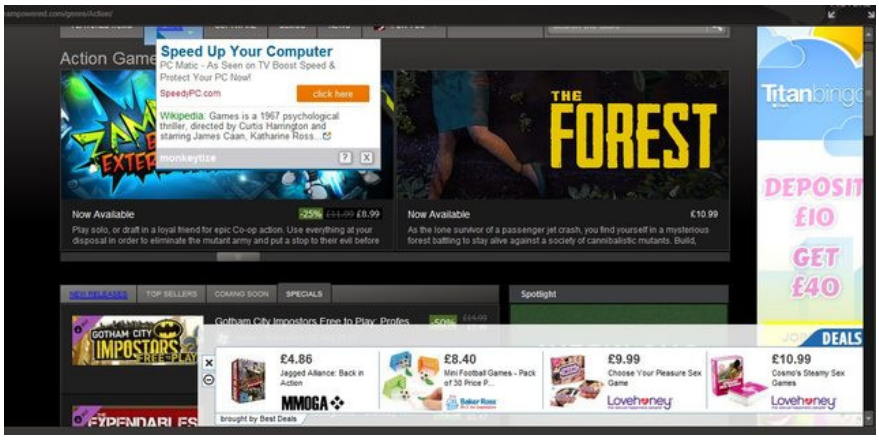
Instructions for removing malware from Steam

If popup windows and advertisements appear on the Steam game platform, chances are that adware and unwanted programs have intruded your system.

If **popup windows** and **advertisements appear on the Steam game platform** , chances are that adware and unwanted programs have " *intruded* " your system illegally. These adware infiltrate your system mainly because it is integrated into free software, programs, and utilities that you download from the Internet, then when you install the software. The software has just been downloaded on the computer and accidentally installed these adware.



Often ads can be items, coupons, . displayed on popup windows or banners.

When Steam is attacked by adware, you may notice:

1. Ads are attached on the website you visit.
2. Content of websites randomly turns into hyperlink.
3. The browser displays popup windows that suggest you to update or install fake software.
4. Unwanted programs are installed on the system without your knowledge.

In addition to displaying ads and collecting data, adware can be the cause of slowing down your computer. In addition, it is also the cause of slow internet connection on the system by downloading ads.

Therefore, when installing any software from the Internet, pay attention to the installation process because the installer will include installation options such as malware and adware. Be careful with what you agree to install.

Always choose the **Custom Installation** option and deselect all that you suspect, especially the software you don't want to install. Choose to download the software on trusted sites.

Remove malware from Steam

Step 1: Use Malwarebytes AdwCleaner to scan the system

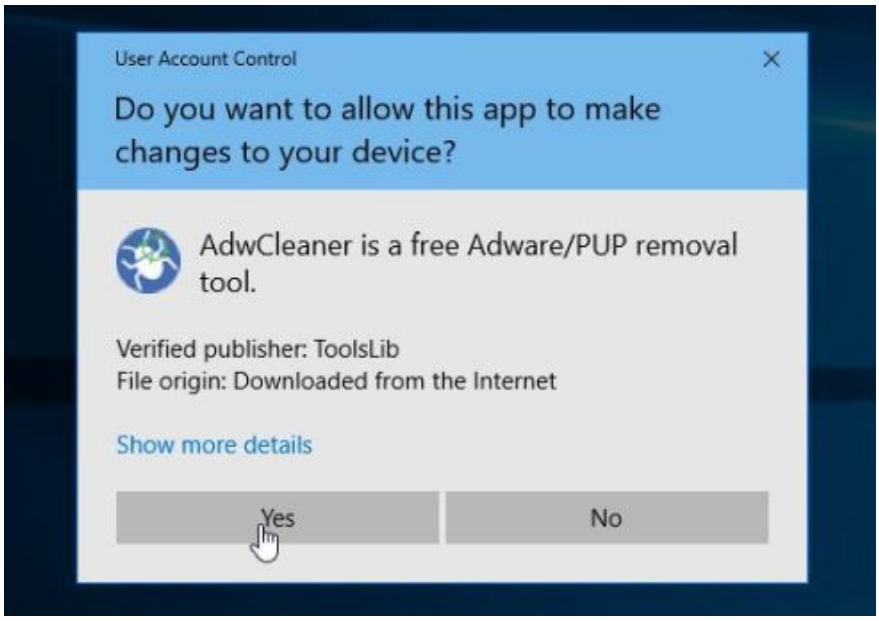
AdwCleaner is a free utility that will scan your system and web browsers to find and remove malware installed on your system.

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

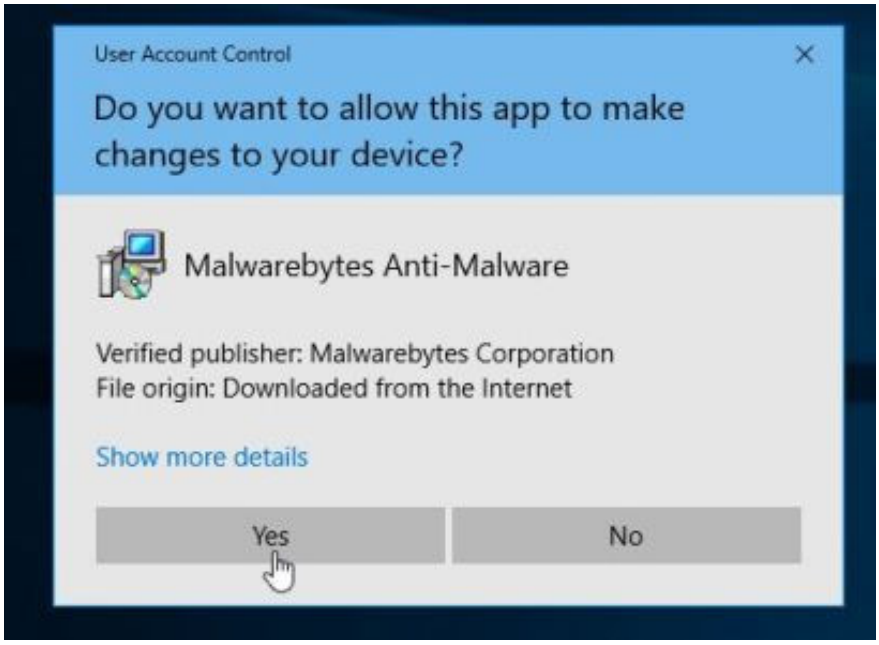
Malwarebytes Anti-Malware is **an on-demand system scan** tool that will remove programs and malware from Steam from your computer. The important thing is that Malwarebytes Anti-Malware will run in parallel with other antivirus software without conflict.

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

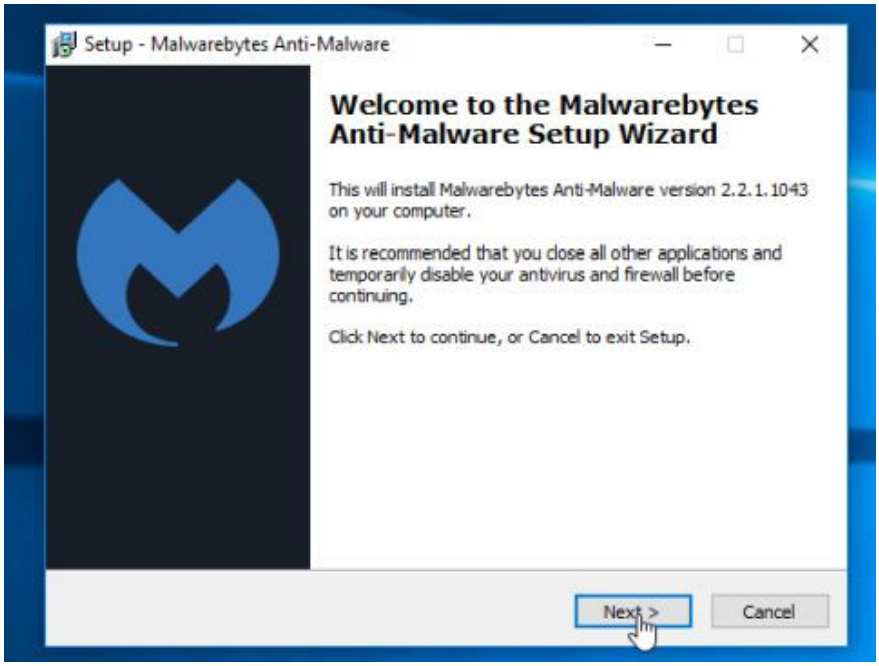
Download Malwarebytes Anti-Malware to your computer and install it here.

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.

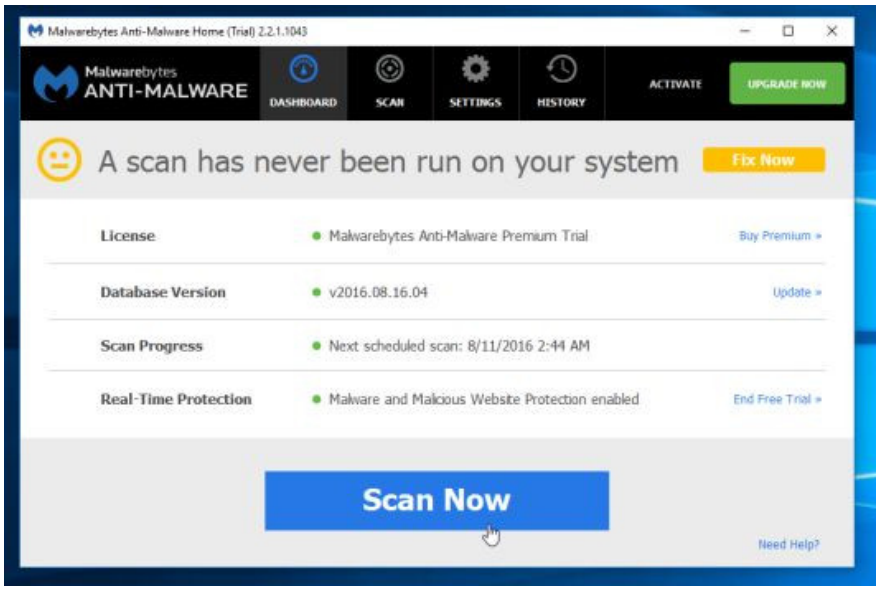


3. Follow the on-screen instructions to install **Malwarebytes Anti-Malware Setup Wizard** .

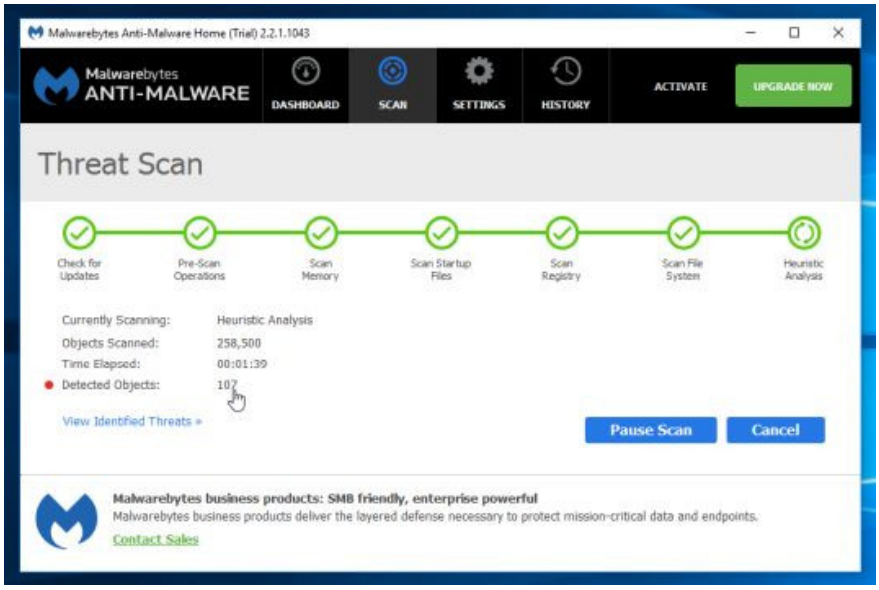


Click Next to install Malwarebytes Anti-Malware, until the last window click **Finish** to complete.

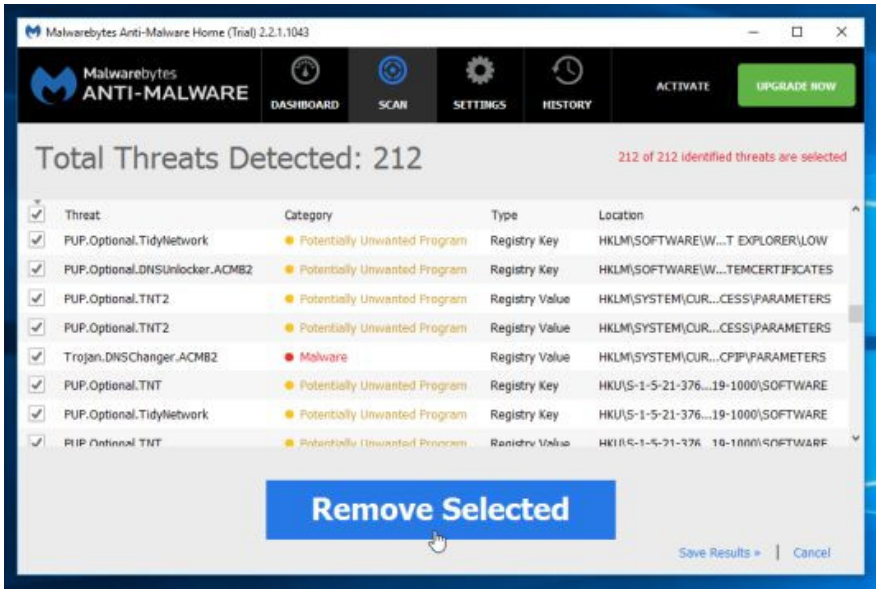
4. After installation is complete, Malwarebytes Anti-Malware will automatically open and update antivirus data. To start the scanning process, click the **Scan Now** button.



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



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: Continue scanning the system 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.

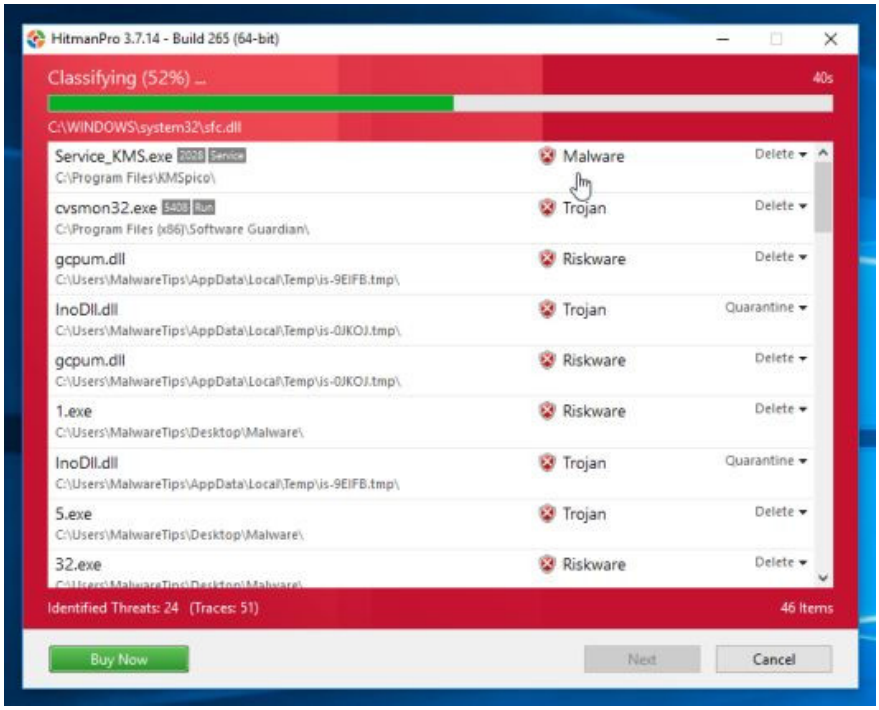
1. Download HitmanPro to your device and install it.

Download HitmanPro to your device and install it here.

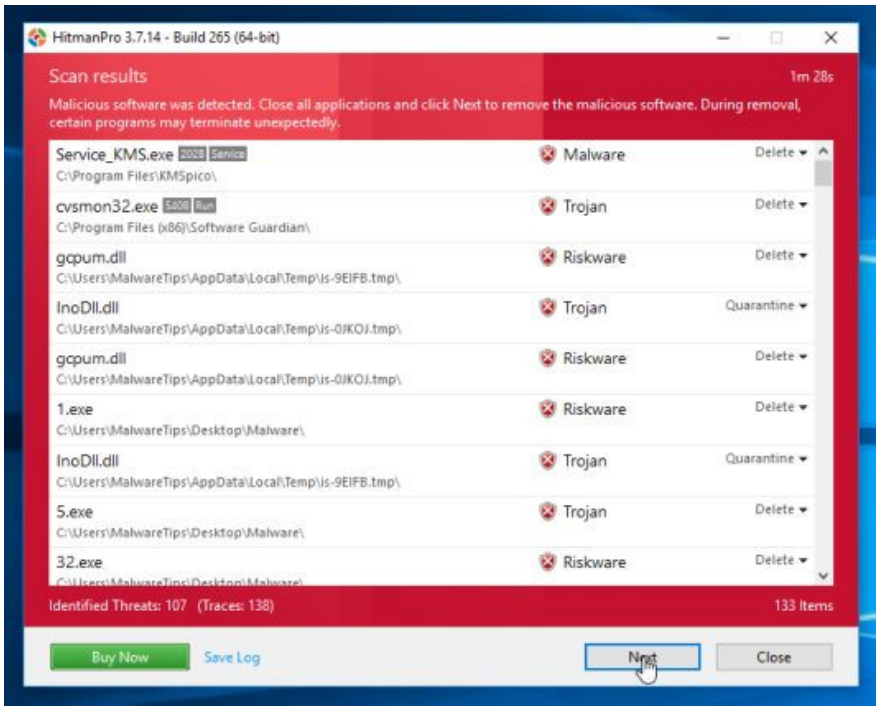
2. Double-click the file named 'HitmanPro.exe' (if using a 32-bit version) or double-click the file '*HitmanPro_x64.exe* ' (if using a 64-bit version).

Click select Next to install HitmanPro on your computer.

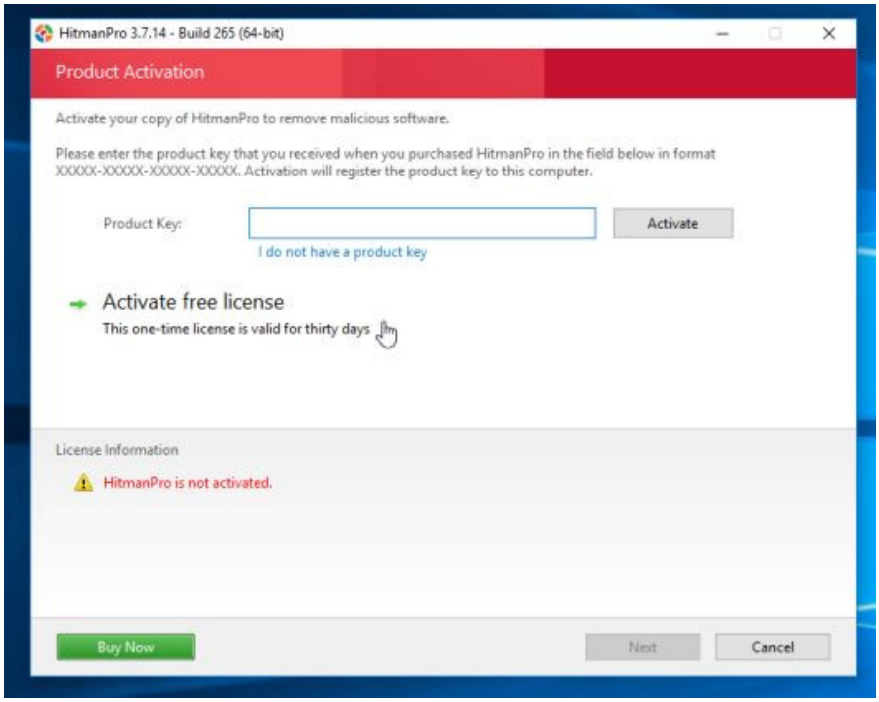
3. And HitmanPro will start the process of scanning malicious programs (malware) on your system.



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.



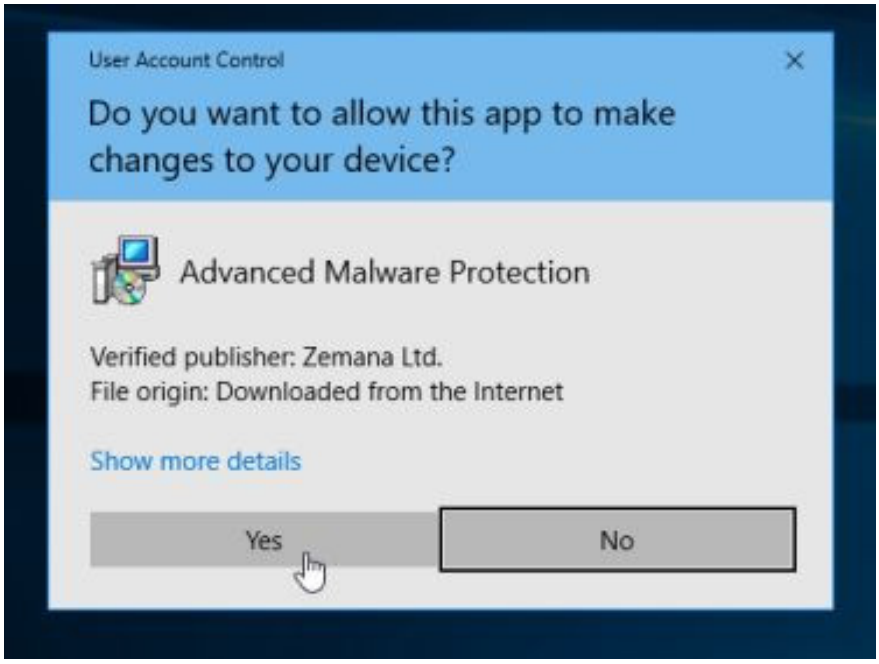
Step 4: Use Zemana AntiMalware to scan the system

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

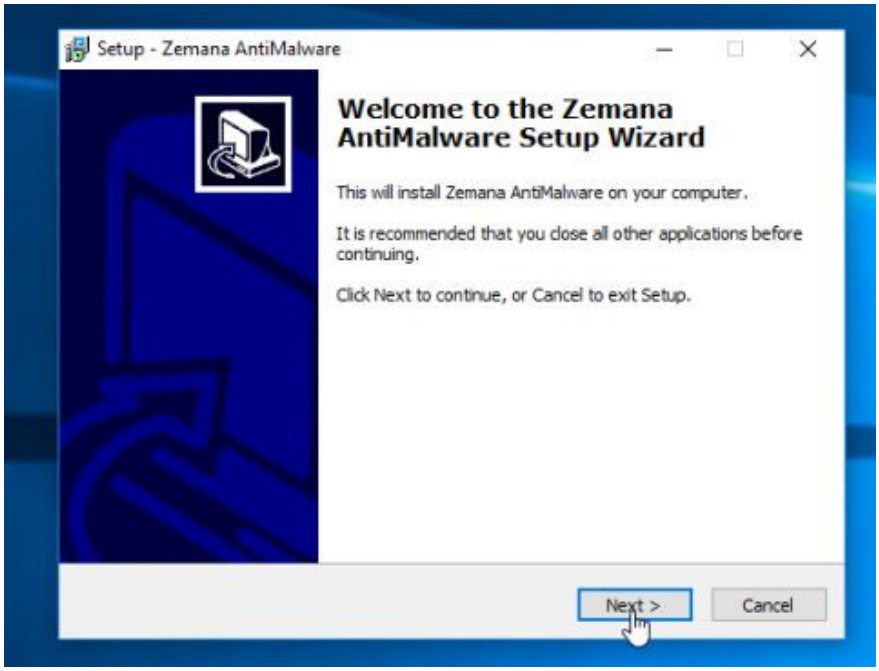
Download Zemana AntiMalware and install it here.

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

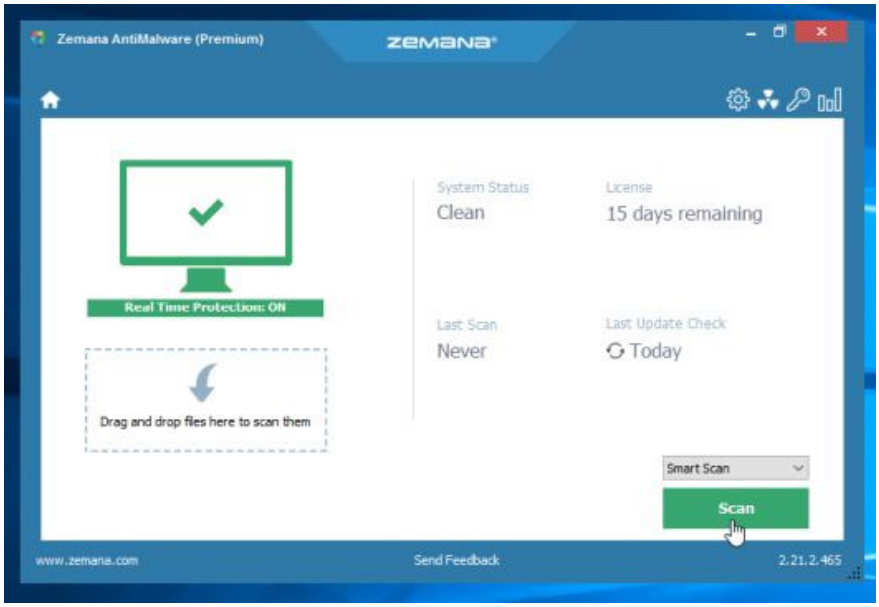
The User Account Control dialog box appears now on the screen asking if you want to run the file. Click Yes to continue the installation process.



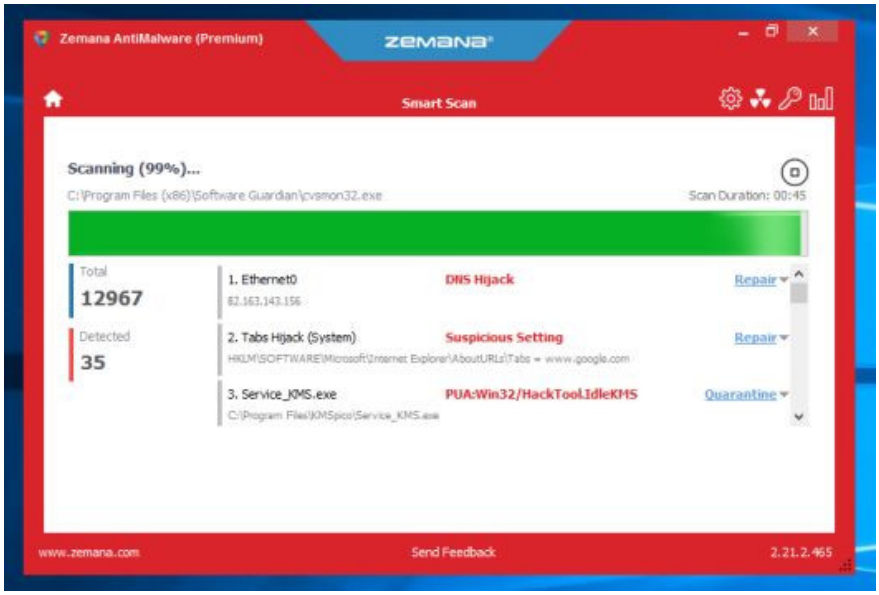
Click **Next** and follow the on-screen instructions to install **Zemana AntiMalware** on your computer.



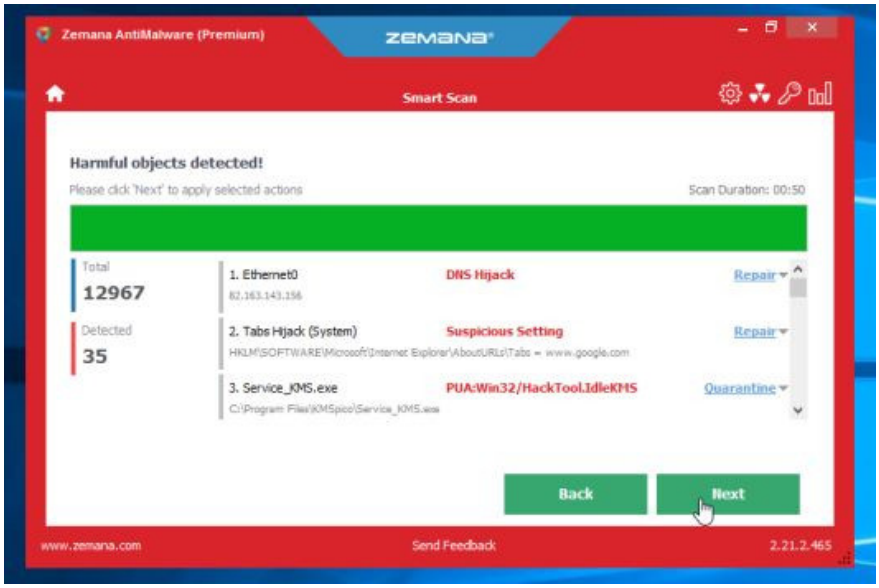
3. When the Zemana AntiMalware window opens, click the **Scan** button.



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



5. When the scan finishes, Zemana AntiMalware will display a list of all detected malicious programs. Click the **Next** button to remove all malicious files from your computer.



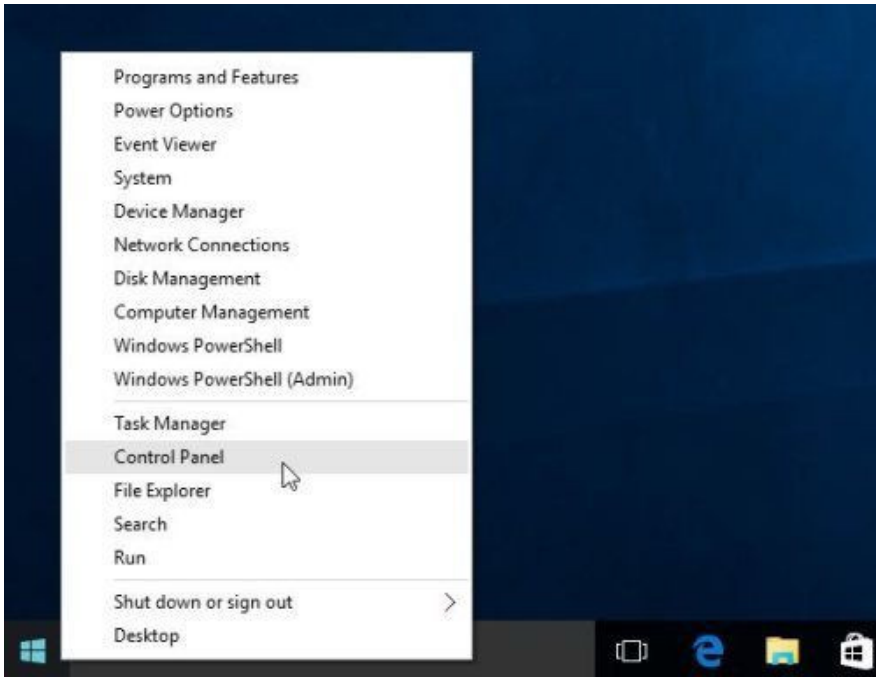
Zemana AntiMalware will remove all malicious files from your computer and will require the system to **reboot** to remove all malicious programs.

Step 5: Reinstall Steam and delete the AppDataLocalSteam folder

1. Uninstall Steam on Windows

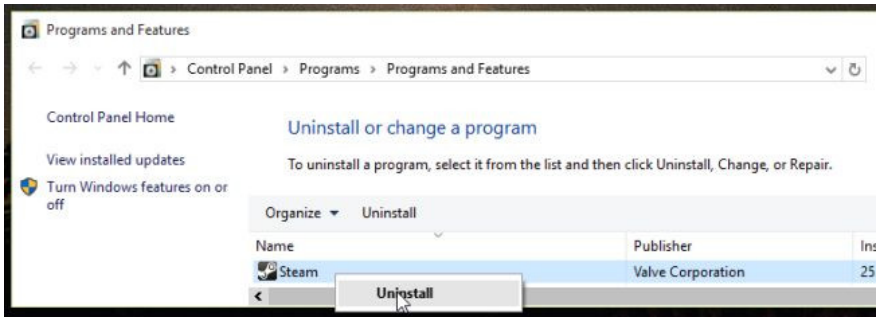
- On Windows 10 or Windows 8:

1. To uninstall any program on Windows 10 or Windows 8 computer, first right-click on the Start button in the top left corner of the screen and then select **Control Panel** .



2. On the Control Panel window, find and click **Uninstall a program** under **Programs** .

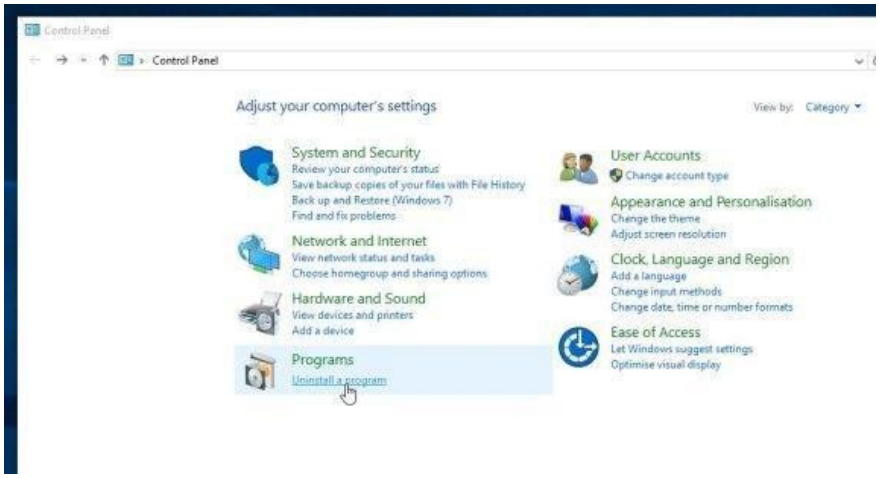
Now the screen shows the **Programs and Features** window, where you scroll down the list of applications, programs installed on the system and uninstall **Steam** and programs of unknown origin.



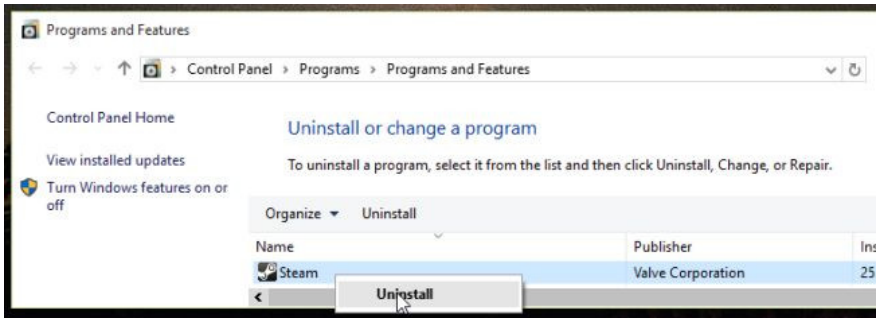
- On Windows 7 and Windows Vista:

1. If you are using Windows 7, Windows Vista or Windows XP, click the **Start** button => **Control Panel.**

2. On the Control Panel window, find and click the **Uninstall a program** option under **Programs** .



Now the screen shows the **Programs and Features** window, where you scroll down the list of applications, programs installed on the system and uninstall Steam and programs of unknown origin.

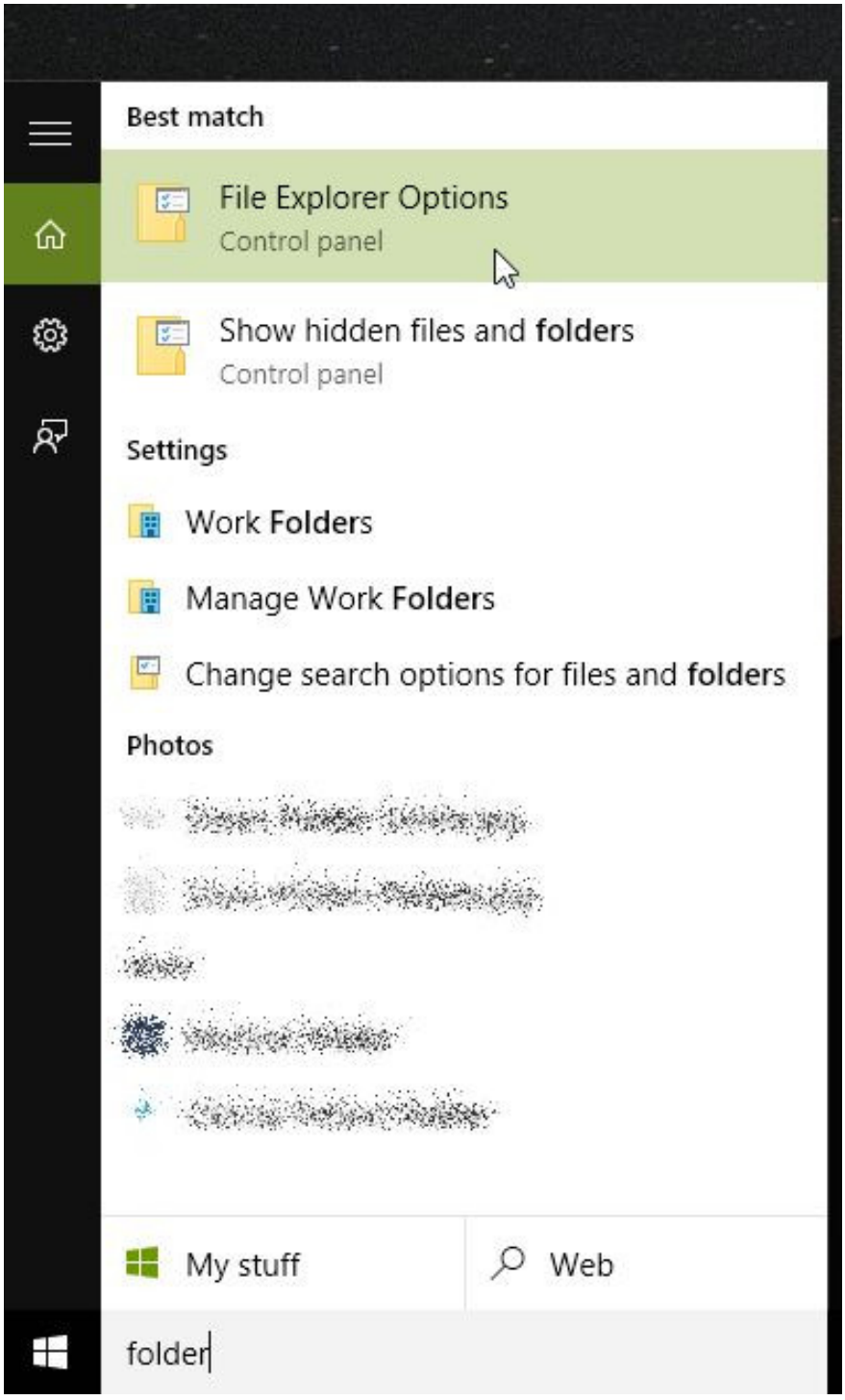


2. The next step to do is **delete the Steam folder** located in C: Users $ USERNAMEAppDataLocalSteam.

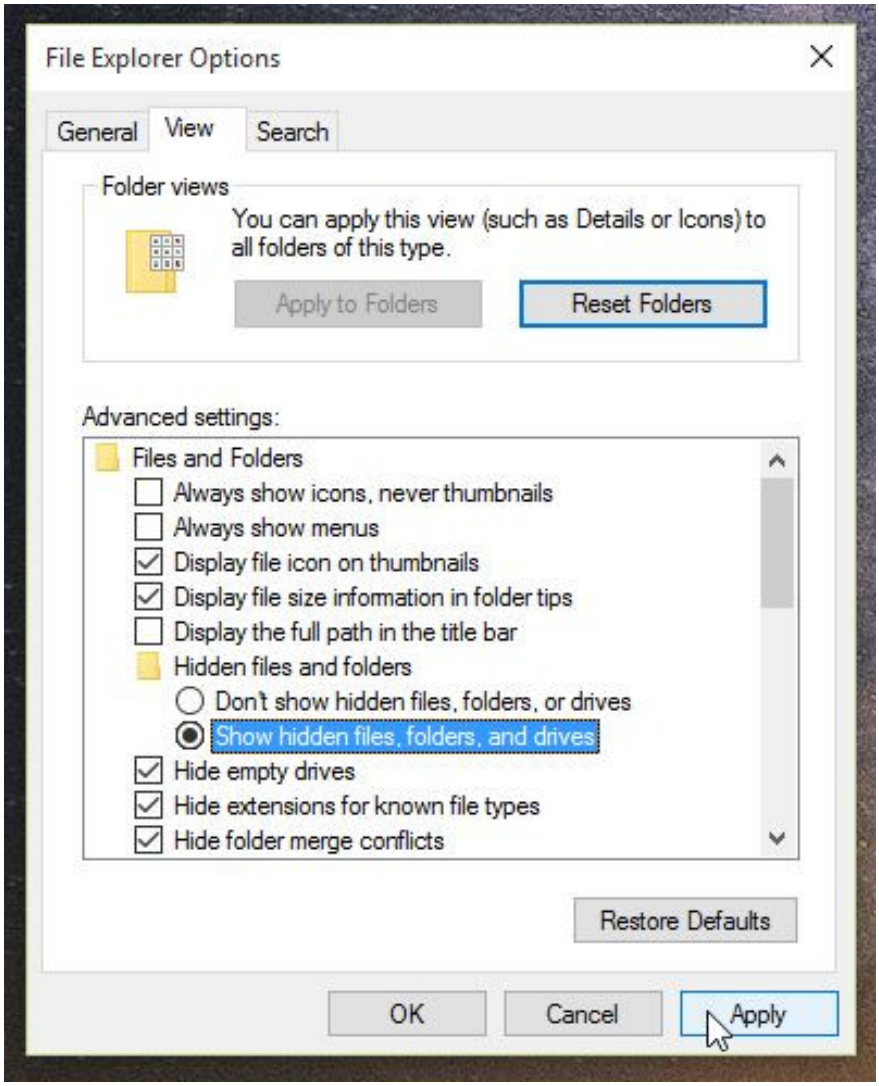
- **Note** : The AppData folder is often hidden, so you must perform additional operations to display the folder.

To do this thing:

1. On Windows 7 or Windows Vista, click **Start => Computer** , then click **Organize** and then click **Folder and Search Options.**
2. On Windows 8 or Windows 10, **enter the folder keyword** in the Search box and then click **Folder Explorer Options** .

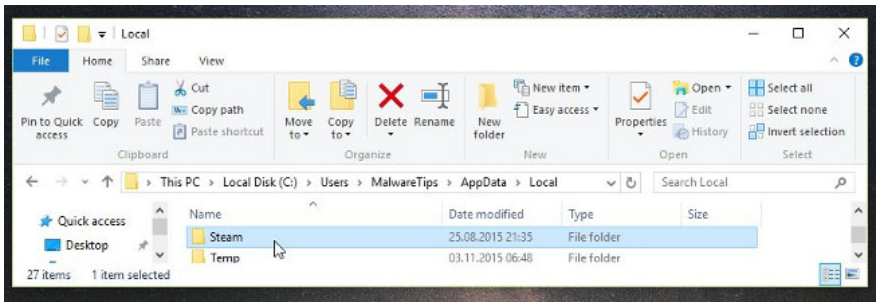


Now the **File Explorer Options** window appears **,** where you click on the View tab, then select **Show hidden files, folders and drives,** then click **Apply => OK** .



In addition, you can refer to detailed steps to hide, show folders and files on Windows 7, 8 and 10 computers here.

3. Now you can see the **AppData** folder, next you navigate to the path: C: Users [Your Username] AppDataLocal then **delete the Steam folder** .



4. Finally, proceed to reinstall **Steam** on your system.

You can download Steam to your device and install it here.

Refer to some of the following articles:

1. Instructions to completely remove Youndoo.com on all browsers

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

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

Good luck!