Survey of Spyware Tools and Counter Measures

Dr. Robert W. Baldwin
Plus Five Consulting, Inc.

Kevin W. Kingdon
Intellitrove, Inc.
Outline

• Spyware Demonstration
• Spyware: Architecture & Features
• Ethics
• Counter Measures: Standard & Specific
• Future of Spyware & Counter Measures
Demonstration

- One of the Better Spyware Programs
Outline

- Spyware Demonstration
- Spyware: Architecture & Features
- Ethics
- Counter Measures: Standard & Specific
- Future of Spyware & Counter Measures
Spyware Feature Discussion

- Windows Has Built-In Logs for Spying
- Spyware Log Files are Very Sensitive
- Spyware Trumps Encryption
  - PGP Password Grabber Reporting Via Piggy-Back Email is Very Hard to Detect
- Smart Card May Not Help
  - Spyware Observes Decrypted Contents of Files
  - Trojan Software Can Query Smart Card (Future)
- Log Analysis Is Time Consuming
Malicious Software Taxonomy

- Spyware
- Ad-Ware
- Pop-Ups
- History & Logs
- Cookies
- Viruses & Worms
- Parental Controls

Dangerous vs. Harmless
Monitor vs. Modify
Spyware Logical Scope

- Word
- Chat
- Email
- Web
- Net Meeting

- Application Launch, Network Connections
- Screenshots, Keystrokes, File Access
- Microphone, Modem (Voice!), Camera
Spyware System Architecture

- Target
- File or Mail Server
- Spy Inside
- Spy Outside
- Internet
- Firewall
Spyware Hardware

KeyKatcher
- PS/2 Inline
- 64-256 Kbytes
- Password
- TTY Dump
- Limited Search

High-End
Built Into
Brand Name
Keyboards
Spyware Hardware Scope
Outline

• Spyware Demonstration
• Spyware: Architecture & Features
• Ethics
• Counter Measures: Standard & Specific
• Future of Spyware & Counter Measures
Spyware Ethics

The Easiest Way to Spy.
And by far, the most Powerful.

A simple Greeting Card turns into a robust spy tool.

Spouses ~ Designed for You.

The ONLY spy software that installs 100% invisibly & Remotely - simply by signing up at this web site!
Spyware Ethics

• “Within 36 hours I had enough evidence to approach the police and the man was arrested …”
• “One of the BEST investments I EVER made.”
• “I found all 17 of his girlfriends … Thank you for saving me from marrying … this undeserving person.”
• “Now that I know about my boss’ layoff plans, I’m updating my resume.”
# Spyware Ethics

<table>
<thead>
<tr>
<th>Legitimate</th>
<th>Dubious</th>
<th>Criminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect &amp; Educate Children</td>
<td>Spy on Spouse</td>
<td>Steal Credit Card Numbers</td>
</tr>
<tr>
<td>Mitigate Corporate Liability</td>
<td>Spy on Boss</td>
<td>Steal Trade Secrets</td>
</tr>
<tr>
<td>Gather Evidence for Police</td>
<td>Spy on Dissidents, Fish for Criminals</td>
<td>Steal National Secrets</td>
</tr>
</tbody>
</table>
Outline

• Spyware Demonstration
• Spyware: Architecture & Features
• Ethics
• Counter Measures: Standard & Specific
• Future of Spyware & Counter Measures
Counter Measures Architecture

Target File or Mail Server

Spy Inside

Firewall

Internet

Spy Outside
CM: Existing Windows Features

- Scan for Unsigned System Files
- Scan for Newly Created Files
- Task Manager Reports Some Spyware
- MS Configuration Manager Reports Some Spyware Startup Items
- Disk & Network I/O Performance Monitors or LEDs Reflect Some Spyware Activity
CM: Standard Security Products

• Network and Personal Firewalls
  – Block Installation and Reporting
  – Can Detect Spyware Activity

• Central Email Virus & Executable Blocker
  – Helps Thwart Remote Installation

• Personal Email Scanner
  – Helps Block Installation and Reporting
CM: Ineffective Products

• Anti Virus Scanners
  – Norton, McAfee, Trend Micro Websites State: They Will *Not* Detect Spyware; “Monitoring Software Is Not Malicious”

• Ad-Ware Scanners
  – Don’t Target Keystroke Loggers, Etc.

• Ad-Ware and Pop-Up Blockers
  – Only Examine Browser-Related Activity
CM: Specific Tools

• Anti-Spyware Websites & Newsletters

• Window Washer, SpyBot & Others
  – Remove Information Examined by Spyware

• SpyBot, SpyCop, and Many More
  – Like Early Virus Scanners: Signature Based
  – Scan for Active Program Files & Installer Files
  – Scan for Registry Entries, Directories
CM: Specific Tools: SpyBot
CM: Specific Tool: SpyCop

Results of Scan
- Realtime Spy by Spytech Software
- Spector/Spector Pro/EBLaster by SpectorSoft
- SpyAgent by Spytech Software

Suspicious Files (double click for more information or to rename):
- C:\WINDOWS\sbrowse.exe
- C:\WINDOWS\system32\xmssysmru.exe
- C:\WINDOWS\SystemSA32.dll

Status
Your system may contain Spy software.
Counter Measures Discussion

• Free & Commercial Tools Very Effective Against Commercial Spyware
  – Program Quality & Usability Varies
  – Keeping Up With Spyware Signatures
• No Toolkits for Making Spyware (So Far!)
• Manual Scanning is the Norm
  – Future: Real Time Scanning with Automatic Removal or Quarantine
CM: Discussion

• Software Countermeasures Do NOT Work Against Spy Hardware
  – When Boss Spills Coffee on Your Keyboard …

• The Paranoid Need Both!
  – Spyware as Intrusion Detection Tool
  – Spyware to Detect Spyware Installation
Outline

• Spyware Demonstration
• Spyware: Architecture & Features
• Ethics
• Counter Measures: Standard & Specific
• Future of Spyware & Counter Measures
Future of Black Hat Spyware

- Spyware as Stepping Stone For Big Attack
  - Place Backdoor in MS Office Source Code
- Virus Writers Building Black Hat Spyware
  - Spyware Building Kits
  - Harder to Detect & Remove
  - Windows is Big Attractive Target
- Anti-Anti Spyware (That Works)
  - There Are Viruses That Disable ZoneAlarm
- More Recording of Phone, Fax, Copier, Printouts, Microphone & WebCam
Future of White Hat Spyware

- Private & Government Investigators
- Enterprise Features
  - Central Installation, Control, Upgrade
  - Eliminate Black Hat Features
- Better Analysis Tools
  - Adaptive Logging And Reporting Details
- Merge With Network Monitoring
Future of Counter Measures

• Fear of Lawsuits Keep Anti-Virus Vendors Out
• Spyware Detection Based on Behavior
  – Not Just Name & Content Signatures
  – Running All The Time; Check Downloads
• IT Approved Signed Executables
• Need Foundation For Better Anti-Spyware
  – Palladium & Phoenix StrongROM
• Rediscover the “Trusted Systems” Technologies from 1980s
Questions?

• More Information At:
• www.PlusFive.com
• www.Intellitrove.com