Instructions for finding and deleting the original Keylogger from your computer

Keyloggers are extremely dangerous programs that hackers install on any user's system for the purpose of stealing passwords, credit card information, etc. Keyloggers store all keystrokes that users use. work on your computer and provide hackers with important user information.

Keyloggers are extremely dangerous programs that hackers install on any user's system for the purpose of stealing passwords, credit card information, etc. Keyloggers store all keystrokes that users use. work on your computer and provide hackers with important user information.

Each type of keylogger is dangerous because they can record your keystroke, keep track of your activities, and be able to record Open sites.

If you are using a computer with Keylogger installed, it means that your important information can be easily stolen. Therefore it is best to check if your computer has a Keylogger installed. In the following article, Network Administrator will show you how to find and remove root keylogger on your system.

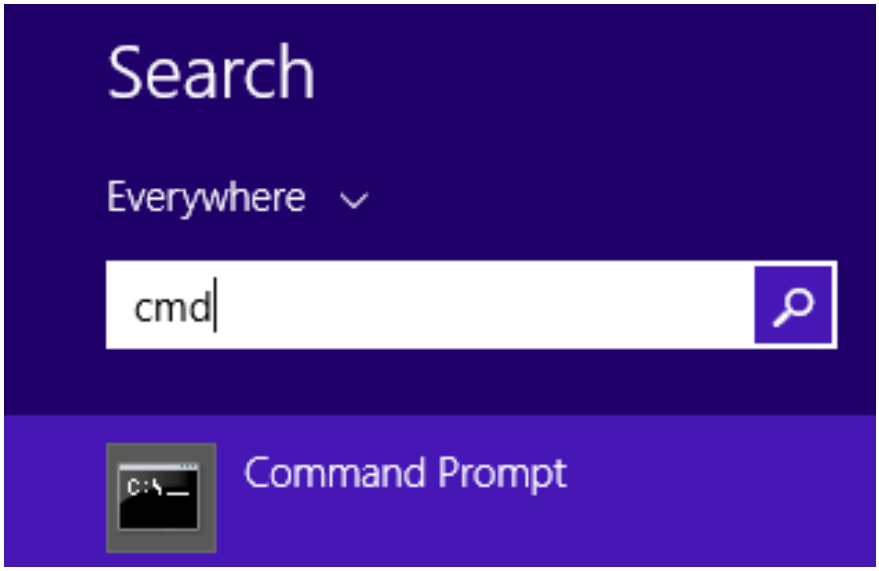
If you don't know much about keyloggers, don't skip this article: Learn about keyloggers

How to find and delete keyloggers on your computer

1. Find and remove Keylogger with Task Manager

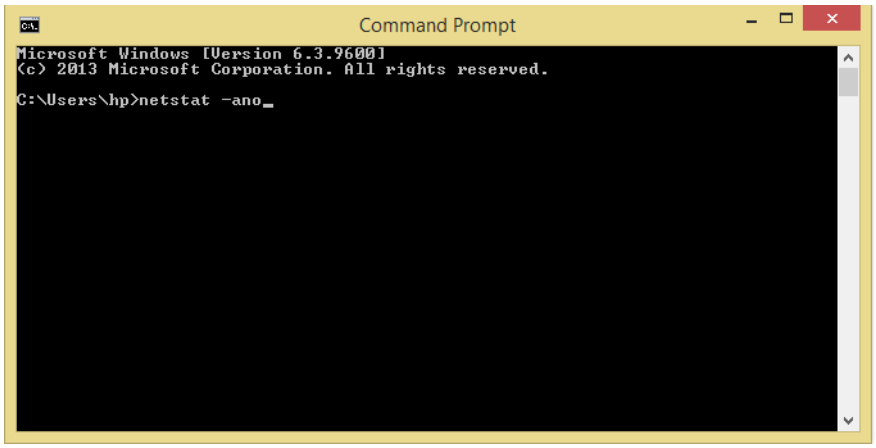
Using Task Manager to detect if Keylogger is installed on your system, you simply need to follow the steps below:

First open the Command Prompt by entering **cmd** in the Search box on the Start Menu and then clicking **Command Prompt** on the list of search results.

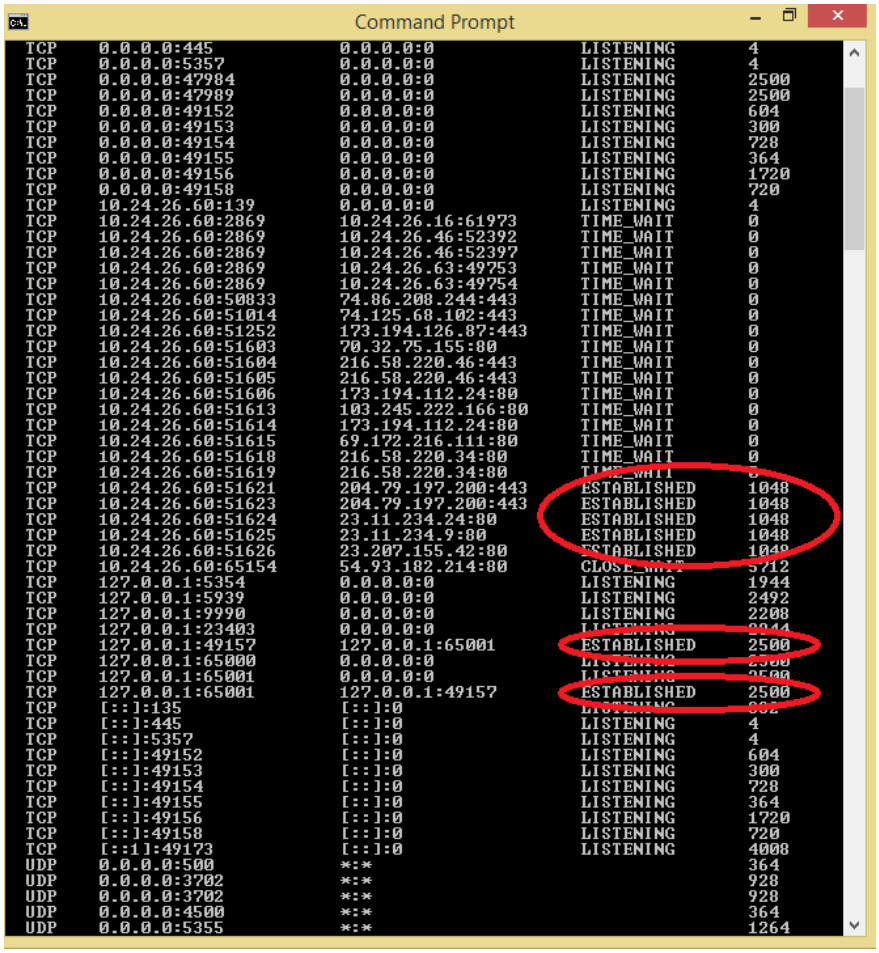


Next, on the Command Prompt window, enter the command below and press Enter:

```
netstat -ano
```



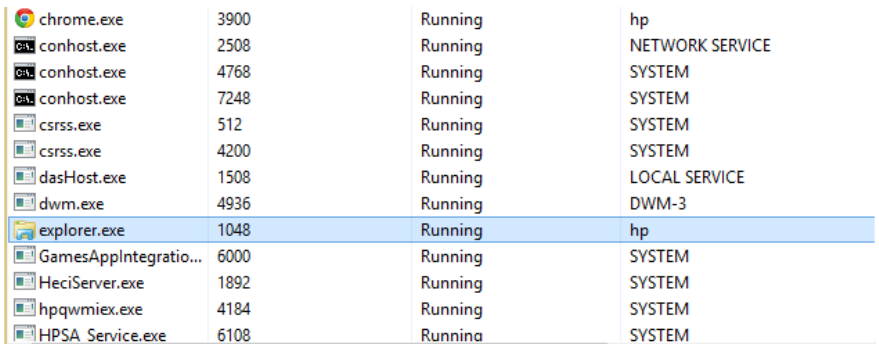
At this time, the Command Prompt window will display as shown below:



The data you receive will display in 5 columns. You only need to pay attention to the lines set to **Established** .

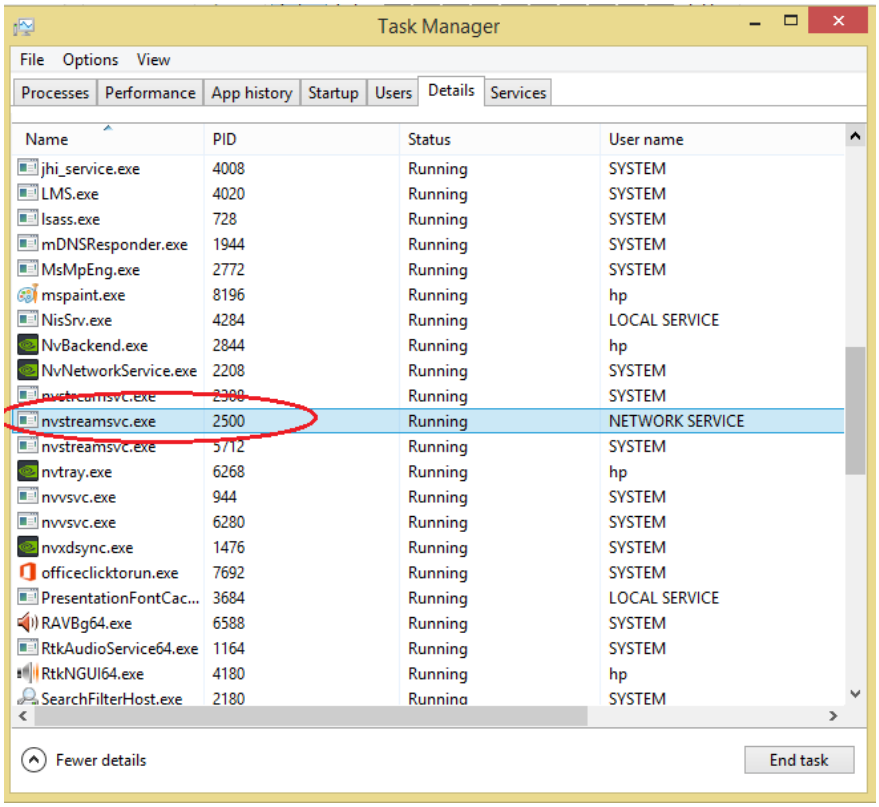
In the above illustration, you will see that the 2 PIDs are set to Established, the first value is 1048 and the second value is 2500.

Next open Task Manager and access the **Details** tab.



Now you can see that explorer.exe has the ID of value 1048. However, this is an important system service, so it can be confirmed that this is a safe program, not a keylogger.

Next go back to the Task Manager window again and find the process with 2500 PID.



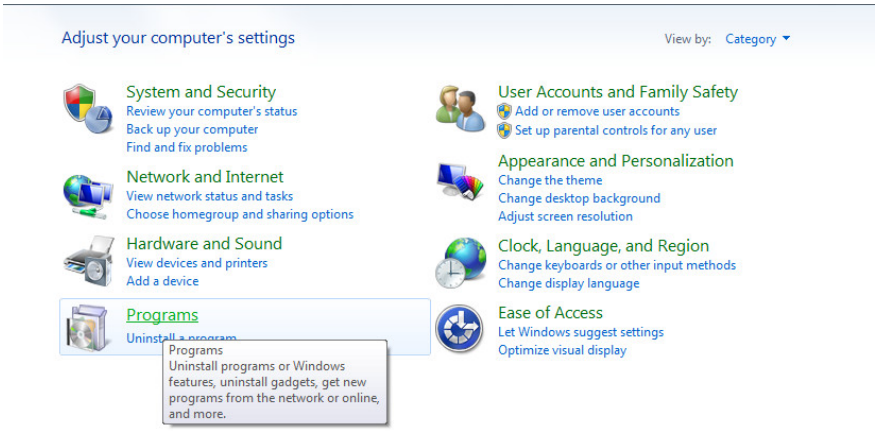
You will see nvstreamsvc.exe has an ID of 2500. However, after finding out, nvstreamsvc.exe is a program installed by nvidia with a graphics card. Therefore it can be confirmed that the system does not have any keyloggers installed.

Follow the same steps to check if your system has any keyloggers installed.

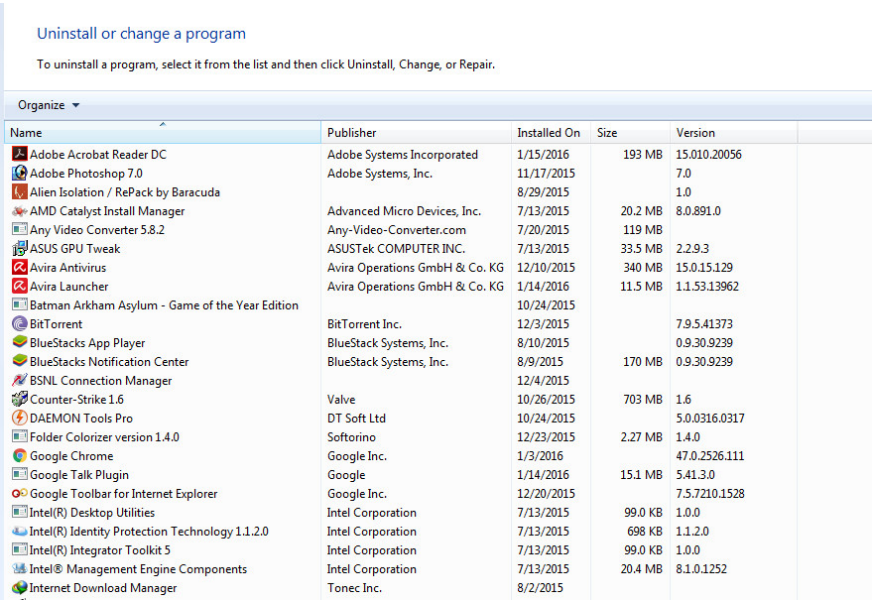
2. Find Keylogger through installed programs

Sometimes in some cases keyloggers can be found in the programs you install on the system, if the hackers are not hiding these programs.

1. You go to **Start => Control Panel** .
2. On the Control Panel window, click **Programs and Features** or **Uninstall a program** .



Now on the screen, a list of all the programs you have installed is displayed. If you discover any programs that you do not install, it is likely that those programs are installed by hackers. Right-click the program and select **Uninstall** .



When these programs are removed, the keylogger will also be removed from your system, and you are now in a "safe" state.

3. Software to detect keyloggers on computers

In some cases, users can apply the solution thanks to the support of the 3rd application to remove the root keylogger on their system. Currently there are many **Anti-Rootkit** tools available on the market, but the most effective tool is worth mentioning.

Here are 3 of the best tools you can consult:

- Malwarebytes Anti-Rootkit Beta:

Malwarebytes Anti-Rootkit Beta (MBAR) is a free tool designed to help users quickly detect and remove Rootkis - types of malware that operate in hidden and sophisticated mode on the system.

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

- Norton Power Eraser:

Norton Power Eraser is a simple solution for detecting and removing criminal software and viruses that, when using traditional methods, are undetectable.

Download the device and install it here.

- Kaspersky Security Scan:

Kaspersky Security Scan is able to scan the system with extremely fast speed, enabling you to check whether there are viruses, malware or spyware on your system to find a way to destroy the virus in time. and these malicious software.

Download Kaspersky Security Scan to your device and install it here.

4. Other measures

If you have done the above but still suspect that the keylogger is installed on your computer, you can use **safe mode with networking** to work. To enter safe mode with networking, press F8 when turning on the device and use the arrow keys to find this mode, then press Enter to select. When you access **safe mode with networking,** you are only allowed to run files on your operating system and stop all other activities, so the keyloggers installed on your computer will no longer be able to track you.

This is one of the extremely useful features that you should not ignore.

5. Useful tips to deal with keylogger

There are some keyloggers that are very dangerous, they can only be detected using professional methods. Therefore, to keep the data safe before the keylogger you should use notepad while entering your username and password into the login form. Save the username and password into notepad and copy it to your browser. Because some keyloggers do not have the right to record keyboard operations of notepad.

If you have sensitive, important data stored on your computer, they need to be protected from these keyloggers. It takes a lot of time to find and detect keyloggers because it can come from the Internet because many software is downloaded from many unofficial websites. Finding safe software downloads is also worth your attention, and when installing the software make sure you monitor the entire process so you don't get unwanted tools installed.

Refer to some of the following articles:

1. How to find out if your computer has Keylogger?

2. How to block Windows 10 from collecting user information?

1. How to create Keylogger with Notepad

1. How do hackers attack your Facebok account and how to prevent this process?

Good luck!