Prevent virus wmpscfgs.exe

There are a lot of problems when Task Manager always displays the wmpscfgs.exe application, but does not do anything to turn it off, and has a lot of troubles.

There are a lot of problems when Task Manager always displays the wmpscfgs.exe application, but does not do anything to turn it off, and has a lot of troubles.

Symptoms of the system when infected with this virus:

- If the computer has Malwarebytes or Superantispyware, this virus will always be detected. But when you reboot the system, it appears again, even if you scan with safe mode

- Warning Internet Explorer is not the system's default browser, and it is always displayed whether or not you click the IE icon. If you encounter this situation, it's best to move the IE window to the corner of the screen and leave it there.

- The Windows UAC feature does not function properly, constantly asking users when they activate any * .exe or startup application.

- Microsoft Security Essentials identifies system startup programs as viruses.

If your computer has the above symptoms, then 80% of them have been infected with wmpscfgs.exe, and the following are **some tips to prevent this virus** (don't worry or care about security programs). in this situation):

Prevent:

- Start in **safe mode** (simply because the system only uses very few applications in safe mode).

- Set the display mode for all types of hidden and system files in **Tool** > **Folder Options** , check **Show hidden files and folders box** , do not check **Hide Extensions for known file types box**

- Move to the following folder: **C: Program FilesInternet Explorer** and **C: UsersuserAppDataLocalTemp** , you will see the file **wmpscfgs.exe** . Please delete immediately!

- Open **Task Manager** , select **show all processes** , find the application called **wmpscfgs.exe** , if it is active then **Kill** .

- Next, open regedit and find the following key: **HKLM** -> **Software** -> **Microsoft** -> **Windows** -> **CurrentVersion** -> **Run**

- Find the keyword ' **Adobe_reader** ' with **% ProgramFiles% Internet** related data **Explorerwmpscfgs.exe** , delete it. However, for some cases without this key, this is why the virus comes back after every reboot.

- You must check each installation program in the system, all information is stored in the **HKLM** key -> **Software** -> **Microsoft** -> **Windows** -> **CurrentVersion** -> **Run** , look carefully in all the storage keys Here, if you see the occurrence of wmpscfgs.exe, continue deleting.

- On the other hand, the virus can automatically rename from **mcagent.exe** to **mcagent .exe** (there is space between the name and the exe extension). Next, it will continue to automatically replicate with the same name every time a user activates an application, which means it will replicate before the user executes any program. And it will repeat this with all applications in the system's RUN key.

- If you find the path of mcagent.exe, you will see 2 or 3 * .exe files with the same name:

+ **mcagent.exe** > capacity about 39 KB, newly created by wmpscfgs.exe
+ **mcagent .exe** > is the original file of mcagent renamed
+ **mcagent.exe.delme** (comes with a random number or some)> deletes this file

- First, delete the suspended applications - corresponding, of or related to the above infectious file in **Task Manager** , then manually delete the * .exe files with a capacity of ~ 39 KB and rename the remaining files to their original names. Repeat the above step for each application found in **RUN** . The only thing this virus does not infect is the **windows defender** application. Removing or reinstalling the entire application cannot erase the infected files in the directory, and that's why Microsoft Security Essentials identifies all startup applications - a virus startup.

- After completing the above steps, restart the system. Then recheck the entire application in Task Manager, if there are any " *suspicious* " programs, just repeat the above step.

Good luck!

You finished reading the article "**Prevent virus wmpscfgs.exe**" 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.
