

internet connection related question

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-03/3996.html

From: jk (tempestneo2@tempestwolf.com)

Date: 03/23/03

From: "jk" <tempestneo2@tempestwolf.com>

Date: Sat, 22 Mar 2003 19:18:36 -0800

Hi!

I just installed winxp on a brand new harddrive, then installed PC-cillin anti-virus. I went online a few times just fine, surfing the net a little bit, not much. A couple days ago I went online and Messenger (not MSN Messenger) popped up with spam. After that, my computer started receiving ALOT of data and more and more system resources (processor in particular) seemed to be being hogged, even after I managed to disconnect from the internet. I hit the power switch to reboot the computer (much as I hated to reboot, knowing all the possibilities of whatever it was that had hit my system worming its way in deeper or doing more damage).

When the computer rebooted, all ran normal... until I went back online. My computer "pinged" a couple of times as if to say "here I am!" then AGAIN the data flow resumed into my computer. My computer pings once in a while back, but overall, about 99% of the time, it is simply receiving. No processor slowdown, however.

I disabled messenger, disabled all known auto-updates, ran four different updated antivirus scans on this computer (norton, mcafee, panda, and pc-cillin) but it shows up clean. I've also hunted through the registry, and through quite a bit of the windows and program files folders on my harddrive searching for anything I don't recognize. I've also installed "Ad Aware" on my computer, but, again, that still hasn't solved the problem.

I've also set up the firewall, though I think it's a little late as my computer seems to be inviting the info in. Nothing I've done has affected this download of data. I've checked the firewall's log and found this line

repeated:

```
2003-03-21 21:37:37 DROP UDP 65.56.233.69 239.255.255.250
3168 1900 161 - - - - -
```

The first ip address is mine (though it changes a bit on each line), I think, and the second I can only guess is the other computer mine's having a nice conversation with.. and THAT one is the same every time. The numbers after the second ip address change, also.

I've never had these problems on my old win98se hd, and I'm still using all the same programs, except for the OS.

Anyone have any ideas of what exactly is going on and what I can do to get this to stop?!?

Thanks in advance,

jk