

Re: Application Popup Messenger Service SPAM

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-10/10133.html>

From: Karl Levinson [x y] MVP (levinson_k@excite.com)

Date: 10/24/02

From: "Karl Levinson [x y] MVP" <levinson_k@excite.com>

Date: Thu, 24 Oct 2002 14:50:54 -0400

"jj" <unixquest@hotmail.comNoSpam> wrote in message
news:M0Gt9.43828\$CJ5.8337855@news3.news.adelphia.net...
> *"Users can disable Messenger through their operating system's control
panel,
> although doing so could interfere with some anti-virus and other
> applications that send such messages. Kovacs even provides instructions on
> his Web site. "*
>
> *RE: a new kind of spamming*
> <http://www.cnn.com/2002/TECH/internet/10/21/pop.upsam.ap/index.html>
>
> *sorry for not reading efore posting. So sutting down Messanger service is
> all that is needed?*

NO NO NO. Use a firewall. You don't need or want TCP and UDP ports 135 through 139 or 445 to pass to the internet or from the internet in either direction. It is a very large security risk. Hackers can get a list of login IDs on your system and then try to log in and crack the password, among other things. If you don't believe me, check out the live real-time hacking statistics at www.dshield.org and check out how often hackers scan those ports, then ask yourself why they're scanning those ports so often.

It is not a bad idea to also disable the Messenger service, but I think it is a mistake to not also use a firewall, unless you have a really good reason to do so.

=====

Which firewall should I choose? Which firewall is the best?

(6.2) What are some ways for me to enable Intrusion Detection or IDS?

(6.3) How can I enable or configure the Windows XP ICF Internet Connection Firewall?

(6.4) How can I enable or configure TCP/IP Filters or IPsec policies to

protect my computer, filter, block, encrypt or tunnel traffic?

A: The answer to this question varies depending on your computer systems, your security requirements and your personal preferences. Below are some firewalls and other forms of firewall-like packet filtering:

NO MATTER WHICH FIREWALL YOU CHOOSE...

No matter which firewall you choose, you should seriously consider downloading and installing MyNetWatchman or Dshield. These are free programs that work with your firewall software or hardware to automatically report hacking attempts to the hacker's ISP. You get to see information about whether that IP address has been used to scan or hack other computers, or whether it might be targeting just your computer. You also get to see whether the ISP has responded or taken action against the offending user. You can get this software at one of the links below:

www.mynetwatchman.com
www.dshield.org

Also, no matter which firewall you choose, the lists below of port numbers for common software services may be helpful when configuring your firewall or when trying to monitor the firewall logs for signs of intrusion:

www.iana.org/assignments/port-numbers
www.iisfaq.com/default.asp?View=P106

FIREWALL SOFTWARE:

www.sygate.com [free for non-commercial use, also works like a sniffer]
www.kerio.com [free for non-commercial use]
www.agnitum.com [free for non-commercial use]
www.zonealarm.com [free for non-commercial use, also blocks pop-ups]
www.iss.net [Black Ice]
www.symantec.com [Norton]
www.webattack.com
www.download.com
www.tucows.com
[Windows XP users can also consider using the ICF firewall that comes with XP, more info below]

FIREWALL DEVICES [HOME / SOHO]:

www.linksys.com [starts around \$70 US]
www.netgear.com [starts around \$70 US]
<http://search.ebay.com/search/search.dll?query=firewall> [prices on new and used firewalls]

=====

How can I stop or block pop-up windows [such as porn, advertisements, IM or Messenger Service pop-ups] on my computer?

microsoft.public.win2000.security: Re: Application Popup Messenger Service SPAM

A: Here is the short answer. To block all the types of pop-ups out there, follow some or all of the following steps:

- * Use software that blocks pop-ups and/or ad-ware;
- * Use a firewall and antivirus with the latest updates;
- * Disable unnecessary programs that start when Windows starts, by using MSCONFIG or Startup Cop;
- * Disable or unbind NetBIOS over TCP/IP / File and Print Sharing on your network interface;
- * Disable the Messaging service;
- * Configure your chat program to not start up automatically with Windows, to require confirmation before accepting an incoming chat, and/or to only allow chat requests from people on your buddy/favorites list.

Keep reading below for more information.

There are several different types of pop-ups:

*** WEB BROWSER POP-UPS**

One very common type of pop-up is a new web browser window that pops up while you are surfing the Internet. These pop-ups are often generated by certain web sites including some porn sites, some shopping web sites, and some web sites that offer free services like email or news. These pop-ups often appear when you click to either enter or leave a web page.

There are a number of third-party software programs, both free and not free, which are supposed to help block pop-up windows. Try searching your favorite Internet search engine, Usenet support newsgroup software web site and/or see the links below. [Try searching for the words "stop OR block pup-ups," for example]:

www.google.com/groups?threadm=enZy0PscCHA.1828%40tkmsftngp08 <--- SEE THIS LINK FIRST

[The above link is an excellent list of software to block pop-ups in a post by Jim Byrd]

www.webwasher.com

www.adshield.org

www.popupstopper.com

www.zonealarm.com [the Zone Alarm firewall also blocks pop-ups]

www.webattack.com/Freeware/misctools/fwpopblock.shtml

www.webattack.com

www.download.com

www.tucows.com

www.google.com/groups?q=stop+OR+block+pop-ups

www.google.com/search?q=stop+OR+block+pop-ups

If the pop-ups happen when you launch your web browser [e.g. Internet Explorer], then you should check the home page setting in your web browser [e.g. in Internet Explorer, click on Tools, Internet Options, Home Page, Address]. Make sure the home page is not set to an objectionable site. [If

microsoft.public.win2000.security: Re: Application Popup Messenger Service SPAM

your home page has been changed and you want to change it back, you set it to www.msn.com or to your favorite web site.]

If the pop-ups seem to pop up at random and not just when you open and close your web browser or enter and leave a certain web page, you may want to also use MSCONFIG or Startup Cop to check the programs that are starting up when Windows starts, in case there is an unwanted program hidden there. For more information on how to do this, see the section in this FAQ entitled "I think there may be a suspicious program, Trojan, ad-ware, "porn dialer," etc. starting up on my computer when Windows starts."

*** MESSENGER SERVICE / WINDOWS MESSAGING / NETBIOS POP-UPS**
Another type of pop-up is the Windows messaging pop-up. If you are receiving these types of pop-ups, NetBIOS / SMB / Windows Networking / Windows File and Print Sharing on your computer may be visible from the Internet, which is usually considered a serious security risk.

To determine whether this security risk applies to you, see the section in this FAQ entitled "How can I scan my computer or firewall to look for open ports or confirm that my machine is secure?" In particular, the web site <https://grc.com/x/ne.dll?bh0bkyd2> or any of the tools under the "Vulnerability Assessment" subsection can be used to scan your computer.

To block this first type of pop-up and also increase the security of your computer, use one or more of the techniques below:

A) USE A FIREWALL.

This is highly recommended. See the section in this FAQ entitled "Which firewall should I choose? Which firewall is the best?" for more information.

B) DISABLE OR UNBIND NETBIOS OVER TCP/IP / FILE AND PRINT SHARING ON THE NETWORK INTERFACE.

This is slightly complicated and varies depending on what operating system you are using. If you wish to do this, try searching your favorite Internet search engine for words such as "how to disable netbios windows" for your version of Windows such as XP, or follow one or more of the links below. [Using a firewall is still highly recommended even if you follow this step.]

<http://www.google.com/search?q=disable+netbios+%2Bhow+windows>
<http://comp.bio.uci.edu/security/netbios.htm>

C) DISABLE THE MESSENGER SERVICE.

This will stop the pop-ups and may be a good idea. However, just disabling the Messenger service without also taking other actions leaves you extremely vulnerable to other more serious intrusions from the Internet.

To disable the Messenger service on Windows 2000 / XP / .NET, you would click on Start, Settings, Control Panel, Administrative Tools, Services, stop the Messenger service and set the service to Startup Type = Disabled. Using a firewall and disabling NetBIOS is still strongly recommended. [If you don't, hackers on the Internet can probably get a list of all login IDs

on your computer and start trying to guess your passwords.]

* INSTANT MESSENGER POP-UPS [AOL AIM, MSN MESSENGER, YAHOO MESSENGER, ICQ, ETC.]

Instant messenger pop-ups are different from NetBIOS / Messenger service pop-ups. You can tell IM pop-ups because they appear within your instant messenger chat program.

The instructions for protecting yourself from unwanted chat messages differ depending on which instant messenger program you are using [e.g. AOL AIM, MSN Messenger, Yahoo, etc]. The instructions would probably involve looking at and changing the settings within your IM client software. For example, some IM software will let you block everyone from contacting you except for the people on your "buddy" or "favorites" list, or can give you a prompt asking whether you want to accept the chat.

Another solution might be to set your instant messenger client so that it does not start automatically with windows, so that you have to double-click on your IM icon before anyone can contact you. Again this is in your IM client settings. For more information, check the documentation that came with your IM software and/or a support web page or Usenet newsgroup specifically for that IM program.