

Re: IM Programs

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-03/0623.html>

From: dewt (dewt@kc.rr.com)

Date: 03/13/02

From: dewt <dewt@kc.rr.com>

To: c_brauckmiller@LEK.COM, security-basics@security-focus.com

Date: Tue, 12 Mar 2002 19:17:29 -0600

i'm all for a list like that, but i think a stateful IDS rule would be more effective, detecting and blocking the actual protocol (like the authentication part of it). I think it's quite evil that these services are intentionally designed to bypass firewalls, which is sometimes there for a reason. (begin troll) Maybe we should sue them under the dmca for bypassing copyrighted authentication mechanisms!

On Monday 11 March 2002 01:25 pm, c_brauckmiller@LEK.COM wrote:

> *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 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 aproach 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*

