

Re: Pop-ups

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-08/1919.html

From: Kevin Davis³ (zkevindavisz_at_cfl.rr.com)

Date: 08/11/03

Date: Mon, 11 Aug 2003 02:56:54 GMT

On Sun, 10 Aug 2003 09:30:20 -0700, "tshortridge"
<mistwalker2000@adelphia.net> wrote:

> *Has anyone found an answer to stopping these permanently?*
> *Does microsoft offer any downloads against all pop-ups*
> *through messenger?*

Installing only a firewall to stop pop-up messages is a "putting all your eggs in one basket" approach to computer security.

If the user is a home user there is a likelihood that not only do they not use the messenger service, but don't even know it exists. However, there are some popular consumer anti-virus products that use them like Norton's. The user should find out if they need the service and shut it off if not needed as well as installing and configuring a firewall. If there is any doubt, it is probably best to leave it on, but certainly don't rely only on a software firewall to protect you.

Software firewalls like most software, have been susceptible to vulnerabilities. Good security advice would have them install an inexpensive hardware SOHO router/"firewall" (like a linksys or netgear), a personal software firewall, *and* disable the messenger service (if not needed).

To be truly as secure as reasonably possible, a multi-layered defense is required. Additional actions such as applying critical OS updates/patches, unbinding NetBeui from TCP/IP, and disabling NetBIOS over TCP/IP is also highly recommended. An excellent place to start learning about the various things you can do to secure yourself is

http://www.sans.org/rr/catindex.php?cat_id=26

Turning off the messenger service provides the user with 2 benefits. First, it will provide a more secure system in that the user will not be susceptible to any vulnerabilities that may exist in the messenger service today or that may be found in the future.

A great example is sendmail. It is (or at least was) installed and running on Linux systems as a daemon by default and had been regarded as very secure. Recently they found a serious vulnerability that had been there for over 15 years. Who knows how long the hackers knew about it? How many people left themselves vulnerable by leaving that service on and didn't need it?. Relying on one and only one line of defense (a software firewall) is foolish. You should harden your system as well as install a firewall. Doing one does not mean that you shouldn't do the other.

Second, it will return some system resources that were being used by a service that was useless to the user.

In the case that the user is a corporate user and the messenger service is being used, then it should not be disabled. However, if you advise him to install a firewall on his own you could be advising them to do something that could cause their termination. Many businesses deal very harshly with this type of behavior. If the user is a corporate user, they should alert their System Admin of these pop-ups getting through so they can block the traffic at their border routers/firewalls and solicit their advice as to what they can do, if anything, as a corporate user to avoid receiving the pop-ups.

What could possibly go wrong?