

Messenger active when disabled, messages getting through firewall

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2002-11/16865.html

From: Andy (andythorne@bigfoot.com)

Date: 11/02/02

From: "Andy" <andythorne@bigfoot.com>

Date: Fri, 1 Nov 2002 15:58:38 -0800

Ok, not sure if this is the exact place to post, but I've had quite a few problems in the last 3 weeks.

I had a windows XP (Home) update, and on the same day had an update for my Norton systemworks/firewall, and each installed successfully.

I don't use messenger, but I keep getting messages popping up on my screen – phone xxxxx (of course it's a premium rate line they refer to) the system process being used is csrss.exe, which win XP seems to want to keep hold of.

I obviously can't block everything from microsoft, and I assume that this is being exploited to send this garbage. Also, since the update, my FDD & CD drives access (or try to access) at log-on, and log-off, as well as at seemingly random times (sometimes when I click on a link – it happened whilst on the microsoft site)

Although I don't use messenger, how do i make sure it isn't even on my system? the 'remove programs – windows components is as clear as mud. If I check the messenger box (whilst messenger shows 0.00 disk space, and click next, does this remove or install the damn thing? MS gave this one a lot of thought – no indication whether you are actually going to uninstall or install the thing.

Another thing that happened around the same time is that playing online games became awkward. I usually play Delta Force BHD, via the novalogic servers. Now, when I finish one game, I have to exit the entire session, remove some files from the BHD 'cache' folder, and restart the game, whereas before, I could carry on normally.

I have a 24-7 virus scan and firewall, which is all updated regularly, with a full system-scan every night, so it's not likely to be a virus problem – any help on

microsoft.public.windowsxp.security_admin: Messenger active when disabled, messages getting through firewall
these matters is appreciated.