

Re: [fw-wiz] Blocking Yahoo IM

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2002-11/1180.html>

From: kadokev@msg.net

Date: 11/21/02

From: kadokev@msg.net

To: Kowsik Guruswamy <kowsik@doublek.net>

Date: Thu Nov 21 07:10:01 2002

AIM is still the hands-down winner for getting past firewalls by tunnelling in all sorts of different protocols (their FTP tricks are particularly interesting), but Yahoo! gets an honorable mention for their ugly implementation of HTTP 'polling' for IM, and the ugly attempts the client uses to tunnel their proprietary YMSG protocol through SMTP.

I've been playing with writing a fake YMSG server to try to get the clients to believe they are connected, with very little success. Most of the published reverse-engineering covers the obsolete V9 protocol.

> *You might need to use dst IPs for blocking. Yahoo! is pretty nasty in that*
> *they tunnel IM traffic through finger, discard, chargen, smtp and even*
> *http...*
>
> *Ugly, ugly...*

FYI, Yahoo! recently started pushing the new "Messenger 5.5" client to existing users. The new version changes the order in which the various ports are attempted, and is more insistent at trying different ports and destination IPs.

I have started to block their servers by IP network, so far I've found a half dozen different subnets (ranging from a couple of /24's to a /19), all used for the messenger servers.

If you think you are successfully blocking Yahoo Messenger, by protocol or by destination IP, you might want to take another look.

Kevin Kadow