Anatomy of a Data Breach

Tim Matthews
Director, Product Marketing
Relevant Modes of Data Loss

Well Meaning Insider
- Lost Laptop
- Data Spills
- Posting to P2P Networks

Malicious Insider
- Stolen USB Drive
- Anonymizing Proxies

External Adversaries
- Nationalists
- Crime Rings
- Hactivists
Adversary Profile: Nationalists

Means of Attack

• Extensive research on target
• Adversary Objective
  • Exfiltration or disruption of operations

Examples

• Hydraq (Aurora)
• Stuxnet
• GhostNet
• TitanRain
• Moonlight Maze
Adversary Profile: Crime Rings

- Targeted attack, Banking trojans, Phishing
- **Adversary Objective**
  - Incursion and exfiltration leading to mass fraud and brand damage

**Means of Attack**

- Epsilon breach
- Zeus, Clampi
- Storm Botnet, Mariposa, McColo

**Examples**
Adversary Profile: Malicious Insiders

Means of Attack
- IP theft via email/webmail, USB, laptop
- Adversary Objective
  - Financial gain, revenge

Examples
- Many financial organizations
- GM design document theft
- NASA espionage bust
- CD/DVD, P2P, TOR
Adversary Profile: Hacktivists

Means of Attack

- Abuse of insider access, social-engineering and/or quasi-legal technical tools
- **Adversary Objective**
  - Political activism and revenge

Examples

- U.S. Army
- U.S. Department of State
- Major financial institutions
Overview of Data Breach Trends
Trends in Causes of Data Breaches

Data Breaches by Sector

<table>
<thead>
<tr>
<th>Sector</th>
<th>Avg. # of Identities Exposed</th>
<th>Avg. # of Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>235,383</td>
<td>25,000</td>
</tr>
<tr>
<td>Education</td>
<td>37,210</td>
<td>25,000</td>
</tr>
<tr>
<td>Government</td>
<td>34,135</td>
<td>25,000</td>
</tr>
<tr>
<td>Healthcare</td>
<td>24,331</td>
<td>25,000</td>
</tr>
</tbody>
</table>

Volume of Data Breaches by Sector

- Financial: 11%
- Education: 18%
- Healthcare: 27%
- Government: 13%
- Retail/wholesale: 12%
- Insurance: 5%
- Community/non-profit: 3%
- Hospitality: 2%
- Arts/media: 2%
- Military: 2%
- Law enforcement: 2%
- Other: 4%
Threat Landscape Trends

1. Targeted Attacks continued to evolve

2. Social Networking + social engineering = compromise

3. Hide and Seek (zero-day vulnerabilities and rootkits)

4. Attack Kits get a caffeine boost

5. Mobile Threats increase
Four Phases of an Attack

1. Incursion
   Routes of entry
   - System vulnerabilities
   - Default password
   - SQL injection
   - Targeted malware

2. Discovery
   Map out systems and hunt for targets for compromise

3. Capture
   - Compromise of primary systems
   - Capture of exposed data

4. Exfiltration
   Captured data sent to home base in encrypted payloads
Textbook Controls are Failing to Protect Data

Access Controls and Compartmentalization should act as filters for confidential information, but are not sufficient protection for most companies.

Data is then lost via:
- Laptops
- Removable Media
- Network Communications

Anatomy of a Data Breach
Data Breach Scenarios
Disgruntled Employee

Setup

– Utility did Data Loss Prevention (DLP) risk assessment with Symantec
– Configured to detect large downloads of confidential data
– DLP detected an employee doing mass downloads to a thumb drive
– Investigations revealed employee was planning defection to competition

Implications

– Damaging leak of enterprise IP was detected and controlled before loss
– This profile (technically simple malicious activity) fits most cases of theft
– Large scale rollout of these protections now underway
Hacker

• Setup
  – March 2010: Shell reports breach of personal details of over 170k employees
  – Details leaked to political adversaries of Shell: GreenPeace, Friends of Earth
  – Investigation is now ongoing but suspicions are “Hacktivists” stole the data

• Implications
  – Data has been purposefully leaked on to the open Internet
  – Personal details (ph #s, home addresses) exposed to the outside world
  – Security risk to Shell employees
Donor Database Inadvertently Leaked

**Setup**
- Well meaning insider mistakenly posted donor details
- No process in place to monitor or detect such exposures

**Implications**
- Identities of campaign contributors on display
- WikiLeaks activists discovered the breach and distributed it
- Embarrassing breach disclosure process ensued
Summary of Relevant Defensive Techniques
Recommended Countermeasures

Basic Protections

• Deploy device control
• Encrypt laptops
• Update access control policies
• Employ security awareness training
• Conduct regular data loss risk assessments
• Monitor traffic to anonymizing proxies
• Monitor P2P traffic
Recommended Countermeasures

Advised Controls for “At Risk” Organizations

• Identify critical information assets
• Develop content-aware policies to drive remediation
• Detect high risk data exposure and data flow
• Prevent large scale exfiltration
• Encrypt exposed confidential data
• Blacklist onion routing applications
Summary of Crucial Defensive Technologies

- Advanced Reputation Security
- Security Incident and Event Management
- Host Intrusion Prevention
- Strong Authentication
- Data Loss Prevention
- Encryption
- Network Threat/Vulnerability Monitoring
Recommended Actions

- Begin formulating your data protection policy
- Assess your risk
- Identify key cross functional stakeholders
- Start investigating technology solutions
- Drive a cross functional team to address risk
Thank you!

Tim Matthews
Director, Product Marketing
Tim_matthews@symantec.com