The State of Incident Response

Presented by
Kevin Mandia

August 2, 2006
Agenda

- How Organizations are Detecting Attacks
- What Attackers are Doing
- How Current Attack Trends are Influencing the Incident Response Process
Who Are We?

- Specializing in:
  - Application Security
  - Network Security
  - Incident Response
  - Computer Forensics
  - Professional Education
  - R & D
Who Are We?

- Last 3 Years
  - Responded to over 300 Potentially Compromised Systems.
  - Responded to Intrusions at Over 40 Organizations.
  - Created IR Programs at Several Fortune 500 Firms.
The State of Incident Response

1. The Sophistication of Attack Tools Can Outweigh the Sophistication of our Response Tools.
2. Reporting Requirements Major Top-Brass Concern:
   - Disclosure to Clients
   - Disclosure to Shareholders
3. Incident Owners have to Be Politically Savvy to Achieve Corporate Goals
   - Incident Response “Owners” are not High Enough on the Food Chain to be the Deciderers.
4. Diligent IR Does Not Always Parallel Management Objectives.
Inexperienced Personnel.
- Ad-Hoc Approach.
- Not Enough Rotations.
- Lack Sophisticated Skill Sets

Methods to Gather Live Response Data are too Time Consuming, Cumbersome, and May Even be Ineffective.

Technology Widgetness.

Resolution Always Requires more Resources than Expected.
9. Lack of Formal Documentation
10. Windows is the Primary Victim/Target
11. Kernel Level Rootkits More Common ???
How Organizations are Detecting Attacks
1. How are Organization’s Detecting Incidents?

- Antivirus Alerts?
  - Perhaps, but do not count on it...
  - Alerts are often ignored – and perhaps value-less without an in-depth review of the system.
  - Quarantined files often remain a mystery

Anti-Virus merely alerts an organization that something bad might have occurred. No confirmation. Potential loss of critical data.
Findings – Ongoing Intrusion

- The Review of 10 Malicious Executable Files Yielded:
  - 12/12 Files were NOT Publicly Available
  - 12/12 Files were NOT Detected by AV
  - 11/12 Files Reviewed were Packed via 2(5) Different Methods

It is Highly Unlikely AV will ever Trigger on Microsoft Tools or Sysinternal Tools.
2. How are Organization’s Detecting Incidents?

- IDS Alerts?
  - Rare Detection Mechanism.

Port 22
Port 443
VPN

IDS

Port 22
Port 443
VPN
3. How are Organization’s Detecting Incidents?

- **Clients (Outside Company)**
  - More Often than Pro-Active Countermeasures.
  - Malicious Software Discovered on Compromised End-User Systems.
  - Recently (December 2005) Found a Keylogger Configuration File that Contained Approximately 1,157 Keyword Search Terms, and URL’s for Approximately 74 Online Banking Facilities.
Something Wrong Here?
From: Financial

To: @classi.net

Sent: Thursday, February 23, 2006 10:58 AM

Subject: Important notice!

Dear Valued Financial customer,

Financial has a strict policy to ensure all of our customer’s emails associated with their bank account’s are confirmed. Upon inspection this email was registered with your account’s, however not confirmed. Please confirm your email by clicking the link below:

http://www/acount_stats.asp

Email verification must be performed within 1 business day from receiving this email. Failure to comply will result in online banking suspension and limited account activity until an account specialist can contact you regarding this error. This can be avoided simply by following our online verification link above.

Sincerely,
Carter Franke
Financial, Safe Harbor Dept.
Financial, Account Services

Financial Equal Housing Lender
Copyright © 2006 Financial All rights reserved.
4. How are Organization’s Detecting Incidents?

- **End Users (Internal)**
  - Continual Termination of Antivirus Software.
  - Installing New Applications Simply Does Not Work.
  - Commonly Used Applications Do Not Run.
  - You Cannot “Save As”.
  - Task Manager Closes Immediately When You Execute It.
5. How Are Organization’s Detecting Incidents?

- Something Obvious …
What Attackers Are Doing
What Attackers are Doing Now

- Depends on Attack Type
  1. **Attacks for Money**
  2. **Attacks for Information**
  3. Attacks for Access
  4. Attractive Nuisances
  5. Information Warfare
Attacks for Money

- Primarily Attack Client-Side Applications or Individuals

- Target:
  - Personal Information (from Databases)
    - SSN
    - CC Numbers
    - Private Bank Account Numbers
    - Routing Numbers
    - Emails (to Phish)
  - Credentials
    - User IDs and Passwords
Attacks for Money

- Technical Characteristics:
  - Involve Email Attack Vector (Phishing) Merged With WWW Technology (Browser Issues)
  - Dependence on Keystroke Logging
  - Dependence on Client Solicitation
  - May Implement Wanton Propagation
    - Use of Spreader Mechanism
  - Persistence of Malware on Victim System Often not a Concern

Often a Decentralized Security Problem.
Case Study One

Attack for Profit
Attacks for Information

- **Target:**
  - Target Specific Organizations
  - Wanton Spreading Less Common
  - Information of Interest:
    - Intellectual Property
    - Databases
    - Documents
    - Spreadsheets
    - ????
Attacks for Information

- Technological Characteristics:
- Rely on Continued Access
  - Valid Credentials
  - Persistent Backdoors
- Post Exploitation Sophistication - Malicious Code More Persistent
  - In-Memory Library Injection in Windows Expanding
- Requires **Surreptitious** Theft of Data
  - Highly Used Ports
  - Web Traffic
  - Segmentation of Files (rar)
- Often Move Fast

Often a Centralized Security Problem.
Case Study Two

Information Pilfering
How Current Attack Trends are Influencing the Incident Response Process
How Current Attack Trends are Influencing the Incident Response Process

1. The Need to Acquire and Analyze the Contents of RAM
2. The Need to Locate Well-Hidden, User Space Malicious Code
   - Review of System Volume Restore
   - Windows Services Mayhem
     - Altering the Image Path
     - Replacing Legitimate Services
     - Using SVCHOST Invocation
3. The Need for Malware Triage
   - Identification and Remediation
4. The Need for Speed
The Need to Acquire and Analyze the Contents of RAM
Obtaining Memory Dumps and Process Space

- Contents of Physical Memory
  - `\device\PhysicalMemory`
- Pagefile
  - `pagefile.sys`
  - Could be More than One
- Memory from Individual Processes
  - `Userdump`
Obtaining Physical Memory (Ram)

- Unix – Simple
  - /dev/kmem
  - /dev/mem
  - /dev/kcore

- Windows – Not as Simple.
  - Windows Operating Systems do not Provide Such a File Objects.
  - Windows Does have a “/Device/PhysicalMemory” Section Object.
  - Use “dd”, by Mr. George M. Garner, Jr.
Obtaining RAM – “dd” Command Line

E:\>dd.exe if=\\.\physicalmemory of=f:\win2khost-physicalmemory.dd bs=4096
Forensic Acquisition Utilities, 3, 16, 2, 1030
dd, 1, 0, 0, 1030
Copyright (C) 2002 George M. Garner Jr.

Command Line: dd.exe if=\\.\physicalmemory of=f:\win2khost-physicalmemory.dd bs=4096
Based on original version developed by Paul Rubin, David MacKenzie, and Stuart Kemp
Microsoft Windows: Version 5.0 (Build 2195.Professional)
26/02/2003  03:48:35 (UTC)
25/02/2003  22:48:35 (local time)
Current User: WIN2K\Administrator

Total physical memory reported: 523760 KB
Copying physical memory...
E:\dd.exe:
    Stopped reading physical memory:
The parameter is incorrect.
Output e:\win2khost-physicalmemory.dd 536801280/536801280 bytes
    (compressed/uncompressed)
131055+0 records in
131055+0 records out
Obtaining the Page/Swap File

- By copying `\\\physicaldrive0`, You Obtain the Entire Contents of the First Physical Disk—including the Page File.
- Access Data has a tool to do this.
Obtaining Specific Process Memory

- By Obtaining a Memory Dump of the Suspect Application, One Can:
  - Determine the Purpose of the Application
  - View the Command Line Used to Launch the Application
  - View the Application’s Data Stored in Memory
  - Reveal Potential Commands Executed or Spawned
    - Process Memory Dump of cmd.exe
“Userdump.exe” is Part of the OEM Support Tools for Windows:


Note that Userdump has Several Useful Options.

- Capture of Multiple Processes on a Single Command Line and Displaying Running Processes

```shell
E:\>userdump 744 f:\svchost_PID744.dmp
User Mode Process Dumper (Version 3.0)
Copyright (c) 1999 Microsoft Corp. All rights reserved.
Dumping process 744 (svchost_.exe) to f:\svchost_PID744.dmp...
```
Using userdump

- E:\>userdump 1272 f:\cmd_1272.dmp
- E:\>userdump 1372 f:\ftp_1372.dmp
- E:\>userdump 1160 f:\cmd_1160.dmp

<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>Priority</th>
<th>Status</th>
<th>User Time</th>
<th>System Time</th>
<th>Total Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmd</td>
<td>1272</td>
<td>8</td>
<td>1</td>
<td>25</td>
<td>984</td>
<td>0:00:00.20</td>
</tr>
<tr>
<td>ftp</td>
<td>1372</td>
<td>8</td>
<td>1</td>
<td>39</td>
<td>1176</td>
<td>0:00:00.20</td>
</tr>
<tr>
<td>cmd</td>
<td>1160</td>
<td>8</td>
<td>1</td>
<td>28</td>
<td>976</td>
<td>0:00:00.20</td>
</tr>
<tr>
<td>nc</td>
<td>1424</td>
<td>8</td>
<td>3</td>
<td>40</td>
<td>1012</td>
<td>0:00:00.10</td>
</tr>
<tr>
<td>cmd</td>
<td>1092</td>
<td>8</td>
<td>1</td>
<td>34</td>
<td>968</td>
<td>0:00:00.10</td>
</tr>
<tr>
<td>cmd</td>
<td>1468</td>
<td>8</td>
<td>1</td>
<td>30</td>
<td>984</td>
<td>0:00:00.30</td>
</tr>
<tr>
<td>cmd</td>
<td>496</td>
<td>8</td>
<td>1</td>
<td>24</td>
<td>964</td>
<td>0:00:00.20</td>
</tr>
<tr>
<td>T_NC</td>
<td>1348</td>
<td>8</td>
<td>1</td>
<td>28</td>
<td>1004</td>
<td>0:00:00.20</td>
</tr>
<tr>
<td>T_PSLIST</td>
<td>1484</td>
<td>8</td>
<td>2</td>
<td>87</td>
<td>1216</td>
<td>0:00:00.40</td>
</tr>
<tr>
<td>0011D68E</td>
<td>0000 0000 0066 7470 2039 352E 3230 382E 3132 332E 3634 0D0A 0032</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0011D6A8</td>
<td>5C64 6C6C 3E00 2C34 3533 2C34 3536 2C33 3834 2062 7974 6573 2066</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0011D6C2</td>
<td>7265 650D 0A00 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0011D6DC</td>
<td>0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0011D6F6</td>
<td>0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0011D710</td>
<td>0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

`ftp 95.208.123.64...2
\d1l>, 453,456,384 bytes f ree`
| 00004010 | 0020 F706 00FA 1401 7855 5345 5220 6674 | . . . . . . xUSER ft p .................. |
| 00004020 | 700D 0A00 0000 0007 000A 0000 0000 0000 | .<.................. |
| 00004030 | 003C EF06 0000 0200 0088 EF06 0002 0000 | ..C.w............. |
| 00004040 | 00D3 43F9 77E8 0607 0000 0007 0002 0000 |

| 000FDFF0 | 0000 0000 0033 3331 2041 6E6F 6E79 6D6F | .....331 Anonymou us access allowe d, send identity (e-mail name) a s password...... |
| 000FDFF0 | 7573 2061 6363 6573 7320 616C 6C6F 7765 |
| 000FE000 | 642C 2073 656E 6420 6964 656E 7469 7479 |
| 000FE010 | 2028 652D 6D61 696C 206E 616D 6529 2061 |
| 000FE020 | 7320 7061 7373 776F 7264 2E0D 0A00 0000 |
The Need to Locate Well-Hidden, User Space Malicious Code
**User Space Hiding Techniques**

- Malware named after Legitimate Windows Services
  - Swupdtmr.exe
  - symwsc.exe
  - Spoolsv.exe
  - Svchost.exe
- Malware Named Something Similar to Legitimate Windows Services
  - Winservices.exe
- Use of Windows Services to Hide/Start Malware
- Use of Malicious dlls
- Most Malware Placed in `%systemroot%` or Subdirs
Case 1: Altering the Image Path

1. The Existing “sysmonlog” Service is Stopped.
2. The Backdoor File was Copied to: “%SYSTEMROOT%\system32\drivers\”
3. The New File was Modified to have the Same Time Stamps as %SYSTEMROOT%\system32\kernel32.dll.
4. The Registry Value “HKLM\System\CurrentControlSet\Services\Sysmonlog\ImagePath” was changed to “%SystemRoot%\system32\drivers\smlogsvcs.exe”
Case 1: Altering the Image Path

1. The Registry Value
   “HKLM\System\CurrentControlSet\Services\SysmonLog\Start” is Set to 2
   • Ensures that the Service Starts Automatically Upon Reboot.

2. The Registry Value
   “HKLM\System\CurrentControlSet\Services\SysmonLog\ObjectName” is set to “LocalSystem”.
   • Causes the Backdoor Service to Run with the Privileges of the “LocalSystem” Account.
### The Nuisance of SVCHOST

<table>
<thead>
<tr>
<th>Name</th>
<th>Pid</th>
<th>Pri</th>
<th>Thd</th>
<th>Hnd</th>
<th>Mem</th>
<th>User Time</th>
<th>Kernel Time</th>
<th>Elapsed Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>0:00:00.000</td>
<td>43:56:44.437</td>
<td>0:00:00.000</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>8</td>
<td>84</td>
<td>276</td>
<td>228</td>
<td>0:00:00.000</td>
<td>0:03:53.796</td>
<td>0:00:00.000</td>
</tr>
<tr>
<td>smss</td>
<td>708</td>
<td>11</td>
<td>3</td>
<td>21</td>
<td>376</td>
<td>0:00:00.015</td>
<td>0:00:00.671</td>
<td>171:49:34.562</td>
</tr>
<tr>
<td>csrss</td>
<td>800</td>
<td>13</td>
<td>13</td>
<td>682</td>
<td>4716</td>
<td>0:00:18.296</td>
<td>0:03:11.406</td>
<td>171:49:31.953</td>
</tr>
<tr>
<td>winlogon</td>
<td>824</td>
<td>13</td>
<td>19</td>
<td>577</td>
<td>3936</td>
<td>0:00:00.781</td>
<td>0:02:39.234</td>
<td>171:49:31.500</td>
</tr>
<tr>
<td>services</td>
<td>868</td>
<td>9</td>
<td>15</td>
<td>343</td>
<td>4724</td>
<td>0:01:30.703</td>
<td>0:02:38.031</td>
<td>171:49:30.859</td>
</tr>
<tr>
<td>lsass</td>
<td>880</td>
<td>9</td>
<td>18</td>
<td>385</td>
<td>1256</td>
<td>0:00:30.375</td>
<td>0:02:09.281</td>
<td>171:49:30.812</td>
</tr>
<tr>
<td>svchost</td>
<td>1040</td>
<td>8</td>
<td>15</td>
<td>201</td>
<td>4712</td>
<td>0:00:00.937</td>
<td>0:00:02.937</td>
<td>171:49:29.375</td>
</tr>
<tr>
<td>svchost</td>
<td>1116</td>
<td>8</td>
<td>10</td>
<td>419</td>
<td>4336</td>
<td>0:00:04.390</td>
<td>0:00:10.968</td>
<td>171:49:29.093</td>
</tr>
<tr>
<td>svchost</td>
<td>1312</td>
<td>8</td>
<td>4</td>
<td>80</td>
<td>3088</td>
<td>0:00:01.578</td>
<td>0:00:05.781</td>
<td>171:49:28.406</td>
</tr>
<tr>
<td>svchost</td>
<td>1456</td>
<td>8</td>
<td>14</td>
<td>238</td>
<td>4964</td>
<td>0:00:02.546</td>
<td>0:00:02.437</td>
<td>171:49:28.000</td>
</tr>
<tr>
<td>explorer</td>
<td>1676</td>
<td>8</td>
<td>17</td>
<td>535</td>
<td>14832</td>
<td>0:04:26.484</td>
<td>0:09:37.394</td>
<td>171:49:26.675</td>
</tr>
<tr>
<td>BRSVC01A</td>
<td>1856</td>
<td>8</td>
<td>3</td>
<td>29</td>
<td>1072</td>
<td>0:00:00.015</td>
<td>0:00:00.031</td>
<td>171:49:26.187</td>
</tr>
<tr>
<td>BRSS01A</td>
<td>1884</td>
<td>8</td>
<td>1</td>
<td>23</td>
<td>1500</td>
<td>0:00:00.906</td>
<td>0:00:00.281</td>
<td>171:49:26.140</td>
</tr>
<tr>
<td>spoolsv</td>
<td>1892</td>
<td>8</td>
<td>17</td>
<td>215</td>
<td>7708</td>
<td>0:00:04.593</td>
<td>0:00:09.250</td>
<td>171:49:26.125</td>
</tr>
<tr>
<td>OOTHotkey</td>
<td>1944</td>
<td>8</td>
<td>4</td>
<td>72</td>
<td>3680</td>
<td>0:00:00.468</td>
<td>0:00:01.656</td>
<td>171:49:25.765</td>
</tr>
<tr>
<td>hkmcmd</td>
<td>1976</td>
<td>8</td>
<td>5</td>
<td>163</td>
<td>5824</td>
<td>0:00:00.171</td>
<td>0:00:02.609</td>
<td>171:49:25.500</td>
</tr>
<tr>
<td>agrsmsgs</td>
<td>1984</td>
<td>8</td>
<td>2</td>
<td>37</td>
<td>1816</td>
<td>0:00:00.156</td>
<td>0:00:00.296</td>
<td>171:49:25.390</td>
</tr>
<tr>
<td>Apoint</td>
<td>1992</td>
<td>8</td>
<td>1</td>
<td>74</td>
<td>5044</td>
<td>0:00:01.500</td>
<td>0:00:07.640</td>
<td>171:49:25.328</td>
</tr>
<tr>
<td>TouchED</td>
<td>2000</td>
<td>8</td>
<td>1</td>
<td>27</td>
<td>1928</td>
<td>0:00:00.031</td>
<td>0:00:00.015</td>
<td>171:49:25.234</td>
</tr>
<tr>
<td>TFNF5</td>
<td>2024</td>
<td>8</td>
<td>1</td>
<td>20</td>
<td>1732</td>
<td>0:00:00.015</td>
<td>0:00:00.062</td>
<td>171:49:24.953</td>
</tr>
</tbody>
</table>
Case 2: Altering the ImagePath

- The Following Key Contained the Location of the Backdoor “dll”.
  - Note: The Backdoor Will Be in the “%SYSTEMROOT%” Directory Instead of the “%SYSTEMROOT%\system32” Directory.

HKLM\SYSTEM\ControlSet001\Services\<x>\ImagePath
Case 3: Hiding Backdoors Yet Again

- The Legitimate service named BITS (the Background Intelligent Transfer Service) is Modified to Load the Backdoor Program (“qmgrxxx.dll”) instead of the legitimate service (“qmgr.dll”).
- The BITS Service was Configured to Start Automatically upon System Initialization.
Case 3: Hiding Backdoors Yet Again

- Reviewing Running Services Configuration Data does not Assist you in Finding this Backdoor:

C:\psservice config bits

<Text Omitted>

BITS has been disabled.

TYPE : 20 WIN32_SHARE_PROCESS
START_TYPE : 2 AUTO_START
ERROR_CONTROL : 1 NORMAL
BINARY_PATH_NAME : C:\WINDOWS\System32\svchost.exe -k netsvcs
LOAD_ORDER_GROUP :
TAG :
DISPLAY_NAME : Background Intelligent Transfer Service
DEPENDENCIES : Rpcss
SERVICE_START_NAME: LocalSystem
FAIL_RESET_PERIOD : 0 seconds
FAILURE_ACTIONS : Restart  DELAY: 60000 seconds
                     : Restart  DELAY: 60000 seconds
                     : Restart  DELAY: 60000 seconds
Case 3: Hiding Backdoors Yet Again

- You Must Review the Registry for ServiceDLL Information

**BITS**

```
Type = REG_DWORD 0x00000020
Start = REG_DWORD 0x00000002
ErrorControl = REG_DWORD 0x00000001
ImagePath = REG_EXPAND_SZ
%SystemRoot%\System32\svchost.exe -k netsvcs
```

DisplayName = Background Intelligent Transfer Service

```
DependOnService = REG_MULTI_SZ "Rpcss"
DependOnGroup = REG_MULTI_SZ
ObjectName = LocalSystem
Description = <removed text>
Parameters
ServiceDll = REG_EXPAND_SZ
C:\WINDOWS\System32\qmgr.dll
```

Security [17 1]
The Need for Malware Triage

Elf file type is EXEC (Executable file)
Entry point 0x8048080
There are 2 program headers, starting at offset 0x52
Program Headers:

<table>
<thead>
<tr>
<th>Type</th>
<th>Offset</th>
<th>VirtAddr</th>
<th>PhysAddr</th>
<th>FileSize</th>
<th>MemSiz</th>
<th>Flags</th>
<th>Align</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOAD</td>
<td>0x000000</td>
<td>0x08048000</td>
<td>0x08048000</td>
<td>0x00590</td>
<td>0x00590</td>
<td>R E</td>
<td>0x100</td>
</tr>
<tr>
<td>LOAD</td>
<td>0x000590</td>
<td>0x08049590</td>
<td>0x08049590</td>
<td>0x0002c</td>
<td>0x0002c</td>
<td>RW</td>
<td>0x100</td>
</tr>
</tbody>
</table>
Malware Triage Answers …

- What is the Intent and Capability of the Attacker?
- Did the Attacker Take Stuff?
- How Can We Find Him on our Network?
  - Host-Based Signatures?
  - Network-Based Signatures?
- How Can We Keep the Attacker Out? Minimize His Impact?
Performing Malware Analysis

- Keep Your Goals in Mind:
  - WHAT IS THE TOOL?
    - Network Listener / Backdoor
    - Network Listener / Sniffer
    - Network Scanner
    - Port Redirector
    - Password Cracker
    - Password Dumper
    - Keylogger
Our Goal During Presentation

- Demonstrate Methods to Quickly Identify and Categorize Malware by Performing a:
  - Review of IAT
  - Review of Disassembled Code for Recognizable Constructs
Our Goal During Presentation

- Realization that Disassembly and Debugging are Activities Currently Reserved for a Few Brave Men/Women.
- Most Firms do not want to Expend the Resources to fully Analyze Malicious Code
- There is a Need for Quick Strike Identification and Development of Countermeasures
Static Analysis

- File “FingerPrinting”
- Virus Scan
- Packed or Not Packed?
- Strings
- Hex Editor
- Web Searching
- Disassembly
File Fingerprinting

- Fingerprint the Files you are Examining so that You will Know if they Change during Your Analysis
  - MD5Sum
  - File Size
  - File Name
  - Time/Date Stamps
  - Resource Section
  - Compile Date

- Use md5deep or Cygwin’s md5sum

  \[
  \text{md5sum hello* > md5sum_hello_files.txt}
  \]

  \[
  \text{cat md5sum_hello_files.txt}
  \]

  611957bd6a2ad9642027904a65f3638e  hello

  7ab03b44ac6a20b0fa0cc80b636b0f51  hello.c

- When you have Completed your Analysis (or at various points along the way) you Should Check the md5sums to Ensure the Values have not Changed!

  \[
  \text{md5sum -c md5sum_hello_files.txt}
  \]
Virus Scan

- Always Scan New Malware with an Up to Date Virus Scanner.
- Someone Else may have Already Discovered and Documented the Program you are Investigating!!

- Norton AntiVirus version 10.0.1.13
- Sophos Anti-Virus 5.0.2
- Microsoft AntiSpyware (Beta1) version 1.0.509
- Ad-Aware SE build 1.06r1
- Etrust PestPatrol version 5.0.1.5.
Comparison with 14 Different AV Products
Armor Features

- Encryption
- Compression
- Obfuscation
- Anti-Patching
  - CRC Checking
- Anti-Tracing
  - SoftICE, ICEDump Detection Code.
  - Crashes OS if they are Found in Memory
- Anti-Unpacking

- Restrictive Runtimes
- Restrictive Dates
- Password Protected
- Configuration Files
- Configuration Configurations
Packers

- **UPack** by [Dwing](#). 08.IV.2005.
- **Mew** by [Northfox](#). 22.IX.2004.
- **UPX** by [Laszlo & Markus](#). 03.VII.2004.
- **Packman** by [bubba](#). 27.II.2005.
- **CExe** by [Scott](#). 20.III.2003.
- **PE Diminisher** by tERAPHY. 11.IX.1999.
- **PESpin** by [cyberbob](#). 09.III.2005.
- **NSPack** by [North star Tech](#). 05.VI.2005.
- **eXPressor** by CGSoftLabs. 28.III.2005.
- **Thinstall** by [Jonathan Clark](#). 29.III.2005.
- **PECompact** by [DevelTek](#). 06.IV.2005.
- **AS-Pack** (shareware) by [Solodovnikov Alexey](#). 07.I.2002.
- **NeoLite** (shareware) by [NeoWorx Inc](#). 04.IV.1999.
- **ARM Protector** by [SMoKE](#). 22.IX.2004.
Packed or Not Packed -- PEiD

- PEiD is a Free Program that Identifies Signatures Associated with Over 450 Different “packers” and Compilers.
Unpackers

- Ollydbg with the Ollydump plugin.
- IDAPro with the “Universal Unpacker Plugin”.
- DeYoda by C-ripper. 18.II.2001.
- DePE-PACK by Unknown One. 03.V.2002.
- StealthKiller by Snow Panther. 04.IX.2002.
Unpacking FSG - UnFSG

- UnFSG
- Conduct a Google Search for “unpack” and “FSG”
- Downloaded UnFSG by “smola”
Unpacking with UPX

```
C:\Mandia\toolanalysis>upx -d as.exe -o unpackedas.exe
Ultimate Packer for executables
UPX 1.25w       Markus F.X.J. Oberhumer & Laszlo Molnar       Jun 29th

<table>
<thead>
<tr>
<th>File size</th>
<th>Ratio</th>
<th>Format</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>32768 -&gt; 14848</td>
<td>45.31%</td>
<td>win32/pe</td>
<td>unpackedas.exe</td>
</tr>
</tbody>
</table>

Unpacked 1 file.
```
Strings

C:\analysis>strings
Strings v2.1
Copyright (C) 1999-2003 Mark Russinovich
Systems Internals - www.sysinternals.com
usage: strings [-s] [-n length] [-a] [-u] [-q] <file or directory>
-s Recurse subdirectories
-n Minimum string length (default is 3)
-a Ascii-only search (Unicode and Ascii is default)
-u Unicode-only search (Unicode and Ascii is default)
-q Quiet (no banner)
Conducting Web Research

- Look at Unique Strings, Email Addresses, Network Info
- Search the Web
  - Be Careful → Google Cache Does Not Equal Anonymous
  - You Might Find other Victims, or Complete Analysis
  - Do not Forget Newsgroups
- It Helps if you Know Chinese (or Russian)
  
  http://www.google.com/language_tools?hl=en
Disassembly

- Executable File Formats
  - Windows: PE (Portable Executable)
    www.microsoft.com/whdc/system/platform/firmware/PECOFF.mspx
  - Linux: ELF (Executable and Linking Format)
    www.skyfree.org/linux/references/ELF_Format.pdf
DisAssembly Cheat Sheet

- Quick Snapshot of Recognizing “likely evil” Constructs in Disassembled Code
  - Use of the Network
  - Use of Raw Sockets
  - Use of Encryption
  - Use of XOR Encoding
- No Hardcore Reversing Skills Necessary
The Need for Speed
Questions?