On the Case with *Sam Spade*

by M. E. Kabay, PhD, CISSP  
Security Leader  
INFOSEC Group  
AtomicTangerine, Inc.

In this newsletter, I thought some readers would enjoy seeing the steps in finding out the details of yet another e-mail scam: fraudulent click-throughs.

On Dec. 23, 2000, I received an HTML invitation from a stranger to try a "new game." Unimpressed by the warmth of the invitation and suspicious of any attachment, I looked at the source code and found some peculiar aspects:

```html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>Untitled</title>
</head>
<body><P ALIGN=CENTER>
<A HREF="http://www.findcommerce.com/tracking/sarefer.dll?HostBannerID=23589" TARGET="_top" onmouseover="window.status='CLICK IT';return true"> <font size="+1">click here</font></A><IMG SRC="http://www.whispa.com/tracking/exposure.dll?263589" WIDTH=1 HEIGHT=1 BORDER=0><br><br>To join new game for free<br>No charge</p>
</body>
</html>
```

The source suggested that the intent of this information was primarily to track responses, not to convey information.

I then turned to the Sam Spade 1.14 network utility (see [http://www.samspade.org/ssw/](http://www.samspade.org/ssw/) for details of this useful freeware) and quickly found that the headers were forged.

Between the asterisks below is what the program returned to me (note that the commentary - e.g., "My comments are just hints" - is the program's, not mine.):

```
***
12/27/00 16:22:21 Input  
The Received: headers are the important ones to read

My comments are just hints, and should be considered only
```
an opinion. I may have guessed wrong, or things may have
changed since I was written

Sender: Lisa@netvision.net.il
Received: from mgw-mp.sric.sri.com (mgw-mp.sric.sri.com
[128.18.23.110]) by spdmgaae.compuserve.com
(8.9.3/8.9.3/SUN-1.9) with ESMTP id PAA02807 for
<mkabay@compuserve.com>; Sat, 23 Dec 2000 15:13:11 -0500
(EST)
This received header was added by your mailserver
spdmgaae.compuserve.com received this from mgw-mp.sric.sri.com
(IP addresses match)

Received: from mailgw1.netvision.net.il ([194.90.1.14])
by mgw-mp.sric.sri.com (Netscape Messaging Server 3.6)
with ESMTP id AAA14C6 for
<mkabay@atomictangerine.com>; Sat, 23 Dec 2000 12:12:38 -0800
mgw-mp.sric.sri.com received this from mailgw1.netvision.net.il
(IP addresses match)

Received: from mailgw.netvision.net.il
(c2189.racs.surfree.net.il [212.3.197.189]) by
mailgw1.netvision.net.il (8.9.3/8.9.3) with ESMTP id
WAA00219 for <mkabay@atomictangerine.com>; Sat, 23 Dec 2000 22:12:33 +0200 (IST)
mailgw1.netvision.net.il received this from someone claiming
to be mailgw.netvision.net.il
but really from 212.3.197.189(c2189.racs.surfree.net.il)
All headers below may be forged

Message-Id: <200012232012.WAA00219@mailgw1.netvision.net.il>
From: Lisa@mailgw1.netvision.net.il
To: mkabay@atomictangerine.com
Subject: new game try it
Date: 23 Dec 2000 22:14:52 +0200
Mime-Version: 1.0
Content-Type: text/html

***

Visiting the proposed URL
(http://www.findcommerce.com/tracking/sarefer.dll?HostBannerID=263589)
simply forwarded me to a "not found" page at:
http://www.safe-audit.com/unavailable.html?INVHBID

Visiting the hidden URL
(http://www.whispa.com/tracking/exposure.dll?263589) resulted in no
response at all; trying to backtrack through the directory tree
resulted in closed connections.
Checking the registration of "whispa.com" (easily done using SamSpade) showed the registrant to be a London company Global Market Ltd., with this contact information:

Administrative Contact, Billing Contact:
Leo, Scheiner (SL2005) leo@NETCOMUK.CO.UK
Global Market Ltd.
29 Fairholme Gardens
London
N3 3ED
UK
44 181 346 0770 (FAX) 44 181 346 8316

Technical Contact:
Digiweb, Inc. (HDI2-ORG) hostmaster@DIGIWEB.COM
Digiweb, Inc.
4716 Pontiac Street
College Park, MD 20740
US
301-982-1688 Fax - 301-982-9782

The registration for "findcommerce.com" is the same.

The Tech Contact phone number had been disconnected. The U.K. number city code 181 had been changed to 208, and I was able to get through to the changed number.

I spoke with Leo Scheiner, the administrative contact, who turned out to be a good guy. He very kindly explained the situation. The company normally counts hits on banner ads; it has nearly 100,000 subscribers. These subscribers are paid according to how many people click on those banner ads from their sites.

In this case, the perpetrator was a sleazy operator. It seems that this crook was trying to generate revenue by fraudulently generating clicks on his assigned URL. He did so by using unsolicited commercial e-mail to trick gullible people into creating fruitless clicks on his assigned URL.

MORAL: Don't click on URLs that you receive in junk e-mail.

To contact M. E. Kabay:

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit <http://www.atomictangerine.com>.

Copyright 8 2000 M. E. Kabay. All rights reserved.
Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.