Introduction

• Bejtlich ("bate-lik") biography
  – General Electric, (07-present)
  – TaoSecurity (05-07)
  – ManTech (04-05)
  – Foundstone (02-04)
  – Ball Aerospace (01-02)
  – Captain at US Air Force CERT (98-01)
  – Lt at Air Intelligence Agency (97-98)

• Author
  – Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
  – Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
  – Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
  – Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
Overview

- Still speaking Truth to Power
- Verizon Data Breach Report
- 7 Stages of Security Team Evolution and Cheap IT
- Defender’s vs Intruder’s Dilemmas
- Digital Situational Awareness
- Incident Phases of Compromise
- Info Sec Incident Classification

Bring them on! I prefer a straight fight to all this sneaking around.

Han Solo, SWEPIV
Alexander Solzhenitsyn (1918-2008), author of The Gulag Archipelago: “Don’t lie! Don’t participate in lies! Don’t support a lie!”

Ref: 7 Aug 2008 Economist magazine
Highlights from 2009 Verizon Data Breach Report 1

Results from 600 incidents over five years make a strong case against the long-abiding and deeply held belief that insiders are behind most breaches.

Who is behind data breaches?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>74%</td>
<td>Resulted from external sources (+1%).</td>
</tr>
<tr>
<td>20%</td>
<td>Were caused by insiders (+2%).</td>
</tr>
<tr>
<td>32%</td>
<td>Implicated business partners (-7%).</td>
</tr>
<tr>
<td>39%</td>
<td>Involved multiple parties (+9%).</td>
</tr>
</tbody>
</table>

Closely resembling the stats from our 2008 report, most data breaches continue to originate from external sources. Though still a third of our sample, breaches linked to business partners fell for the first time in years. The median size of breaches caused by insiders is still the highest but the predominance of total records lost was attributed to outsiders. 91 percent of all compromised records were linked to organized criminal groups.

Figure 8. Total records compromised by source

<table>
<thead>
<tr>
<th>Source</th>
<th>Records Compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only External</td>
<td>266,788,000</td>
</tr>
<tr>
<td>Multiple Sources</td>
<td>15,796,000</td>
</tr>
<tr>
<td>Only Partner</td>
<td>1,509,000</td>
</tr>
<tr>
<td>Only Internal</td>
<td>1,330,000</td>
</tr>
</tbody>
</table>
Highlights from 2009 Verizon Data Breach Report 2

Figure 6. Breach sources over time by percent of breaches

Figure 7. Median number of records compromised per breach

Table 1. Pseudo risk calculation

<table>
<thead>
<tr>
<th>Source</th>
<th>Likelihood</th>
<th>Impact (number of records)</th>
<th>Risk (pseudo)</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>74%</td>
<td>37,847</td>
<td>28,175</td>
</tr>
<tr>
<td>Internal</td>
<td>20%</td>
<td>100,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Partner</td>
<td>32%</td>
<td>27,000</td>
<td>8,700</td>
</tr>
</tbody>
</table>
# Highlights from 2009 Verizon Data Breach Report 3

**Figure 31. Time span of breach events by percent of breaches**

<table>
<thead>
<tr>
<th>Event</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years</th>
<th>Unsure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-attack Research</td>
<td></td>
<td></td>
<td>15%</td>
<td>11%</td>
<td>26%</td>
<td>0%</td>
<td>19%</td>
</tr>
<tr>
<td></td>
<td>4%</td>
<td>26%</td>
<td>15%</td>
<td>11%</td>
<td>26%</td>
<td>0%</td>
<td>19%</td>
</tr>
<tr>
<td>Point of Entry to Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>27%</td>
<td>21%</td>
<td>29%</td>
<td>17%</td>
<td>6%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Compromise to Discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0%</td>
<td>8%</td>
<td>16%</td>
<td>25%</td>
<td>49%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Discovery to Containment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0%</td>
<td>6%</td>
<td>37%</td>
<td>42%</td>
<td>15%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Figure 32. Breach discovery methods by percent of breaches

- Third-party detection of fraudulent activity: 55%
- Third-party notification (not due to fraud): 15%
- Employee discovery during work activities: 13%
- Unusual system behavior or performance: 11%
- Event monitoring or log analysis: 6%
- Routine internal audit: 2%
- Blackmail or extortion: 2%
- Confession or brag by perpetrator: 1%
- Routine third-party audit: 0%

Figure 34. Detective controls by percent of breach victims

- System Device Logs: 71%
- Intrusion Detection System: 30%
- Automated Log Analysis: 20%
- SEIM (Info and Event Mgt.): 13%
- Log Review Process: 11%
Highlights from 2009 Verizon Data Breach Report 5

Figure 35. Incident response practices by percent of breach victims

- Incident Response Team: 32%
- Incident Response Plan: 28%
- Incident Awareness and Response Training: 25%
- Regular Mock-incident Testing: 3%

Figure 19. Malware customization by percent of breaches involving malware
Cheap IT Is Ultimately Expensive

- It is not cheaper to run legacy platforms, operating systems, and applications because "updates break things."
- It is not cheaper to delay patching because of "business impact."
- It is not cheaper to leave compromised systems operating within the enterprise because of the "productivity hit" taken when a system must be interrupted to enable security analysis.
- It is not cheaper to try to manually identify and remove individual elements of malware and other persistence mechanisms, rather than rebuild from the ground up (and apply proper updates and configuration improvements to resist future compromise).
- It is not cheaper to watch intellectual property escape the enterprise in order to prove that intruders are serious about stealing an organization's data.
7 Stages of Security Team Evolution

1. **Ignorance.** "Security problem? What security problem?"
2. **Denial.** "I hear others have security problems, but we don't."
3. **Incompetence.** "We have to do something!"
4. **Heroics.** "Stand back! I'll fix it!"
5. **Capitalization.** "Now I have some resources to address this problem."
6. **Institutionalization.** "Our organization is integrating our security measures into the overall business operations."
7. **Specialization.** "We're leveraging our unique expertise in X and Y to defend ourselves and contribute back to the security community."
The intruder only needs to exploit one of the victims in order to compromise the enterprise.
Intruder’s Dilemma

The defender only needs to detect one of the indicators of the intruder’s presence in order to initiate incident response within the enterprise.

Intruder

Defender

Host security monitoring
Network security monitoring
Enterprise log monitoring
Live response and forensic analysis

OSSEC

Network security monitoring

Defender

Victims

F-Response
Digital Situational Awareness Methods

- External notification
- Vulnerability assessment
- Adversary simulation or penetration testing
- Incident detection and response (3 paradigms)
  1. Detection is futile.
  2. Sufficient knowledge.
  3. Indicators plus retrospective security analysis.
- Counterintelligence operations
  - See who is selling or offering to sell your information or access to your information.
  - Solicit the underground for your organization's data or for access to your organization.
  - Penetrate adversary infrastructure.
  - Infiltrate the adversary group.
  - Pose as an individual underground member.
Incident Phases of Compromise

- **Reconnaissance.** Identify target assets and vulnerabilities, indirectly or directly. Cat 6.

- **Exploitation.** Abuse, subvert, or break a system by attacking vulnerabilities or exposures. If the intruder does not seek to maintain persistence, then this could be the end of the compromise. Cat 2 or 1.

- **Reinforcement.** The intruder deploys his persistence and stealth techniques to the target. Still Cat 2 or 1, leading to Breach 3.

- **Consolidation.** The intruder ensures continued access to the target by establishing remote command-and-control. Breach 3.

- **Pillage.** The intruder executes his mission. Here we assume data theft and persistence are the goals.
  - **Propagation.** Intruders usually expand their influence before stealing data, but this is not strictly necessary. At this point the incident classifications should be applied to the new victims.
  - **Exfiltration.** The intruder steals data. Depending on the type of data, Breach 2 or 1.
  - **Maintenance.** The intruder ensures continued access to the victim until deciding to execute another mission.
### Information Security Incident Classification for Individual System Compromise

**Richard Bejtlich 05 June 2009**

<table>
<thead>
<tr>
<th>Classification</th>
<th>Number</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vuln 3</td>
<td>1</td>
<td>Green</td>
<td>Intruder must apply substantial effort to compromise asset and exfiltrate sensitive data</td>
</tr>
<tr>
<td>Vuln 2</td>
<td>2</td>
<td>Light Green</td>
<td>Intruder must apply moderate effort to compromise asset and exfiltrate sensitive data</td>
</tr>
<tr>
<td>Vuln 1</td>
<td>3</td>
<td>Yellow</td>
<td>Intruder must apply little effort to compromise asset and exfiltrate sensitive data</td>
</tr>
<tr>
<td>Cat 6</td>
<td>4</td>
<td>Orange</td>
<td>Intruder is conducting reconnaissance against asset with access to sensitive data</td>
</tr>
<tr>
<td>Cat 3</td>
<td>5</td>
<td>Red</td>
<td>Intruder is attempting to exploit asset with access to sensitive data</td>
</tr>
<tr>
<td>Cat 2</td>
<td>6</td>
<td>Orange</td>
<td>Intruder has compromised asset with access to sensitive data but requires privilege escalation</td>
</tr>
<tr>
<td>Cat 1</td>
<td>7</td>
<td>Red</td>
<td>Intruder has compromised asset with ready access to sensitive data</td>
</tr>
<tr>
<td>Breach 3</td>
<td>8</td>
<td>Purple</td>
<td>Intruder has established command and control channel from asset with ready access to sensitive data</td>
</tr>
<tr>
<td>Breach 2</td>
<td>9</td>
<td>Purple</td>
<td>Intruder has exfiltrated nonsensitive data or credentials/access techniques that will facilitate access to sensitive data</td>
</tr>
<tr>
<td>Breach 1</td>
<td>10</td>
<td>Black</td>
<td>Intruder has exfiltrated sensitive data or is suspected of exfiltrating sensitive data based on volume, etc.</td>
</tr>
</tbody>
</table>

**Note:** Traditional incident response teams use events of impact 6 or higher to denote true "incidents," i.e., compromise of an asset.

**Crisis 3. 11** / Intruder has publicized data loss via online or mainstream media.

**Crisis 2. 12** / Data loss prompts government or regulatory investigation with fines or other legal consequences.

**Crisis 1. 13** / Data loss results in physical harm or loss of life.

**Crisis 0. 14** / Organization ceases to exist.
• http://taosecurity.blogspot.com/2009/05/lessons-from-cdx.html
• http://taosecurity.blogspot.com/2009/05/highlights-from-2009-verizon-data.html
• http://taosecurity.blogspot.com/2009/05/cheap-it-is-ultimately-expensive.html
• http://taosecurity.blogspot.com/2009/06/information-security-incident.html
Questions?

Know your network before an intruder does

Richard Bejtlich
richard@taosecurity.com
taosecurity.blogspot.com