Big Brother and Ndisuio.sys
A new Internet phenomenon?

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

Ndisuio.sys, a very mysterious system file is present in Windows XP and is a driver for wireless things such as wi-fi and bluetooth. However, there have been many issues with this file downloading immense amounts of data and perhaps causing activity that is "big brother"ish.

The fact that hardly any information on this file downloading data is available by Microsoft makes things quite suspicious about it. It has even been noted that it looked as if it was transferring data to major companies like Comcast, Road Runner, Time Warner, BTC and Verizon.

The good news is, it turns out this file duplicates data that is sent/received, so wherever you go, it will also transfer the data to that file but it does not leave the computer/network so it's not spyware. So it's not as much of a big brother situation then it looks like. It simply performs internal communication tasks and stands for NDIS user I/O, hence, NDISUIO. NDISUIO is also used as a driver by many developers as it makes certain wireless network tasks easier such as implementing it for 802.11x connections. Some firewalls also use it as it can get the data in order to filter it.

But duplicating this data can hog resources for no reason, so disabling it is the best thing to do. The data rate of this file's received data is huge, so that indicates that the data transfer is not over the Internet, but locally. So it's just a duplicate of network activity but because it's local everything transfers faster but uses more resources then casual internet usage as there's more data involved at a given time span of 1 second, for example.

To disable this file, go to the control panel, administration tools, services, Wireless Zero Configuration, double click and disable it. This file is probably required to run if you use any linksys wireless devices.