WebMail Forensics

Thomas Akin, CISSP
Director, Southeast Cybercrime Institute
Kennesaw State University
Overview

• Web Browser Forensics
  – Internet Explorer
  – Netscape

• WebMail Services
  – Cookies, History, & Cache, oh my…

• WebMail Headers

• Obscuring WebMail Headers

• Yahoo! Mail
  – History, Cache, URLs

• Hotmail
  – History, Cache, URLs

• Helpful Tools

• Other Services
  – Hushmail
  – Ziplip
Web Browser Forensics

**Internet Explorer**
- Internet Favorites
- Cookies
- History
- Typed URLs
- Temporary Internet Files
- Autocompletion

**Netscape**
- Bookmarks
- Contacts
- History
- Preferences
- Typed URLs
- Cookies
- Cache
Favorites
Cookies
History
Typed URLs
Temporary Internet Files

```
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5>ls -1F

 total 2241
 drwxrwxrwx 1 user  group  0 Jul 15 20:52 8TIJC9YR
 drwxrwxrwx 1 user  group  0 Jul 15 20:42 8XURWJU7\n drwxrwxrwx 1 user  group  0 Jul 15 20:42 8ZN7MCDX\n drwxrwxrwx 1 user  group  0 Jul 15 20:42 E5HAFITO\n drwxrwxrwx 1 user  group  0 Jul 15 20:42 GTUNS9AB\n drwxrwxrwx 1 user  group  0 Jul 15 20:42 OTQZ8LAB\n drwxrwxrwx 1 user  group  0 Jul 15 20:42 PNZU1XWE\n drwxrwxrwx 1 user  group  0 Jul 15 20:42 ZYW3JP4L\n-rw-rw-rw- 1 user  group  67 Jul 14 14:24 desktop.ini
-rw-rw-rw- 1 user  group  2293760 Jul 15 20:52 index.dat

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5>1s -1F ZYW3JP4L

 total 41
-rw-rw-rw- 1 user  group  11670 Jul 15 17:08 DEU8529a_728[1].gif
-rw-rw-rw- 1 user  group  9349 Jul 14 18:24 TP30000000000000002.0204.04_ZAHola.6.2.18.185,verdenab,8,204,102,0_ZAHelpful\3F%20Consider%20leaving%20a%20tip%216,14,17,185,times,11,0,0,0[1].jpg
-rw-rw-rw- 1 user  group  424 Jul 14 20:00 aoladp[1].htm
-rw-rw-rw- 1 user  group  67 Jul 14 14:54 desktop.ini
-rw-rw-rw- 1 user  group  16601 Jul 14 18:21 search[2]
```

CONTINUING EDUCATION at KENNESAW STATE UNIVERSITY
Auto-completion
WebMail Clients

Web based email clients are susceptible to the same problems of all clients that utilize web browsers:

Browsers store *tons* of data on the local hard drive....
The user must perform some action that causes the page to be cached on the system...

i.e. Reading a Message bring the message up in the browser and causes it to be cached. Sending a message does not since the browser doesn’t display the sent message...
In addition to standard email headers, most webmail clients contain useful information on their origin:

```
This message is not flagged. [ Flag Message - Mark as Unread ]

From Thom Thomas Tue Jul 15 18:34:03 2003
  X-Apparently-To: badboy83210@yahoo.com via 216.136.130.41; 15 Jul 2003 18:34:04 -0700 (PDT)
  Return-Path: <takin00@hotmail.com>
  Received: from 64.4.27.104 (EHLO hotmail.com) (64.4.27.104) by mta114.mail.scd.yahoo.com with SMTP; 15 Jul 2003 18:34:04 -0700 (PDT)
  Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC; Tue, 15 Jul 2003 18:34:04 -0700
  Received: from 130.218.62.189 by by8fd.by8.hotmail.msnn.com with HTTP; Wed, 16 Jul 2003 01:34:03 GMT
  X-Originating-IP: [130.218.62.189]
  X-Originating-Email: [takin00@hotmail.com]
  From: "Thom Thomas" <takin00@hotmail.com> | This is spam | Add to Address Book
  To: badboy83210@yahoo.com
  Bcc: 
  Subject: here are the headers
  Date: Tue, 15 Jul 2003 21:34:03 -0400
  Mime-Version: 1.0
  Content-Type: text/plain; format=flowed
  Message-ID: <BAY8-F104ntDEJmGzrL000148b4@hotmail.com>
  X-OriginalArrivalTime: 16 Jul 2003 01:34:04.0105 (UTC) FILETIME=[57485390:01C34B3A]
  Content-Length: 223

a header, a header, my kingdom for a header...
```
Obscuring WebMail Headers

- Open Relay
- False Received From Headers
- Anonymizer
- Open Proxy
- SSH Tunnel (or port redirector)
Open Relays

- Spoofers use Open Relays to attempt to hide the person and IP address of the system that sent the email.
- By itself, email sent through open relays still contains the IP address of the actual sender.
- Combined with other techniques, open relays can be a hindrance to investigations.
Open Relay

- Where to look for evidence:
- Email Header will contain the originating IP address.
- Open Relay log files will also contain the originating IP address.
False Received From Header

• Leads the investigator to the wrong server by adding a seemingly valid Received: from header.

• To avoid detection, the spoofer’s real address will be recorded somewhere in the Received: from headers, but the investigator will not know which one.
% telnet aramis.kennesaw.edu 25
Trying 130.218.62.92...
Connected to aramis.kennesaw.edu.
Escape character is '^]'.
  helo pigseye.kennesaw.edu
250 Aramis.kennesaw.edu Hello PigsEye.Kennesaw.EDU [130.218.100.16], pleased to meet you
mail from: georgew@korea.net
250 2.1.0 georgew@korea.net... Sender ok
rcpt to: takin@aramis.kennesaw.edu
250 2.1.5 takin@aramis.kennesaw.edu... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Received: from korea.net (korea.net [61.78.36.151])
  by pigseye.kennesaw.edu (8.12.1/8.12.1) with SMTP id h2P17ctR04AA5D
  Mon, 24 Feb 2003 19:04:13 -0500 (EST)
Date: Mon, 24 Feb 2003 19:06:39 -0500 (EST)
Subject: Camp David
To: "Thomas Akin" <takin@kennesaw.edu>
From: "George W" <georgew@korea.net>
Message-Id: <200302250024.h1P0NbTr027946@korea.net>

Thomas,

You and Abby coming up to Camp David this weekend? Hope to see you soon...

W

250 2.0.0 h1P0RqTr027955 Message accepted for delivery
False Received From Header

From georgew@korea.net  Mon Feb 24 19:29:01 2003
Return-Path: <georgew@korea.net>
Received: from pigseye.kennesaw.edu (PigsEye.Kennesaw.EDU [130.218.100.16])
    by Aramis.kennesaw.edu (8.12.1/8.12.1) with SMTP id h1P0RqTr027955
    for takin@aramis.kennesaw.edu; Mon, 24 Feb 2003 19:28:05 -0500 (EST)
Received: from korea.net (korea.net [61.78.36.151])
    by pigseye.kennesaw.edu (8.12.1/8.12.1) with SMTP id h2P17ctR04AA5D
    for takin@kennesaw.edu; Mon, 24 Feb 2003 19:04:13 -0500 (EST)
Date: Mon, 24 Feb 2003 19:06:39 -0500 (EST)
Subject: Camp David
To: "Thomas Akin" <takin@kennesaw.edu>
From: "George W" <georgew@korea.net>
Message-Id: <200302250024.h1P0NbTr027946@korea.net>

Thomas,

You and Abby coming up to Camp David this weekend? Hope to see you soon...

W
False Received From Header

Where to look for evidence

- Email Received: from headers will contain the actual IP address of the originating system, you just won’t know which Received: from header is correct.
- Trace backwards by looking at the log files of the servers the email claims to have passed through. Once you get to a server that has no record of the email, the previous system is the originating IP.
Members Homepage

Begin Surfing Privately

Just type in the URL and click go!

http://mail.yahoo.com

Search: [Default] for [search]

Select Your Settings: [Normal] [Maximum] [Custom]

ATTENTION USERS: When you click "GO" and leave this page, you may see a warning from Internet Explorer that you are "redirected to a page that is not secure." YOU CAN DISREGARD THIS WARNING and click 'OK'. You are still completely protected by Anonymizer. [Click here to find out more.]

Attention Members

Upgrade Now For Extra Protection
Anonymizer (Web)

Email sent from IP address 64.32.161.244
Anonymizer (Web)

Where to look for evidence:

- The email headers and web mail log files will point back to the anonymizer.
- You will need to look at the anonymizer’s log files to determine what IP address accessed the web email account at the specific time the email was sent.
- If the anonymizer is a paying service then you can also request subscriber information for the account that was using the anonymizer to send the web based email.
Open Proxy
Email sent from IP address 64.32.161.244
Open Proxy

Where to look for evidence:

- The email headers and web based email logs will contain the IP address of the open proxy.
- The Open Proxy log files will contain the IP address of the originating system.
login as: takin
Sent username "takin"
takin@cyberpass.net's password:
Last login: Wed Feb 19 09:34:05 2003 from ip-64-32-161-244.dsl.atl.megapath.net

--- News Update 01-10-03 ---

In our continued effort to fight spam you will now be required to provide auth information before sending mail. Please visit http://email.anonymizer.com for instructions on setting this up.

--- News Update 05-08-01 ---

* SSH 2 Connections are now Supported *

SSH 2 has improved security features!
Your Client Doesn't Support SSH2?
No Problem!
Available now on the Anonymizer Website F-Secure SSH Client. Available for both Windows and Macintosh platforms.
http://www.anonymizer.com/software/Fsecure.html

You are logged into SSH tunneling. Your connection will be terminated after 24 hours.

Multiple logins are not permitted. Abuse of SSH tunneling will not be tolerated.

Have a nice day.
Anon SSH Tunnel

Email sent from IP address 64.32.161.244

SSH Tunneling....
Anon SSH Tunnel

Where to look for evidence:

- The email headers will contain the IP address of the SSH server the person was logged into.
- SSH servers, by default, do not record what tunnels are created through them.
- SSH servers do record login information so you will need to determine who was logged into the system through ssh at the time the email was sent. One of these log entries will be the originating IP.
Combining Techniques: Tunnels with an Open Proxy

- Spoofer uses a SSH Client connects to a SSH Server creating a tunnel to an Open Proxy port 80 (usually)
- Spoofer then reconfigures their browser to connect to the SSH Tunnel which is redirected to the Open Proxy port 80.
- They then browse to a web based email system and send their email.
- The headers record the IP address of the Open Proxy, not the originating system.
Combining Techniques: Tunnel with an Open Proxy

Where to look for evidence:

- The email headers and web based email logs will contain the IP address of the Open Proxy.
- The Open Proxy logs files will contain the IP address of the SSH server used.
- SSH tunnels are not logged, so you will have to determine who was logged into the server through ssh at the time the email was sent. One of these will be the originating IP.
Local Analysis
Yahoo! Mail & HotMail

- Index.dat & fat.db
- Cache Files
- Typed URLs
- Auto-completion
- Cookies
- History Files
Examples

• Live Examples: Cookies
• Live Example: History Files
• Live Example: URL interpretation
• Live Example: Manually Parsing index.dat
Tools to make your life easier

- Web Cache Illuminator (www.nstarsolutions.com)
- Cache Monitor (www.webattack.com)
- Cache Auditor (www.webattack.com)
- Internet Cache Explorer (www.webattack.com)
- STG Cache Audit (www.webattack.com)
My Favorites

Internet Explorer
- Cache Auditor
- Internet Cache Explorer

Netscape
- Web Cache Illuminator
IE's Cache (Internet Cache Explorer)
IE Cache for Yahoo! Mail

Specifically look for yahoo URLs containing:

• Compose
• ShowFolder
• ShowLetter
• Preferences
• Options
• Login

• Examples...
IE’s Cache (Internet Cache Explorer)
Testing with netscape

On Tue, Jul 15, 2003 at 08:13:03PM -0400, BadBoy 001 wrote:
> testing with going to sent folder
>
> >
> > > MSN 8 helps eliminate e-mail viruses. Get 3 months FREE!
> > http://join.msn.com/?page=features/virus
>
> --

Thomas Akin, CISSP
Director, Southeast Cybercrime Institute
Live Examples...

- Live examples of retrieving WebMail information:
  - Received emails
  - Sent emails
  - Folders
  - Address books
Network Forensics

- Using Sniffers to capture webmail data...
  - Clear http
  - Encrypted https
  - Login & Password recovery
  - Capturing both incoming & outgoing email text
Other Options

How clients such as Hushmail, ZipLip, and Anonymous Remalers are attempting to enhance email privacy:

- Hushmail
- ZipLip
- Anonymizers
- Etc…
Thank you

Questions?

Thomas Akin
Southeast Cybercrime Institute
Kennesaw State University
1000 Chastain Road #3301
Kennesaw, GA 30144-5591
takin@kennesaw.edu
www.cybercrime.kennesaw.edu