Virus 'interyield jmp9' attacks the system, this is the way to get rid of this virus

'Interyield.jmp9' (interyield jmp9.com) is an unwanted program Potentially Unwanted Program (PUP). When this program is installed on your system, it will edit the settings on the system to display monetized ads or redirect the search on the browser to advertising sites.

' *Interyield.jmp9* ' (interyield jmp9.com) is an unwanted program " *Potentially Unwanted Program (PUP)* ". When this program is installed on your system, it will edit the settings on the system to display monetized ads or redirect the search on the browser to advertising sites. If your computer is attacked by adware ' *Interyield-jmp9* ', then your computer will display popup windows and your computer speed will slow down as malicious programs run. on background.

The advertising program will make users feel uncomfortable because it always displays popup windows while users use the computer, and that is one of the reasons why computer users are slowing down. gradually. In addition, these advertising programs are also considered browser attackers, it will change browser settings to display more ads.

'Interyield' is integrated on free software that users download from the Internet. In the process, users installed those software accidentally installing 'Interyield' without knowing it.

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.

Steps to remove root virus "interyield jmp9" on the system

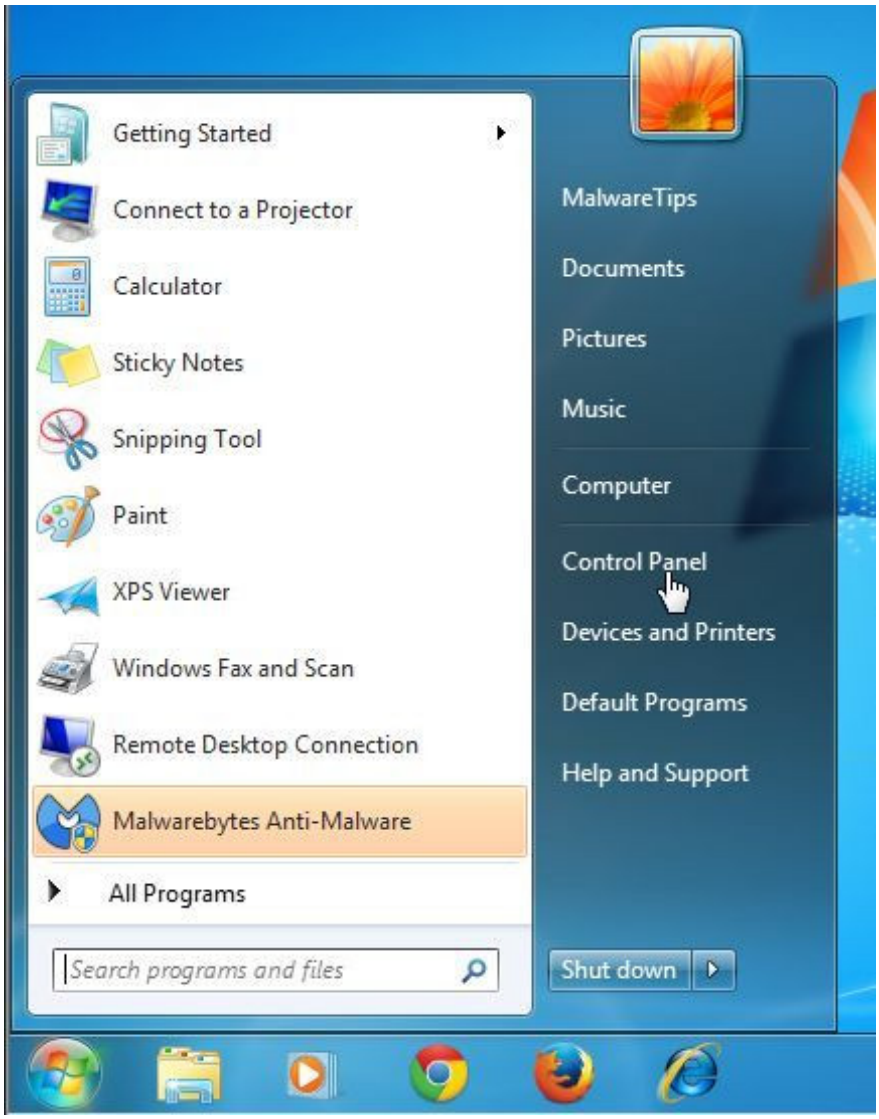
Step 1: Remove the advertising program "Interyield.jmp9.com"

The first step you need to do is find and remove the malicious programs installed on your computer.

1. Access **the Uninstall menu** .

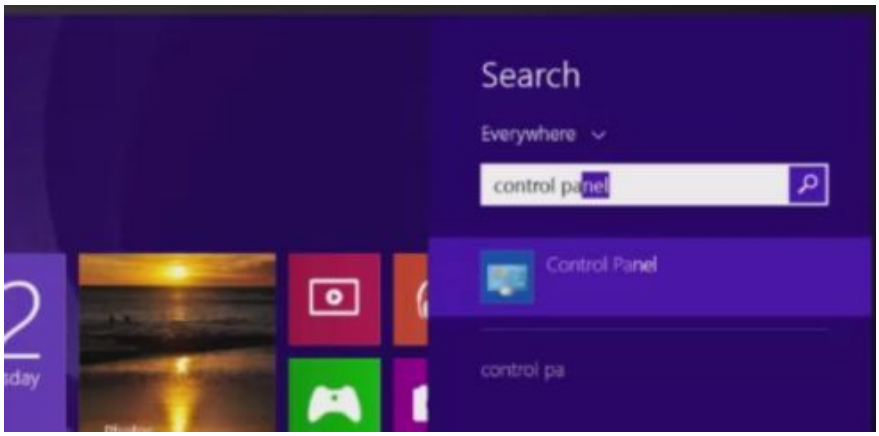
- On Windows 7 and Windows Vista:

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** .

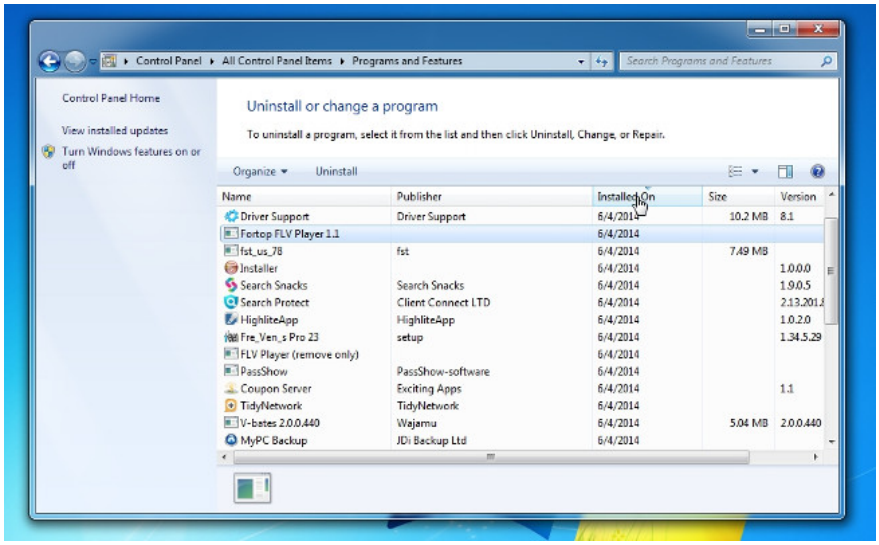


2. On the Control Panel window, click on the option to ' *Uninstall a program* ' located in the **Programs** section.

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 programs:

V-bates, PriceMeter, Supra Savings, WeDownload Manager, PureLead, Search Assist, Re-Markable, Zombie Alert, Wajam, Coupon Server, Lollipop, HD-Total-Plus, BlockAndSurf, Safe Saver, SupTab, Search Protect, Lollipop, Software Updated Version, DP1815, Video Player, Convert Files for Free, Plus-HD 1.3, BetterSurf, Trusted Web, PassShow, LyricsBuddy-1, PureLeads, Media Player 1.1, RRSavings, Feven Pro 1.2, Websteroids, Bull Savings, TidyNetwork, Search Snacks , MyPC Backup, Re-markit.



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 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.

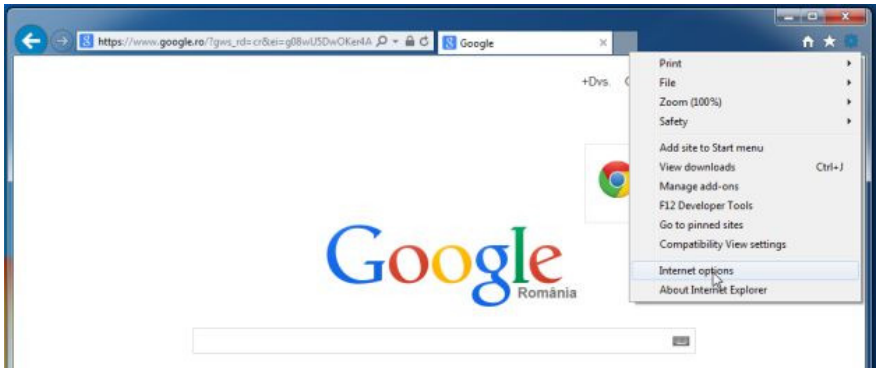
Step 2: Remove popup window 'Interyield.jmp9.com' in Explorer, Firefox and Google Chrome browsers

- On Internet Explorer:

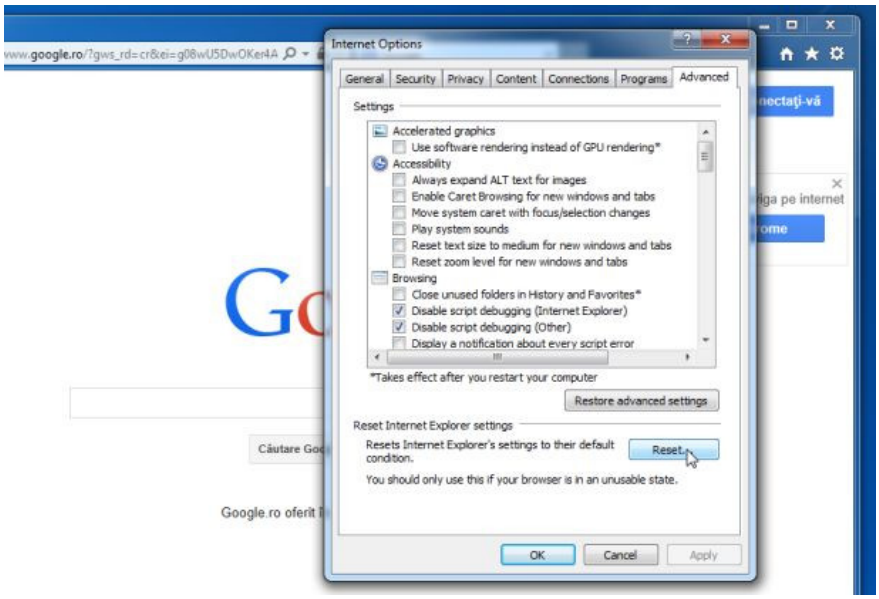
You can reset Internet Explorer browser settings to the initial default setting status to remove the popup popup window ' *Interyield.jmp9.com* '.

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

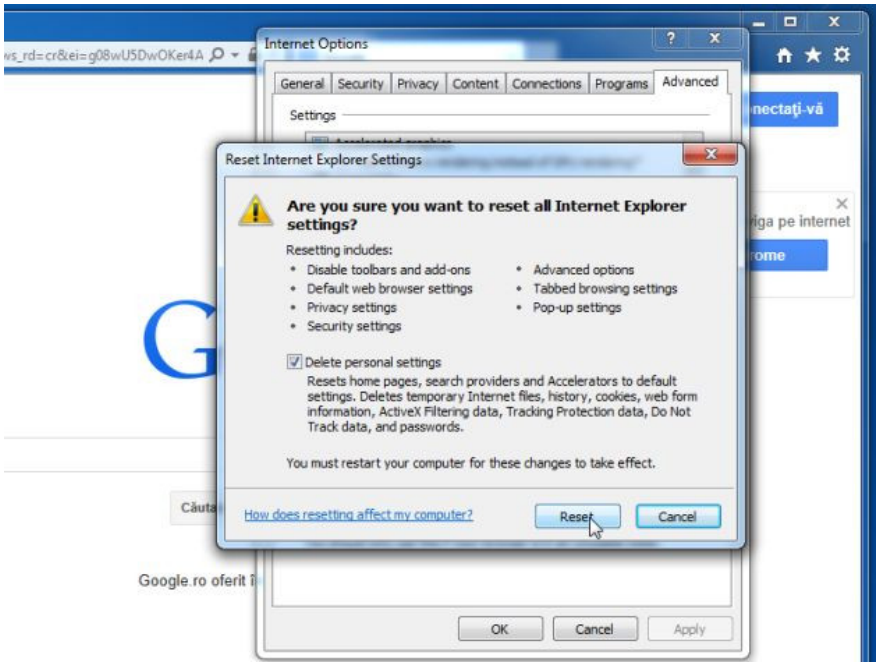
1. Open Internet Explorer, then click the jagged icon in the top right corner of the screen, select Internet Options.



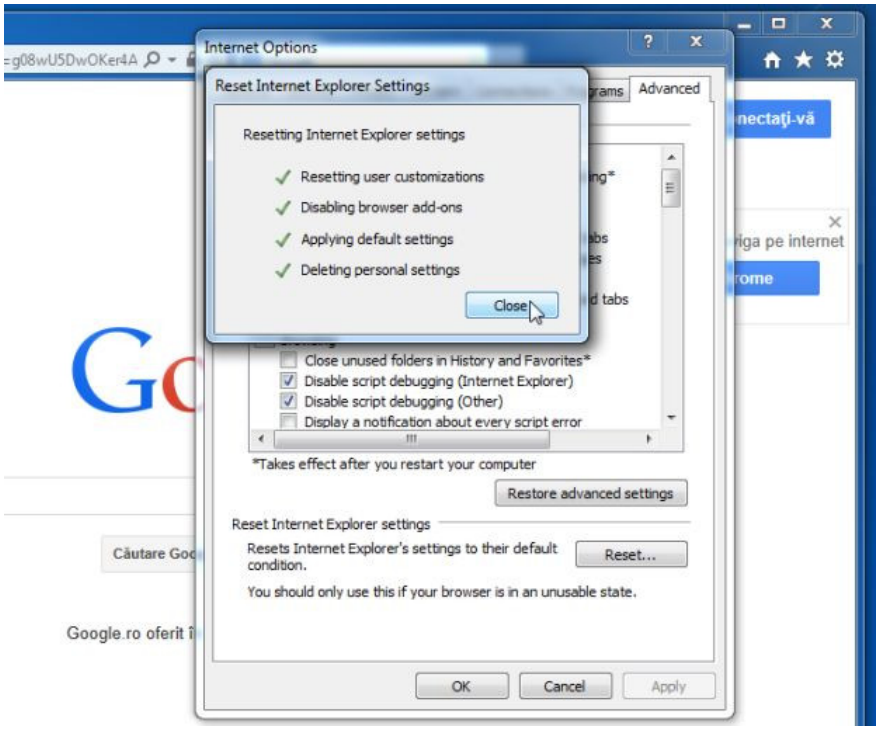
2. At this time, the Internet Options window will appear, where you click the **Advanced tab** , then click **Reset** .



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

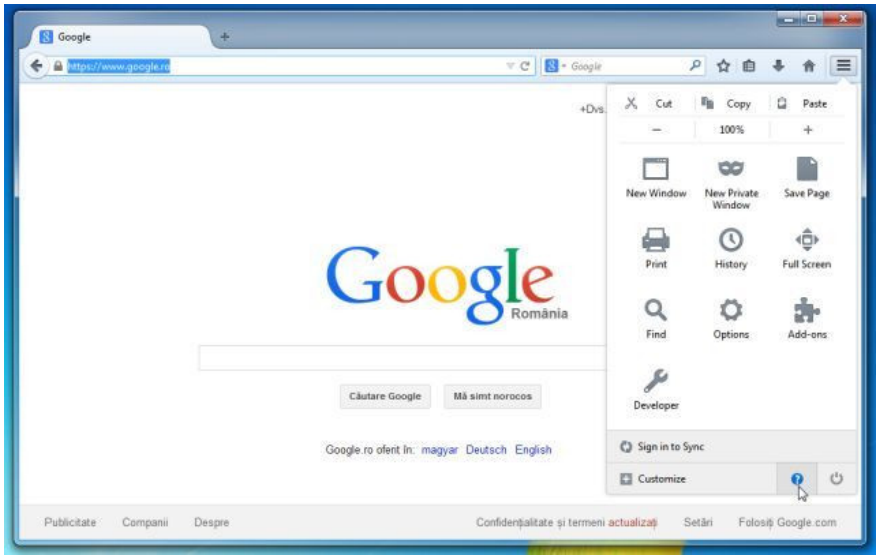


4. After the reset process finishes, click the **Close** button to close the confirmation dialog window. Finally restart your Internet Explorer again.



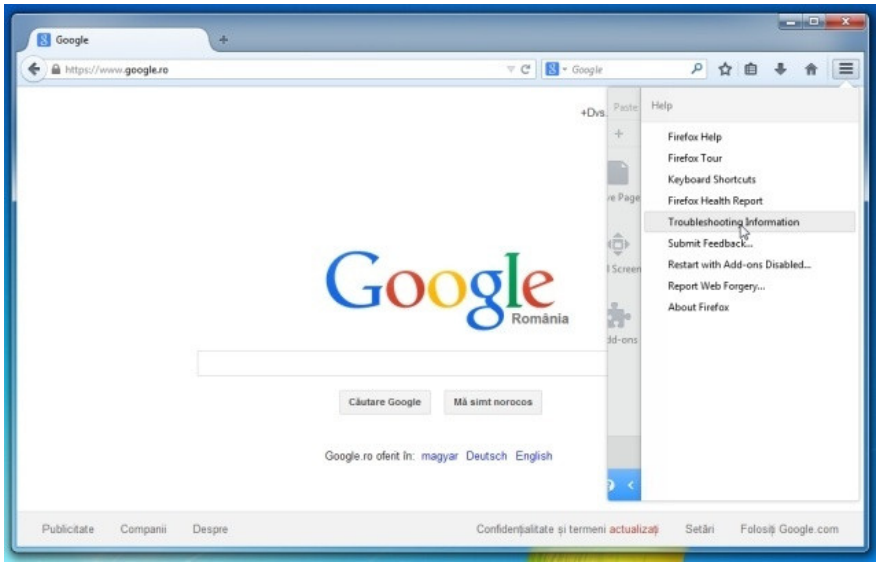
- On Firefox browser:

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

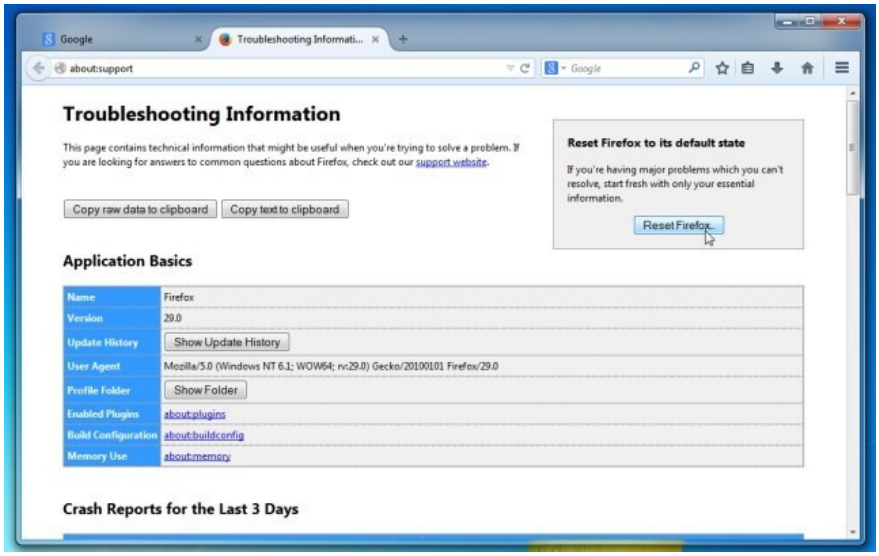


2. On the Help Menu, click **Troubleshooting Information**

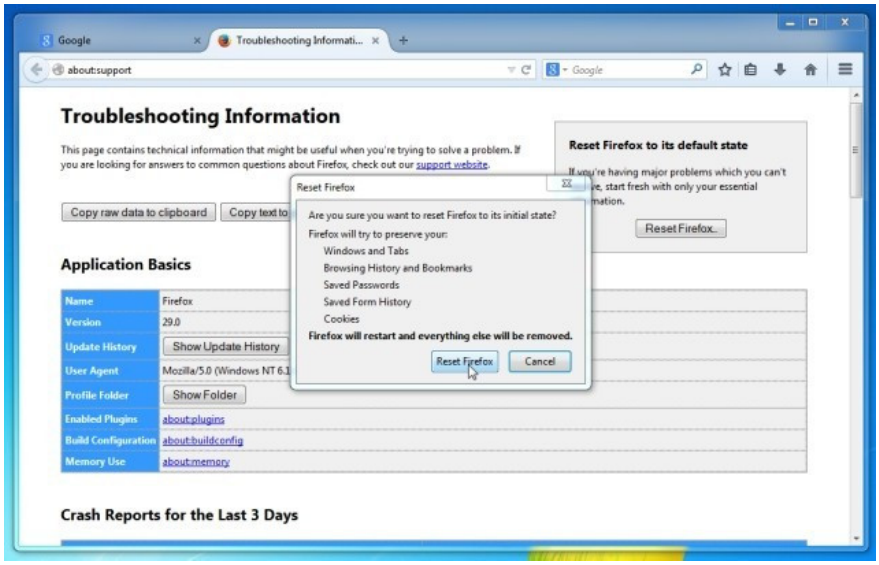
If you cannot access the Help menu, enter about: support in the address bar to open the Troubleshooting information page.



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



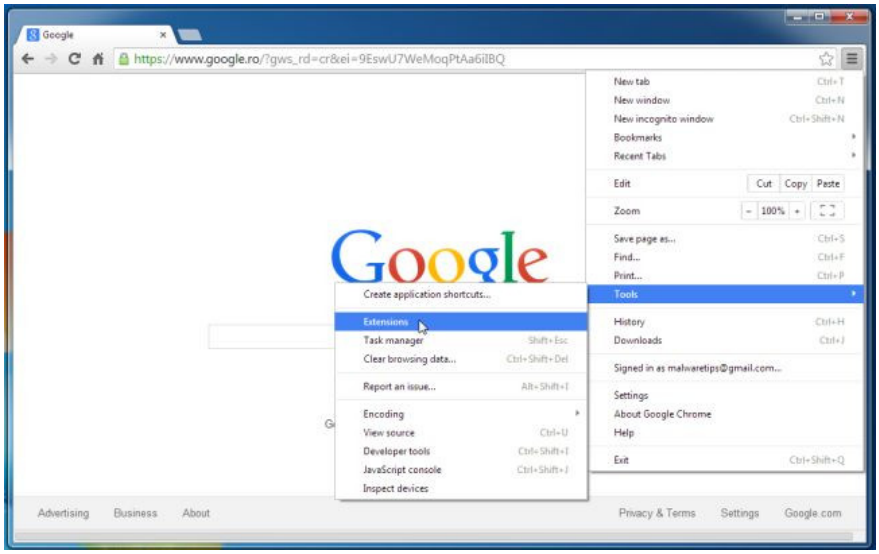
4. Continue to click the Refresh button Firefox on the confirmation window.



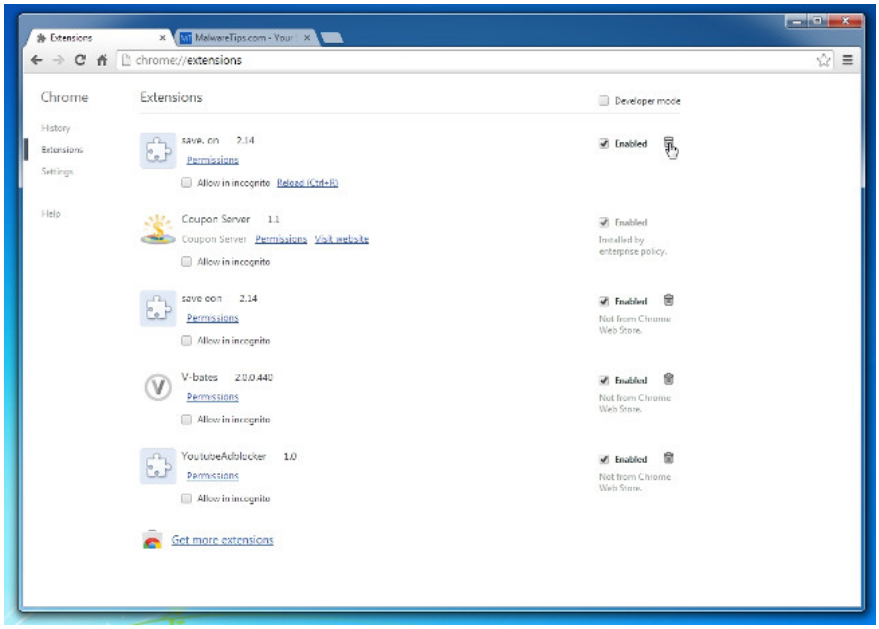
5. Firefox will automatically close the window and return to the original default installation state. Once completed, a window displaying the information will appear. Click Finish.

- On Google Chrome browser:

1. Click the 3 dash lines or 3 dots in the top right corner of the browser window, select Tools => "Extensions".



2. On the **Extensions** window, find and delete extensions: HD-Total-Plus, SafeSaver, DP1815, Video Player, Convert Files for Free, Plus-HD 1.3, BetterSurf, Media Player 1.1, PassShow, LyricsBuddy- 1, YInteryield.jmp9.com 1.2, Media Player 1.1, Savings Bull, Feven Pro 1.1, Websteroids, Savings Bull, HD-Plus 3.5 and extensions of unknown origin by selecting the trash can icon.



Step 3: Use AdwCleaner to remove 'Interyield.jmp9.com'

AdwCleaner is a free utility that will scan your system and web browsers to find and remove unwanted ads, malicious files, and unwanted extensions installed on. browser that you do not know.

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 is open, click the button Scan 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 4: Remove the 'Interyield.jmp9.com' 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.

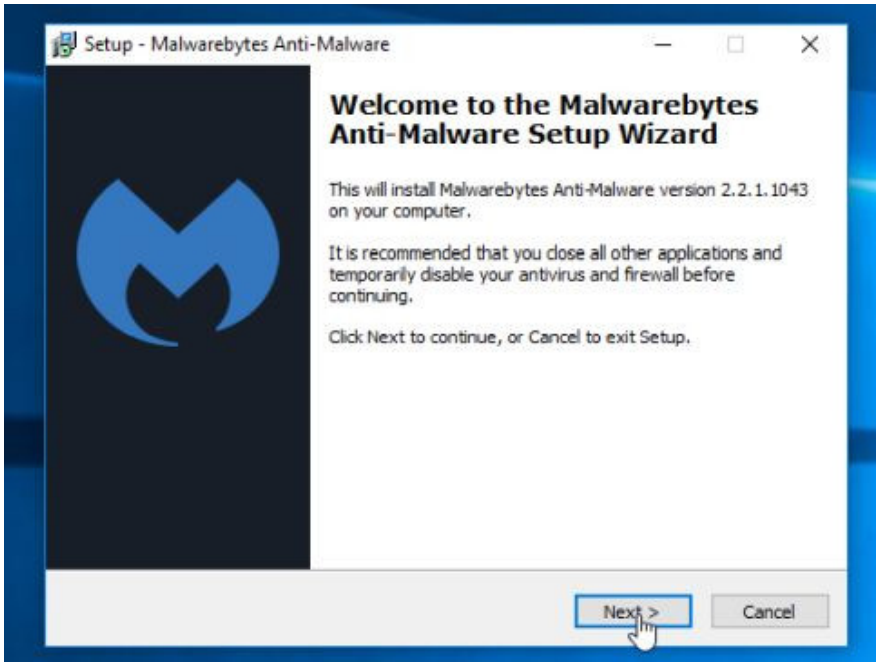
1. Download Malwarebytes Anti-Malware to your computer and install it.

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.

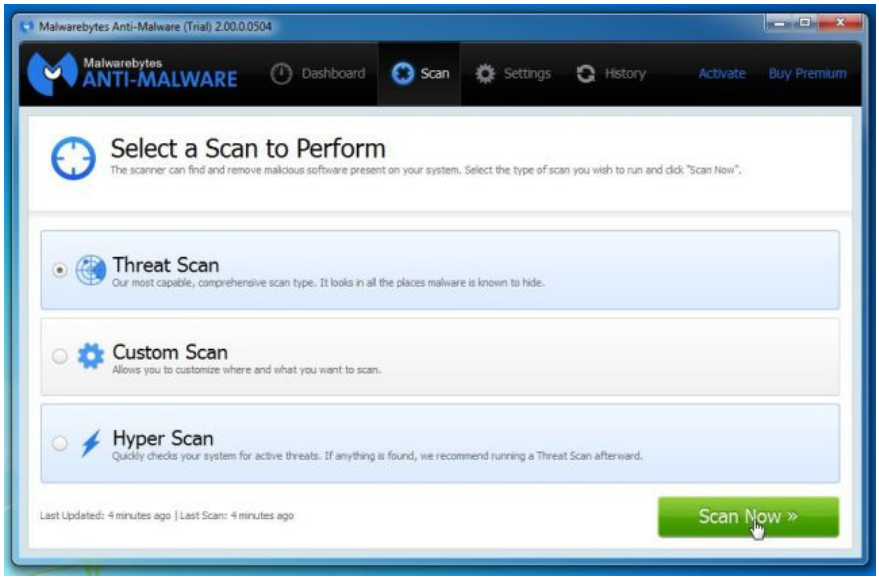
3. Follow the on-screen instructions to install Malwarebytes Anti-Malware Setup Wizard.



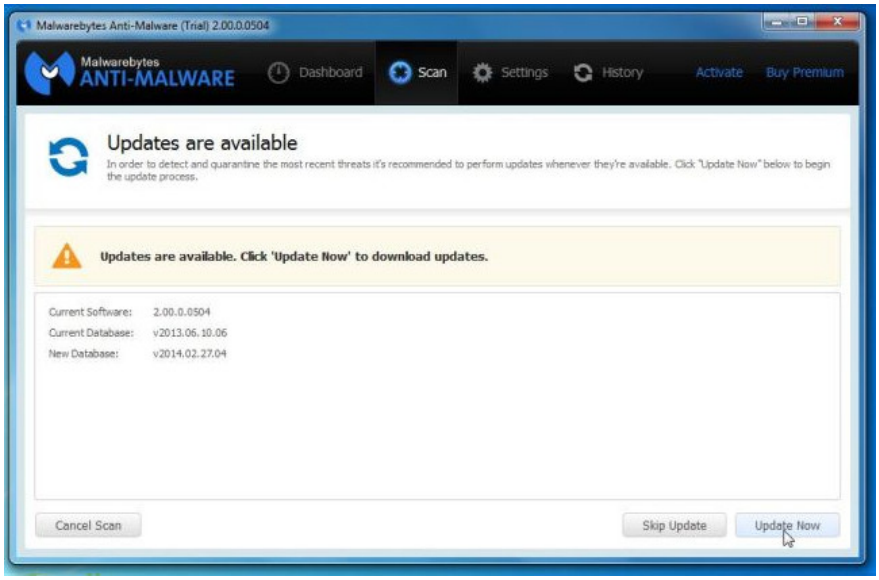
Click **Next** to install Malwarebytes Anti-Malware, until the last window click **Finish** to complete.

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.

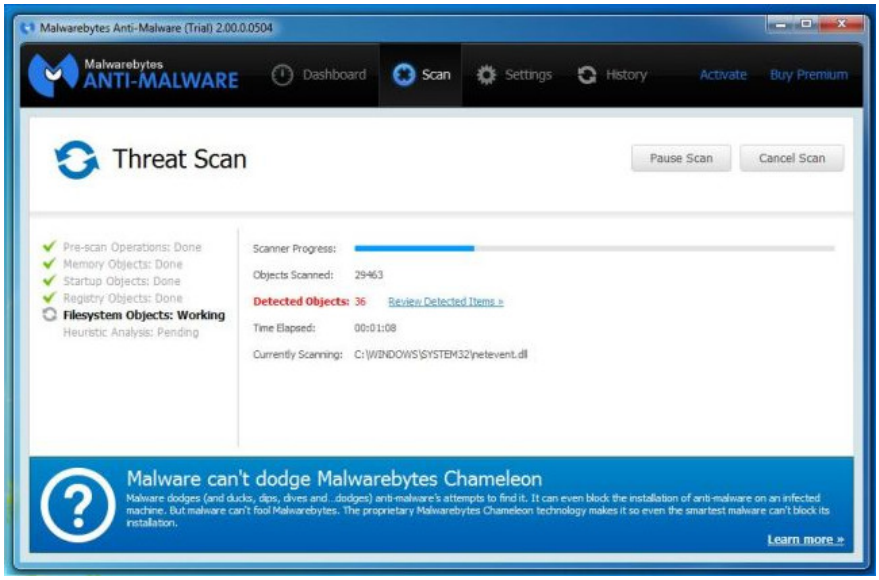
Alternatively, you can click the **Scan tab** and select **Threat Scan** , then click **Scan Now** .



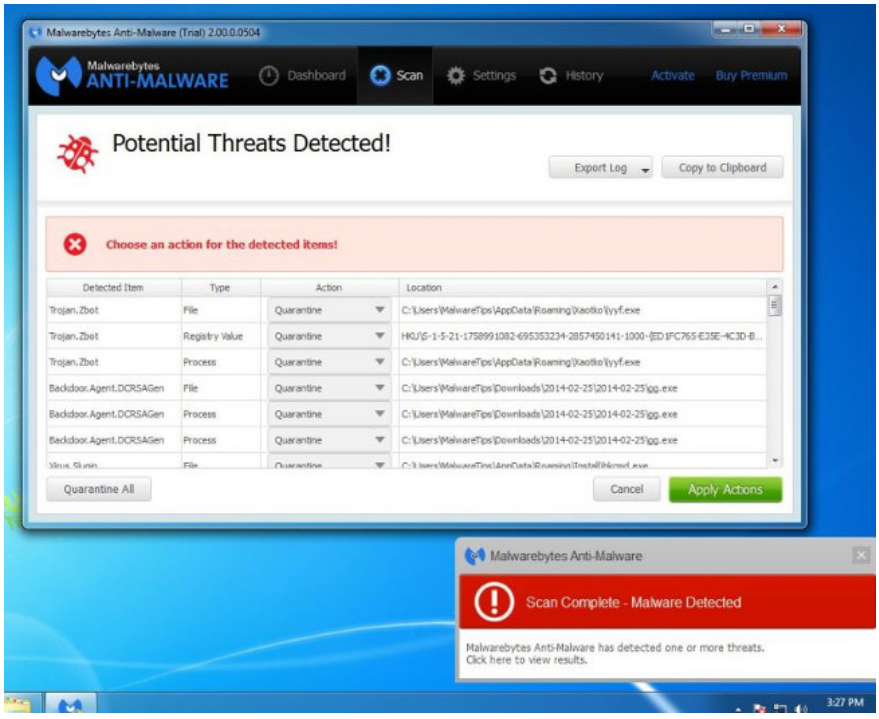
5. Malwarebytes Anti-Malware will start checking for the latest updates. If there are any new updates, click the **Update Now** button.



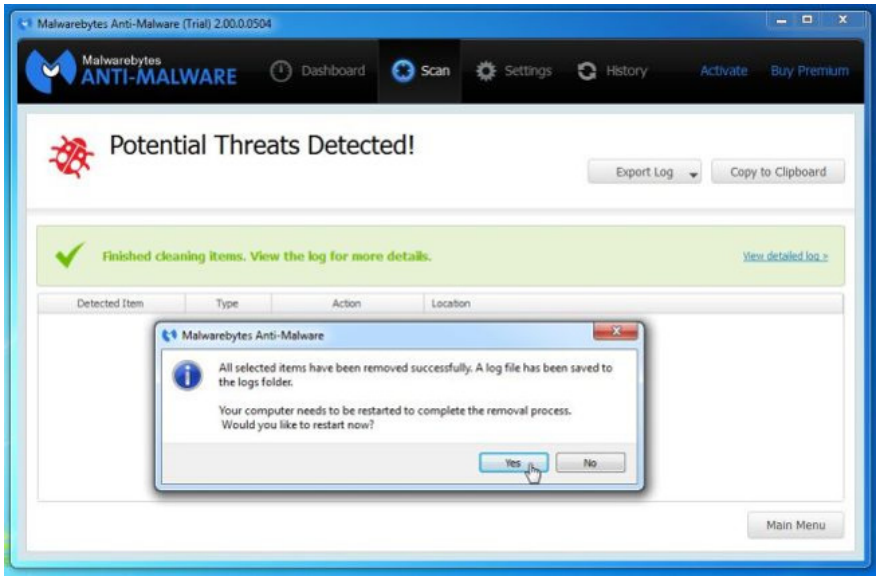
6. Malwarebytes Anti-Malware will start scanning your system to find and remove programs and malware on your system.



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 5: Use HitmanPro to scan the system again

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.

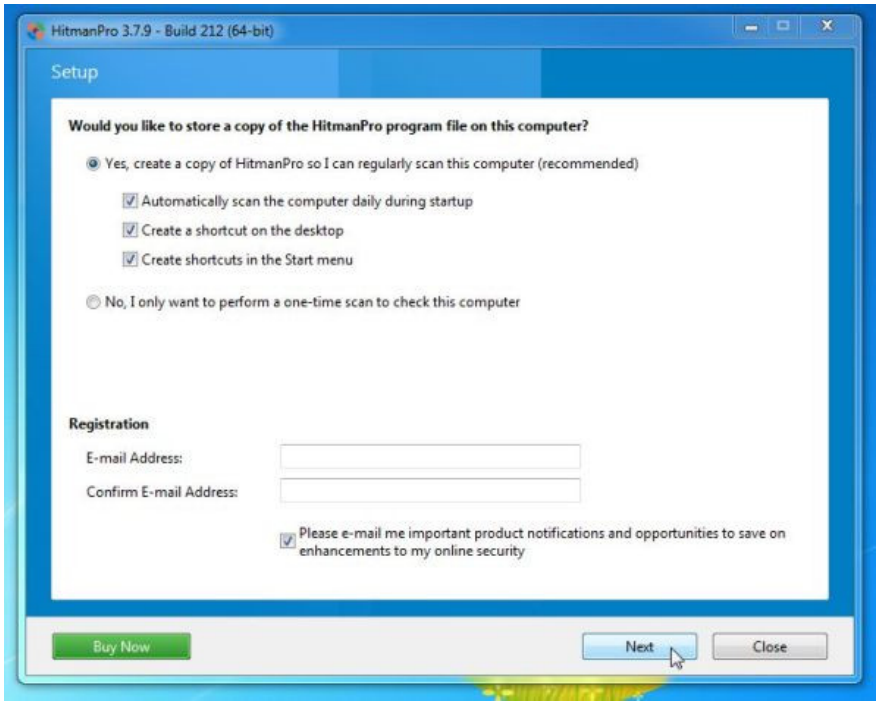
The program will scan your computer at a fairly fast speed (in less than 5 minutes) and never slow down your computer like other antivirus programs.

1. Download HitmanPro to your device and install it.

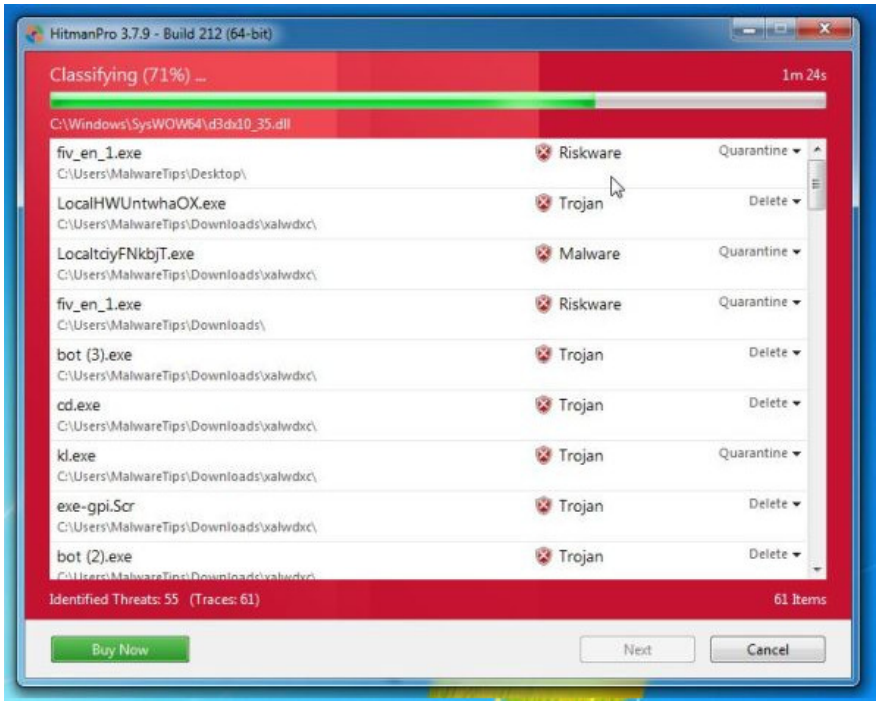
Download HitmanPro to your device and install it here.

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:

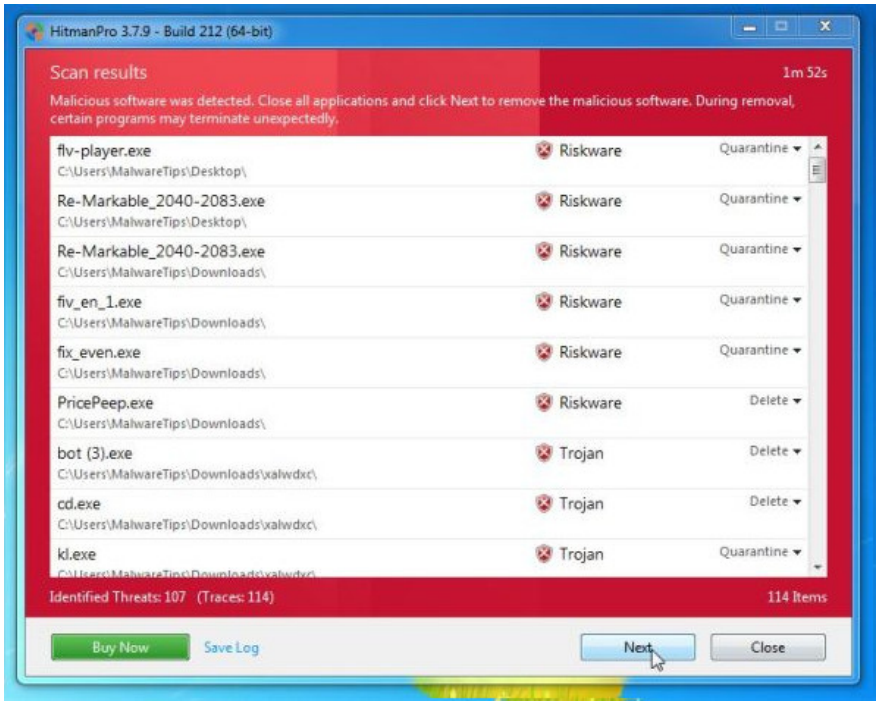
Click **Next** to install HitmanPro on your computer.



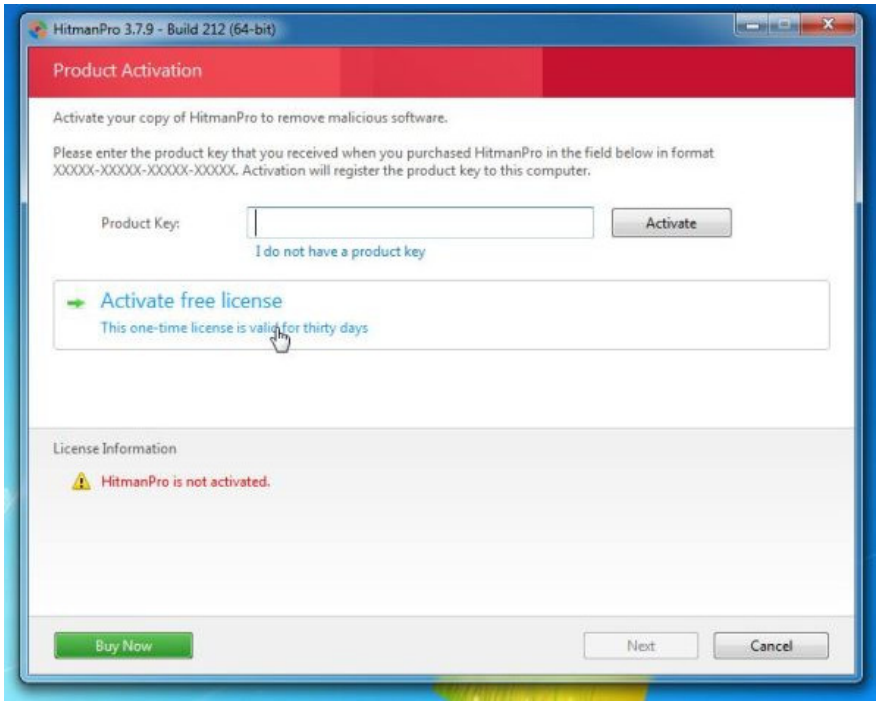
3. And HitmanPro will start the process of scanning the malicious files Interyield.jmp9.com from your computer.



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



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



Refer to some of the following articles:

1. How to remove malicious programs GS.Enabler, SK.Enabler, SK.Enhancer, WS.Enabler?

1. How to remove the original Babylon Toolbar on IE, Chrome and Firefox?

1. To protect your Facebook account in the most private way, read this article

Good luck!

You finished reading the article "**Virus 'interyield jmp9' attacks the system, this is the way to get rid of this virus**" 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.
