

25 September 2007

By: Marius Oiaga, Technology News Editor



## [Is Your Copy of Windows Vista Secretly Connecting to the Internet?](#)

*Here is how you can find out...*

Information is everything nowadays. It is not only a source of wealth and power, but also a means of being in control. And one thing that you absolutely need to [keep on a short leash is your copy of Windows Vista](#), and of Windows XP for that matter. It is not uncommon that programs you installed or even the native services in Vista are accessing the Internet in the background without you ever knowing about it. Usually, background processes in Vista or in XP consume so few resources that you never notice a degradation in performance. But this is the case with genuine and legitimate processes. In a worst case scenario, a piece of malicious code such as a Trojan Horse or a Downloader has infected your machine and is communicating via your Internet connection. Your computer could be a zombie machine in a botnet network, spamming immense quantities of emails and drastically impacting the performance of the operating system. Fortunately, both Windows Vista and Windows XP provide you with the means to monitor your Internet activity. Netstat is a command line utility designed to allow you a closer view at "protocol statistics and current TCP/IP network connections. The netstat utility displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols)." All you have to do is enter "cmd" in the Search box under the Start Menu. Either right-click on the highlighted result and choose "Run as administrator" from the contextual menu, or press Ctrl + Shift + Enter to launch command prompt with elevated privileges. Type "netstat -b 5 > activity.txt" and hit Enter. Wait a smaller or larger period of time, and then press Ctrl + C to break the logging operation. Next type "activity.txt" and hit Enter. A Notepad file will open containing all the logged Internet activity. You can simply scroll down and identify all the processes that are communicating with the web in the background. Suspicious activities can be identified easily, either because of their name, unlike any of the applications you recognize, or because they were active when they shouldn't have been. Alternatively, there is a great free tool from Sysinternal that you can use, dubbed TCPView for Windows v2.51, courtesy of Mark Russinovich, Microsoft technical Fellow. You will be able to download TCPView via this link right [here](#) on Softpedia. "TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, NT, 2000 and XP TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpsvcon, a command-line version with the same functionality. TCPView works on Windows Server 2008/Vista/NT/2000/XP and Windows 98/Me", Russinovich stated.