

microsoft.public.windowsxp.security_admin: Help pls. XP won't stop messaging.

Help pls. XP won't stop messaging.

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-05/1793.html

From: AJ (*i_inventREMOVETHIS_at_ANDTHIShotmail.com*)

Date: 05/15/03

Date: Thu, 15 May 2003 17:23:18 +1000

Hello,

Can someone please help. I have a small home network which uses a gateway router for the cable modem. The subnet is 192.168.0 and .1 is the router. My work pc is WinNT wkstn with ZAP. My laptop is WinXP Pro with ZA. The family PC is WinXP Pro with ZA.

The NT pc shows no activity in ZAP unless I initiate it. And it doesn't have messenger installed.

The 2 XP's are showing constant Internet and network activity. ZA is flashing constantly on both. I've configured the XP's to show a tray icon for the network and for the Internet. Both are also constantly flashing. (But not a wink out of the NT pc. It behaves perfectly.)

(I've done most of my analysis on the family pc, but the laptop is reacting similarly.) ZA keeps asking if I should let "messenger" access the Internet, both incoming and outgoing, but incoming is predominant. It identifies the correct messenger file, msmgs.exe, which is in the correct location and properties gives it the right credentials. On the family pc I killed the "messenger" process. That temporarily reduced the Internet activity. (The kids use MSN, otherwise I'd uninstall it.) The network was still producing lots of traffic though. This coincided with an instance of "svchost.exe" (there are several instances of it actually). I identified the instance of it that coincided with the activity and killed it. That greatly reduced the network traffic. Both kills were only temporary because they reinvoked themselves and soon the activity was back at the same level.

When I hit the stop button in ZA, the pc attempts to send a few bytes about every 1.5 seconds. The little Internet icon in the systray pulses at that rate.

When it's all travelling freely without my intervention, it appears to be receiving about 20kb per minute and sending intermittently.

Much of the traffic is with the router (192.168.0.1) and port 1900 gets

Help pls. XP won't stop messaging.

microsoft.public.windowsxp.security_admin: Help pls. XP won't stop messaging.

mentioned regularly. I've run ZoneLog over the ZA logfiles and come up with no reports of any concern.

Norton AV with the latest updates doesn't identify anything, and the free version of Ad-Aware identified and deleted some cookies and 2 registry entries. My wife unwittingly let a website install a Gator app. I uninstalled it and got Ad-Aware to do the rest.

Any clues? What else can I do?

Andrew