IR Process & Smart Phones

Terrance Maguire

tmaguire@cmdlabs.com

443-451-7330

Overview

- Smart phones
  - Android, iPhone, Blackberry

- Volatile data
  - Running processes
  - Malware / spyware

- File system examination
  - Installed applications
Bank Robbery

- Fake banking applications for Android
- ZeuS in the mobile (Zitmo)
  - Symbian and possibly Blackberry
- Starts by compromising computers
  - Captures online banking details
  - Asks users for cell phone number and model
- Intercepts SMS associated with online banking
  - Mobile transaction authentication numbers
  - Approve unauthorized bank transactions

DroidDream

- Targeting legitimate application developers
  - Embed malicious code within their applications
  - Trojaned apps put on Android market place
- Broad capabilities
  - Root the operating system
  - Exfiltrate IMEI and IMSI
Mobile Incident Response

- Closely monitor access to sensitive data
- Mobile Forensic Preparedness
  - forensic preservation of volatile data
  - Forensic examination of mobile device
- Limited network visibility
  - Banks with mobile applications
  - Organizations with company mobile devices

UNIX IR Refresher

- Network traffic shows intruder connecting
  Snort: 18:39:02 victim.3800 > attacker.3096: P
  3707982354:3707982447(93) ack 220800367
- Network connections show intruder
  
<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td># netstat -a</td>
<td></td>
</tr>
<tr>
<td>victim.3800</td>
<td>attackerIP.3096ESTABLISHED</td>
</tr>
<tr>
<td>victim.32828</td>
<td>irc-server.6667 ESTABLISHED</td>
</tr>
<tr>
<td>victim.telnet</td>
<td>investigator.2666 ESTABLISHED</td>
</tr>
</tbody>
</table>
- Processes show intruder activities
  
<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td># ps -ef</td>
<td></td>
</tr>
<tr>
<td>hacked 11749</td>
<td>1 0 Mar 30 ? 0:13 irc-client</td>
</tr>
</tbody>
</table>
Incident Response Data

- Full memory dump
- Volatile Data
- Non Volatile Data
- Network Logs

Android Systems

- Remember it’s UNIX
- Linux based OS
  - Droid x
  - G1/MyTouch
- File systems
  - YAFFS2
  - ext4
Android Memory Forensics

• Physical memory dump
  – DMD module developed by Joe Sylve
• Insert module on device (insmod dmd)
  – Creates /dev/dmd device
• Get start and end memory address(es)
  – grep –i "system ram" /proc/iomem
• Dump memory to removable media
  – echo "0x80c00000 0x9f00000" /sdcard/mem.dump" > /dev/dmd

Android Memory Forensics

• Examination of Android physical memory
  – Volatility plugin for Android memory
  – Developed by Andrew Case, Digital Forensics Solutions
Android Volatile Data

• Running processes through adb shell

$ ps
USER    PID   PPID  VSIZE  RSS  WCHAN   PC NAME
root     1     0    284   196   c00belac 0000c86c S/init
root     2     0     0     0   c006687c 0000000 kthread

• top

User 2%, System 2%, IOW 0%, IRQ 0%
User 9 + Nice 0 + Sys 7 + Idle 295 + IOW 0 + IRQ 0 + SIRQ 0 = 311

PID CPU% S #THR   VSS  RSS PCY UID Name
2161 2% R 1 860K 432K fg root top
1259 0% S 63 259604K 62492K fg system system_server
2141 0% S 8 153252K 24456K fg app_99 jackpal.androidterm
715 0% S 1 0K 0K fg root pvrflip/0

• /system/xbin/busybox netstat
Forensic Acquisition

- mre$ ./adb shell
  $ su

- # dd if=/dev/block/userdata bs=1024 | /system/bin/busybox nc 192.168.2.2 755
  7028736+0 records in
  7028736+0 records out
  7197425664 bytes transferred in 24211.203 secs

Remote Acquisition

- F-Response
  - ARM agent
  - On SDCard
- Expanding Android device support
  - Segmentation Faults on some devices
File System Examination

- Android file system forensics

Malware Analysis

- DroidDream
  - Root exploit
  - Data theft
  - Updates
Live Response Lessons

- Don’t trust the operating system
  - May give false information
  - Seek corroborating sources of evidence
- No extensive examination and searching
  - If it is that interesting, acquire memory and disk
- Don’t copy large amounts of data remotely
  - Slow and prone to failure
  - Get physical access if possible

Android Challenges

- Root access
  - alters the system
- YAFFS2 file system
  - File carving as an alternative

Hope for the future:
- Recovery partition and boot loader acquisition
  - Does not require rooting the device
- File system moving to ext4
  - Similar to common Linux file systems
iPhone Overview

- Remember it’s UNIX!
- Volatile data
  - Jailbreak (redsn0w)
  - Terminal, adv-cmds, and top
- File System
  - Physical acquisition

iPhone Volatile Data

- Process list
  - ps and top
- Network connections
Non Jailbroken iPad2

Physical Acquisition
Encryption Barriers

File System Examination

- Apple HFSX / HFS+
- Keyword searches
- File carving
  - Screen captures
Keychains

- F:\MacSamples>sqlite3.exe
  "iPhone2\Keychains\keychain-2.db"
- SQLite version 3.6.16
- Enter ".help" for instructions
- Enter SQL statements terminated with a ";"
  - sqlite> select labl,acct,svce from genp;
  - |eric.rooster@yahoo.com|Yahoo-token
  - |erooster@live.com|
  - |erikroost@hotmail.com|
  - |therooster@hotmail.com|
  - |therooster@hotmail.com|com.apple.itunesstored.keychain
  - erooster|MMODBracketsAccount|
  - LumosityBrainTrainer|erooster|LumosityBrainTrainer

Text Messages
Epilog

- Deleted SQLite entries

Keylogger

- User entered strings
Locations

- cells.plist
- cells-local.plist

Blackberry

- Loaded modules and dependencies
  - javaloader
- File System
  - Blackberry Desktop Manager
  - Mounted logically
Compromised Blackberry

- Malicious program running on Blackberry

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Size</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>net_rim_platform_resource_en_US</td>
<td>4.0.2.49</td>
<td>2288</td>
<td>Thu Sep 01 15:20:30 2005</td>
</tr>
<tr>
<td>net_rim_platform_im_resource_en_US</td>
<td>4.0.2.49</td>
<td>1824</td>
<td>Thu Sep 01 15:20:24 2005</td>
</tr>
<tr>
<td>net_rim_app_manager</td>
<td>4.0.2.49</td>
<td>1796</td>
<td>Thu Sep 01 15:20:32 2005</td>
</tr>
<tr>
<td>net_rim_app_manager_console</td>
<td>4.0.2.49</td>
<td>3364</td>
<td>Thu Sep 01 15:20:33 2005</td>
</tr>
<tr>
<td>&lt;edited for length&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net_rim_bb_phone_app</td>
<td>4.0.2.49</td>
<td>79768</td>
<td>Thu Sep 01 15:23:38 2005</td>
</tr>
<tr>
<td>net_rim_bb_task_app</td>
<td>4.0.2.49</td>
<td>38732</td>
<td>Thu Sep 01 15:35:35 2005</td>
</tr>
<tr>
<td>InstantMessaging</td>
<td>4.1.7</td>
<td>329920</td>
<td>Fri Aug 12 13:54:17 2005</td>
</tr>
<tr>
<td>Smartphone</td>
<td>0.0</td>
<td>28988</td>
<td>Sat Jan 30 09:54:08 2010</td>
</tr>
</tbody>
</table>

167 modules; 9282004 bytes total

MobileSpy

Copyright 2010 cmdLabs LLC. All rights reserved.
Blackberry Backup (IPD)

Blackberry Options

- Mass Storage Mode
  - Access device via desktop OS
  - Enabled by default
  - Requires password access
- Access items in file system
  - Saved BBIM chats
  - Malware artifacts