

Re: Messenger Service Spam

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-11/7808.html>

From: x y (x@y.com)

Date: 11/21/02

From: "x y" <x@y.com>

Date: Thu, 21 Nov 2002 09:47:13 -0500

I agree. I'd be more upset at Zone Alarm than Microsoft. I'd be concerned whether the firewall is blocking anything at all for you.

Microsoft has a choice of disabling Windows Networking by default, or enabling it by default. You and others would be upset either way, so they picked one. I think the Windows Messenger service can do some useful things, so it makes sense that it would be enabled.

"Gary Flynn" <flynnngn@jmu.edu> wrote in message
news:3DDC87D5.4FCED6EE@jmu.edu...

> *Greg wrote:*

>>

>> *I have been recieving spam via the windows messenger*

>> *service, I have done some research and have a few*

>> *questions.*

>>

>> *I am now fully updated will that solve this issue?*

>

> *Nope.*

>

>> *Will Microsoft be addressing this issue?*

>

> *Maybe in their next OS. They kinda did with the XP*

> *firewall.*

>

>> *If I disable the windows messenger service will this have*

>> *any adverse effects on my system? And is this the best way*

>> *to solve this?*

>

> *You might lose messages like "print complete" or*

> *"new mail received" if you use Outlook in an Exchange*

> *environment. There are likely others.*

>

>> *I have ZoneAlarm Pro why isnt it stopping this?*

>

> *Now that is the \$64 question.*

>

microsoft.public.security: Re: Messenger Service Spam

- > *I haven't used Zonealarm in a long time but I can't*
- > *imagine it not being configurable to kill those*
- > *messages. If I remember correctly, the older*
- > *versions were shipped in "medium" security*
- > *mode which didn't block netbios and RPC and*
- > *the newer versions are shipped in "high" security*
- > *mode which do block those ports. But I'm really*
- > *straining some old brain cells there.*
- >
- > *Obviously, you can try kicking the security*
- > *level up.*
- >
- > *If you allow netbios in because you want to share*
- > *your folders with the Internet (ugh), they can get*
- > *you that way through TCP 139 using 'net send'.*
- >
- > *However, it seems the most common way this is being*
- > *done on a mass scale is through UDP 135 so if you*
- > *block that, you'll probably be free of them.*
- >
- > *More technical info at:*
- >
- > *<http://www.jmu.edu/computing/security/info/winmsg.shtml>*
- >
- > --
- > *Gary Flynn*
- > *Security Engineer – Technical Services*
- > *James Madison University*
- >
- > *Please R.U.N.S.A.F.E.*
- > *<http://www.jmu.edu/computing/runsafe>*