Backtracking EMAIL Messages

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

Tracking email back to its source: Twisted Evil
cause i hate spammers... Evil or Very Mad

Ask most people how they determine who sent them an email message and the response is almost universally, "By the From line." Unfortunately this symptomatic of the current confusion among internet users as to where particular messages come from and who is spreading spam and viruses. The "From" header is little more than a courtesy to the person receiving the message. People spreading spam and viruses are rarely courteous. In short, if there is any question about where a particular email message came from the safe bet is to assume the "From" header is forged.

So how do you determine where a message actually came from? You have to understand how email messages are put together in order to backtrack an email message. SMTP is a text based protocol for transferring messages across the internet. A series of headers are placed in front of the data portion of the message. By examining the headers you can usually backtrack a message to the source network, sometimes the source host. A more detailed essay on reading email headers can be found .

If you are using Outlook or Outlook Express you can view the headers by right clicking on the message and selecting properties or options.

Below are listed the headers of an actual spam message I received. I've changed my email address and the name of my server for obvious reasons. I've also double spaced the headers to make them more readable.

Return-Path: <s359dyxtt@yahoo.com>

X-Original-To: davar@example.com

Delivered-To: davar@example.com

Received: from 12-218-172-108.client.mchsi.com (12-218-172-108.client.mchsi.com [12.218.172.108])
by mailhost.example.com (Postfix) with SMTP id 1F9B8511C7
for <davar@example.com>; Sun, 16 Nov 2003 09:50:37 -0800 (PST)

Received: from (HELO 0udjou) [193.12.169.0] by 12-218-172-108.client.mchsi.com with ESMTP id <536806-74276>; Sun, 16 Nov 2003 19:42:31 +0200

Message-ID: <n5-l067n7z$46-z$-n@eo2.32574>

From: "Maricela Paulson" <s359dyxtt@yahoo.com>

Reply-To: "Maricela Paulson" <s359dyxtt@yahoo.com>

To: davar@example.com

Subject: STOP-PAYING For Your PAY-PER-VIEW, Movie Channels, Mature Channels...isha

Date: Sun, 16 Nov 2003 19:42:31 +0200

X-Mailer: Internet Mail Service (5.5.2650.21)

X-Priority: 3

MIME-Version: 1.0

Content-Type: multipart/alternative; boundary="MIMEStream=_0+211404_90873633350646_4032088448"

According to the From header this message is from Maricela Paulson at s359dyxxt@yahoo.com. I could just fire off a message to abuse@yahoo.com, but that would be waste of time. This message didn't come from yahoo's email service.

The header most likely to be useful in determining the actual source of an email message is the Received header. According to the top-most Received header this message was received from the host 12-218-172-108.client.mchsi.com with the ip address of 21.218.172.108 by my server mailhost.example.com. An important item to consider is at what point in the chain does the email system become untrusted? I consider anything beyond my own email server to be an unreliable source of information. Because this header was generated by my email server it is reasonable for me to accept it at face value.

The next Received header (which is chronologically the first) shows the remote email server accepting the message from the host 0udjou with the ip 193.12.169.0. Those of you who know anything about IP will realize that that is not a valid host IP address. In addition, any hostname that ends in client.mchsi.com is unlikely to be an authorized email server. This has every sign of being a cracked client system.

Here's is where we start digging. By default Windows is somewhat lacking in network diagnostic tools; however, you can use the tools at to do your own checking.

davar@nqh9k:[/home/davar] $whois 12.218.172.108

AT&T WorldNet Services ATT (NET-12-0-0-0-1)
12.0.0.0 - 12.255.255.255
Mediacom Communications Corp MEDIACOMCC-12-218-168-0-FLANDREAU-MN (NET-12-218-168-0-1)
12.218.168.0 - 12.218.175.255

ARIN WHOIS database, last updated 2003-12-31 19:15
Enter ? for additional hints on searching ARIN's WHOIS database.

I can also verify the hostname of the remote server by using nslookup, although in this particular instance, my email server has already provided both the IP address and the hostname.

davar@nqh9k:[/home/davar] $nslookup 12.218.172.108

Server: localhost
Address: 127.0.0.1

Name: 12-218-172-108.client.mchsi.com
Address: 12.218.172.108

Ok, whois shows that Mediacom Communications owns that netblock and nslookup confirms the address to hostname mapping of the remote server,12-218-172-108.client.mchsi.com. If I preface a www in front of the domain name

portion and plug that into my web browser, http://www.mchsi.com, I get Mediacom's web site.

There are few things more embarrassing to me than firing off an angry message to someone who is supposedly responsible for a problem, and being wrong. By double checking who owns the remote host's IP address using two different tools (whois and nslookup) I minimize the chance of making myself look like an idiot.

A quick glance at the web site and it appears they are an ISP. Now if I copy the entire message including the headers into a new email message and send it to abuse@mchsi.com with a short message explaining the situation, they may do something about it.

But what about Maricela Paulson? There really is no way to determine who sent a message, the best you can hope for is to find out what host sent it. Even in the case of a PGP signed messages there is no guarantee that one particular person actually pressed the send button. Obviously determining who the actual sender of an email message is much more involved than reading the From header. Hopefully this example may be of some use to other forum regulars.