

Re: New MSN Messenger Exploit?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-03/1456.html

From: Dave (c@t)

Date: 03/04/03

From: "Dave" <c@t>

Date: Tue, 4 Mar 2003 14:37:19 -0500

I understand what both of you are saying and appreciate it. This is what is puzzling me: First for someone to initiate a conversation with me thru messenger, I must accept them. Second, when they do start a conversation, the dialog box pops up from the tray and if i dont click on it right away, it stays minimized in the taskbar. This person got onto my screen without a prompt to accept them or without me click on the dialog box. It just opened maximized on my screen. I understand that random spamming is possible, but how did they by-pass the security or privacy measures in place to avoid this. See what I'm saying? I do have a screen shot if that will help.

Thanks

"sparhawk" <sparhawk@hotmai.com> wrote in message news:014201c2e221\$1a730960\$a001280a@phx.gbl...

> mac address has everything to do with ip. the mac address
> is supposed to be hard coded into the network card though
> sometimes it can be fake by linksys or other routers just
> in case your provider forces you to have one assigned
> network card (if they told you to change nic they don't).
> what happens is you are leasing the ip for so long usually
> 24 hours sometimes 72 so if you don't want to replace
> your nic check how long it's leasing for and keep the
> computer off for that long in most cases that's about 24
> hours if you can go a weekend it would probably be best
> and you will have a new ip as the lease will run out and
> the server will unlist the mac address of your nic.

>

> sparhawk

>

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

> >Dave;

> >I forgot to mention, I get something similar to you once
> in a while.

> >They are MSN Messenger windows, however they are
> different on the top,

> >if I remember correctly.

> >
> >The NIC shouldn't have anything to do with the IP.
> >The NIC does determine the MAC address though.
> >
> >Try the release and renew a few more times.
> >
> >Check the settings and verify that your firewall is
> updated and
> working properly:
> ><https://grc.com/x/ne.dll?bh0bkyd2>
> >
> >I wish I could tell more, but that is it.
> >
> >--
> >Jupiter Jones
> >Check the following link for some great problem solving
> newsgroups.
> ><http://support.microsoft.com/newsgroups/default.aspx>
> >Please respond to newsgroup only. Everyone can benefit
> from the
> message.
> >
> >
> >"Dave" <c@t> wrote in message
> >news:OUqZgLh4CHA.1636@TK2MSFTNGP10.phx.gbl...
> >> Thats OK!
> >> I did mention is it not messenger service because of
> all the blabla
> >with
> >> that, LOL. But this is weird? I did try to release my
> IP earlier,
> >but i kept
> >> the same one, so I phoned my ISP and they said a new
> NIC was the
> >only way,
> >> even though it's dynamic. I wonder if this is a brand
> new exploit? I
> >have
> >> searched high and low and don't know what to make of
> it?
> >> This person did not show up on my contact list, and i
> didnt even get
> >> prompted to accept them?
> >>
> >> "Jupiter Jones" <jones_jupiter@hotmail.com> wrote in
> message
> >> news:#8FIwAh4CHA.2156@TK2MSFTNGP10.phx.gbl...
> >>> Dave;
> >>> Sorry for the misunderstanding.
> >>> I try to read what is meant as well as what is said.
> >>> Usually I am closer than I was this time.

> >> >
> >> > *If you have a dynamic IP, you can attempt to change
> it yourself.*
> >> > *Start/Run, type "cmd", click ENTER.*
> >> > *Type "ipconfig /release", ENTER*
> >> > *Then*
> >> > *Type "ipconfig /renew", ENTER*
> >> > *This releases your IP and renews the IP.*
> >> > *When I have done it, I usually get the same IP.*
> >> > *I have to try a few times before I get a different
> IP.*
> >> >
> >> > *If you have static IP, your ISP needs to change the
> IP.*
> >> >
> >> > *--*
> >> > *Jupiter Jones*
> >> > *An easier way to read newsgroup messages:*
> >> >
> *[http://www.microsoft.com/windowsxp/pro/using/newsgroups/se
> tup.asp](http://www.microsoft.com/windowsxp/pro/using/newsgroups/setup.asp)*
> >> > *Please respond to newsgroup only for everyone's
> benefit.*
> >> >
> >> >
> >> > *"Dave" <c@t> wrote in message*
> >> > *news:u8fpkSf4CHA.2428@TK2MSFTNGP09.phx.gbl...*
> >> > > *Hey Jupiter,*
> >> > > *I appreciate all the links, but this is not
> messenger service,*
> > *which*
> >> > *has*
> >> > > *been disabled along with all the networking
> features. This is*
> >> > *windows*
> >> > > *messenger. I run Ad Aware, Spybot, Norton*
> > *corporate firewall,*
> > *Norton*
> >> > > *corporate AV, browser hijacker blaster, BHO Demon,*
> > *Ad Shield and*
> >> > *more. When*
> >> > > *someone adds you to their messenger list, it
> usually prompts you*
> > *to*
> >> > *accept*
> >> > > *or block and then when someone on your list tries
> to initiate a*
> >> > > *conversation, the dialog box doesnt maximize on
> its own, you*
> > *have to*
> >> > *click*

microsoft.public.windowsxp.security_admin: Re: New MSN Messenger Exploit?

> >> > > *it above the tray or maximize from the taskbar.*
> *This person*
> *>spammed*
> >> > *me*
> >> > > *yesterday, so i changed my passport account and*
> *deleted my old*
> >> > *passport thru*
> >> > > *"control userpasswords2". Well today, the same*
> *person with the*
> *>same*
> >> > *message*
> >> > > *popped up again? no prompting, the conversation*
> *box just opened*
> >> > *right up. I*
> >> > > *have tried 4 trojan programs, online scans from*
> *trend micro and*
> *>who*
> >> > *knows*
> >> > > *what else. I am now gonna phone my ISP and see if*
> *they can give*
> *>me a*
> >> > *new IP,*
> >> > > *maybe that will help. If you have any thoughts,*
> *please let me*
> *>know,*
> >> > *this is*
> >> > > *really bugging me.*
> >> > > *Thanks a bunch.*
> >> > >
> >> > > *"Jupiter Jones" <jones_jupiter@hotmail.com>*
> *wrote in message*
> >> > > *news:e\$zzw8e4CHA.1680@TK2MSFTNGP12.phx.gbl...*
> >> > > > *Dave;*
> >> > > > *If they are Messenger Service ads, that is*
> *different from MSN*
> >> > > > *Messenger.*
> >> > > > *For Messenger Service ads:*
> >> > > > *You need to install or enable a firewall:*
> >> > > >
> > *<[http://support.microsoft.com/default.aspx?scid=KB;EN-](http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q330904&)*
> *US;Q330904&*
> >> > > > *Disabling Messenger Service can be a good idea,*
> *but it does*
> *>not*
> >> > *solve*
> >> > > > *the real problem.*
> >> > > > *The ads are not the real problem, the ads are*
> *only a symptom.*
> >> > > > *The real problem is open ports that allow*
> *unwanted traffic*
> *>into*

> >> > *the*
> >> >> > *computer.*
> >> >> > *Disabling Messenger does nothing for the open*
> *ports.*
> >> >> > *The firewall controls the traffic.*
> >> >> > *This will not work if you have AOL.*
> >> >> > *AOL is not compatible with Windows XP Internet*
> *Connection*
> *Firewall*
> >> >> > *(ICF)*
> >> >> >
> >> >> > *Disable Messenger Service:*
> >> >> > *Start/Control Panel, click Administrative Tools,*
> *click*
> *Services.*
> >> >> > *Go down to "Messenger".*
> >> >> > *Right click "Messenger" and select Properties.*
> >> >> > *Then under Start-up select DISABLE*
> >> >> > *Click OK and follow prompts*
> >> >> >
> >> >> > *Ad-Aware may be appropriate (free version):*
> >> >> > <http://www.lavasoft.de/>
> >> >> >
> >> >> > *For internet pop-ups:*
> >> >> > <http://www.panicware.com/>
> >> >> >
> <http://www.bysoft.se/sureshot/stopthepop/index.html>
> >> >> > <http://www.popupbuster.com/PopUpBuster/>
> >> >> > <http://www.kolumbus.fi/eero.muhonen/FS/>
> >> >> > <http://www.endpopups.com/>
> >> >> > <http://www.adshield.org/>
> >> >> >
> >> >> > --
> >> >> > *Jupiter Jones*
> >> >> > *An easier way to read newsgroup messages:*
> >> >> >
> > [http://www.microsoft.com/windowsxp/pro/using/newsgroups/s](http://www.microsoft.com/windowsxp/pro/using/newsgroups/setup.asp)
> *etup.asp*
> >> >> > *Please respond to newsgroup only for everyone's*
> *benefit.*
> >> >> >
> >> >> >
> >> >> > *"Dave" <c@t> wrote in message*
> >> >> > *news:uaqatue4CHA.1932@TK2MSFTNGP12.phx.gbl...*
> >> >> > > *Hello,*
> >> >> > > *I got spammed on Windows messenger yesterday,*
> *this person*
> *was*
> >> > *not on*
> >> >> > *my*
> >> >> > > *contact list and I was not asked to accept*

> *them. All of a*
> >*sudden*
> >> > *the*
> >> > > *box*
> >> > > > *popped up on my screen. Normally when a friend*
> *contacts me,*
> >*i*
> >> > *have*
> >> > > > *to click*
> >> > > > > *on the box above the tray to open it. Well*
> *this new just*
> >*popped*
> >> > > > *right up? So*
> >> > > > > *I changed my Passport account and today, with*
> *my new*
> >*Passport, I*
> >> > *got*
> >> > > > *spammed*
> >> > > > > *by the same person or at least it was the same*
> *address. I*
> >> > *deleted*
> >> > > > *the info*
> >> > > > > *from my old passport thru "control*
> *userpasswords2" and they*
> >> > *still*
> >> > > > *got thru*
> >> > > > > *without prompting me to add them or even*
> *without opening the*
> >> > *dialog*
> >> > > > *box?*
> >> > > > > *Whats going on? I am not confusing this with*
> *the other*
> >> > *messenger*
> >> > > > *exploit,*
> >> > > > > *this IS windows messenger????*
> >> > > > >
> >> > > > >
> >> > > > >
> >> > > > >
> >> > >
> >> > >
> >> > >
> >> >
> >> >
> >>
> >>
> >
> >
> >
> >
> >
> >