Agenda

• **About the Report**
• **Analysis of 2009 Incident Response Investigations**
  • About the Sample Set
  • Investigative Conclusions
  • Anatomy of a Data Breach
• **Analysis of 2009 Penetration Tests**
  • About the Sample Set
  • Top 10 Lists
• **The Global Remediation Plan**
• **Conclusions**
• **Bonus Material in the Report**
• **Where to get it?**
• **Contacts**
About The Report

- Planning started in early 2009
- 10x the number of PenTest vs. Investigations
- A tool for organizations in prioritizing 2010 initiatives
- This is NOT a survey; only real-life data
- Also, we did NOT try to pass the weight test
Analysis of Incident Response Investigations

Why? Organizations are Reacting!

• Perform Actions to Stop an Attack
  • Understand the attack
  • Understand the losses

• Provide Reporting to Interested Parties

• Assist Law Enforcement
  • Apprehend criminals
Incident Response – About the Sample Set

218 Investigations

• 24 countries

• 18% Found Inconclusive
  – No evidence of critical data leaving
  – Many factors impact an inconclusive case

• Average of 156 Days Lapse Between Initial Breach and Detection (!?!?!)

Copyright Trustwave 2010
Confidential
Incident Response – About the Sample Set

Types of Detection

- Public Detection 8.0%
- Self-Detection 9%
- Law Enforcement 3%
- Regulator Detection 80%
Incident Response – About the Sample Set

Countries Represented in 2009

Australia
Belgium
Canada
Chile
Cyprus
Denmark
Dominican Republic
Ecuador
Germany
Greece
Hong Kong
Ireland
Luxembourg
Malaysia
Puerto Rico
Saudi Arabia
South Africa
Sri Lanka
Switzerland
Ukraine
United Arab Emirates
United Kingdom
United States
Virgin Islands
Incident Response – About the Sample Set

**Industries**

- Technology: 4.0%
- Education: 1.4%
- Manufacturing: 1.4%
- Hospitality: 38.0%
- Retail: 14.2%
- Financial Services: 19.0%
- Food and Beverage: 13.0%
- Business Services: 5.0%
- Other: 4.0%
Incident Response – About the Sample Set

Company Size

- >>1 - 499
- >>500 - 2,499
- >>2,500 - 9,999
- >>10,000 +
Incident Response – Investigative Conclusions

Types of Data at Risk

- Payment Card Data (98%)
- Other ~ 2%
  - Authentication Credentials (<1%)
  - Financial Information (<1%)
  - Other Sensitive Data (<1%)
  - Health Care (<1%)
Incident Response – Investigative Conclusions

Types of Target Assets

- Software-based POS (83%)
- E-commerce (11%)
- Payment Processing (3%)
- Workstation (<1%)
- Web-based Portal (<1%)
- ATM (2%)
Incident Response – Investigative Conclusions

System Administration Responsibility

Third Party 81%
Self 19%
Incident Response – Investigative Conclusions

Attacker Source Address Geography
Incident Response – Investigative Conclusions

Window of Data Exposure

\[
\begin{align*}
\text{Median} &= 101.50 \text{ days} \\
\text{Mean} &= 131.96 \text{ days} \\
\text{Median} &= 686.00 \text{ days} \\
\text{Mean} &= 930.25 \text{ days}
\end{align*}
\]
Anatomy of a Data Breach

Three Components:

1. Initial Entry
2. Data Harvesting
3. Exfiltration
Anatomy of a Data Breach – Initial Entry

Top Methods of Entry Included:

- **Remote Access Applications [45%]**
  - Default vendor supplied or weak passwords [90%]
- **3rd Party Connections [42%]**
  - MPLS, ATM, frame relay
- **SQL Injection [6%]**
  - Web application compromises [90%]
- **Exposed Services [4%]**
- **Remote File Inclusion [2%]**
- **Email Trojan [<1%]**
  - 2 recent Adobe vulnerability cases
- **Physical Access [<1%]**
Anatomy of a Data Breach – Data Harvesting

Top Methods of Harvesting (using Malware):

In 54% of our case, attackers used Malware to harvest data.
Anatomy of a Data Breach – Exfiltration

Top Methods of Data Exfiltration:

- >> Native Remote Access Application (27%)
- >> Native FTP Client (10%)
- >> Malware Capability: FTP (17%)
- >> Malware Capability: SMTP (4%)
- >> Exposed Private Web Application Interface (1.5%)
- >> HTTP File Upload Site (1.5%)
- >> Malware Capability: IRC (2%)
- >> Backdoor: Malicious PHP-based Web Shell (1%)
- >> Physical Access (<1%)
- >> Anonymous FTP (<1%)
- >> Encrypted Backdoor (<1%)
- >> Microsoft Windows Network Shares (28%)
Analysis of Penetration Tests

Why? Organizations are Proactive!

• Understand Security Posture
  – Multiple vectors
    – External network
    – Internal network
    – Wireless
    – Physical/social
    – Application
    – “What is our risk to compromise?”

• Provide Reporting to Executives and Technical Staff

• Assist in Prioritization of Risks
Penetration Tests – About the Sample Set

• 1,894 Penetration Tests
  – 48 countries

• Many Included a Mixture of Vectors
  – Network, application, wireless, physical

• Tests Averaged 80 hours in Length
Penetration Tests – About the Sample Set

Countries Represented in 2009

Australia
Argentina
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Croatia
Denmark
Dominican Republic
Ecuador
Egypt
France
Georgia
Germany
Greece
Hungary
Hong Kong
India
Japan
Iceland
Ireland
Lithuania
Luxembourg

Macedonia
Malaysia
Malta
Mexico
Moldova
Netherlands
Nigeria
Rep. of Cape Verde
Romania
Russian Federation
Saudi Arabia
Singapore
South Africa
Sri Lanka
Sweden
Switzerland
Taiwan
Turkey
Ukraine
United Arab Emirates
United Kingdom
United States
Penetration Tests – About the Sample Set

Industries

- Transportation (2.9%)
- Hospitality (3.1%)
- Food & Beverage (4.5%)
- Other (11.1%)
- Business Services (12.6%)
- Financial Services (16.1%)
- Retail (21.6%)
- Technology (23.5%)
- Telecommunication (1.8%)
- Education (1.7%)
- Manufacturing (1.1%)
Penetration Tests – About the Sample Set

Company Size

Cases

- >>1- 499
- >>500- 2,499
- >>2,500- 9,999
- >>10,000 +
Penetration Tests – About the Top 10s

• Intersection of Frequency & Criticality

• Not Meant to Replace other Industry Lists
  – Validate them?

• Organized in the Following Way:
  – Vulnerability
  – Definition
  – Impact
  – Circa
  – Attack Difficulty
# Penetration Tests – Top 10 – External Network

<table>
<thead>
<tr>
<th>Rank</th>
<th>Vulnerability Name</th>
<th>Circa</th>
<th>Attack Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unprotected Application Management Interface</td>
<td>1994</td>
<td>Easy</td>
</tr>
<tr>
<td>2</td>
<td>Unprotected Infrastructure Management Interface</td>
<td>1993</td>
<td>Easy</td>
</tr>
<tr>
<td>3</td>
<td>Access to Internal Application via the Internet</td>
<td>1997</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>Misconfigured Firewall Permits Access to Internal</td>
<td>1993</td>
<td>Hard</td>
</tr>
<tr>
<td>5</td>
<td>Default or Easy to Determine Credentials</td>
<td>1979</td>
<td>Trivial</td>
</tr>
<tr>
<td>6</td>
<td>Sensitive Information, Source Code, etc. in Web Dir</td>
<td>1990</td>
<td>Easy</td>
</tr>
<tr>
<td>7</td>
<td>Static Credentials Contained in Client</td>
<td>1980</td>
<td>Easy</td>
</tr>
<tr>
<td>8</td>
<td>Domain Name Service (DNS) Cache Poisoning</td>
<td>2008</td>
<td>Medium</td>
</tr>
<tr>
<td>9</td>
<td>Aggressive Mode IKE Handshake Support</td>
<td>2001</td>
<td>Easy</td>
</tr>
<tr>
<td>10</td>
<td>Exposed Service Version Issues (Buffer Overflows)</td>
<td>1996</td>
<td>Hard</td>
</tr>
</tbody>
</table>
Penetration Tests – Top 10 – External Network

#1 and #2 – Unprotected Management Interfaces

**Definition:** Leaving a default application (#1) or infrastructure (#2) management interface available from the Internet.

**Impact:** Complete control of an organization externally facing environment; loss of data is eminent.

**Circa:** Both 1994 (applications) and 1993 (infrastructure). Referencing early commercial Web server software and web-based managed devices.

**Attack Difficulty:** Easy-Medium
## Penetration Tests – Top 10 – Internal Network

<table>
<thead>
<tr>
<th>Rank</th>
<th>Vulnerability Name</th>
<th>Circa</th>
<th>Attack Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Address Resolution Protocol (ARP) Cache Poisoning</td>
<td>1999</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Microsoft SQL Server with Weak Creds for Admin</td>
<td>1979</td>
<td>Trivial</td>
</tr>
<tr>
<td>3</td>
<td>Weak Password for Admin Level System Account</td>
<td>1979</td>
<td>Trivial</td>
</tr>
<tr>
<td>4</td>
<td>Client Sends LM Response for NTLM Authentication</td>
<td>1997</td>
<td>Medium</td>
</tr>
<tr>
<td>5</td>
<td>Crypto Keys Stored Alongside Encrypted Data</td>
<td>1974</td>
<td>Easy</td>
</tr>
<tr>
<td>6</td>
<td>Cached Domain Credentials Enabled on Hosts</td>
<td>1999</td>
<td>Easy</td>
</tr>
<tr>
<td>7</td>
<td>NFS Export Share Unprotected</td>
<td>1989</td>
<td>Medium</td>
</tr>
<tr>
<td>8</td>
<td>Sensitive Information Transmitted Unencrypted</td>
<td>1991</td>
<td>Trivial</td>
</tr>
<tr>
<td>9</td>
<td>Sensitive Info Stored Outside Secured Zone</td>
<td>1993</td>
<td>Trivial</td>
</tr>
<tr>
<td>10</td>
<td>VNC Authentication Bypass</td>
<td>2006</td>
<td>Trivial</td>
</tr>
</tbody>
</table>
#1 – Address Resolution Protocol (ARP) Cache Poisoning

**Definition:** This is an OSI Layer 2 attack where messages are sent to local machine announcing the MAC address change for their default gateway.

**Impact:** Man in the middle attacks of many protocols are possible rendering credentials and even data exposed to the attacker.

**Circa:** Many articles and discussions around this method appeared in 1999 leading to the development of Dsniff MITM toolkit in 2000.

**Attack Difficulty:** Medium
## Penetration Tests – Top 10 – Wireless

<table>
<thead>
<tr>
<th>Rank</th>
<th>Vulnerability Name</th>
<th>Circa</th>
<th>Attack Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wireless Client Associates While on Wired Network</td>
<td>2004</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Wireless Client Probes from Stored Profiles (KARMA)</td>
<td>2005</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>Continued Use of WEP Encryption</td>
<td>2004</td>
<td>Easy</td>
</tr>
<tr>
<td>4</td>
<td>Easily Determined WPA/WPA2 Pre-Shared Key</td>
<td>2006</td>
<td>Easy</td>
</tr>
<tr>
<td>5</td>
<td>Legacy 802.11 FHSS with No Security Controls</td>
<td>1999</td>
<td>Hard</td>
</tr>
<tr>
<td>6</td>
<td>Lack of Publicly Secure Packet Forwarding Enabled</td>
<td>2004</td>
<td>Medium</td>
</tr>
<tr>
<td>7</td>
<td>Wireless Clients Using “Guest” Instead of “Secured”</td>
<td>2003</td>
<td>Easy</td>
</tr>
<tr>
<td>8</td>
<td>Lack of Segmentation Between Wireless and Wired</td>
<td>1993</td>
<td>Easy</td>
</tr>
<tr>
<td>9</td>
<td>Wireless Device Connected and Left Unattended</td>
<td>2000</td>
<td>Easy</td>
</tr>
<tr>
<td>10</td>
<td>WPA used with TPIK and 802.11e QOS</td>
<td>2008</td>
<td>Hard</td>
</tr>
</tbody>
</table>
Penetration Tests – Top 10 – Wireless

#1 – Wireless Clients Associates While on Wired Network

**Definition:** In many cases, wireless clients will probe and associate with known networks broadcasting in the local vicinity.

**Impact:** Attackers can use this technique to compromise the wireless host and in turn gain access to the wired network.

**Circa:** In 2004, hostapd was introduced and popularized this attack vector.

**Attack Difficulty:** Medium
## Penetration Tests – Top 10 – Physical/Social

<table>
<thead>
<tr>
<th>Rank</th>
<th>Vulnerability Name</th>
<th>Attack Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lack of Plate Covering Gap from Door Lock to Strike Plate</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Motion Sensors Allow Egress from Sensitive Areas</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>Sensitive Data Left in Plain View</td>
<td>Trivial</td>
</tr>
<tr>
<td>4</td>
<td>Credentials/Pretext Not Verified Effectively</td>
<td>Easy</td>
</tr>
<tr>
<td>5</td>
<td>Dumpsters are Accessible and Unlocked</td>
<td>Easy</td>
</tr>
<tr>
<td>6</td>
<td>Bypass Route to Secured Areas Available</td>
<td>Easy</td>
</tr>
<tr>
<td>7</td>
<td>Motion Sensors Mounted Incorrectly – No Coverage</td>
<td>Medium</td>
</tr>
<tr>
<td>8</td>
<td>Unlocked and Otherwise Accessible Computers</td>
<td>Trivial</td>
</tr>
<tr>
<td>9</td>
<td>Network Not Protected Against Rogue Devices</td>
<td>Easy</td>
</tr>
<tr>
<td>10</td>
<td>Sensitive Data Cabling is Accessible from Public Areas</td>
<td>Easy</td>
</tr>
</tbody>
</table>
Penetration Tests – Top 10 – Physical/Social

#1 – Lack of Plate Covering Gap from Door Latch to Strike Plate

**Definition:** Using a stiff card or needle nose pliers, one can release the magnetic retainer and open the door.

**Impact:** Complete access control fail with little to no evidence of attack.

**Attack Difficulty:** Medium

**Circa:** Old as dirt or at least as long as lock-based access controls have been around.
# Penetration Tests – Top 10 – Application

<table>
<thead>
<tr>
<th>Rank</th>
<th>Vulnerability Name</th>
<th>Circa</th>
<th>Attack Difficulty</th>
<th>OWASP (2010)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SQL Injection</td>
<td>1998</td>
<td>Medium</td>
<td>A1</td>
</tr>
<tr>
<td>2</td>
<td>Logic Flaw</td>
<td>1985</td>
<td>Easy</td>
<td>None</td>
</tr>
<tr>
<td>3</td>
<td>Authorization Bypass</td>
<td>1997</td>
<td>Easy</td>
<td>A3</td>
</tr>
<tr>
<td>4</td>
<td>Authentication Bypass</td>
<td>1960</td>
<td>Easy</td>
<td>A4/A7</td>
</tr>
<tr>
<td>5</td>
<td>Session Handling</td>
<td>1997</td>
<td>Medium</td>
<td>A3</td>
</tr>
<tr>
<td>6</td>
<td>Cross-Site Scripting (XXS)</td>
<td>2000</td>
<td>Hard</td>
<td>A2</td>
</tr>
<tr>
<td>7</td>
<td>Vulnerable Third-Party Software</td>
<td>1960</td>
<td>Medium</td>
<td>A6</td>
</tr>
<tr>
<td>8</td>
<td>Cross-Site Request Forgery (CSRF)</td>
<td>1988</td>
<td>Hard</td>
<td>A5</td>
</tr>
<tr>
<td>9</td>
<td>Browser Cache-Related Flaws</td>
<td>1998</td>
<td>Medium</td>
<td>None</td>
</tr>
<tr>
<td>10</td>
<td>Verbose Errors</td>
<td>1980</td>
<td>Medium</td>
<td>None</td>
</tr>
</tbody>
</table>
Penetration Tests – Top 10 – Application

#2 – Logic Flaw

**Definition:** A flaw that allows an attacker to bypass intended applications controls/functions.

**Impact:** Typically fraud related. Depending on the application this could have devastating effects on the data used by the system.

**Circa:** Logic flaws have been part of computing since the beginning, but started to gain recognition as a security issue in the mid-1980s.

**Attack Difficulty:** Easy
The Global Remediation Plan - Clarity

• Compromise = Major Loss of Business

• Overlooked systems and vulnerabilities
  – Lead to compromises

• Targeted Attacks
  – On the rise
  – In 2009, Hospitality was hit HARD; who is next?
The Global Remediation Plan – Industry Comparison

Penetration Tests vs. Investigations

- Technology
- Retail
- Financial Services
- Business Services
- Food & Beverage
- Hospitality
- Transportation
- Telecommunication
- Education
- Manufacturing

% Cases

Copyright Trustwave 2010
Confidential
# The Global Remediation Plan – The Plan

<table>
<thead>
<tr>
<th>Rank</th>
<th>Strategic Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Perform and Maintain a Complete Asset Inventory; Decommission Old Systems</td>
</tr>
<tr>
<td>2</td>
<td>Monitor Third Party Relationships</td>
</tr>
<tr>
<td>3</td>
<td>Perform Internal Segmentation</td>
</tr>
<tr>
<td>4</td>
<td>Rethink Wireless</td>
</tr>
<tr>
<td>5</td>
<td>Encrypt Your Data</td>
</tr>
<tr>
<td>6</td>
<td>Investigate Anomalies</td>
</tr>
<tr>
<td>7</td>
<td>Educate Your Staff</td>
</tr>
<tr>
<td>8</td>
<td>Implement and Follow a Software Development Life Cycle (SDLC)</td>
</tr>
<tr>
<td>9</td>
<td>Lock Down User Access</td>
</tr>
<tr>
<td>10</td>
<td>Use Multifactor Authentication Every Where Possible</td>
</tr>
</tbody>
</table>
Conclusions

• Attackers are using old vulnerabilities

• Attackers know they won’t be detected

• Organizations do not know what they own or how their data flows

• Blind trust in 3rd parties is a huge liability

• Fixing new/buzz issues, but not fixing basic/old issues

• In 2010, take a step back before moving forward
Bonus Material in The Report

The Global Security Report 2010 contains details of the content in this presentation plus many informative pieces:

- “Off-the-Shelf versus Custom Malware”
- “Penetration Testing versus Vulnerability Scanning”
- “How Layer 2 Attacks Work”
- “The FHSS Myth”
- “Top 5 Techniques to Unlawfully Enter a Data Center”
- “Automated versus Manual”
Where to get it?

• On the Black Hat Web site
  • http://www.blackhat.com
  • Immediately following this talk!

• On the Trustwave Web site
  • https://www.trustwave.com/whitePapers.php
  • February 9th, 2010
Contacts

Phone: +1 312 873-7500
E-mail: GSR2010@trustwave.com
Web: https://www.trustwave.com/spiderlabs
Twitter: @SpiderLabs / @Trustwave

Nicholas J. Percoco
Senior Vice President, SpiderLabs
Trustwave
Phone: +1 312 873-7471
Email: npercoco@trustwave.com
Twitter: @c7five
Thank You!