The State of the Hack

Kevin Mandia
MANDIANT

Who Am I?

- Adjunct Professor
  - Carnegie Mellon University
    - 95-856 Incident Response
    - Master of Information System Management
  - The George Washington University
    - Computer Forensics III
    - Masters in Forensic Science
- Author for McGraw-Hill
- Honeynet Project
Who Am I?

- Last 5 Years
  - Responded to over 300 Potentially Compromised Systems.
  - Responded to Intrusions at Over 40 Organizations.
  - Created IR Programs at Several Fortune 500 Firms.

Evolution of IT Attacks

- -- 1998
  - Technical Problem
  - Unix Systems
  - Servers
  - Attacks were a Nuisance

- 1998 -- 2002
  - Technical/Business Problem
  - Windows Systems
  - Servers
  - Attacks were About Money

- 2002 -- Now
  - Technical/Business/Legal Problem
  - Windows Systems
  - Client Systems / End Users
  - Attacks are About Money
Agenda

- Incident Detection
- Case Studies
- Challenges When Responding to Security Incidents

Incident Detection
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

2. How are Organization’s Detecting Incidents?

- **IDS Alerts?**
  - Rare Detection Mechanism.
3. How are Organization’s Detecting Incidents?

- Clients (Outside Company)
  - Malicious Software Discovered on Compromised End-User Systems.

4. How are Organization’s Detecting Incidents?

- End Users (Internal)
  - System Crashes (Blue Screens of Death)
  - 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?
- Proactive Audits or Security Scans

6. How Are Organization’s Detecting Incidents?
- Something Obvious …
7. How are Organizations Detecting Incidents?

- Notification from other Victims.
- Notification from Government Agencies.
Incident is Detected

Network Monitoring

Incident Detected on Host 1

Corporate Network

Internet

Backdoor Channel

Performing Live Response

1. Last Accessed Time of Files
2. Last Written Time of Files
3. Creation Time of Files
4. Volatile Information
5. Services Running
6. Event Logs
7. Registry Entries
8. Host Status (Uptime, Patch Level)
9. IIS and Other Application Logs

Live Data Collection Performed to Verify Incident and Determine Indicators / Signature of the Attack
### Review Running Processes …

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>4164</td>
<td>8</td>
<td>1</td>
<td>26</td>
<td>1408</td>
<td>0:00:00.015</td>
</tr>
<tr>
<td>As</td>
<td>4492</td>
<td>8</td>
<td>1</td>
<td>30</td>
<td>1324</td>
<td>0:00:00.062</td>
</tr>
<tr>
<td>C</td>
<td>4340</td>
<td>8</td>
<td>1</td>
<td>31</td>
<td>1428</td>
<td>0:00:00.031</td>
</tr>
<tr>
<td>C</td>
<td>4524</td>
<td>8</td>
<td>1</td>
<td>31</td>
<td>1428</td>
<td>0:00:00.031</td>
</tr>
<tr>
<td>CMD</td>
<td>4276</td>
<td>8</td>
<td>1</td>
<td>29</td>
<td>1988</td>
<td>0:00:00.015</td>
</tr>
<tr>
<td>net</td>
<td>4204</td>
<td>8</td>
<td>1</td>
<td>42</td>
<td>2736</td>
<td>0:00:00.015</td>
</tr>
<tr>
<td>CMD</td>
<td>4136</td>
<td>8</td>
<td>1</td>
<td>30</td>
<td>2024</td>
<td>0:00:00.015</td>
</tr>
<tr>
<td>cidaemon</td>
<td>4260</td>
<td>4</td>
<td>4</td>
<td>166</td>
<td>396</td>
<td>0:00:21.781</td>
</tr>
<tr>
<td>cidaemon</td>
<td>4596</td>
<td>4</td>
<td>4</td>
<td>153</td>
<td>384</td>
<td>0:00:21.218</td>
</tr>
<tr>
<td>CMD</td>
<td>4528</td>
<td>8</td>
<td>1</td>
<td>31</td>
<td>1988</td>
<td>0:00:00.031</td>
</tr>
<tr>
<td>net</td>
<td>4256</td>
<td>8</td>
<td>1</td>
<td>44</td>
<td>2736</td>
<td>0:00:00.015</td>
</tr>
</tbody>
</table>

### Established Network Connections …

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>10.231.3.131:1943</td>
<td>10.230.231.39:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1945</td>
<td>10.230.121.14:445</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1950</td>
<td>10.230.211.65:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1953</td>
<td>10.230.121.32:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1955</td>
<td>10.230.121.100:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1961</td>
<td>10.230.211.95:445</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1964</td>
<td>10.230.211.83:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1969</td>
<td>10.230.231.70:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1972</td>
<td>10.230.20.117:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1975</td>
<td>10.230.20.29:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1978</td>
<td>10.230.131.36:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1981</td>
<td>10.230.221.36:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1984</td>
<td>10.231.8.167:139</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>10.231.3.131:1986</td>
<td>10.230.121.58:445</td>
<td>TIME_WAIT</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Review of the Application Event Log

6192, Application, Symantec Antivirus, ERROR, HOSTXXX, 9/21/2006 3:39:31 AM, 40, None, Symantec Antivirus has determined that the virus definitions are missing on this computer. This computer will remain unprotected from viruses until virus definitions are downloaded to this computer.

Review of Listening Ports

svchost.exe [2800]
TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING
TCP 0.0.0.0:90 0.0.0.0:0 LISTENING
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
TCP 0.0.0.0:21096 0.0.0.0:0 LISTENING
How Are Attackers Gaining Initial Entry?

How are Attackers Gaining Entry?

- Vulnerable Services?
How are Attackers Gaining Entry?

- Web Application Vulnerabilities?

How Are Attackers Gaining Entry?

- End User Attacks
How Are Attackers Gaining Entry?

- Never Find Victim 0?
- Valid Credentials

Case Studies

The State of the Hack
Case Studies – End User Attacks

The Challenges to Incident Response
High-Level Direction

Challenges

Lack of Poignant, High Level Direction.

High Level Direction

- Define the “Win”
- Know the Concerns of ALL Parties.
- Assign/Assume Incident Ownership
- Determine How Good Does the Incident Response Need to Be
  - Priority of IR Role VS. Day Job
  - Business as Usual VS. Business Interruption
- Level of Resources Assigned to the Incident
  - Number of People
  - Level of Escalation
  - Sense of Urgency
Evolution of Incident Response

- Executive Concerns
- Legal Concerns
- Technical Concerns

Management Concerns (Board and CEO)

- What is the Incident’s Impact on Business?
- Do We have to Notify our Clients?
- Do We have to Notify our Regulators?
- Do We have to Notify our Stock Holders?
- What is Everyone Else Doing about this Sort of thing?
Legal Counsel Concerns

- Are we required to notify our clients, consumers, or employees about the security breach?
- What constitutes a “reasonable belief” that protected information was compromised – the standard used in many states to determine whether notification is required?

Legal Counsel Concerns

- What are the applicable regulations or statutes that impact our organization’s response to the security breach?
- Which state laws are applicable? Which might be in the future?
- Are there any contractual obligations that impact our incident response strategy?
Legal Counsel Concerns

- How might public knowledge of the compromise impact the organization?
- What is our liability if PII was compromised?
- What is our liability if the compromised network hosted copyrighted content (pirated movies, music, software...)
- Does notifying our customers increase the likelihood of a lawsuit?

Legal Counsel Concerns

- Is it permissible to monitor/intercept the intruder’s activities?
- How far can/should we go to identify the intruder?
- Who knows about the incident?
- Should the organization notify our regulators? Law enforcement?
Technical Management (CIO)

- How long were we exposed?
- How many systems were affected?
- What data, if any, was compromised (i.e., viewed, downloaded, or copied)?
- Was any Personal Identifiable Information (PII) compromised?
- What countermeasures are we taking?

Technical Management (CIO)

- What are the chances that our countermeasures will succeed?
- Who else knows about the security breach?
- Is the incident ongoing? Preventable?
- Is there a risk of insider involvement?
Questions?