

Is Your Computer Connecting To Websites Without Your Knowledge

2011-07-20 00:39:12 by Southern

If you are worried that some programs on your PC are secretly making connections to websites in the background, here's a quick tip that uses a simple DOS command to detect and prevent such suspicious activity:

1. Type cmd in your Windows Run box.
2. Type "netstat -b 5 > activity.txt" and press enter. After say 2 minutes, press Ctrl+C.
3. Type "activity.txt" on the command line to open the log file in notepad (or your default text editor)

A screenshot of a Notepad window titled "a.txt - Notepad". The window contains the output of a netstat command. The output shows several lines of network activity, including established connections and time-wait states. The connections are listed with their protocol, local address, remote address, and state. The processes involved are listed in brackets on the left side of each line.

```
File Edit Format View Help
| TCP_LABNOL:4667_sjc-v116.sjc.youtube.com:http_ESTABLISHED
|[explore.exe]
TCP_LABNOL:1131_wr-in-f83.google.com:http_ESTABLISHED
[opera.exe]
TCP_LABNOL:1133_kc-in-f125.google.com:5222_ESTABLISHED 5
[googletalk.exe]
TCP_LABNOL:4667_sjc-v116.sjc.youtube.com:http_ESTABLISHED
|[explore.exe]
TCP_LABNOL:1128_wr-in-f83.google.com:http_TIME_WAIT 0
TCP_LABNOL:1129_google.navigation.opendns.com:https_TIME_WAIT
TCP_LABNOL:1132_google.navigation.opendns.com:https_TIME_WAIT
```

The file activity.txt will have a log of all process that made a connection to the Internet in the last two minutes. It will also show which process connected to which website in this time. And not just the web browsers (like iexplore.exe or opera.exe), the log will also show your IM clients, download managers, email programs or any software that requires a net connection.

Scroll though the activity.txt file and look for any process names or website addresses that you are not aware of. If you track one , go to the task manager (or Process Explorer) to find the location of the executable on your computer and eliminate it.

[Amit Agarwal](#)

<http://www.southernwolf.net/modules.php?name=News&file=article&sid=3102>