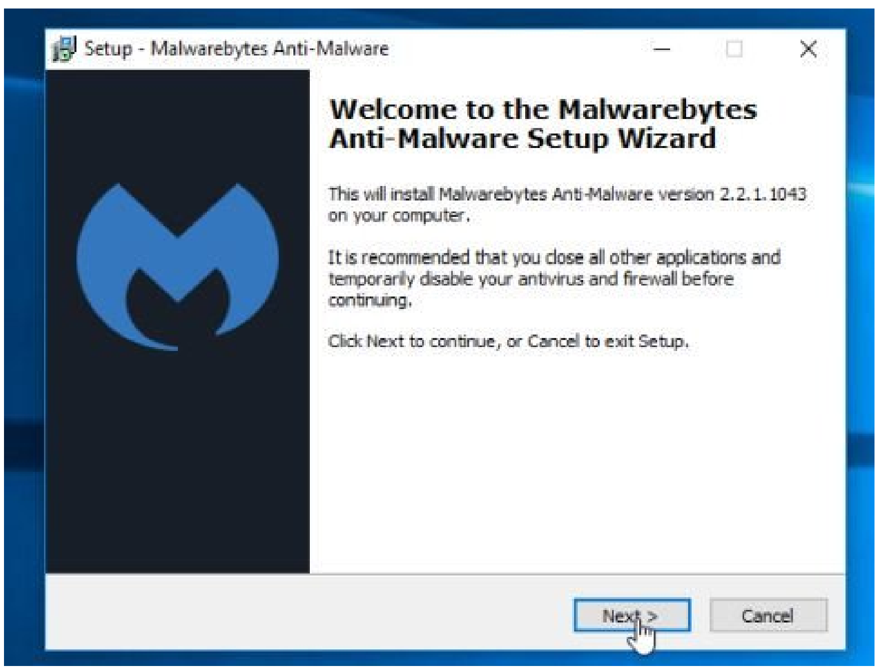
Download Malwarebytes Anti-Malware to your computer and install it here.

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.

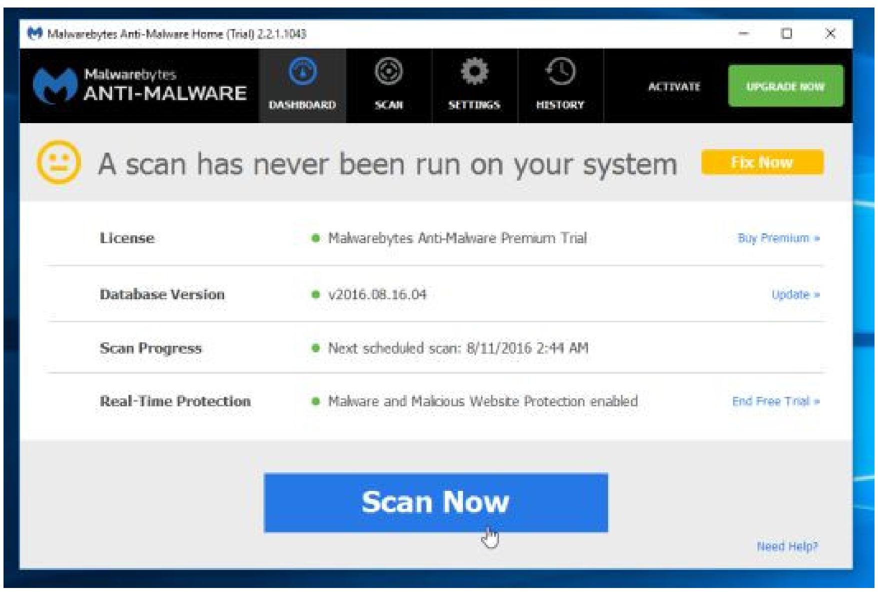


3. Follow the on-screen instructions to install Malwarebytes Anti-Malware Setup Wizard.

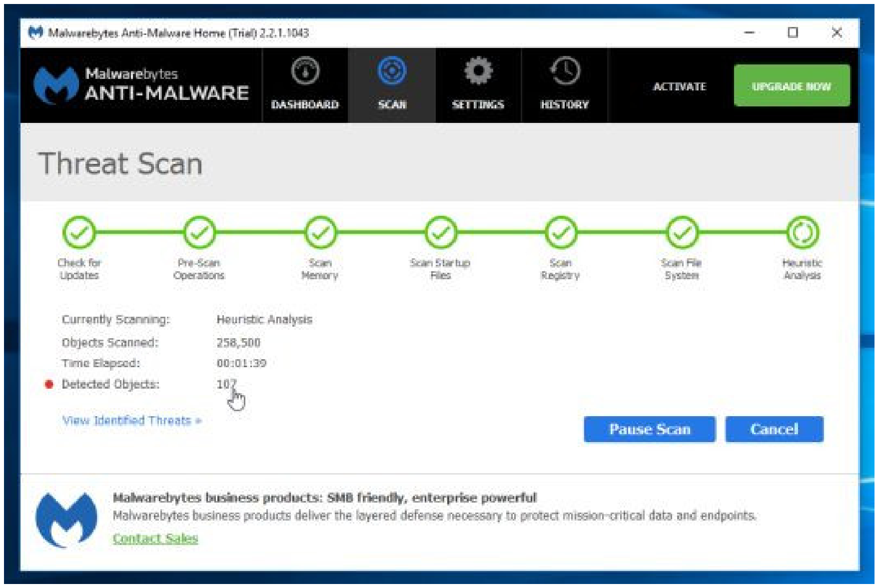


Click **Next** to install Malwarebytes Anti-Malware, until the last window click **Finish** to complete.

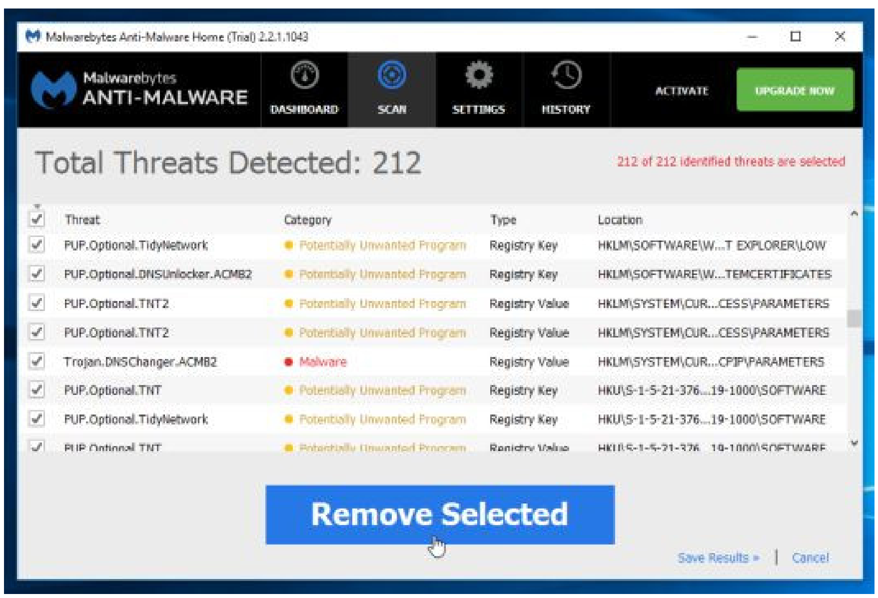
4. After installation is complete, Malwarebytes Anti-Malware will automatically open and **update** antivirus data. To start the scanning process, click the **Scan Now** button.



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.

HitmanPro will find and remove malware (malware), adware (adware), bots and other malware.

Step 5: Use HitmanPro to scan and test the system

1. Download HitmanPro to your device and install it.

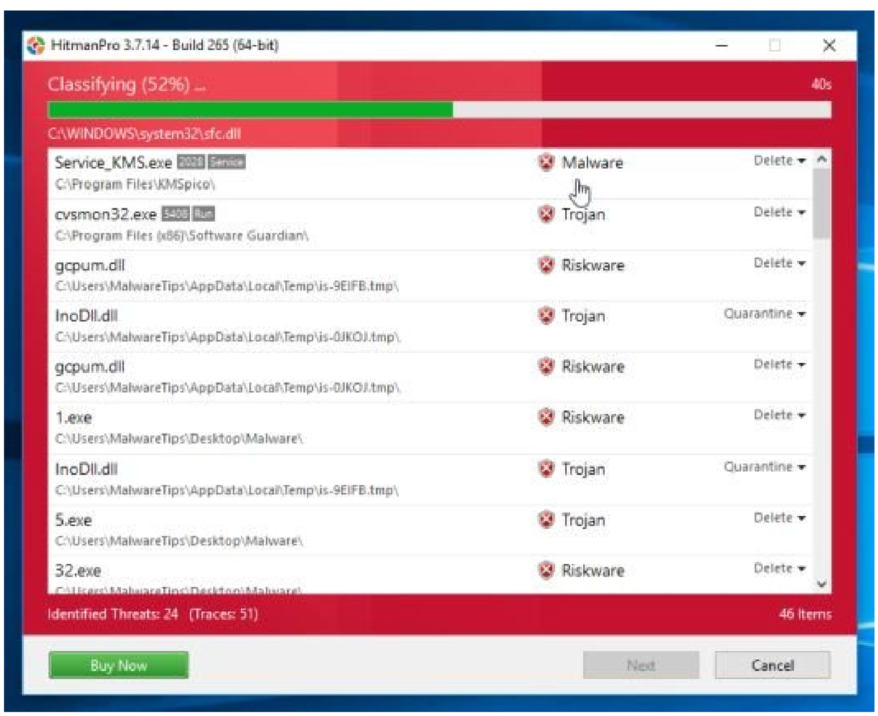
    1. Download HitmanPro (32-bit version) to your device and install it here.

2. Download HitmanPro (64-bit version) to your device and install it here.

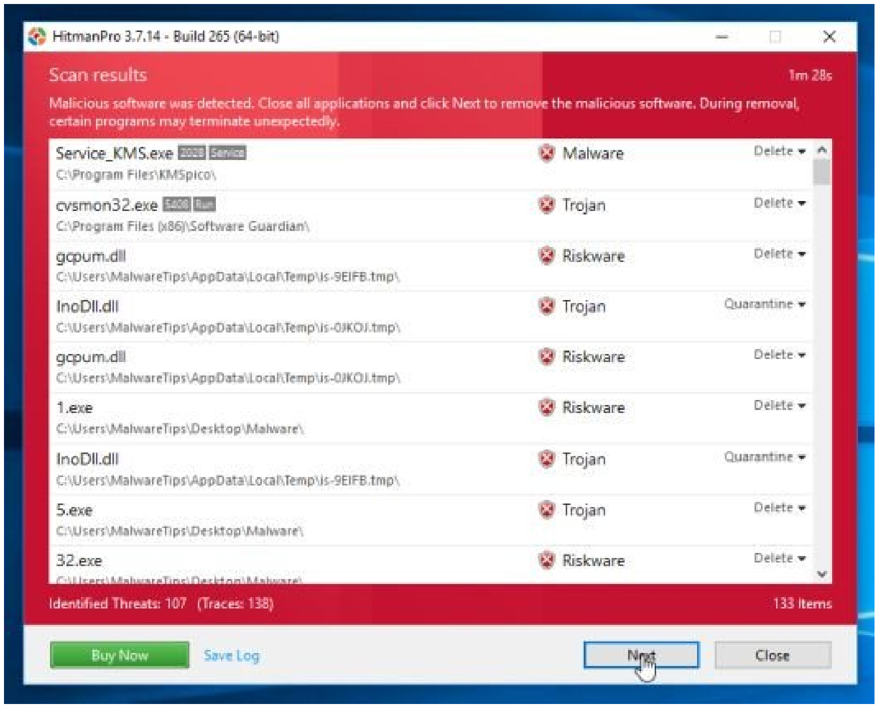
2. Double-click the **'HitmanPro.exe' file** (if using 32-bit win) or the **'HitmanPro_x64.exe'** file (if using win 64-bit) to open the application.

Next, click **on Nex** t to install HitmanPro on your computer.

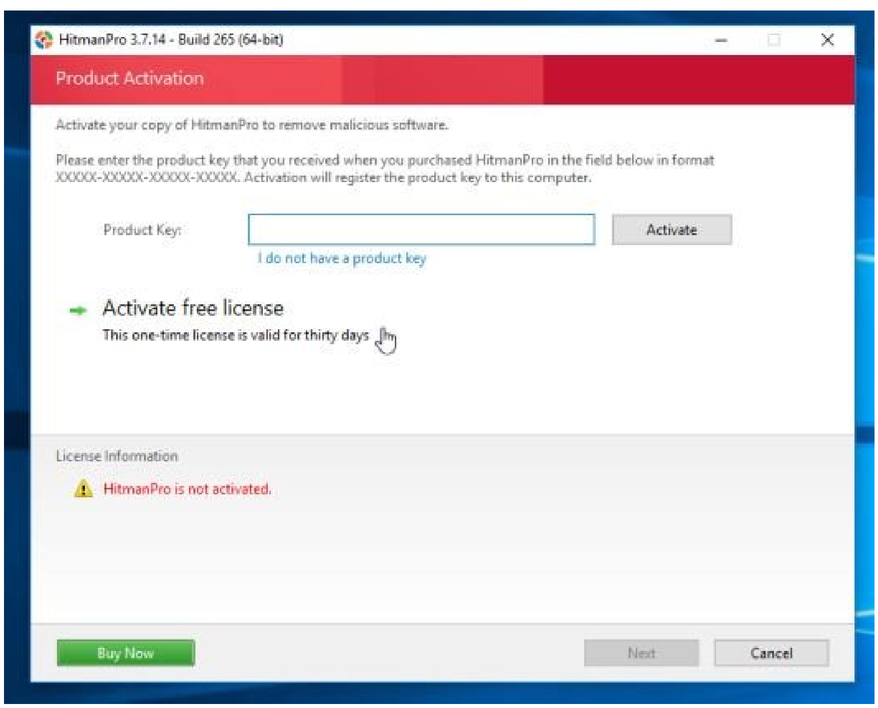
3. HitmanPro will start scanning your computer for malware (malware).



4. When the process finishes, the screen will display a list of all the malicious programs that the application finds. Click **Next** to remove the malware (malware).



5. Click **Activate free license** to start testing the application within 30 days, and to remove all malicious files on your computer.



Step 6: Use Zemana AntiMalware to scan the system

Use Zemana AntiMalware to remove Hao123 extension. com on the browser and other malicious programs on your computer.

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

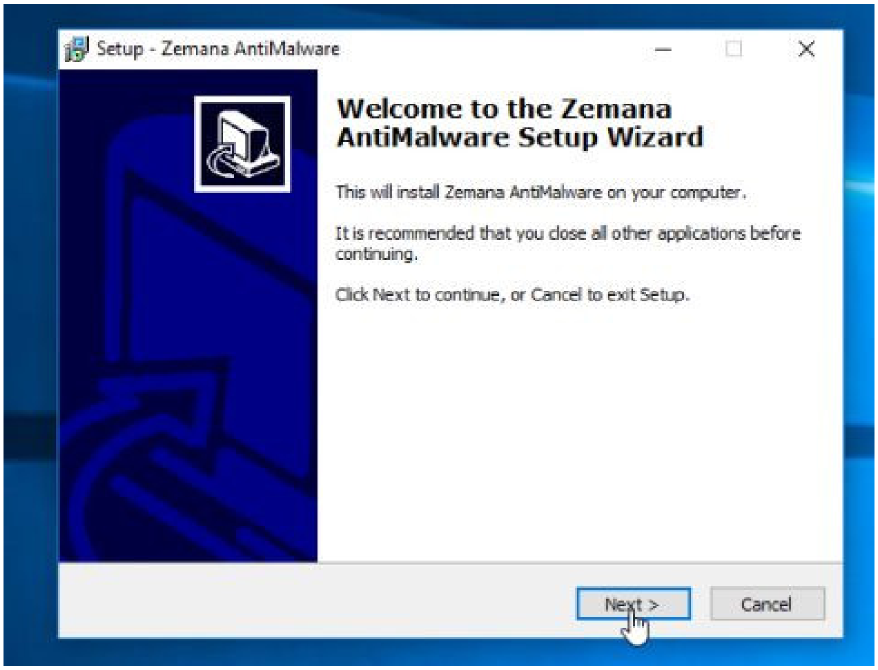
Download Zemana AntiMalware and install it here.

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

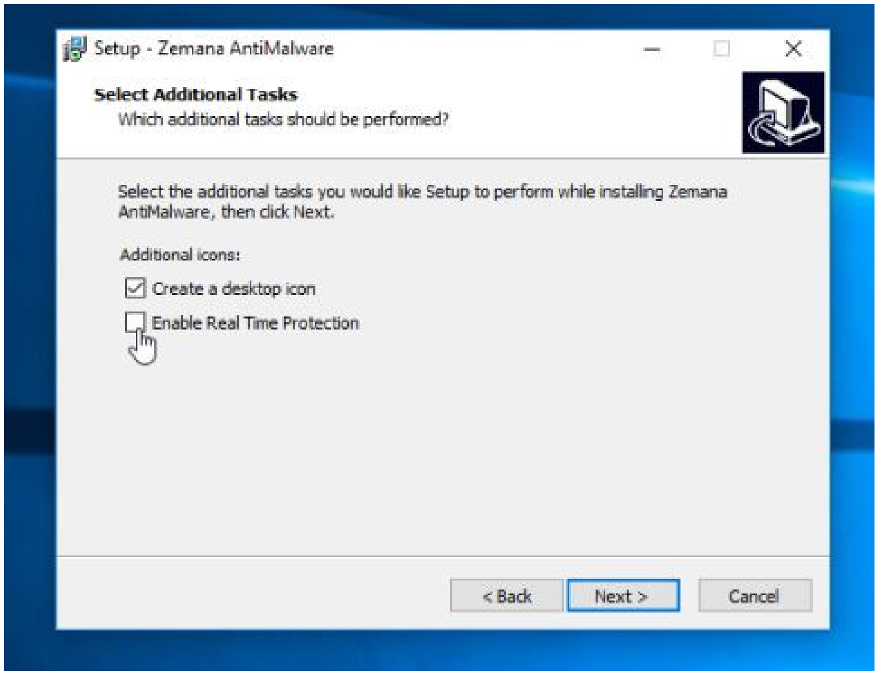
The **User Account Control** dialog box appears now on the screen asking if you want to run the file. Click **Yes** to continue the installation process.

Picture 23 of Steps to remove page Hao123. com

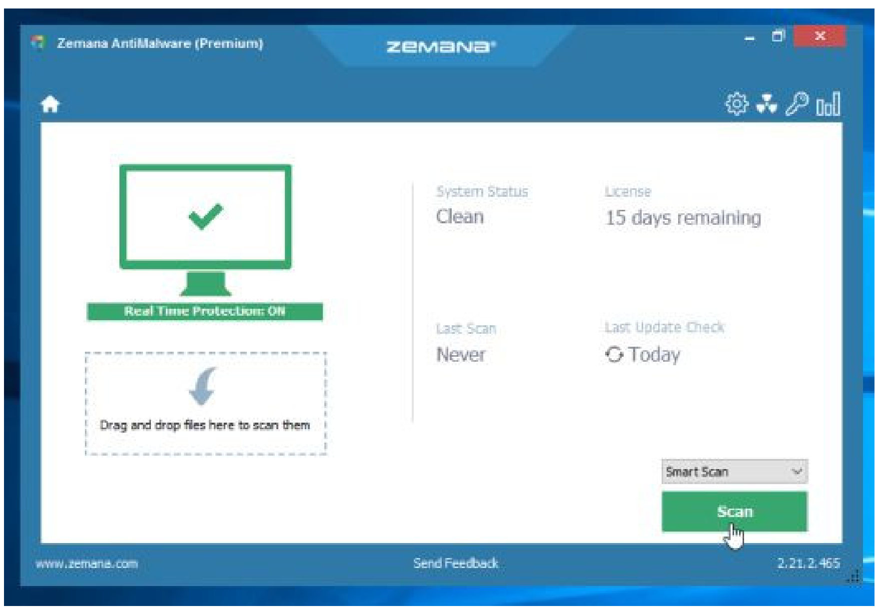
3. Click **Next** and follow the on-screen instructions to install Zemana AntiMalware on your computer.



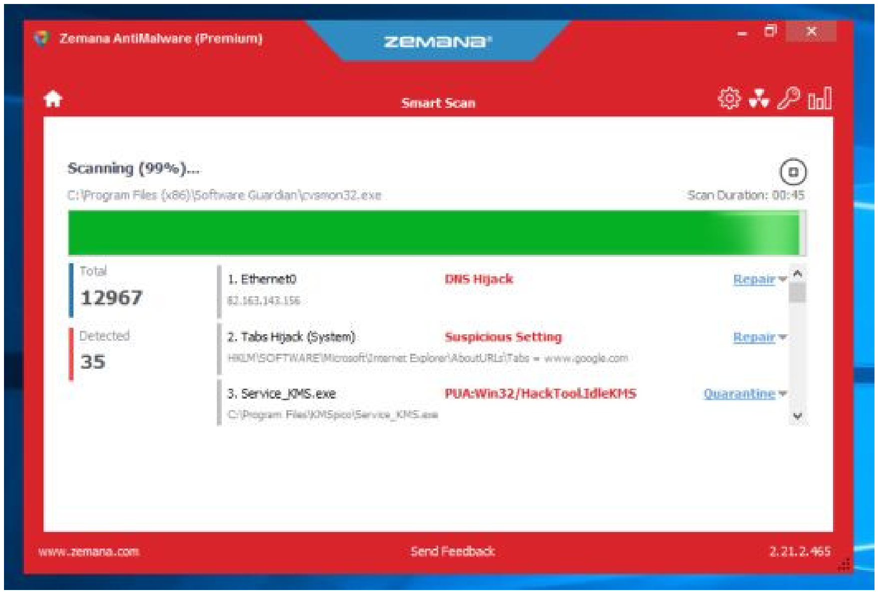
Go to the Select Additional Task window, you can uncheck the **Enable Real Time Protection** option and click Next.



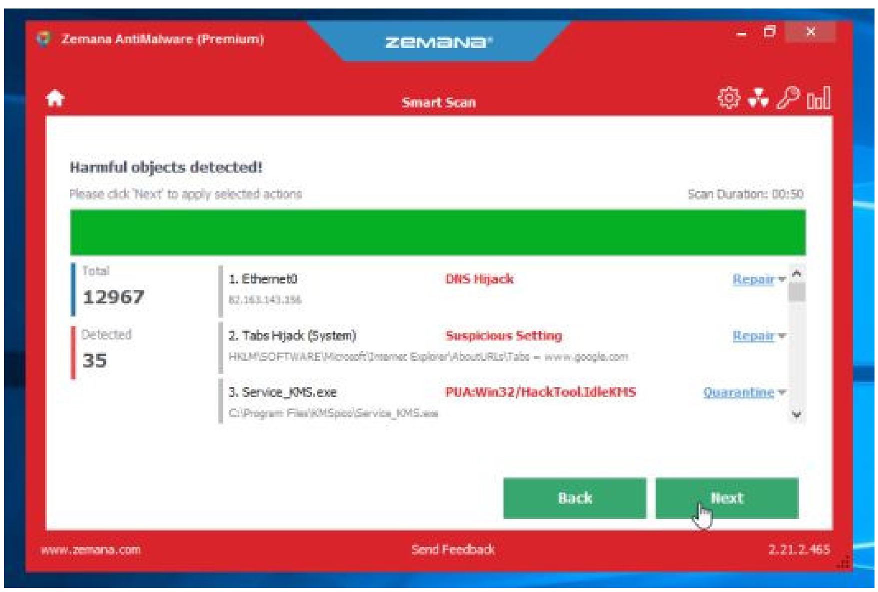
4. When the Zemana AntiMalware window opens, click **the Scan button** .



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.



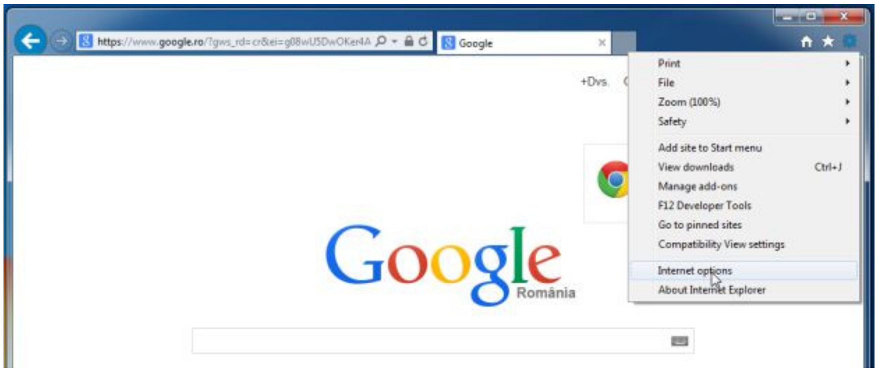
Zemana AntiMalware will remove all malicious files from your computer and will require the system to reboot to remove all malicious programs.

Step 7: Reset your browser to the default setting state

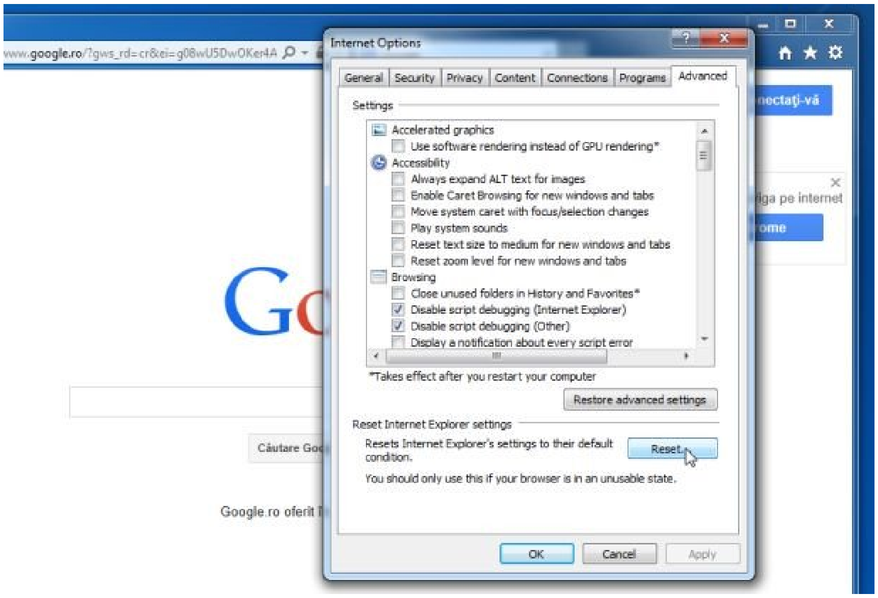
- On Internet Explorer:

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

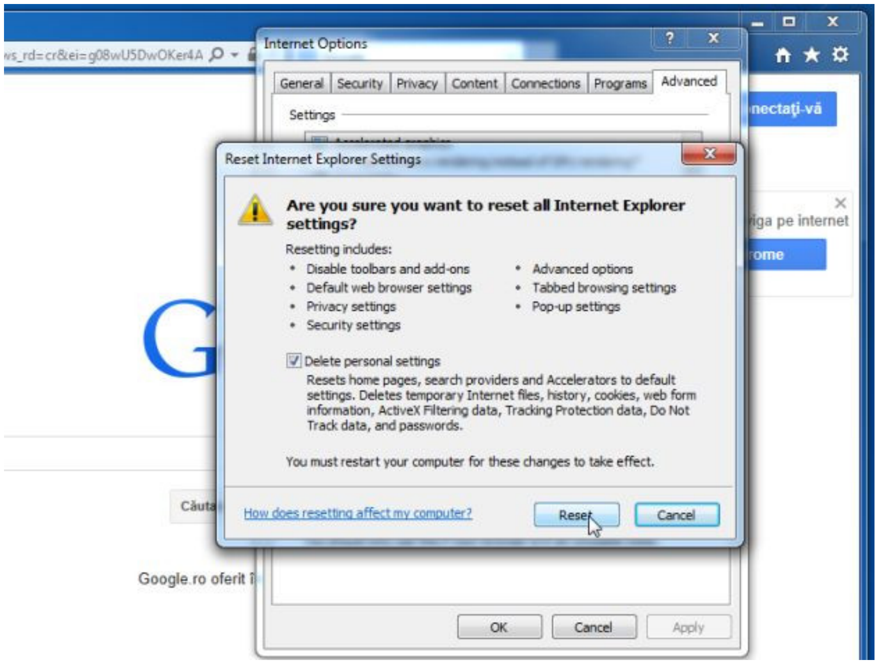
1. Open Internet Explorer, then click the jagged icon in the top right corner of the screen, select Internet Options.



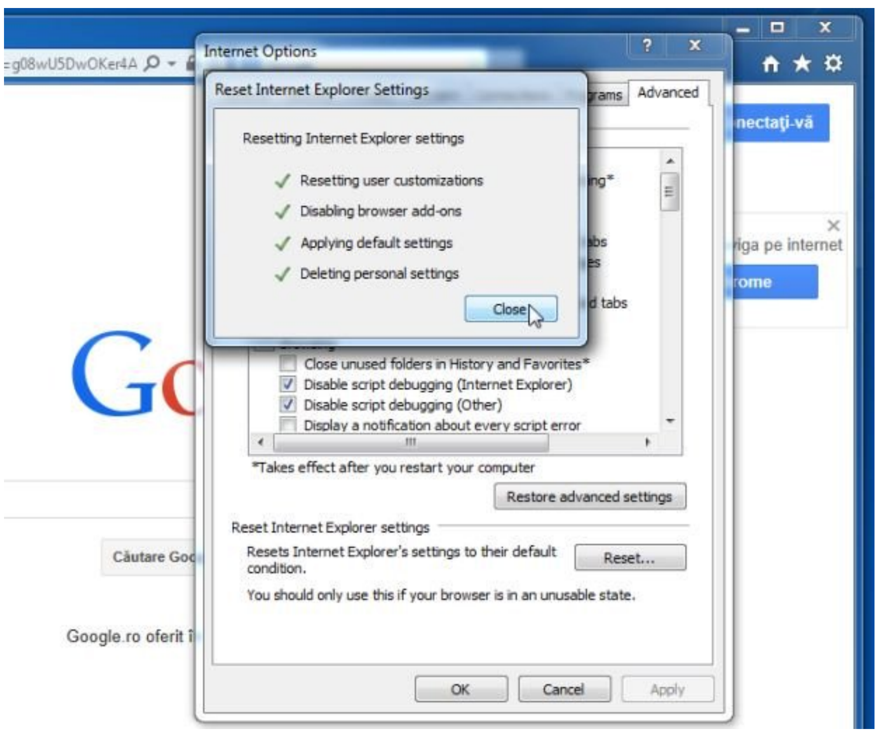
2. At this time, the **Internet Options** window will appear, where you click the **Advanced tab** , then click **Reset** .



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

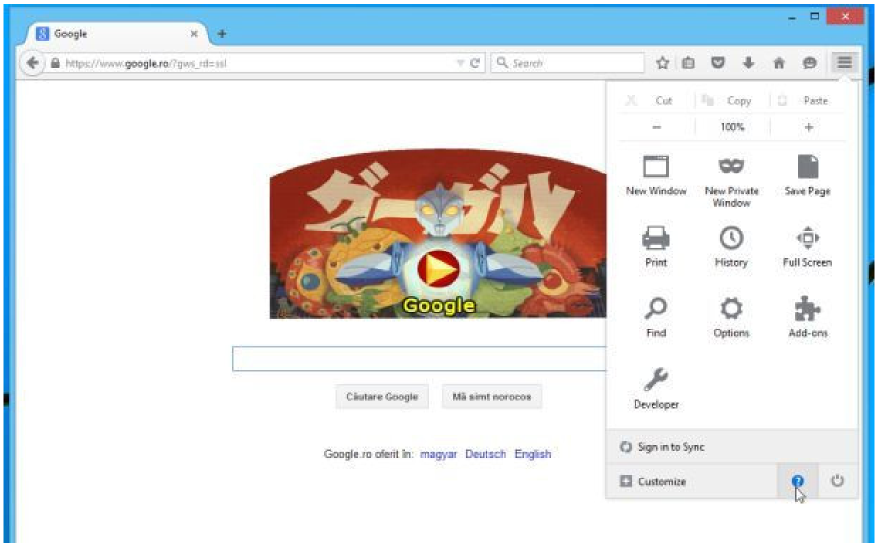


4. After the reset process finishes, click the Close button to close the confirmation dialog window. Finally restart your Internet Explorer again.



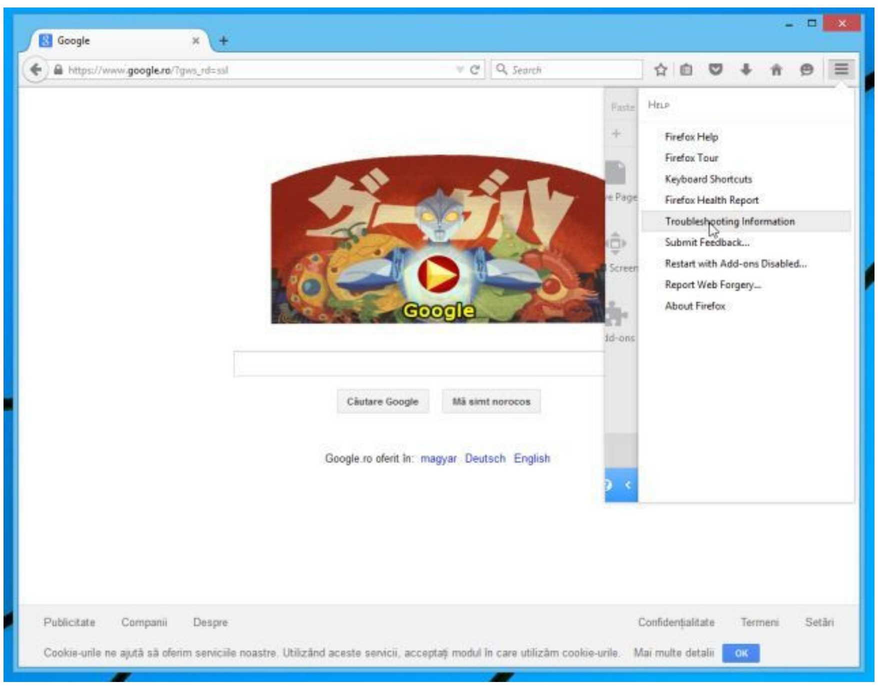
- On Firefox browser:

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

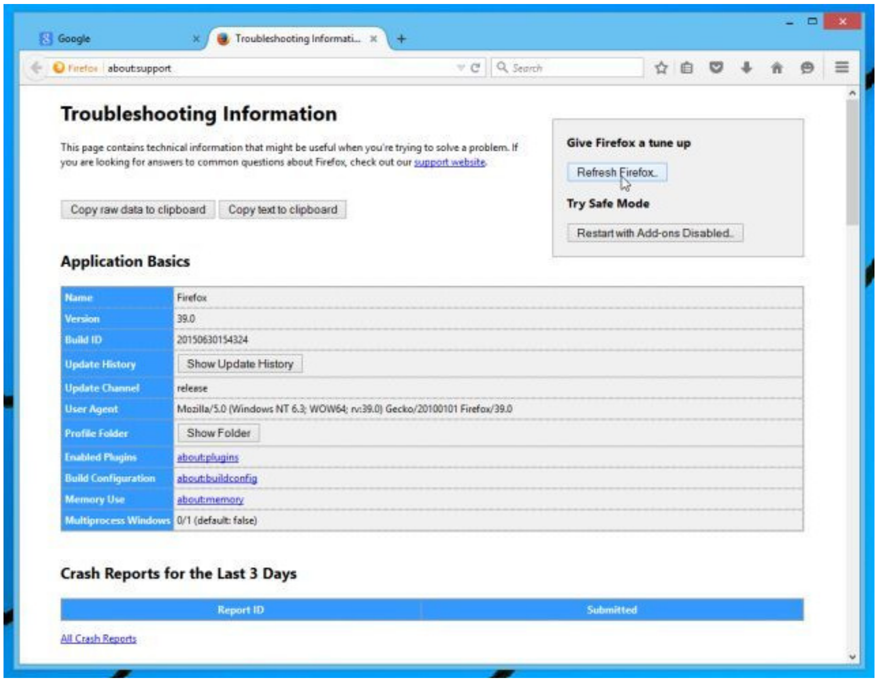


2. On the Help Menu, click Troubleshooting Information.

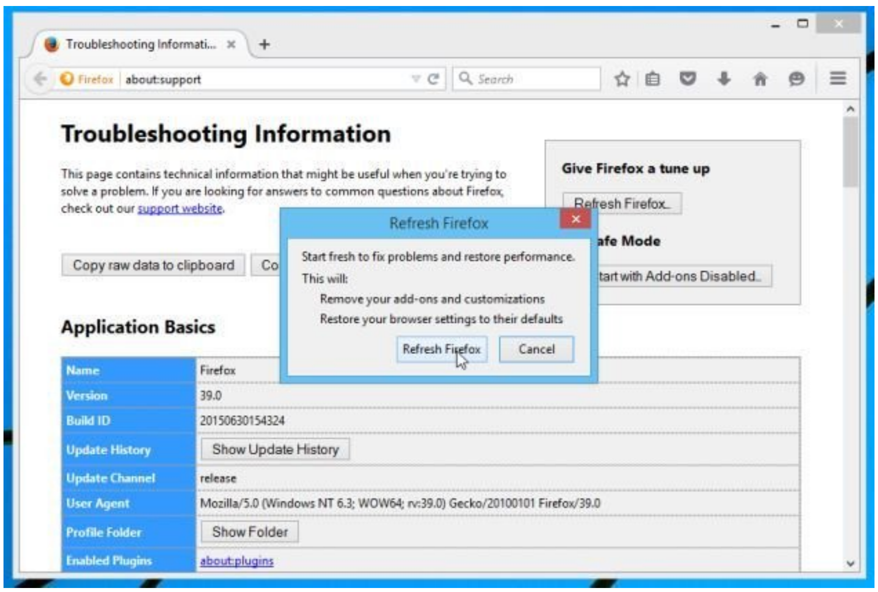
If you cannot access the Help menu, enter **about: support** in the address bar to open the Troubleshooting information page.



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



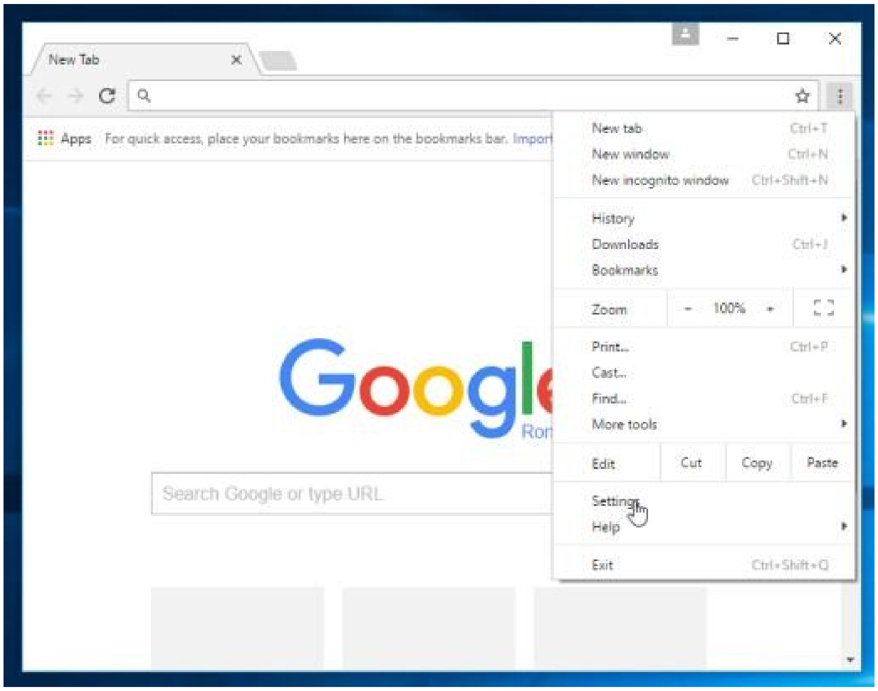
4. Continue to click the **Refresh** button **Firefox** on the confirmation window.



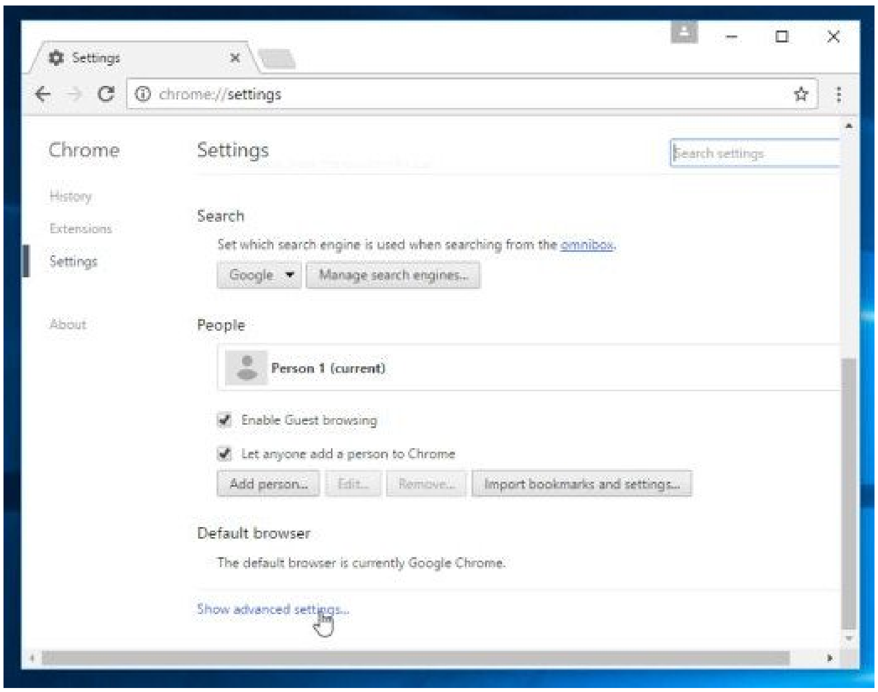
5. Firefox will automatically close the window and return to the original default installation state. Once completed, a window displaying the information will appear. Click **Finish.**

- On Chrome browser:

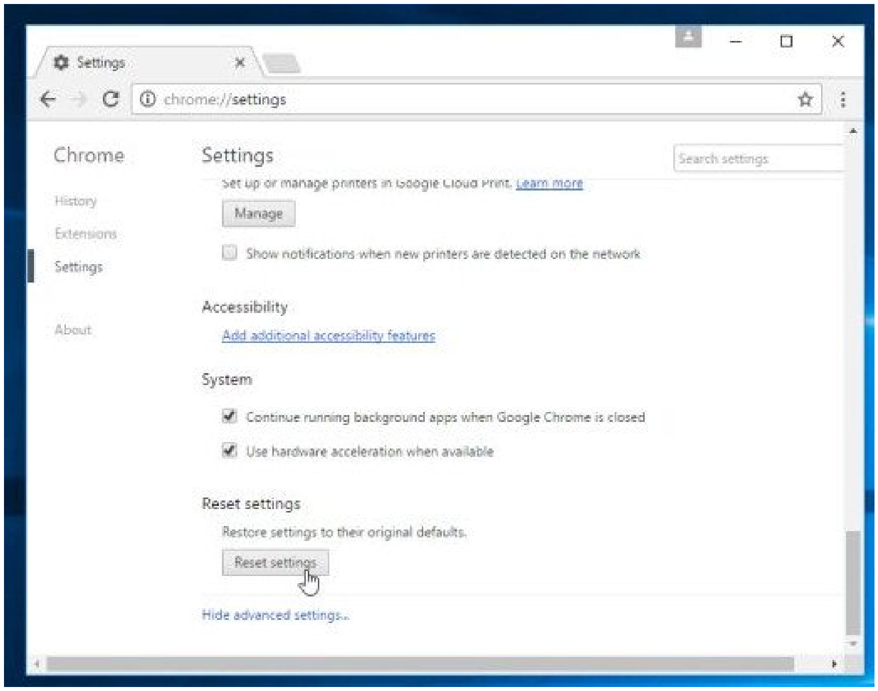
1. Click on the 3 dash line icon in the top corner of the screen, select **Settings** .



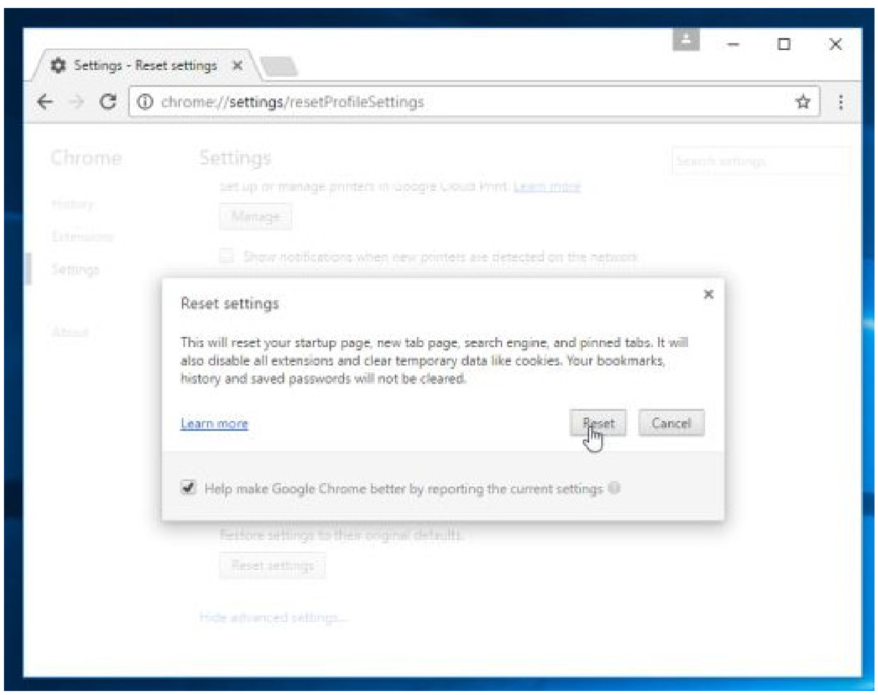
2. Now on the screen appears the Settings window, here you scroll down to find and click **Show advanced settings** (show **advanced settings**).



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.



Refer to some of the following articles:

1. How to remove Trustedsurf.com on Chrome, Firefox and Internet Explorer
2. Rooted Delta Search on Chrome, Firefox and Explorer browsers
3. Instructions to disable Flash Player on all browsers

Good luck!

You finished reading the article "**Steps to remove page Hao123. com**" 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.