

Re: [Full-disclosure] obtai an IP of an MSN Messenger contact

Re: [Full-disclosure] obtai an IP of an MSN Messenger contact

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-04/msg00152.html>

- *From:* "Ian stuart Turnbull" <ian.t7@xxxxxxxxxxxxxx>
 - *Date:* Wed, 05 Apr 2006 21:25:39 +0100
-

Many thanks for that. In fact I should've known this myself [rap over knuckles with ruler] as its the Apache logs that started me on this hacking thing. After checking my logs I noticed some strange entries and I believe on this post I posted some of these strange HTTP requests. I was tols that they were known exploits in AWSTATS which I fortunately don't have installed. Funny because the IP's of these attackers were in the log as well.

Now I feel just a little foolish.

Still thanks for the good info – nice one

Ian t

From: n3td3v <n3td3v@xxxxxxxxxx>
To: full-disclosure@xxxxxxxxxxxxxxxxxxxxx
Subject: Re: [Full-disclosure] obtai an IP of an MSN Messenger contact
Date: Wed, 5 Apr 2006 21:01:13 +0100
MIME-Version: 1.0
Received: from lists.grok.org.uk ([195.184.125.51]) by bay0-pamc1-f5.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.1830); Wed, 5 Apr 2006 13:02:29 -0700
Received: from lists.grok.org.uk (localhost [127.0.0.1]) by lists.grok.org.uk (Postfix) with ESMTP id EE8F49B8; Wed, 5 Apr 2006 21:01:36 +0100 (BST)
Received: from zproxy.gmail.com (zproxy.gmail.com [64.233.162.196]) by lists.grok.org.uk (Postfix) with ESMTP id 4AFD4861 for <full-disclosure@xxxxxxxxxxxxxxxxxxxxx>; Wed, 5 Apr 2006 21:01:14 +0100 (BST)
Received: by zproxy.gmail.com with SMTP id x3so18967nzdfor <full-disclosure@xxxxxxxxxxxxxxxxxxxxx>; Wed, 05 Apr 2006 13:01:14 -0700 (PDT)
Received: by 10.35.39.2 with SMTP id r2mr1632pyj; Wed, 05 Apr 2006 13:01:14 -0700 (PDT)
Received: by 10.35.81.8 with HTTP; Wed, 5 Apr 2006 13:01:13 -0700 (PDT)
X-Message-Info: JGTYoYF78jF1123Vdz1Tm0nLljUyMP7/Ma7BNwoBhSo=
X-Original-To: full-disclosure@xxxxxxxxxxxxxxxxxxxxx
Delivered-To: full-disclosure@xxxxxxxxxxxxxxxxxxxxx
DomainKey-Signature: a=rsa-sha1; q=dns; c=noaws; s=beta; d=gmail.com; h=received:message-id:date:from:to:subject:in-reply-to:mime-version:content-type:references;
References:
<BAY112-F27B14A594D5CB1C1C6771F99CA0@xxxxxxxx><C6DE7C2B-BDD2-47AE-8890-ED1C9F5-
X-BeenThere: full-disclosure@xxxxxxxxxxxxxxxxxxxxx
X-Mailman-Version: 2.1.5

Re: [Full-disclosure] obtai an IP of an MSN Messenger contact

Re: [Full-disclosure] obtai an IP of an MSN Messenger contact

Precedence: list

List-Id: An unmoderated mailing list for the discussion of security issues<full-disclosure.lists.grok.org.uk>

List-Unsubscribe: <<https://lists.grok.org.uk/mailman/listinfo/full-disclosure>>, <<mailto:full-disclosure-request@xxxxxxxxxxxxxxxxxxxxxx?subject=unsubscribe>>

List-Archive: <<http://lists.grok.org.uk/pipermail/full-disclosure>>

List-Post: <<mailto:full-disclosure@xxxxxxxxxxxxxxxxxxxxxx>>

List-Help: <<mailto:full-disclosure-request@xxxxxxxxxxxxxxxxxxxxxx?subject=help>>

List-Subscribe: <<https://lists.grok.org.uk/mailman/listinfo/full-disclosure>>, <<mailto:full-disclosure-request@xxxxxxxxxxxxxxxxxxxxxx?subject=subscribe>>

Errors-To: full-disclosure-bounces@xxxxxxxxxxxxxxxxxxxxxx

Return-Path: full-disclosure-bounces@xxxxxxxxxxxxxxxxxxxxxx

X-OriginalArrivalTime: 05 Apr 2006 20:02:29.0538 (UTC)

FILETIME=[DE379020:01C658EB]

On messenger though, not even corporate users use a proxy, even though Yahoo offer their employees the "socks.yahoo.com" network. This is because using a proxy over messenger really does affect the whole operation of refresh ping times on your messenger list status of users going on and offline etc. With your method of just getting someone to view a file hosted on a webserver wouldn't work if you were trying to hack Yahoo, because all employees, for the internet explorer, firefox browser, they all use the socks, socks1, socks2,socks3 and so on, so you would be in a highly unlikely position to actually getting their actual hostname. On messenger its different, the social psychology of corporate users is that they believe they are in a false sense of security, wrapped in cotton wool, because by adding you to their messenger list, you've already got by that "trust" element, and as soon as you do get on a messenger list of a corporate user then you have more or less succeeded in completing the most significant part of the attack to steal corporate data from an individual within a major dot-com. If you want a non-proxy IP from a corporate user, messenger is the application they very rarely use with their corporate proxy, trust me, I know about this stuff.

On 4/5/06, Octal <octetstream@xxxxxxxx> wrote:

>
> If you have control over a webserver, send the friend a link to an invalid
> image on that webserver and tell them to click on it. Once they've clicked
> the link check your server logs for that invalid image and you should have
> their IP address (unless they're using a proxy like mentioned before). You
> can also do this with an email if your "victim's" email client is configured
> to automatically render images when an email is opened. This technique has
> been referred to as a "web bug".

>

>

>

> _____
> Full-Disclosure - We believe in it.

> Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

> Hosted and sponsored by Secunia - <http://secunia.com/>

>

>

Re: [Full-disclosure] obtai an IP of an MSN Messenger contact

Re: [Full-disclosure] obtain an IP of an MSN Messenger contact

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Are you using the latest version of MSN Messenger? Download MSN Messenger 7.5 today!
<http://join.msn.com/messenger/overview>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>