Spyware vs. Anti-Spyware

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

Kevin W. Kingdon
Intellitrove, Inc.

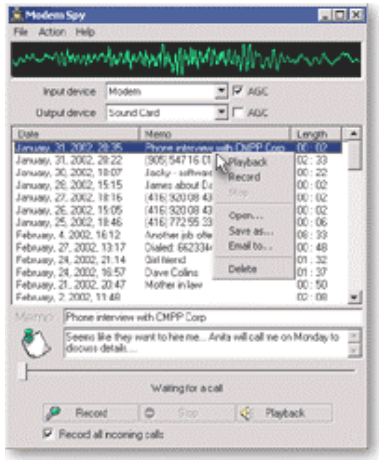
Outline

- Spyware Demonstration & Discussion
- Spyware: What's New & Old
- Anti-Spyware: What's New & Old
- Future of Spyware & Anti-Spyware

Demonstration

- SpyAgent

- ModemSpy

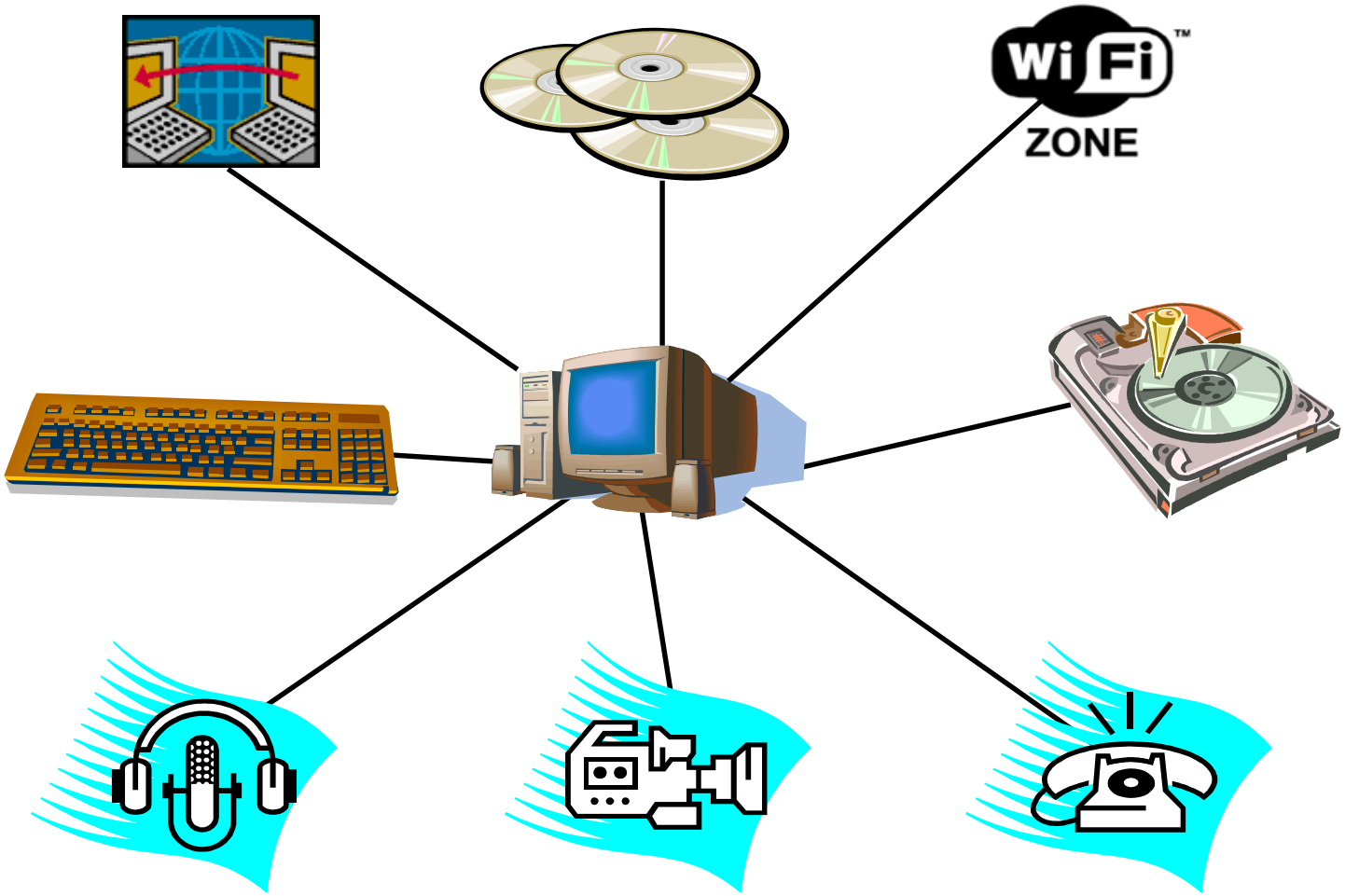


- SoundSnooper

Discussion of Demonstration

- Spyware Log Files are Very Sensitive
- Spyware Trumps Encryption, Certificates, Smart Cards
  - PGP Password Grabber Reporting Via Piggy-Back Email is Very Hard to Detect
- Log Analysis Is Time Consuming
- Sound Recording Legally Tricky
  - Not True for Video

Spyware Info Sources



Plus Five Consulting
and
Intellitrove

Spy Hardware

KeyKatcher
- Used by High School Students

High-End:
Built Into Brand Name Keyboards

Spyware Ethics

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

A simple **Greeting Card** turns into a robust spy tool.

Outline

- Spyware Demonstration & Discussion
- Spyware: What's New & Old
- Anti-Spyware: What's New & Old
- Future of Spyware & Anti-Spyware

What's New in Spyware

- More Specialization for Sub-Markets
  - Child Protection, Corporate, Spouse
  - Hidden Sub-Market: Spying for Profit
- Some Vendors Have Gone Out Of Business
- Corporate Network Surveillance
- FBI Prosecutes Spyware Vendors
  - New Legislation Pending
  - Stealth Install Features Have Gone Underground

What's New in Spyware

- Retreat from "Stench" of Black Hat Spyware
  - Avoid Logging Passwords or Credit-Card Numbers
  - Promoting Corporate Features: Distributed Install & Monitor
- Running in the Kernel for Better Capture & Stealth
  - WinXP Password Logging
- Rootkits Include Keylogging
- Better Hiding of Log Files and Communications
- More Modem and Microphone Spying

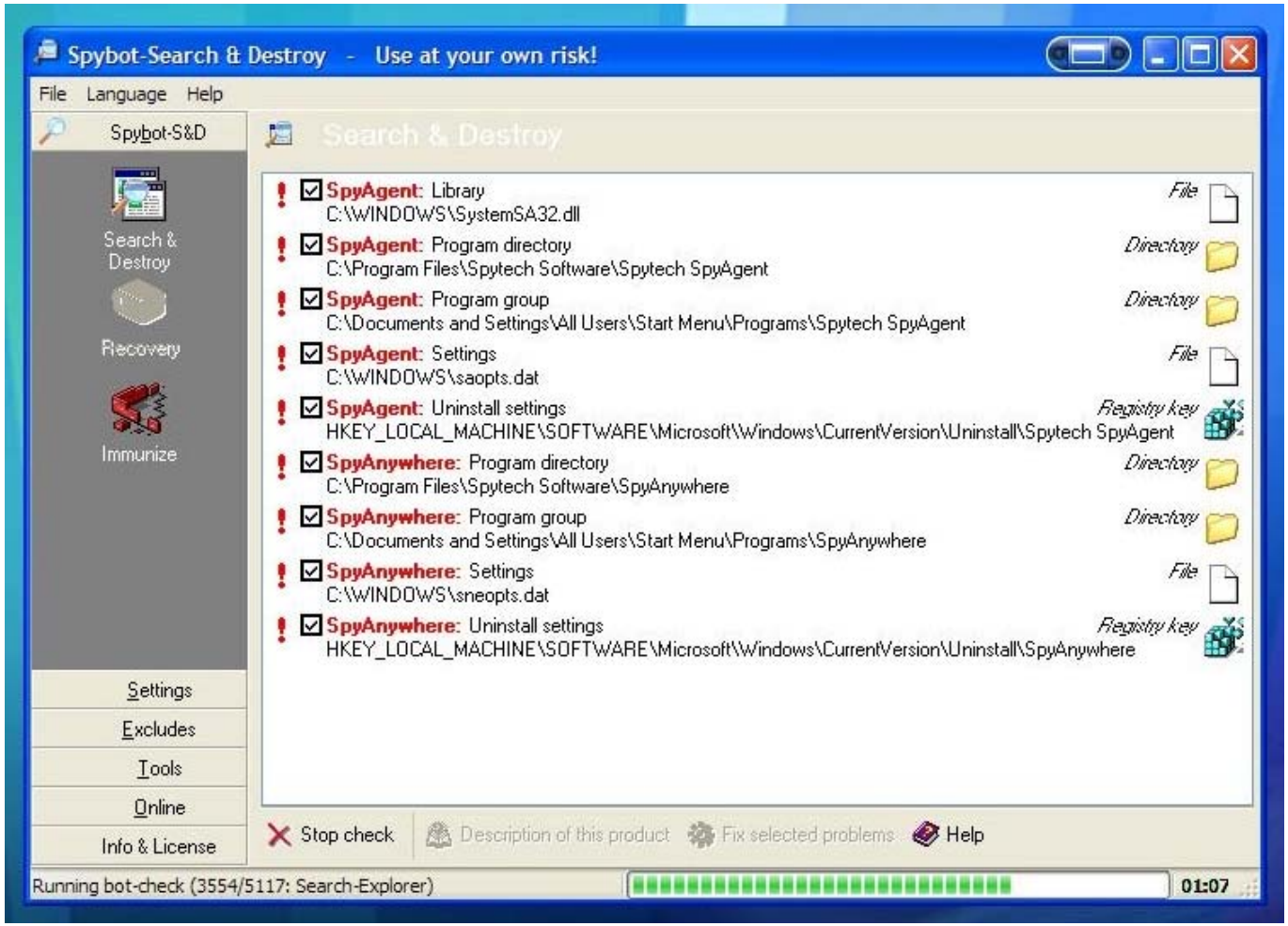
What's Old in Spyware

- SpectorSoft and SpyTech Remain the Leading Vendors
  - Still Lots of "Little Guys"
- No New Technologies for Collection or Stealth
- Remote Control Software Used As Spyware
- "Silent" Installation Common
- Good Reporting for Single Target
- Still Trumps Encryption
- Also Trumps Biometrics, Certificates and Smart Cards

Outline

- Spyware Demonstration & Discussion
- Spyware: What's New & Old
- Anti-Spyware: What's New & Old
- Future of Spyware & Anti-Spyware

Anti-Spyware: SpyBot



Anti-Spyware: SpyCop

What's New in Anti-Spyware

- Symantec and Network Associates Enter Market
  - More Corporate Awareness of Threats
- More Public Awareness of Threats
  - More "Little Guys" Making Spyware & Anti-Spyware
  - More Anti-Spyware Spam
  - Pending Legislation

What's Old in Anti-Spyware

- SpyCop Catches All Popular Spyware
- SpyBot Much Faster but Misses Some Spyware
- Good Security Practices Help
  - Virus Scanners, Email Filters, Firewalls, etc.
- Ad-ware and Popup-Blockers Ineffective Against Spyware

Built-in Windows Anti-Spyware

- Low-End Spyware Caught by Built-In Tools
- SigVerif.exe Finds Unsigned System Files
- Windows Explorer Finds Newly Created Files
- Task Manager Reports Some Spyware
- MsConfig.exe Reports Some Spyware Startup Items
- Disk & Network I/O LEDs Can Show Spyware Activity

Anti-Spyware Tools

- Anti-Spyware Websites & Newsletters
  - www.keylogger.org & www.spywareinfo.com
  - news:alt.privacy.spyware
- SpyBot, SpyCop, and Many More
  - Like Early Virus Scanners: Signature Based
  - Scan for Active Program Files & Installer Files
  - Scan for Registry Entries, Directories
- Window Washer, SpyBot & Others
  - Remove Information Reported by Spyware

Anti-Spyware Discussion

- Free & Commercial Tools Very Effective Against All Popular Spyware
  - Program Quality & Usability Varies
  - Keeping Up With Spyware Signatures Varies
- 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 & Discussion
- Spyware: What's New & Old
- Anti-Spyware: What's New & Old
- Future of Spyware & Anti-Spyware

Future of Black Hat Spyware

- Spyware as Stepping Stone For “The Big Attack”
  - Windows is Big Attractive Target
  - Place Backdoor in MS Source Code
- Crackers Building Black Hat Spyware
  - Better Spyware Building Kits
  - Harder to Detect & Remove
- Anti-Anti Spyware (That Works)
  - Spyware Disabling Anti-Spyware

Future of Black Hat Spyware

- Print Server Sniffing
- Sniffing WiFi Neighborhood
- Sniffing TCP/IP Sessions
- Capture NetMeeting, SSH sessions
- Spy Directly on Office Applications (VBA, VB.Net)
- Separate “Stealth Kits” as Add-On for Commercial Spyware

Future of White Hat Spyware

- Enterprise Features
  - Central Installation, Control, Upgrade
  - Eliminate Smell of Black Hat Features
  - Hire Private Investigators to Avoid Liability
- Better Analysis Tools
  - Adaptive Logging And Reporting Details
  - Easily Spy On 100 Employees
- Merge With Network Monitoring Products

Future of White Hat Spyware

- Child Protection Sub-Market Will Grow
  - Worried Parents Attract Large Vendors
  - Ease of Use, Reliability
  - Thought Police for Schools
- Corporate Policy Enforcement
  - Fax, Copier, Printer, Modem, Net
  - Record Files Saved to Removable Media
- More Recording of Microphone, Telephone, and Video
  - Watch the Babysitter

Future of Anti-Spyware

- Fear of Lawsuits Slows the Anti-Virus Vendors
- Spyware Detection Based on Behavior
  - More Than Name & Content Signatures
  - Running All The Time
  - Check Every Downloads
  - Detect Spyware Reporting
- IT Approved Signed Executables
- Still Waiting for Trusted Computing

Questions?

- For More Information:

  Baldwin@PlusFive.com

  Kevin@Intellitrove.com