Defending the Enterprise Against Spyware and Adware

Robert W. Baldwin, Plus Five Consulting, Inc.
Kevin W. Kingdon, Intellitrove, Inc.
Outline

• Losses from Spyware, Adware, etc.
• Limitations of Traditional Security Products
• Enterprise Anti-Spyware Shopping Criteria
• Trends in Spyware & Anti-Spyware
Spyware as Mainstream Problem

• Spyware = Any Unwanted Software = Malware
  — Key Logger, Screen Capture, Ad-ware, Pop-Up Storms, Extra Links, Hijack Search Page, Window Over Page, etc.

• Wide Media Attention

CNN.com

THE WALL STREET JOURNAL

The New York Times

BusinessWeek
Microsoft Spyware Movie

Protecting Your Computer from Spyware

RISK ADVISORY
SIGNIFICANT RISK
IDENTITY THEFT

Plus Five Consulting
and Intellitrove

RSA Conference 2005
Enterprise Spyware Losses

- Lost Productivity of Employees
  - Performance and Usability

- IT Cost of Fixing
  - Repairing, Replacing

- Rare Yet Major Liabilities
  - ID Theft (Passwords, Digital Identity)
  - Theft of Enterprise Product Plans, Trade Secrets, Customer Data
  - Eavesdropping on Corporate Conversations, Email, Net-Meetings

- Courtroom Embarrassments
Outline

• Losses from Spyware, Adware, etc.

→ Limitations of Traditional Security Products

• Enterprise Anti-Spyware Shopping Criteria

• Trends in Spyware & Anti-Spyware
Traditional Security Products

- Norton Desktop Suite
- McAfee Desktop Suite
- Email Filters on Servers
- Network Firewalls
- Microsoft Security Utilities
Backup & Restore

- Backup System State, User Files and Programs
- Restore to Previous State
  - Hopefully Safe State
  - Could Restore Spyware
- Partial Restore Tricky Without Losing User Data
  - Spyware Inside User File
  - Registry Entries
  - Programs Tied To Registry
- Automatic Checkpoints
  - System & User Data
- Restore in Windows or Pre-OS
- Storage Outside Windows File Sys
Internet Explorer Security Enhancements

• Browser and Email are Major Infection Vectors
  — Some Threats Reduced by Switching Browsers or Email

• IE has Controls for Blocking Images, Pop-Ups, Downloads

• IE has White-Lists (Trusted Sites) and Black-Lists (Restricted Sites)
  — Hard: User Training, Configuration Updating
  — Lost Productivity when Websites Don’t Work Right

• End User can Still Decide to Download “Cute” Application, Add-On or Toolbar That is Spyware
Outline

• Losses from Spyware, Adware, etc.
• Limitations of Traditional Security Products
  ➔ Enterprise Anti-Spyware Shopping Criteria
• Trends in Spyware & Anti-Spyware
Enterprise Anti-Spyware Criteria

• Must Detect Wide Range of Problems
  — Ad-Ware, Pop-Ups, Hijacking, Keystroke logger, Tracking Cookies, ActiveX Objects, Browser Extensions, Start-up, Reconfiguration, etc.

• Quantity and Timeliness of Detectable Problems

• Quality of Fixing Problems

• Scanning

• Prevention and Protection

• Management Features
Enterprise Anti-Spyware Criteria
Scanning

• Running Programs
• Registry
  — Browser Settings
  — Application Settings
  — System Settings
• File System
  — Compressed
  — Attachments
  — Scripts and Macros
• Removable Media
  — Drivers
  — File System
Enterprise Anti-Spyware Criteria
Prevention and Protection

• Trigger Events
  — File Downloads
  — Email Receipt
  — Auto-installed Drivers
  — Process Launch
  — ActiveX Control Install
    • Kill Bits
  — Browser Helper Object Install

• Monitor Configuration Settings
  — System Startup
  — HOSTS Files
  — Winsock LSP Chain
  — Browser Hijacks
  — IE Restricted and Trusted Sites
Enterprise Anti-Spyware Criteria
Management Features

• Silent Install
• Enterprise Configuration Control
• Enterprise Update Hosting
• Centralized Reporting of Scanning, Finding, Fixing
• Support All Installed Versions of Windows
# Anti-Spyware Comparison Matrix

<table>
<thead>
<tr>
<th>Product</th>
<th>Feature Set</th>
<th>Scanning</th>
<th>Prevention</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpyBot Search &amp; Destroy</td>
<td></td>
<td>♦♦♦♦♦</td>
<td>♦♦♦♦♦</td>
<td>♦♦</td>
</tr>
<tr>
<td>Giant AntiSpyware (Microsoft)</td>
<td></td>
<td>♦♦♦♦♦</td>
<td>♦♦♦♦♦</td>
<td>♦♦♦♦♦</td>
</tr>
<tr>
<td>Webroot Spy Sweeper</td>
<td></td>
<td>♦♦♦♦♦</td>
<td>♦♦♦♦♦</td>
<td>♦♦♦♦♦</td>
</tr>
<tr>
<td>CA Pest Patrol</td>
<td></td>
<td>♦♦♦♦♦</td>
<td>♦♦♦♦♦♦</td>
<td>♦♦♦♦♦</td>
</tr>
<tr>
<td>Ad-Aware (Pro)</td>
<td></td>
<td>♦♦♦♦♦</td>
<td>♦♦♦♦♦</td>
<td>♦♦♦♦♦</td>
</tr>
</tbody>
</table>
SpyBot Search and Destroy

- Leading Free Tool to Find & Fix Spyware
- Geek Friendly
Microsoft AntiSpyware

- Giant Acquired by Microsoft December 2004
Webroot Spy Sweeper

- Good for Home and Enterprise
Outline

• Losses from Spyware, Adware, etc.
• Limitations of Traditional Security Products
• Enterprise Anti-Spyware Shopping Criteria

⇒ Trends in Spyware & Anti-Spyware
Trends in Spyware

• “Spyware” Now Broad Popular Term = “Unwanted Software”
  — Blurred with “Virus” and “Spam” and “Back-Doors”

• Growing Burden on Enterprise Productivity

• Automation of Social Engineering

• Financial Incentives Motivating New Tricks:
  — Steal Credit Card Numbers & PayPal ID
  — Drive Customers to Web Sites
  — Profit from Corporate Espionage
Trends in Anti-Spyware

- Microsoft Enters the Market
- Big Names Acquire Small Vendors
- Enterprise Deployment & Management Features
- ISPs Offering Re-branded Tools & Services
  - AOL, Yahoo, MSN
- More Legislation, Though With Limited Effect
- Improved Firewall and Email Filtering
For More Information

- www.SpywareInfo.com
- www.SpywareWarrior.com
- www.webroot.com/spywareinformation
- www.microsoft.com/spyware
- www.spynet.com (Microsoft)
- www.pcmag.com (Search “spyware”)
- For Current Version of This Presentation: www.plusfive.com
  www.intellitrove.com
Questions?

• Robert W. Baldwin, baldwin@plusfive.com
• Kevin W. Kingdon, kevin@intellitrove.com