Defending the Enterprise Against Spyware and Adware

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

RSA Conference 2005

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

WSJ .com THE WALL STREET JOURNAL. ONLINE

The McGraw-Hill Companies BusinessWeek

The New York Times ON THE WEB

Microsoft Spyware Movie

Protecting Your Computer *from Spyware*

RISK ADVISORY
SIGNIFICANT RISK
IDENTITY THEFT

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

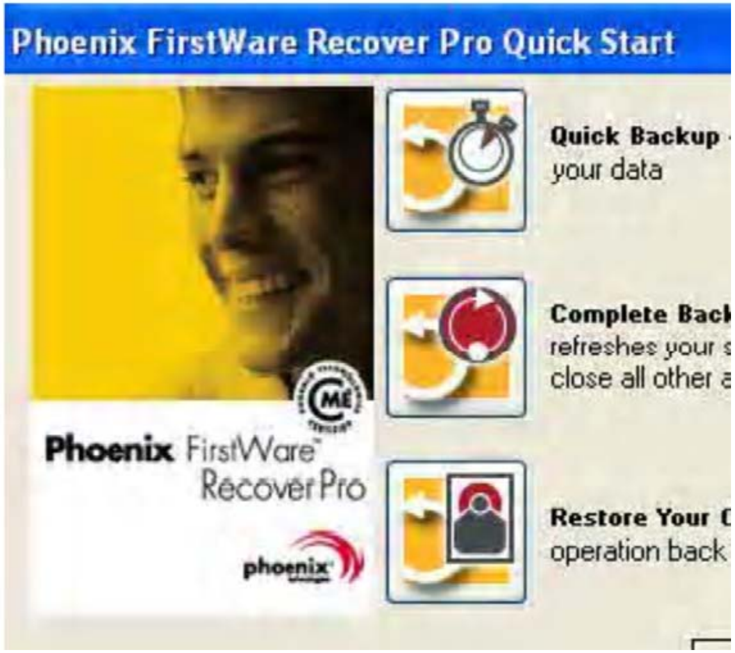
- Enterprise Anti-Spyware Shopping Criteria
- Trends in Spyware & Anti-Spyware

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

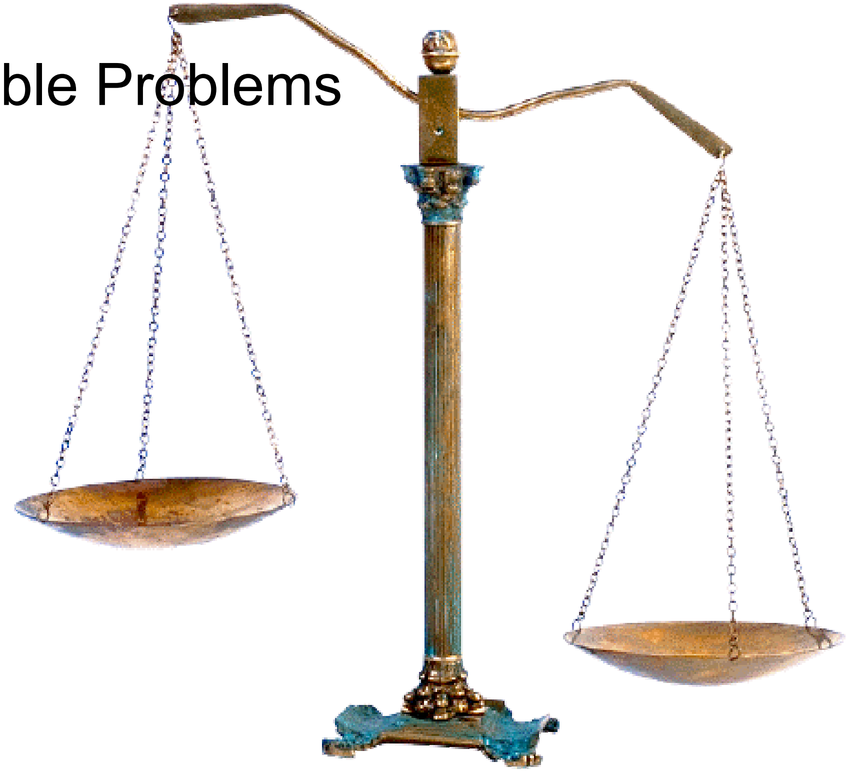
- Losses from Spyware, Adware, etc.
- Limitations of Traditional Security Products

➡ Enterprise Anti-Spyware Shopping Criteria

- Trends in Spyware & Anti-Spyware

Enterprise Anti-Spyware Criteria

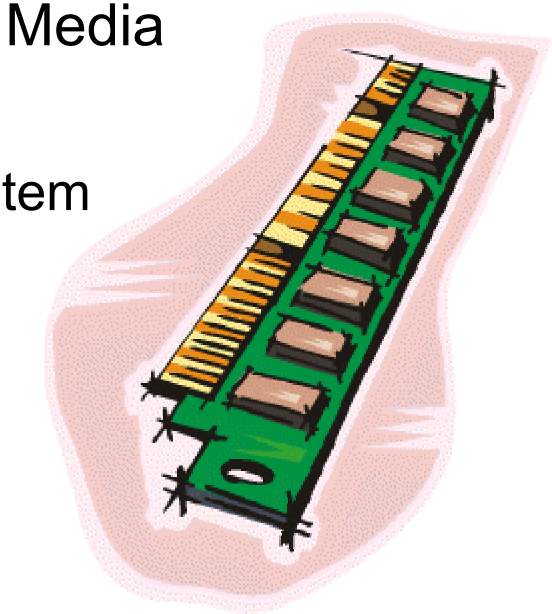
- Must Detect Wide Range of Problems
  - Ad-Ware, Pop-Ups, Hijacking, Keystroke logger, Tracking Cookies, ActiveX Objects, Brower Extensions, Start-up, Reconfiguration, etc.
- Quantity and Timeliness of Detectable Problems
- Quality of Fixing Problems
- Scanning
- Prevention and Protection
- Management 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



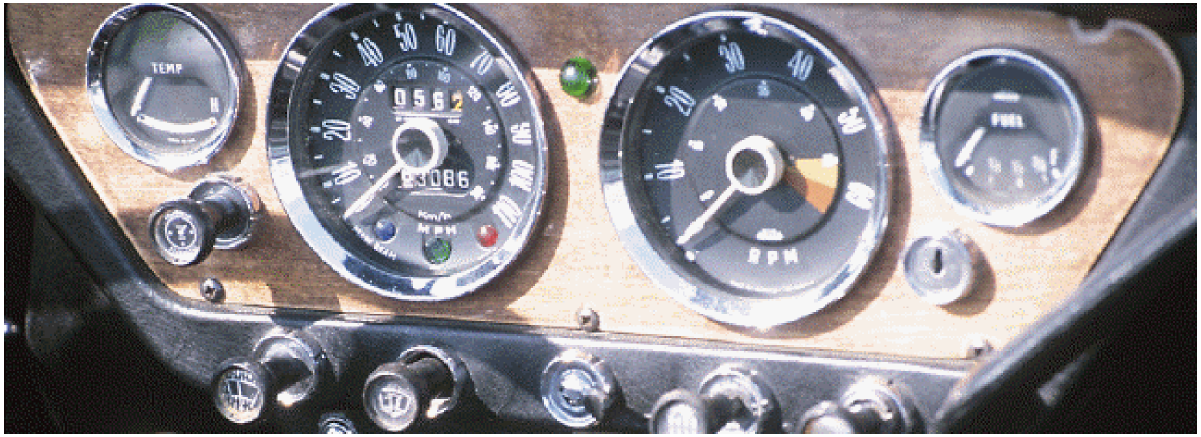
Enterprise Anti-Spyware Criteria Prevention and Protection

- 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

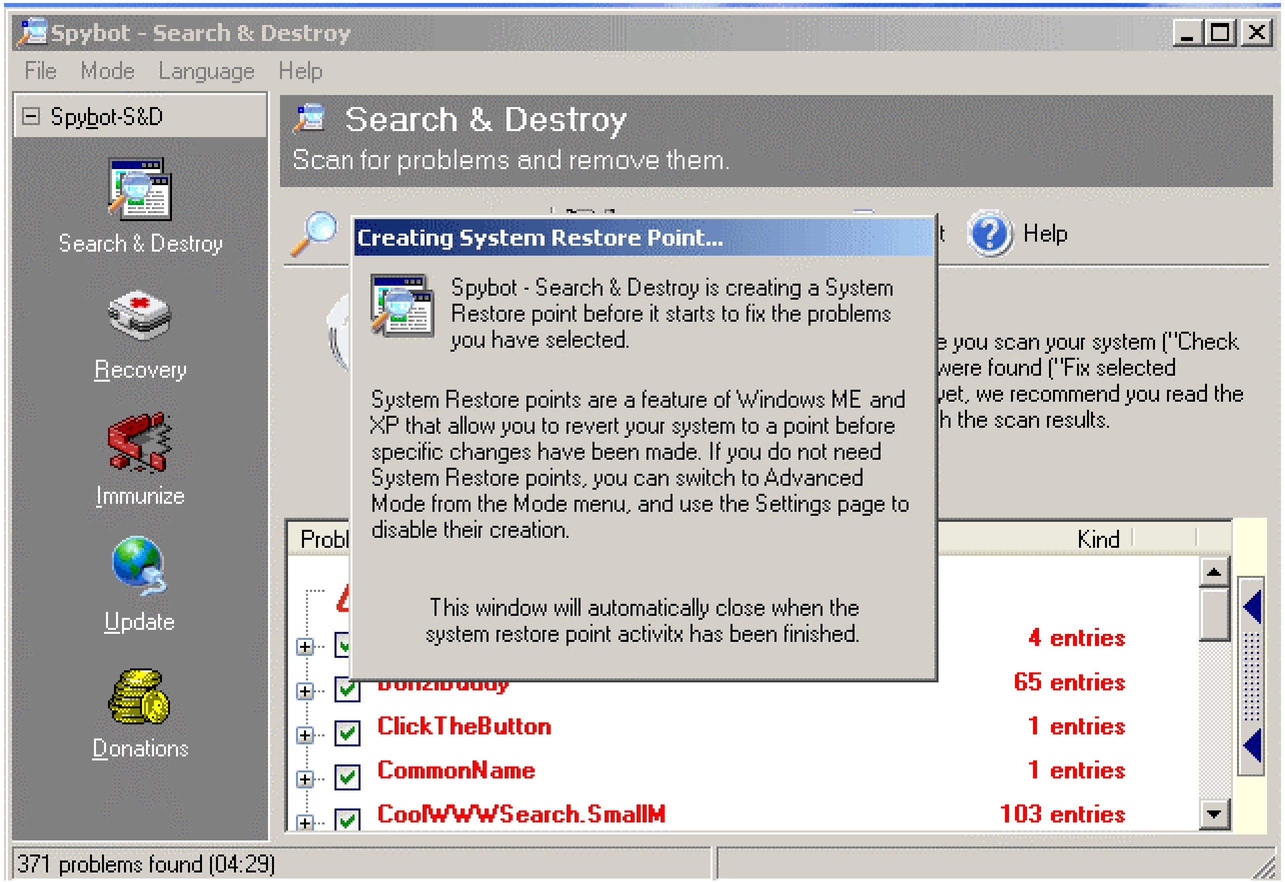


Anti-Spyware Comparison Matrix

Feature Set Product	Scanning	Prevention	Management
SpyBot Search & Destroy	♦ ♦ ♦ ♦	♦ ♦ ♦ ♦	♦ ♦
Giant AntiSpyware (Microsoft)	♦ ♦ ♦	♦ ♦ ♦	♦ ♦ ♦
Webroot Spy Sweeper	♦ ♦ ♦ ♦	♦ ♦ ♦ ♦	♦ ♦ ♦
CA Pest Patrol	♦ ♦ ♦ ♦	♦	♦ ♦
Ad-Aware (Pro)	♦ ♦ ♦	♦ ♦	♦ ♦

SpyBot Search and Destroy

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



Search & Destroy

Scan for problems and remove them.

Creating System Restore Point...

Spybot - Search & Destroy is creating a System Restore point before it starts to fix the problems you have selected.

System Restore points are a feature of Windows ME and XP that allow you to revert your system to a point before specific changes have been made. If you do not need System Restore points, you can switch to Advanced Mode from the Mode menu, and use the Settings page to disable their creation.

This window will automatically close when the system restore point activitx has been finished.

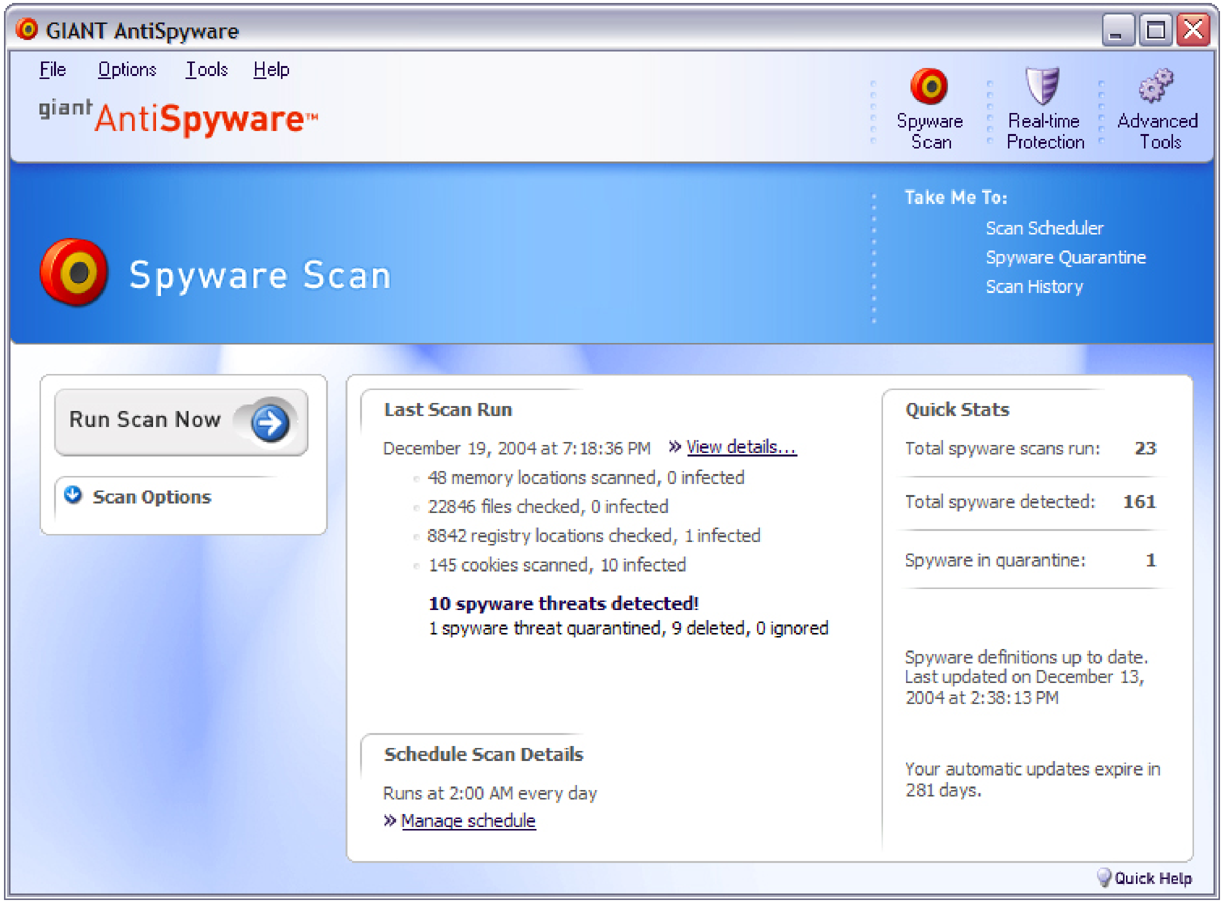
e you scan your system ("Check were found ("Fix selected yet, we recommend you read the h the scan results.

```
                                        4 entries
Bonzibuddy                             65 entries
ClickTheButton                          1 entries
CommonName                              1 entries
CoolWWWSearch.SmallM                  103 entries
```

371 problems found (04:29)

Microsoft AntiSpyware

- Giant Acquired by Microsoft December 2004



Last Scan Run

December 19, 2004 at 7:18:36 PM » View details...

- 48 memory locations scanned, 0 infected
- 22846 files checked, 0 infected
- 8842 registry locations checked, 1 infected
- 145 cookies scanned, 10 infected

10 spyware threats detected!
1 spyware threat quarantined, 9 deleted, 0 ignored

Schedule Scan Details

Runs at 2:00 AM every day
» Manage schedule

Quick Stats

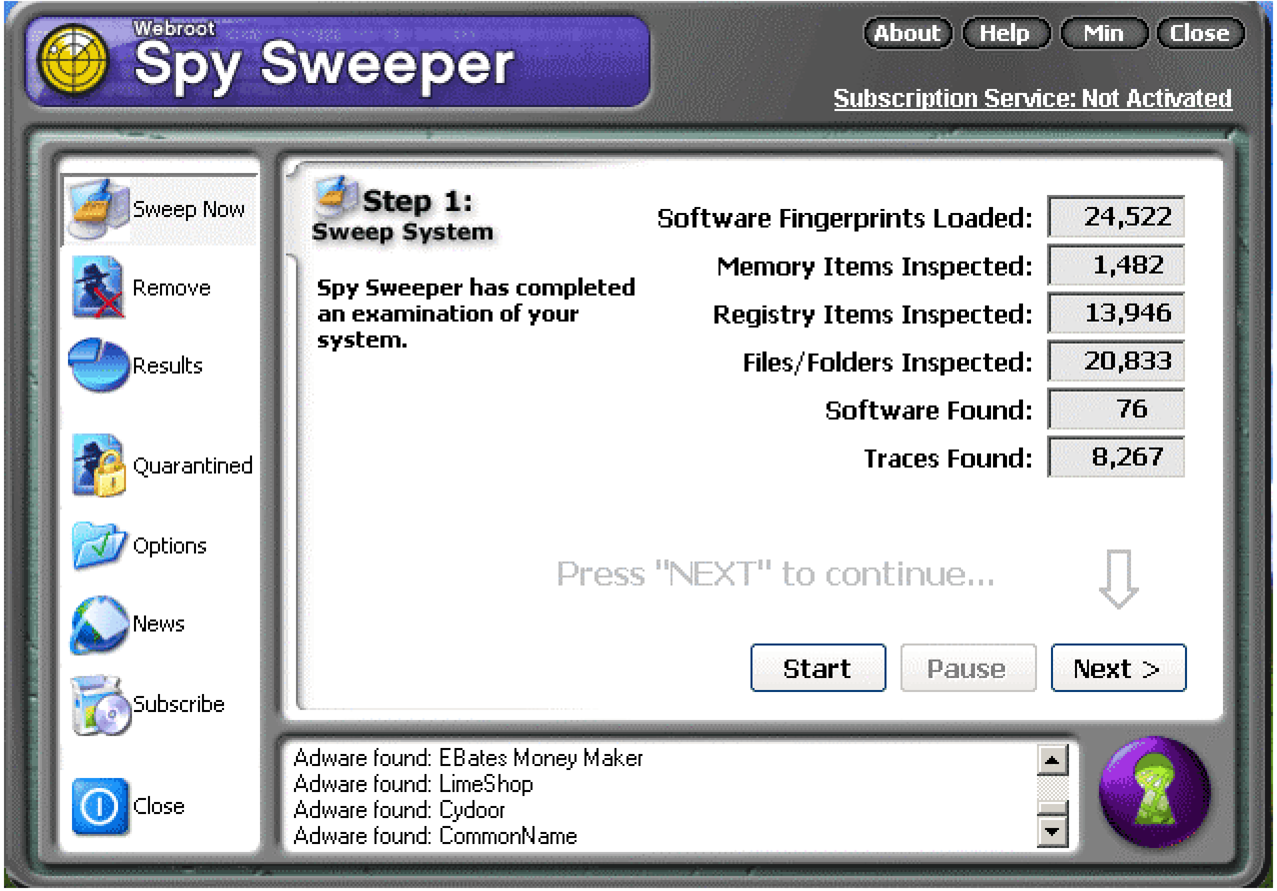
Total spyware scans run:	23
Total spyware detected:	161
Spyware in quarantine:	1

Spyware definitions up to date. Last updated on December 13, 2004 at 2:38:13 PM

Your automatic updates expire in 281 days.

Webroot Spy Sweeper

- Good for Home and Enterprise



Spy Sweeper has completed an examination of your system.

Software Fingerprints Loaded: 24,522
Memory Items Inspected: 1,482
Registry Items Inspected: 13,946
Files/Folders Inspected: 20,833
Software Found: 76
Traces Found: 8,267

```
Adware found: EBates Money Maker
Adware found: LimeShop
Adware found: Cydoor
Adware found: CommonName
```

Outline

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

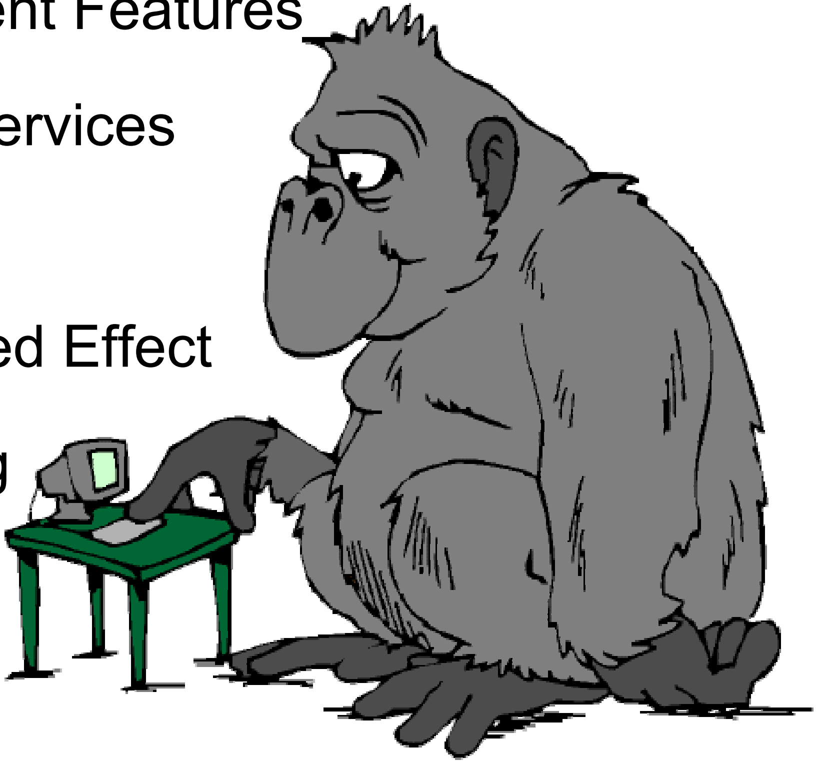
➡ Trends in Spyware & Anti-Spyware

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