

## Re: Spywaer Popup, Messenger Service

**Source:**

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-12/20133.html>

---

**From:** Jim Byrd (*jrbyrd\_at\_spamlessadelphia.net*)

**Date:** 12/30/04

Date: Thu, 30 Dec 2004 10:53:33 -0800

Hi Phil – As Malke pointed out to you before, it is not sufficient to just turn off Messenger Service.

If you get popups even when your browser is not connected to the Internet with a title bar reading "Messenger Service", then these are most likely due to open NetBios TCP ports 135, 139 and 445 and UDP ports 135, 137–138 and a UDP port in the range of 1026–1029.. You really need to block these with a firewall as a general protection measure. You can stop the popups by turning off Messenger Service; however, this still leaves you vulnerable. If you have an NT-based OS such as XP or Win2k, you should probably also specifically block TCP 593, 4444 and UDP 69, 139, 445, and install the very important 824146 patch from MS03-039, here: <http://support.microsoft.com/default.aspx?kbid=824146> to block the Blaster worm as well as several other parasites.

See: Messenger Service Window That Contains an Internet Advertisement Appears <http://support.microsoft.com/?id=330904> which identifies reasons to keep this service and steps to take if you do.

You can test your system and follow the 'Prevention' link to get additional information here:

<http://www.mynetwatchman.com/winpopuptester.asp> Unless you have very good reasons to keep this active, it should be turned off in Win2k and XP. Go here and do what it says:

<http://www.itc.virginia.edu/desktop/docs/messagepopup/> or, even better, get MessageSubtract, free, here, which will give you flexible control of the service and viewing of these messages:

<http://www.intermute.com/messagesubtract/help.html> Recommended.

(FWIW, ZoneAlarm's default Internet Zone firewall configuration blocks the necessary ports to prevent this use of Messenger Service. I don't know the situation with regard to other firewalls.)

Messenger Service is not per se Spyware or something that MS did wrong – It provides a messaging capability which is useful for local intranets and is also sometimes (albeit nowadays infrequently) used by some applications to provide popup messages to users. However, it can also be (and now frequently

microsoft.public.windowsxp.general: Re: Spywaer Popup, Messenger Service

is) used to introduce spam via this open NetBios channel. For a single user home computer, it normally isn't needed and can be turned off which will eliminate the spam popups. This DOESN'T, however, remove the vulnerability of having these ports open, when in fact they aren't needed, since they can be perverted in other ways as well, some of which can be much more damaging than just a spam popup.

--

Please respond in the same thread.

Regards, Jim Byrd, MS-MVP

In news:087e01c4ee8d\$dd233cd0\$a401280a@phx.gbl,

anonymous@discussions.microsoft.com <anonymous@discussions.microsoft.com>

typed:

> Thanks, but i do have McAfee personal firewall however  
> this spy was in before i loaded it, and their bug scan and  
> restore did not fix it. But Disabling Messenger stopped  
> it, Thanks Phil

>

>

>

>> -----Original Message-----

>> BrokenWindows wrote:

>>

>>> Try this,

>>> Control Panel/Admin Tools/Services

>>> Scroll down to Messenger and DISABLE it

>>> Then reboot and problem should be gone.

>>>

>>> "Phil" wrote:

>>>

>>>>

>>>> I have one spywaer left getting into my computer. The  
>>>> popup Heading is Messenger Service. I have the latest  
>>>> version McAfee security with Spywear protection running.  
>>>> It pops up about every 5 Min while I'm online. Can  
>>>> anybody Help

>>>>

>>

>> Actually, the symptom will be gone but the OP will have masked his  
>> real problem which is that he isn't running a firewall. He should  
>> check in his McAfee security center or whatever they call it and  
>> either enable the Personal Firewall or get a different firewall.  
>> Sygate and ZoneAlarm make free ones.

>>

>> Malke

>> --

>> MS MVP - Windows Shell/User

>> Elephant Boy Computers

>> www.elephantboycomputers.com

>> "Don't Panic!"

>> .