

RE: IM Programs

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-03/0646.html>

From: Jim Popovitch (jimpop@rocketship.com)

Date: 03/13/02

From: "Jim Popovitch" <jimpop@rocketship.com>
To: <c_brauckmiller@LEK.COM>, <security-basics@security-focus.com>
Date: Tue, 12 Mar 2002 20:48:41 -0500

Craig, why? Why are you going through so much work to do this? Is there some compelling or underlying security concern? (any more so that java enabled browsers?)

-Jim P.

> -----Original Message-----
> From: c_brauckmiller@LEK.COM [mailto:c_brauckmiller@LEK.COM]
> Sent: Monday, March 11, 2002 2:25 PM
> To: security-basics@security-focus.com
> Subject: IM Programs
>
>
>
>
> Hello all.
>
> After watching this list for a few weeks and following one thread
> regarding
> Instant Messengers, I have this to say. I HATE INSTANT MESSENGERS.
>
> It is virtually impossible to block them with a firewall.
>
> Here is my experience with each thus far.
>
> AOL Instant Messenger – Ok, I have been able to block this one
> with pretty solid
> results. I had to pretty much block 1 class C's worth of
> addresses in the 64
> region of AOL's address range, but have not heard any complaints
> thus far. The
> program is pretty damn smart about getting around rules in your
> firewall. It
> will try and use FTP, TELNET, HTTP, FINGER, NETBIOS over IP,
> APPLETTALK over IP,
> 1080 (SOCKS), 1024, Lotus Notes (TCP 1352) and a few others. I

SecurityFocus BASICS: RE: IM Programs

> pretty much
> locked the subnet down but AIM was somehow getting through. I
> finally figured
> out that my CheckPoint firewall was allowing DNS traffic outbound
> in my rule
> base above rule 1. I had to go to the Properties section and disable the
> implicit access to DNS (TCP/UDP 53). Once I did that, it killed
> AIM altogether.
>
> Yahoo Instant Messenger – Ok, this program sucks in that they
> spread out their
> Authentication servers across multiple machines and subnets. The shotgun
> approach to locking down a full subnet backfired when people
> started to complain
> about not being able to access Yahoo! web mail or Yahoo Finance.
> I still have
> more work to do on this one.
>
> MSN – Eegad. This is probably the most difficult to block. From my
> investigation, if port 1864 is blocked (MSN's Auth port), it will
> use HTTP and
> access one of the main MSN pages. So, I have a choice; kill off
> access to MSN
> outright or allow MSN to run if people manage to install it. :(
>
> ICQ – I have not even played with this one yet, but as I
> remember, it will also
> auto-hack to get around firewalls.
>
> PROPOSAL:
> =====
>
> I'd like to compile as complete a list as possible of ALL IP
> addresses of the
> hosts that the IM clients will attempt to connect to. Its a lot
> of work on the
> firewall, but its the only way I can see to stop the IM traffic
> and still allow
> web traffic to remain as unaffected as possible.
>
> If you want to mail me your IPs, I'll compile a list and post
> them on my web
> site.
>
> Thanks,
>
> Craig Brauckmiller
>
>
>
>
>

RE: IM Programs

>
>
>
>
>

>

>
> **PRIVACY & CONFIDENTIALITY NOTICE**

>
> *The information contained in this e-mail is intended for the
> named recipients
> only. It may contain privileged and confidential information,
> and if you are
> not the addressee or the person responsible for delivering this to the
> addressee, you may not copy, distribute or take action in
> reliance on it. If you
> have received this e-mail in error, please notify us immediately
> by returning
> the original message to the sender by e-mail.*

>
>

-
- **Previous message:** Mauricio Pretto: "Re: apache being bombarded"
 - **In reply to:** c_brauckmiller@LEK.COM: "IM Programs"
 - **Next in thread:** Calhoun, Heath: "RE: IM Programs"
 - **Messages sorted by:** [date] [thread] [subject] [author] [attachment]