

WebMail Forensics

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



CONTINUING EDUCATION at KENNESAW STATE UNIVERSITY



- Web Browser Forensics
 - Internet Explorer
 - Netscape
- WebMail Services
 - Cookies, History, &Cache, oh my...
- WebMail Headers
- Obscuring WebMail Headers

Overview

- 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

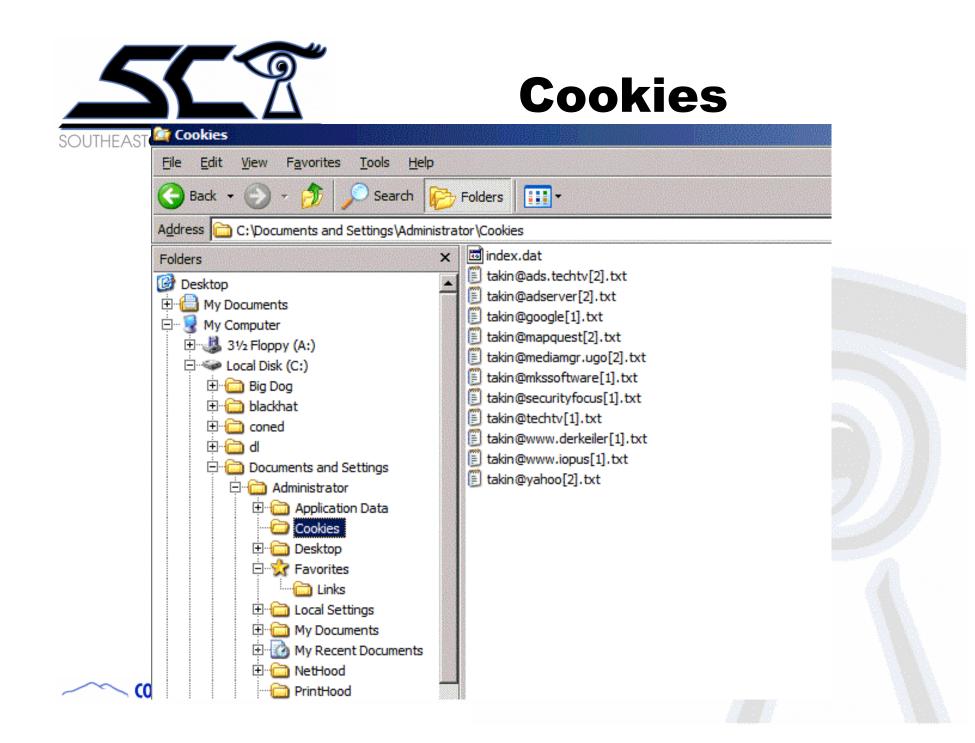
Netscape

- Bookmarks
- Contacts
- History
- Preferences
- Typed URLs
- Cookies
- Cache



Favorites

lress 🔕 <u>http://</u>	Add to Favorites	
	Organize Favorites	
	🔁 Links	• •
	About American Indian Studies Programs	
	Cool Solutions	
	RealOne Home Page	
	Anonymous Remailer FAQ	
	Information Security Magazine Year 2003 Buyers' Guide	
	Mortgage payment calculator and loan information	Crowne Directory
	Crime Scene Evidence File	Groups Directory
	 Top Picks Tutorial Software 	
	Computer Forensics Report	
	httpvip.poly.edu-kulesh-forensics-comp_forensics.pdf	I'm Feeling Lucky
	Category	
	http://www.crypto.com-papers-mk.pdf	





History

SOUTHEASTCYBERCRIMEINSTITUTE

🔯 History		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		
🚱 Back 🔹 🕥 🖌 🏂 🔎 Search 😥 Folders 🔲 🔹		
Address 🙆 C: \Documents and Settings \Administrator \Local Settings \History		
Folders	× Monday	
🖻 🖘 Local Disk (C:)	Today	
🕀 💼 Big Dog		
🕀 💼 blackhat		
🗄 💼 coned		
i i ·· 🛅 di		
🖻 🛅 Documents and Settings		
🛱 🔂 Administrator		
🕀 💼 Application Data		
Cookies		
🕀 💼 Desktop		
🕀 🙀 Favorites		
🖻 🔂 Local Settings		
🕀 🚞 Application Data		
🛱 🔞 History		
🛱 🛄 Monday		
@ 216.239.41.104		
address.mail.yahoo (address.mail.yahoo.com)		
Billing.mail.yahoo (billing.mail.yahoo.com)		
channels.netscape (channels.netscape.com)		
computing (www.computing.net)		



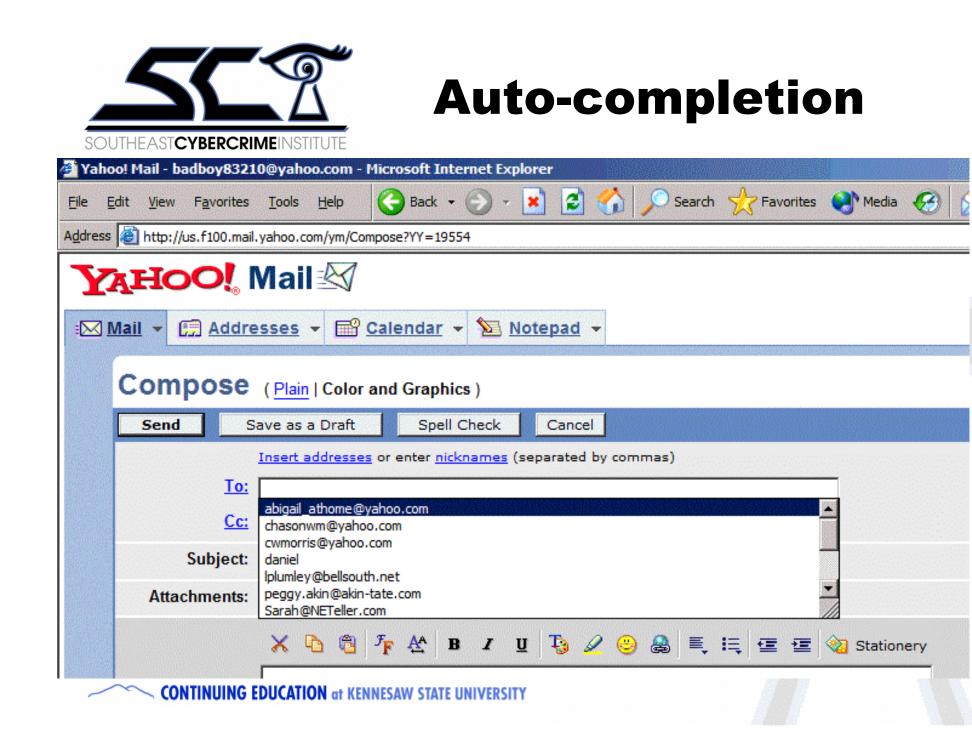
Typed URLs

<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>H</u> elp			
🚊 👜 Internet Explorer	▲ Name	Туре	Data
🕀 🚞 Default HTML Edi	tor (Default)	REG_SZ	(value not set)
🕀 💼 Default MHTML E	ditc aburl1	REG_SZ	http://www.blackhat.com/
🕀 💼 Desktop	abjuri 10	REG_SZ	http://www.karenware.com/
💭 Document Windo	ws aburl11	REG_SZ	http://www.fkeeps.com/
Download	ab url 12	REG_SZ	http://www.iopus.com/
🕀 🛄 Explorer Bars	abjurl13	REG_SZ	http://www.resplendence.com/
Extensions	ab]url14	REG_SZ	http://www.nstarsolutions.com/
Help_Menu_URLs	url 15	REG_SZ	www.nstarsolultions.com
	ab url 16	REG_SZ	http://www.sysinternals.com/
🗈 🔛 International	abjurl17	REG_SZ	http://members.cox.net/dos/batch01.htm
<u>-</u> Main (∓ <mark>)</mark> Media	abjurl 18	REG_SZ	http://www.netscape.com/
• MenuExt	abjurl2	REG_SZ	http://mail.yahoo.com/
PageSetup	abjurl3	REG_SZ	http://mail.yahoo.com
SearchUrl	abjurl4	REG_SZ	http://mail.yahoo.com/config/login?&.done
🕀 💼 Security	abjuri5	REG_SZ	http://mail.yahoo.com/config/login?tries=1
- 🧑 Services	ab)url6	REG_SZ	http://mail.yahoo.com/config/login?tries=1
Settings	ab)url7	REG_SZ	http://www.vim.org
🕀 💼 Toolbar	ab)url8	REG_SZ	http://www.vim.com/
	allo abjurl9	REG_SZ	http://www.webattack.com/
URLSearchHooks		120_02	http://mininesatulation/



Temporary Internet Files

c:\WINDOWS\System32\cmd.exe C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\ Content.IE5≻1s −1F total 2241 0 Jul 15 20:52 8TIJC9YR drwxrwxrwx 1 user group 0 Jul 15 20:42 8XURWLU7 drwxrwxrwx 1 user group 0 Jul 15 20:42 8ZN7MCDX drwxrwxrwx 1 user group 0 Jul 15 20:42 E5HAFITO drwxrwxrwx 1 user group 0 Jul 15 20:42 GTUNS9AB drwxrwxrwx 1 user group 0 Jul 15 20:42 OTQZ8LAB drwxrwxrwx 1 user group 0 Jul 15 20:42 PNZU1XWE drwxrwxrwx 1 user group 0 Jul 15 20:42 ZYW3JP4L drwxrwxrwx 1 user group 67 Jul 14 14:24 desktop.ini 1 user rw-rw-rwgroup 2293760 Jul 15 20:52 index.dat rw-rw-rw-1 user group C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\ Content.IE5≻ls -1F ZYW3JP4L total 41 11670 Jul 15 17:08 DEV8529a_728[1].gif 1 user ru-ru-rugroup 9349 Jul 14 18:24 TP3000000000000000002.0204 1 user -rw-rw-rwgroup 04._ZAHola,6,2,18,185,verdenab,8,204,102,0_ZAHelpful%3F%20Consider%20leaving%20a 20tip21,6,14,17,185,times,11,0,0,0_[1].jpg 424 Jul 14 20:00 aoladp[1].htm rw-rw-rw-1 user group 67 Jul 14 14:54 desktop.ini 1 user rw-rw-rwgroup 16601 Jul 14 18:21 search[2] 1 user group rw-rw-rw-C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\ Content.IE5> C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\





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....



Key to WebMail Forensics

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...



WebMail Headers

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.bay8.hotmail.msn.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.



- 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 '^]'. 220 Aramis.kennesaw.edu ESMTP Sendmail 8.12.1/8.12.1; Mon, 24 Feb 2003 19:27:52 -0500 (EST) helo pigseye.kennesaw.edu 250 Aramis.kennesaw.edu Hello PigsEye.Kennesaw.EDU [130.218.100.16], pleased to meet vou 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 ...

250 2.0.0 h1PORqTr027955 Message accepted for delivery



🐣 aramis.kennesaw.edu - PuTTY _ 🗆 × i:Exit -: PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next 2:Hel 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 h1PORqTr027955 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 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...

Ŵ



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 the has no record of the email, the previous system is the originating IP.



Anonymizer (Web)

SOUTHEASTCYBERCRIMEINSTITUTE

🕯 Anonymizer.	com - Micros	oft Inte	rnet Explo	er								
<u>File E</u> dit <u>V</u> ie	w F <u>a</u> vorites	<u>T</u> ools	<u>H</u> elp	子 Back	- 📀	- 💌 👔	2 🏠	🔎 Search	K Favorit	es 😢 Media	3	3- 실 🗉
ddress 🙋 .and	nymizer.com/to	oolbar.cgi	?params=rh	As 1gtHrBe	0W7UhnZ	zjG%2fFE%	2b1FQIXW	fdxuJtpoIX%2	oLMCjQl7cV%2	fGucAPPtxvPBDa	aYrZMKTGSN	1jZz%2bpvGKS
											17	
ANON	YMIZ											
	Pr	rivacy is	your right									
			но	IE PRO	DUCTS	SIGN UP	SUPPOR		RS MEDIA	DOWNLOADS		
	IS HOMEPAGE	-	M	mher	e Ho	mepag	P					
here.							•					
	T INFORMATION		B	gin Su	rfing F	Privately						
account	•	nye	Jus	t type in the	e URL and	d click go!						
	NLOADS		ht	o://mail.y	ahoo cu			go				
Downloa have pur	d any software chased	e you		o.minan.y	anoo.co			52.55				
					Search:	Default	💌 for		search			
	IONYMOUS EM ails that don't gi					Norma	I O Maxi	mum 🔘 Cus	tom			
identity a	way.		S	lect Your S	Settings:			About the Se				
	A BUG REPORT	[
	ow about any you experienc	æ.				-				warning from In S WARNING and	-	
	OKIES		still	completely	protected	by Anonym	izer. <u>Click h</u>	ere to find out	more.			
View all.	Anonymizer co	okies,										
with des	inpuons.		A	tentior	n Men	nbers						
End your	current Anony	mizer	U	grade	Now	For Ext	tra Pro	otection				



Anonymizer (Web)

SOUTHEASTCYBERCRIMEINSTITUTE

A:Exit -:PrevPg <space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Hel From takin2010@yahoo.com Mon Feb 24 19:41:07 2003 Return-Path: <takin2010@yahoo.com> Received: from web41408.mail.yahoo.com (web41408.mail.yahoo.com [66.218.93.74]) by Aramis.kennesaw.edu (8.12.1/8.12.1) with SMTP id h1P0f7Tr027980 for <takin@aramis.kennesaw.edu>; Mon, 24 Feb 2003 19:41:07 -0500 (EST) Message-ID: <20030225004058.93648.qmail@web41408.mail.yahoo.com> Received: from [130.94.106.247] by web41408.mail.yahoo.com via HTTP; Mon, 24 Feb 2003 16:40:58 PST Date: Mon, 24 Feb 2003 16:40:58 -0800 (PST) From: T Akin <takin2010@yahoo.com> Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="0-1137446318-1046133658=:92908"</takin2010@yahoo.com></takin@aramis.kennesaw.edu></takin2010@yahoo.com></space>
<pre>Return-Path: <takin2010@yahoo.com> Received: from web41408.mail.yahoo.com (web41408.mail.yahoo.com [66.218.93.74])</takin2010@yahoo.com></pre>
<pre>Received: from web41408.mail.yahoo.com (web41408.mail.yahoo.com [66.218.93.74])</pre>
<pre>by Aramis.kennesaw.edu (8.12.1/8.12.1) with SMTP id h1P0f7Tr027980 for <takin@aramis.kennesaw.edu>; Mon, 24 Feb 2003 19:41:07 -0500 (EST) Message-ID: <20030225004058.93648.qmail@web41408.mail.yahoo.com> Received: from [130.94.106.247] by web41408.mail.yahoo.com via HTTP; Mon, 24 Feb 42003 16:40:58 PST Date: Mon, 24 Feb 2003 16:40:58 -0800 (PST) From: T Akin <takin2010@yahoo.com> Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0</takin2010@yahoo.com></takin@aramis.kennesaw.edu></pre>
<pre>for <takin@aramis.kennesaw.edu>; Mon, 24 Feb 2003 19:41:07 -0500 (EST) Message-ID: <20030225004058.93648.qmail@web41408.mail.yahoo.com> Received: from [130.94.106.247] by web41408.mail.yahoo.com via HTTP; Mon, 24 Feb 42003 16:40:58 PST Date: Mon, 24 Feb 2003 16:40:58 -0800 (PST) From: T Akin <takin2010@yahoo.com> Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0</takin2010@yahoo.com></takin@aramis.kennesaw.edu></pre>
<pre>Message-ID: <20030225004058.93648.qmail@web41408.mail.yahoo.com> Received: from [130.94.106.247] by web41408.mail.yahoo.com via HTTP; Mon, 24 Feb +2003 16:40:58 PST Date: Mon, 24 Feb 2003 16:40:58 -0800 (PST) From: T Akin <takin2010@yahoo.com> Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0</takin2010@yahoo.com></pre>
Received: from [130.94.106.247] by web41408.mail.yahoo.com via HTTP; Mon, 24 Feb 2003 16:40:58 PST Date: Mon, 24 Feb 2003 16:40:58 -0800 (PST) From: T Akin <takin2010@yahoo.com> Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0</takin2010@yahoo.com>
+2003 16:40:58 PST Date: Mon, 24 Feb 2003 16:40:58 -0800 (PST) From: T Akin <takin2010@yahoo.com> Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0</takin2010@yahoo.com>
Date: Mon, 24 Feb 2003 16:40:58 -0800 (PST) From: T Akin <takin2010@yahoo.com> Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0</takin2010@yahoo.com>
From: T Akin <takin2010@yahoo.com> Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0</takin2010@yahoo.com>
Subject: Anonymizer Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0
To: takin@Aramis.kennesaw.edu MIME-Version: 1.0
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0-1137446318-1046133658=:92908"
Contract Terrary to lain a characteria anali
Content-Type: text/plain; charset=us-ascii
Email sent from IP address 64.32.161.244
Do you Yahoo!?
- Yahoo! Tax Center - forms, calculators, tips, and more



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

ternet Options .ocal Area Network (LAN) Settings	? × ? × ? ×
Automatic configuration Automatic configuration may override manual settings. To ensuruse of manual settings, disable automatic configuration. Automatically detect settings Use automatic configuration script Address	re the logic for
Proxy server Use a proxy server for your LAN (These settings will not app	oly to Groups Directory
✓ dial-up or VPN connections). Address: 213.138.32.52 Port: 80 Advance ■ Bypass proxy server for local addresses	
dial-up or VPN connections). Address: 213.138.32.52 Port: 80 Advance Bypass proxy server for local addresses	ed
dial-up or VPN connections). Address: 213.138.32.52 Port: 80 Advance Bypass proxy server for local addresses OK Ca	ed Search I'm Feeling Lucky



Open Proxy

SOUTHEASTCYBERCRIMEINSTITUTE

📌 aramis.kennesaw.edu - PuTTY	- D X
i:Exit -: PrevPg <space>:NextPg v:View Attachm. d:Del r:Reply j:Next</space>	?:Hel 🔺
From takin2010@yahoo.com Mon Feb 24 19:54:30 2003	
Return-Path: <takin2010@yahoo.com></takin2010@yahoo.com>	
Received: from web41402.mail.yahoo.com (web41402.mail.yahoo.com [66.218.93.	68])
by Aramis.kennesaw.edu (8.12.1/8.12.1) with SMTP id h1P0sTTr027991	
for <takin@aramis.kennesaw.edu>; Mon, 24 Feb 2003 19:54:30 -0500 (E</takin@aramis.kennesaw.edu>	ST)
Message-ID: <20030225005424.46297.qmail@web41402.mail.yahoo.com>	
Received: from [213.138.32.52] by web41402.mail.yahoo.com via HTTP; Mon, 24	Feb
+2003 16:54:24 PST	
Date: Mon, 24 Feb 2003 16:54:24 -0800 (PST)	
From: T Akin <takin2010@yahoo.com></takin2010@yahoo.com>	
Subject: Open Proxy Test	
To: takin@Aramis.kennesaw.edu	
MIME-Version: 1.0	
Content-Type: multipart/alternative; boundary="0-522879427-1046134464=:4607	3"
Content-Type: text/plain; charset=us-ascii	

This is an email sent from an Open Proxy

Thomas

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.



Anon SSH Tunnel

SOUTHEASTCYBERCRIMEINSTITUTE

🛃 cyberpass.net - PuTTY

	<u>_</u>
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.	A
Multiple logins are not permitted. Abuse of SSH tunneling will not be tolerated .	

Have a nice day.



Anon SSH Tunnel

🐣 aramis.kennesaw.edu - PuTTY _ | D| × i:Exit -: PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Hel From takin2010@yahoo.com Mon Feb 24 20:04:59 2003 Return-Path: <takin2010@yahoo.com> Received: from web41405.mail.yahoo.com (web41405.mail.yahoo.com [66.218.93.71]) by Aramis.kennesaw.edu (8.12.1/8.12.1) with SMTP id h1P14wTr028008 for <takin@aramis.kennesaw.edu>; Mon, 24 Feb 2003 20:04:58 -0500 (EST) Message-ID: <20030225010453.15919.gmail@web41405.mail.yahoo.com> Received: from [168.143.113.101] by web41405.mail.yahoo.com via HTTP; Mon, 24 +Feb 2003 17:04:53 PST Date: Mon, 24 Feb 2003 17:04:53 -0800 (PST) From: T Akin <takin2010@yahoo.com> Subject: SSH Tunnel Test To: takin@Aramis.kennesaw.edu MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="0-1365435436-1046135093=:14932" Content-Type: text/plain; charset=us-ascii SSH Tunneling.... Email sent from IP address 64.32.161.244 Do you Yahoo!? Yahoo! Tax Center - forms, calculators, tips, and more



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.



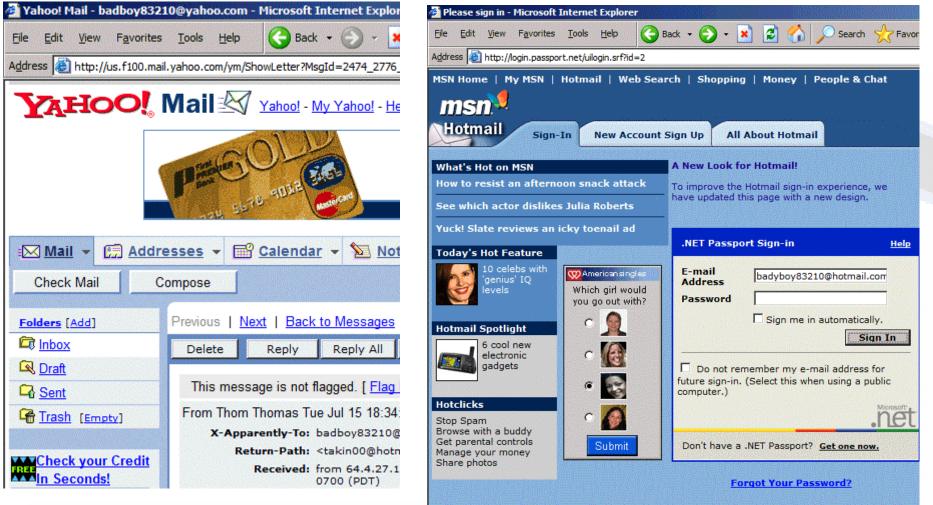
Combining Techniques: Tunnel with an Open Proxy

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



CONTINUING EDUCATION at KENNESAW STATE UNIVERSITY



Yahoo! Mail & HotMail

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

CONTINUING EDUCATION at KENNESAW STATE UNIVERSITY





- 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 (<u>www.nstarsolutions.com</u>)
- Cache Monitor (<u>www.webattack.com</u>)
- Cache Auditor (<u>www.webattack.com</u>)
- Internet Cache Explorer (www.webattack.com)
- STG Cache Audit (<u>www.webattack.com</u>)



My Favorites

Internet Explorer

- Cache Auditor
- Internet Cache Explorer

Netscape

Web Cache Illuminator



IE's Cache (Internet

Cache Explorer)

UT ICE Internet Cache Explorer		
Eile Edit View Options Help		😹
) 🖆 🚅 🖬 👗 🛍 🛍 🎒 🖪 🖪 🔲 🔫 📬 🗎 🕸	4. 8	
Image: Grade with the second seco	Find Delete Properties Fonts	
Address: http://us.f100.mail.yahoo.com/ym/ShowFolder?rb=Inbox&reset=	1&YY=76903ℴ=down&sort=date&pos=0&view=a&head=f&YN=	1
http://us.f100.mail.yahoo.	Mail 🐼 Yahoo! - My Yahoo! - Help Powered 🕼	Search Search
	REBUILD YOUR CRE	DIT
	resses - 🖼 Calendar - 🔽 Notepad -	badboy83210@yahoo.com [<u>Sign Out]</u> <u>Mail Upgrades</u> - <u>Search Mail</u> - <u>Mail Options</u>
Image: Second state of the second s	View: All Unread Flagged	0% of 4.0MB used - <u>Get more space</u> Messages 1-2 of 2 First Previous Next Last
Image: Arrow of the second	Delete Mark as Unread OK □ Sender Subject	Move to folder V OK Date Size
http://us.i1.ying.com/us.y	Thom Thomas <u>here are the headers</u>	Tue 07/15 1k
http://us.i1.yimg.com/us.y	T Yahoo! Welcome to Yahoo! Mail	Mon 07/14 503b
	Check All - Clear All	
	Delete Mark as Unroad V OK	Move to folder 💌 🖂
CacheEntryType: 1 : Normal cach UseCount: 0 Hit Rate: 2 File Size: 37219 Last Modified: Wednesday, 31, De	5 42 3D 65 39 33 71 35 75 B=e93q5u 34 76 68 36 31 6C 39 26 4vh6119s 62 3D 32 3B 20 51 3D 71 b=2; Q=q 31 3D 41 41 43 41 41 41 1=AACAAA 41 41 41 41 41 41 66 51 AAAAAfQ 2D 2D 26 71 32 3D 50 78sq2=Px	▲ ▶
http://mail.yahoo.com/		LOKAI
🧶 Start 🞯 🥭 🐨 🖉 🖉 🖏 📓 🕲 🖂 📴 WebMailFord	nsi 🛛 🖉 Xara X - [Untitle 🛛 🍎 2 Internet Expl 🚽 🔤 C: \WIN	NDOWS\S TCE Internet C « 🛃 🛃 10:04 PM



IE Cache for Yahoo! Mail

Specifically look for yahoo URLs containing:

- Compose
- ShowFolder
- ShowLetter
- Preferences
- Options
- Login
- Examples...



IE's Cache (Internet

Cache Explorer)

ICE Internet Cache Explorer		_ & ×
le <u>E</u> dit <u>V</u> iew <u>O</u> ptions <u>H</u> elp		
) 🛎 🖬 X 🖻 🖻 🚭 🖪	🔊 🔲 📑 📲 🖹 🧇 🚺 💡	
Here Hard Harden Harden	Strip bmp's Copy Find Delete Properties Fonts	
lress: http://lw12fd.law12.hotmail.msn.c	om/cgi-bin/getmsg?curmbox=F000000001&a=5a331240ed51c9ec30d8568d52ab9f40&msg=MSG1058315249.71&start=2761&len=	805&msgread=1
AX	MSN Home My MSN Hotmail Search Shopping Money People & Chat	Sign Out _{net}
http://global.msads.net/a(http://global.msads.net/a(Meb page unavailable offline	Search the Web
	Hotmail Home Inbox Compose Contacts Options Help	
🛅 http://h.msimg.com/m/hm	badyboy83210@hotmail.com Free Newsletters MSN Featured Offers Find Message	
http://h.msimg.com/m/hm http://h.msimg.com/m/hm http://h.msimg.com/m/hm	Save Address(es) Block Previous Next Close From : Thomas Akin <takin@kennesaw.edu> <t< td=""><td>i Web page u</td></t<></takin@kennesaw.edu>	i Web page u
ttp://h.msimg.com/m/hm ttp://h.msimg.com/m/hm ttp://h.msimg.com/m/hm ttp://login.passport.net/1 ttp://login.passport.net/1	To : BadBoy 001 badyboy83210@hotmail.com> Subject : Re: your mail Date : Tue, 15 Jul 2003 20:27:28 -0400	Internet Explorer is unab connected to the Interne
🛅 http://lw12fd.law12.hotma	Reply Reply All Forward Delete Put in Folder Printer Friendly Version	
http://lw12fd.law12.hotma http://lw12fd.law12.hotma http://lw12fd.law12.hotma	Testing with netscape	Please try the following:
	ta	1. To make this page click the Favorit e
http://lw12fd.law12.hotma http://msimg.com/m/hm/t	On Tue, Jul 15, 2003 at 08:13:09PM -0400, BadBoy 001 wrote:	then select the Ma
http://msimg.com/m/hm/t	> testing with going to sent folder >	 On the Tools mer When you work of
http://msimg.com/m/hm/t	>	list.
AlphaSort 🕂 AccessSort 🕢 🕨		Internet Explorer
et One: HMP1=1	· · · · · · · · · · · · · · · · · · ·	Address: 3f
et Three:	96E2C664ECA455A90D6438E87504723 B96E2C664ECA455A90D6438E87504723	■ 00000000 48 4 00000008 4D 4 00000010 47 5 00000018 45 5
A Comecuter Y come Y main		
tart 📔 🧭 🍰 🌽 🐼 🐨 🚳 🛓	8	(+, □, 0) (+



Web Cache Illuminator

& Netscape

	: <u>V</u> iew		: <u>T</u> ools			~×1			(2n)			~			
√⊐ Back	•	→ Forward		😒 Stop	🕼 Refresh	습 Home	Q Search	Favorites	💮 Media	🌀 History	Rail	📑 Print	📝 Edit	•	
A <u>d</u> dress 🧧	C:\Ten	p\cache\!	ndex-T.htm	I										•	<i>∂</i> Go
							<u>c:\1 er</u>	ıp\cache*.	<u>*</u>						
			Cre	<u>ated:</u> 7/	15/03 10:24	30 PM	Files Indexe	<u>1:</u> 33 <u>Ima</u>	ges Filtered:	41 <u>Sorte</u>	<u>d by:</u> Title / <mark>I</mark>	ate			
Google	M033F	K3Q 7/1:	5/03 8:27:5	0 PM											_
Java Se	cript N	104JFT2I.J	S 7/15/03	3 8:38:48 1	PM										
Java Se	cript N	IOLK6KNH	BJS 7/15/	/03 8:23:5	6 PM										
			LJS 7/15/												
			IS 7/15/03												
					7/15/03 8:25:										
				-	7/15/03 8:24:0										
					7/15/03 8:24:3										
					15/03 8:27:42 P										
					/03 8:27:32 PM										
					5/03 8:24:34 P										
					5/03 8:23:56 PM										
					7/15/03 8:27:3										
							.5/03 8:25:08 PI								
			viessage SNN8 7/1			BESPUN //I	i/03 8:24:30 PM								
			ARUO 7.												
			9U.SRF 7												
			4K.SRF 7												
			5/03 8:23:2		201101										
			7/15/03 8		vr										
	_		7/15/03 8												
	-		5 7/15/03												
	-		/15/03 8:23												
	_	-	/15/03 8:23												
	_	-	SS 7/15/0		PM										
		-	/15/03 8:24												
													🛄 My Comp		_



Web Cache Illuminator

& Netscape

Eile Edit View Favorites Iools Help Image: Start Stop Image: Stop Image: Stop Image: Stop Image: Stop Image: Stop Back Forward Stop Refresh Home Search Favorites Media	Mail Print Edit	
Address M C:\Temp\cache\M12L2VVC		i∻ G
	Eine Back	
MSN Home My MSN Hotmail Search Shopping Money People & Chat	Sign Out _{.net}	
msn 🎾	Search the <u>W</u> eb	
	go go	
Hotmail Home Inbox Compose Contacts Options Help		
badyboy83210@hotmail.com Free Newsletters MSN Featured Offers	s Find Message MSN Calendar	
Save Address(es) Block Previous Next Close	Hotmail Services	
From : Thomas Akin <takin@kennesaw.edu></takin@kennesaw.edu>	Free Newsletters	
To: BadBoy 001 <badyboy83210@hotmail.com></badyboy83210@hotmail.com>	<u>MSN Featured</u> Offers	
Subject : Re: your mail	Find Message	
Date : Tue, 15 Jul 2003 20:27:28 -0400	Directories	
Reply Reply All Forward Delete Put in Folder 🔽 Printer Friendly Version		
	Explore MSN	
Testing with netscape	Free Games	
ta	'Net Access Deals	
On Tue, Jul 15, 2003 at 08:13:09PM -0400, BadBoy 001 wrote:	Share Photos	
> testing with going to sent folder	Send Cash	
>	Upgrade your	
> MSN 8 helps eliminate e-mail viruses. Get 2 months FREE*.	Career	
http://join.msn.com/?page=features/virus	Find Old Friends	
	Shop AT&T Wireless	
Thomas Akin, CISSP	More	
Director, Southeast Cybercrime Institute		
	My Computer	►



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
 - Encryped 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