

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](#)

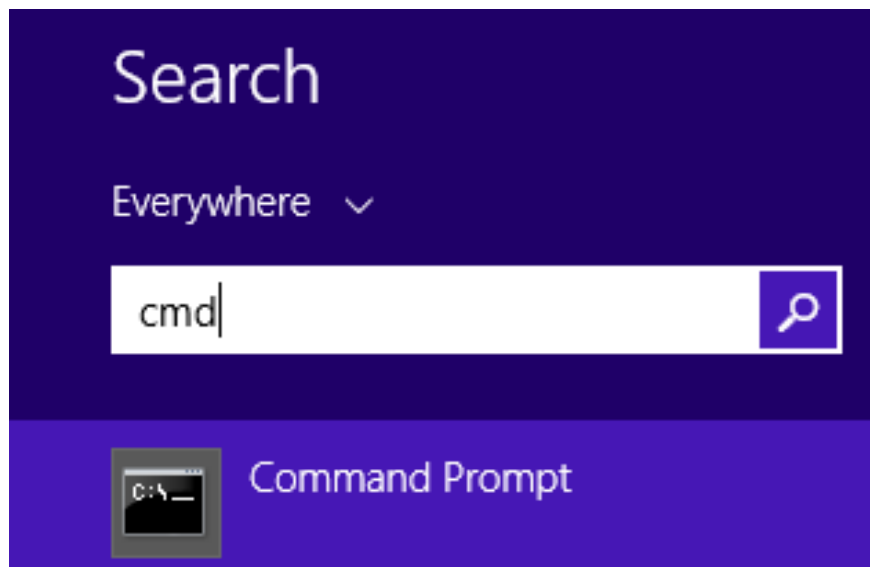
How to find and delete keyloggers on your computer

1. Find and remove Keylogger with Task Manager
2. Find Keylogger through installed programs
3. Software to detect keyloggers on computers
4. Other measures
5. Useful tips to deal with keylogger

1. Find and remove Keylogger with Task Manager

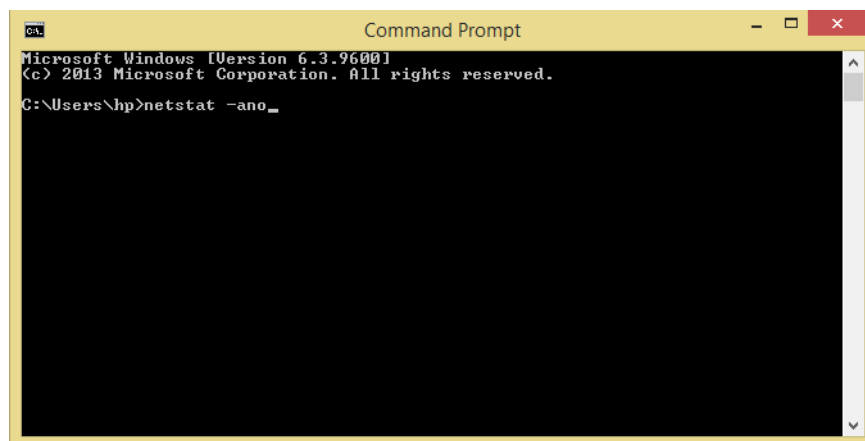
Using Task Manager to detect if Keylogger is installed on your system, you simply need to follow the steps below:

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:

```

Command Prompt
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:47984 0.0.0.0:0 LISTENING 2500
TCP 0.0.0.0:47989 0.0.0.0:0 LISTENING 2500
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING 604
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING 300
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING 728
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING 364
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING 1720
TCP 0.0.0.0:49158 0.0.0.0:0 LISTENING 720
TCP 10.24.26.60:139 0.0.0.0:0 LISTENING 4
TCP 10.24.26.60:2869 10.24.26.16:61973 TIME_WAIT 0
TCP 10.24.26.60:2869 10.24.26.46:52392 TIME_WAIT 0
TCP 10.24.26.60:2869 10.24.26.46:52397 TIME_WAIT 0
TCP 10.24.26.60:2869 10.24.26.63:49753 TIME_WAIT 0
TCP 10.24.26.60:2869 10.24.26.63:49754 TIME_WAIT 0
TCP 10.24.26.60:50033 74.86.208.244:443 TIME_WAIT 0
TCP 10.24.26.60:51014 74.125.60.102:443 TIME_WAIT 0
TCP 10.24.26.60:51252 173.194.126.87:443 TIME_WAIT 0
TCP 10.24.26.60:51603 70.32.95.155:80 TIME_WAIT 0
TCP 10.24.26.60:51604 216.58.220.46:443 TIME_WAIT 0
TCP 10.24.26.60:51605 216.58.220.46:443 TIME_WAIT 0
TCP 10.24.26.60:51606 173.194.112.24:80 TIME_WAIT 0
TCP 10.24.26.60:51613 103.245.222.166:80 TIME_WAIT 0
TCP 10.24.26.60:51614 173.194.112.24:80 TIME_WAIT 0
TCP 10.24.26.60:51615 69.172.216.111:80 TIME_WAIT 0
TCP 10.24.26.60:51618 216.58.220.34:80 TIME_WAIT 0
TCP 10.24.26.60:51619 216.58.220.34:80 TIME_WAIT 0
TCP 10.24.26.60:51621 204.79.197.200:443 ESTABLISHED 1048
TCP 10.24.26.60:51623 204.79.197.200:443 ESTABLISHED 1048
TCP 10.24.26.60:51624 23.11.234.24:80 ESTABLISHED 1048
TCP 10.24.26.60:51625 23.11.234.9:80 ESTABLISHED 1048
TCP 10.24.26.60:51626 23.207.155.42:80 ESTABLISHED 1048
TCP 10.24.26.60:65154 54.93.182.214:80 CLOSE_WAIT 5712
TCP 127.0.0.1:5354 0.0.0.0:0 LISTENING 1944
TCP 127.0.0.1:5939 0.0.0.0:0 LISTENING 2492
TCP 127.0.0.1:9990 0.0.0.0:0 LISTENING 2208
TCP 127.0.0.1:23403 0.0.0.0:0 LISTENING 8044
TCP 127.0.0.1:49157 127.0.0.1:65001 ESTABLISHED 2500
TCP 127.0.0.1:65000 0.0.0.0:0 LISTENING 2500
TCP 127.0.0.1:65001 0.0.0.0:0 LISTENING 2500
TCP 127.0.0.1:65001 127.0.0.1:49157 ESTABLISHED 2500
TCP [::]:135 [::]:0 LISTENING 808
TCP [::]:445 [::]:0 LISTENING 4
TCP [::]:5357 [::]:0 LISTENING 4
TCP [::]:49152 [::]:0 LISTENING 604
TCP [::]:49153 [::]:0 LISTENING 300
TCP [::]:49154 [::]:0 LISTENING 728
TCP [::]:49155 [::]:0 LISTENING 364
TCP [::]:49156 [::]:0 LISTENING 1720
TCP [::]:49158 [::]:0 LISTENING 720
TCP [::]:49173 [::]:0 LISTENING 4008
UDP 0.0.0.0:5000 *: * 364
UDP 0.0.0.0:3702 *: * 928
UDP 0.0.0.0:3702 *: * 928
UDP 0.0.0.0:4500 *: * 364
UDP 0.0.0.0:5355 *: * 1264

```

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

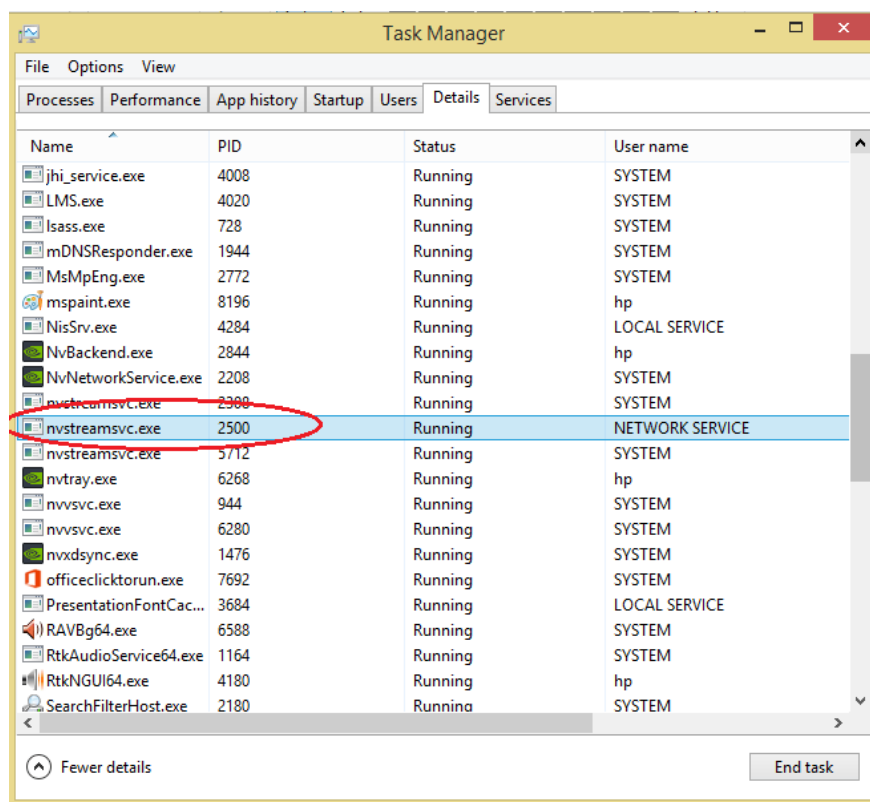
In the above illustration, you will see that the 2 PIDs are set to Established, the first value is 1048 and the second value is 2500.

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

chrome.exe	3900	Running	hp
conhost.exe	2508	Running	NETWORK SERVICE
conhost.exe	4768	Running	SYSTEM
conhost.exe	7248	Running	SYSTEM
csrss.exe	512	Running	SYSTEM
csrss.exe	4200	Running	SYSTEM
dasHost.exe	1508	Running	LOCAL SERVICE
dwm.exe	4936	Running	DWM-3
explorer.exe	1048	Running	hp
GamesAppIntegratio...	6000	Running	SYSTEM
HeciServer.exe	1892	Running	SYSTEM
hpqwmiex.exe	4184	Running	SYSTEM
HPSA Service.exe	6108	Running	SYSTEM

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**.

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Adobe Acrobat Reader DC	Adobe Systems Incorporated	1/15/2016	193 MB	15.010.20056
Adobe Photoshop 7.0	Adobe Systems, Inc.	11/17/2015		7.0
Alien Isolation / RePack by Baracuda		8/29/2015		1.0
AMD Catalyst Install Manager	Advanced Micro Devices, Inc.	7/13/2015	20.2 MB	8.0.891.0
Any Video Converter 5.8.2	Any-Video-Converter.com	7/20/2015	119 MB	
ASUS GPU Tweak	ASUSTek COMPUTER INC.	7/13/2015	33.5 MB	2.2.9.3
Avira Antivirus	Avira Operations GmbH & Co. KG	12/10/2015	340 MB	15.0.15.129
Avira Launcher	Avira Operations GmbH & Co. KG	1/14/2016	11.5 MB	1.1.53.13962
Batman Arkham Asylum - Game of the Year Edition		10/24/2015		
BitTorrent	BitTorrent Inc.	12/3/2015		7.9.5.41373
BlueStacks App Player	BlueStack Systems, Inc.	8/10/2015		0.9.30.9239
BlueStacks Notification Center	BlueStack Systems, Inc.	8/9/2015	170 MB	0.9.30.9239
BSNL Connection Manager		12/4/2015		
Counter-Strike 1.6	Valve	10/26/2015	703 MB	1.6
DAEMON Tools Pro	DT Soft Ltd	10/24/2015		5.0.0316.0317
Folder Colorizer version 1.4.0	Softorino	12/23/2015	2.27 MB	1.4.0
Google Chrome	Google Inc.	1/3/2016	47.0.2526.111	
Google Talk Plugin	Google	1/14/2016	15.1 MB	5.41.3.0
Google Toolbar for Internet Explorer	Google Inc.	12/20/2015		7.5.7210.1528
Intel(R) Desktop Utilities	Intel Corporation	7/13/2015	99.0 KB	1.0.0
Intel(R) Identity Protection Technology 1.1.2.0	Intel Corporation	7/13/2015	698 KB	1.1.2.0
Intel(R) Integrator Toolkit 5	Intel Corporation	7/13/2015	99.0 KB	1.0.0
Intel Management Engine Components	Intel Corporation	7/13/2015	20.4 MB	8.1.0.1252
Internet Download Manager	Tonec Inc.	8/2/2015		

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 Rootkits - 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 Facebook account and how to prevent this process?

Good luck!

You finished reading the article "**Instructions for finding and deleting the original Keylogger from your computer**" 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.