

# Hot Issues in Computer Security: 2005

NARUC: February 15, 2005

**John Simek and Sharon Nelson**

Vice President and President

Sensei Enterprises, Inc.

Fairfax, VA

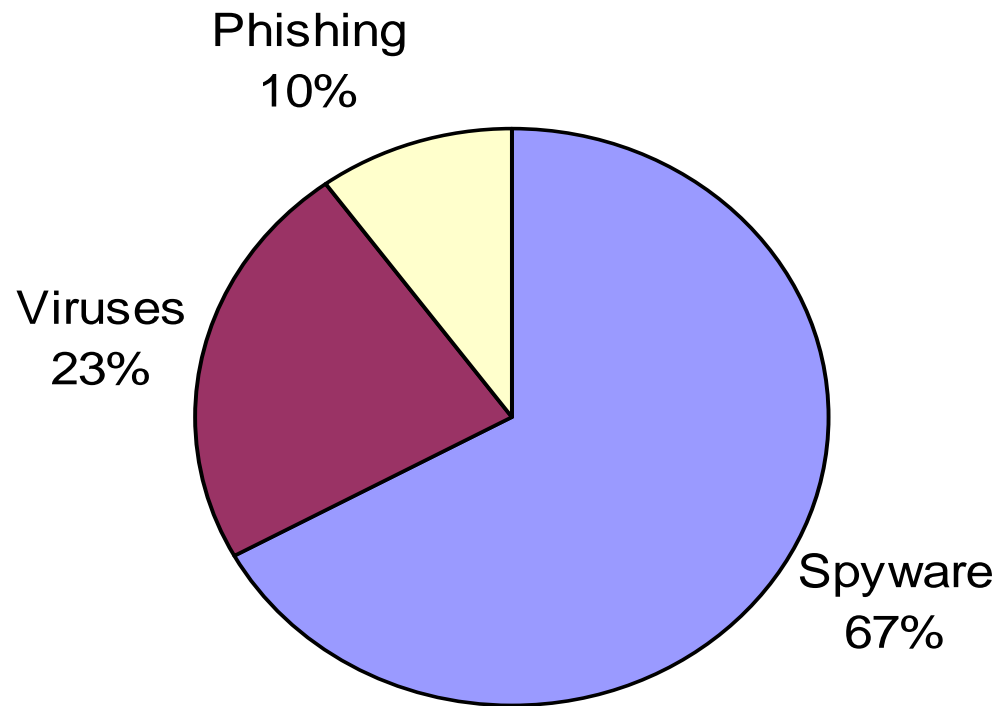
[jsimek@senseient.com](mailto:jsimek@senseient.com)

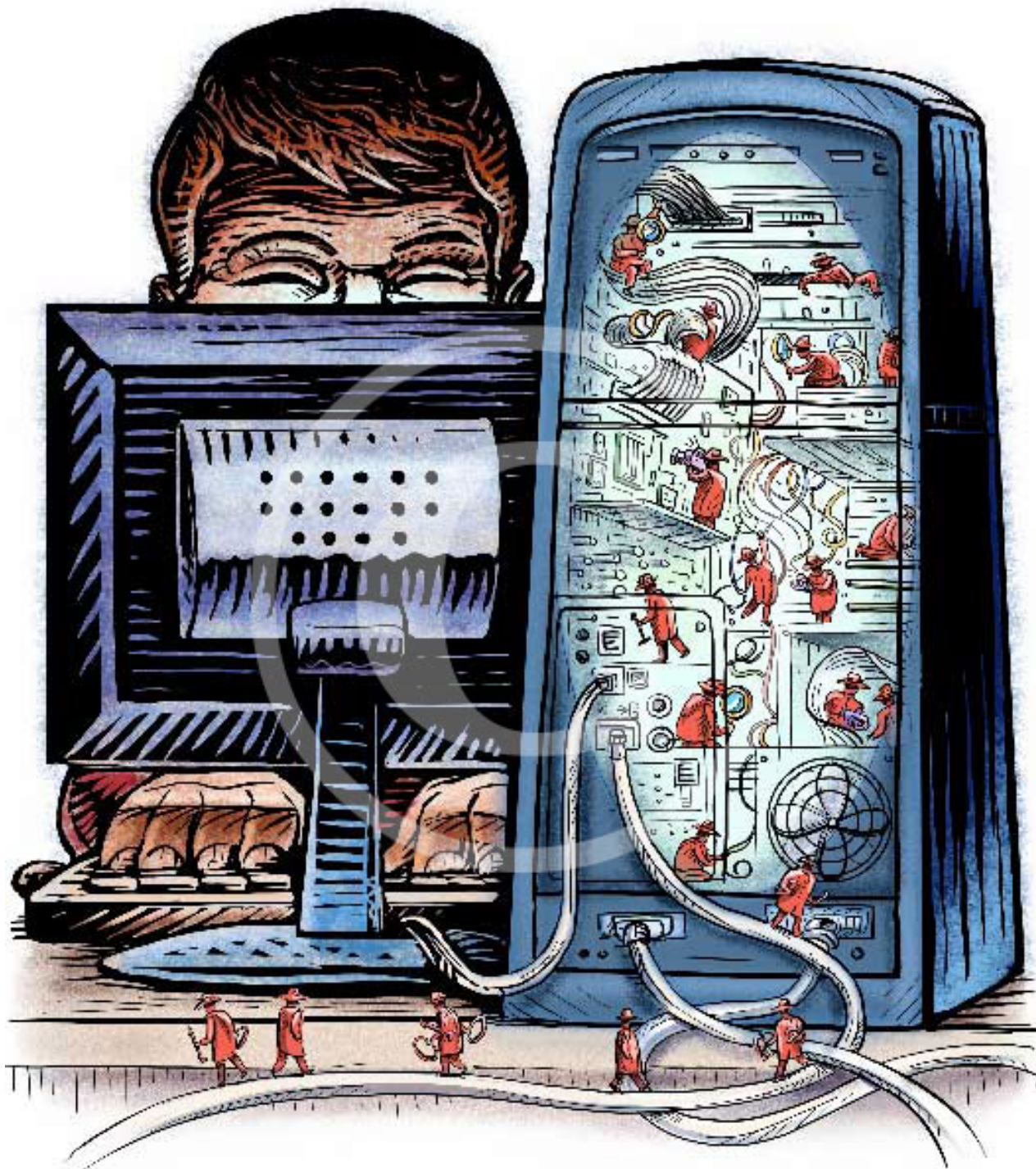
[snelson@senseient.com](mailto:snelson@senseient.com)

# Veritas and Symantec Merger

- ◆ Expected to simplify and enhance network security
- ◆ Survived antitrust review
- ◆ Stockholders must approve
- ◆ Merger targeted for end of 2<sup>nd</sup> quarter

# Hottest Issue for 2005: What Sys Admins Think



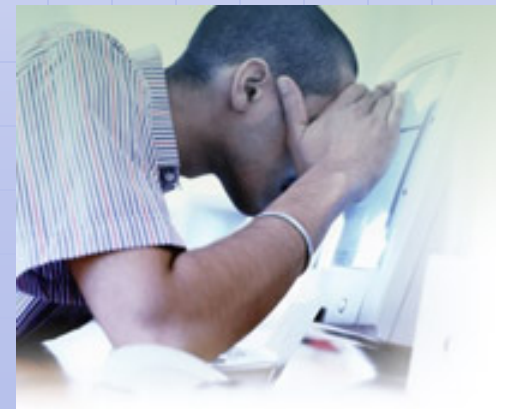


# SPYWARE

When you look at your computer, is it looking back at you?

# What is spyware?

- ◆ Definitions vary/ Generally, it is:
- ◆ Surreptitiously installed
- ◆ To monitor a user's conduct
- ◆ Transmitting data to or holding it for a third party.



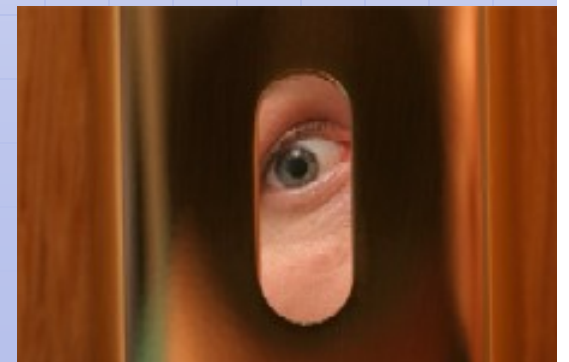
# What is spyware for?

- ◆ Monitoring husbands, wives, and lovers
- ◆ Monitoring employees
- ◆ Monitoring children
- ◆ Industrial espionage
- ◆ Marketing research/tailor ads
- ◆ Identity theft
- ◆ To make zombie machines to relay spam



# Is adware spyware?

- ◆ Generally, yes, though less pernicious
- ◆ Usual intent is research or targeting you for ads or spam
- ◆ Most adware would be outlawed by new federal law
- ◆ Adware is on almost all machines



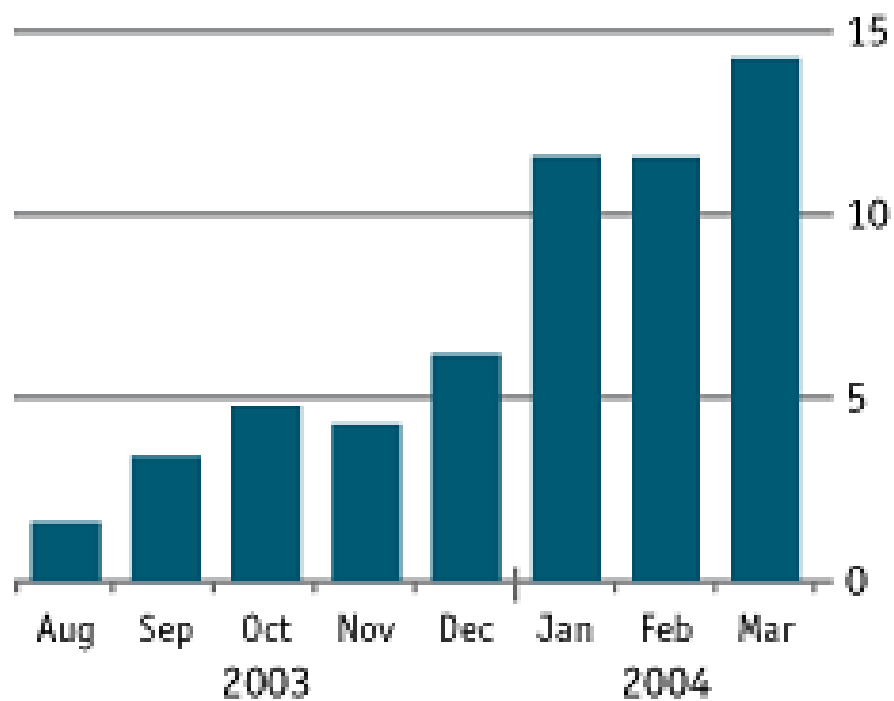
# The Grim Stats About Spyware

- ◆ 85-90% of all machines are infected
- ◆ Microsoft operating systems and software are the most vulnerable
- ◆ No one software is a “silver bullet”
- ◆ Failure to protect client data:  
“per se” malpractice?



## I spy

Spyware detections\*, m

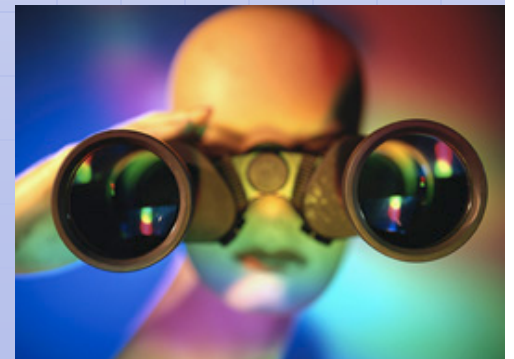


\*Based on survey of over 14m McAfee customers

Source: McAfee

# How do you get spyware?

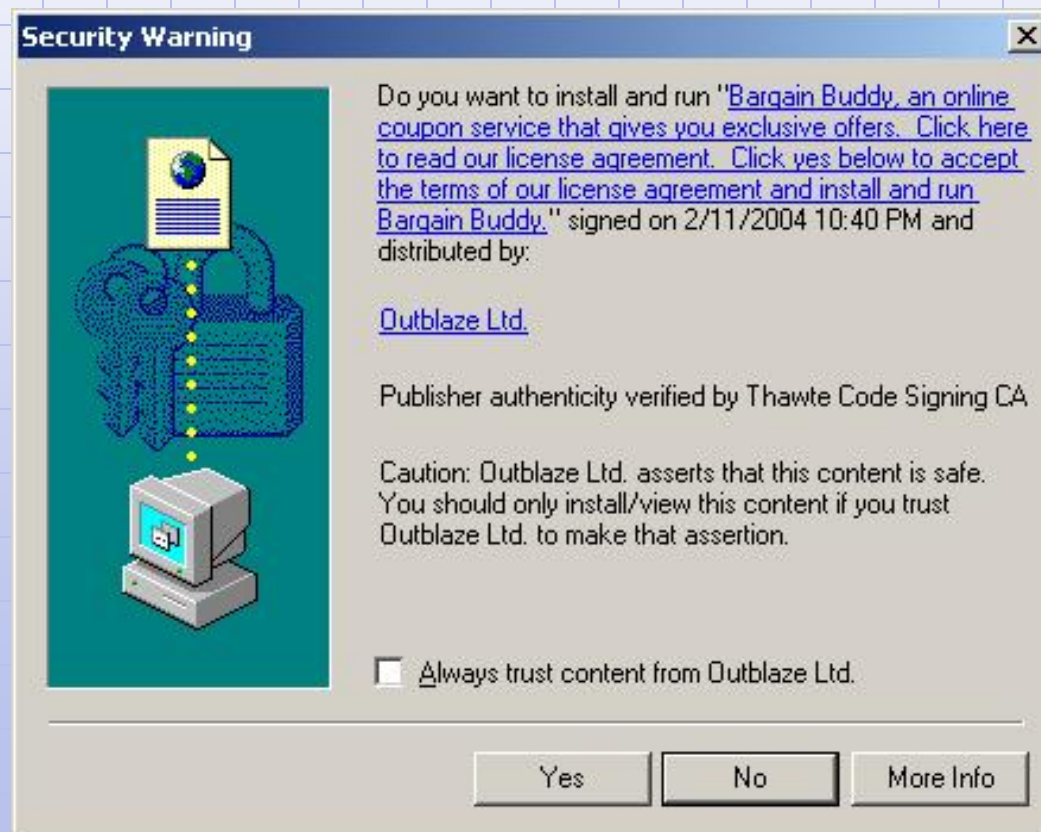
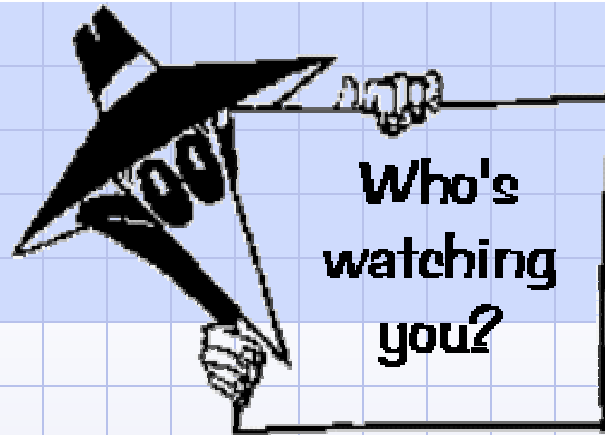
- ◆ You download something and spyware is bundled with it (most common)
- ◆ You open an e-greeting card
- ◆ You try to close or say no to a dialog box and that triggers the spyware install



# How do you get spyware?

- ◆ You go to a website and spyware is installed when you “drive by”
- ◆ Beware of Adult web sites, the worst offenders, also teen-related sites, gaming sites, screensavers, “freebies” generally
- ◆ You open an e-mail or attachment containing spyware





# Spyware/Adware

- ◆ Hotbar
- ◆ Living Waterfall
- ◆ Webshots
- ◆ Weathercast
- ◆ BargainBuddy
- ◆ SaveNow
- ◆ Claria (Gator)
- ◆ Ceres



# Spyware indicators



- ◆ Tons of pop-ups ads
- ◆ Internet home page changes
- ◆ New toolbars appear
- ◆ New icons in your system tray
- ◆ Random error messages
- ◆ New programs in the start-up group

# Spyware indicators

They're watching,  
recording, stealing.



Who is watching you?

- ◆ Machine performance suddenly sluggish
- ◆ More lock-ups and blue screens
- ◆ Significant increase in hard drive activity
- ◆ Inexplicable new behavior of machine

Monitoring Software Review 2005 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.monitoring-software-review.toptenreviews.com//index.html?ttreng=2&trkey=key+logger&OVRAW=Key%20logger&OVKEY=key%20logger&OVMTc=standard>

Google Search Web PageRank 2299 blocked AutoFill Options

Home Resources About Us Contact Us Advertising Sitemap TopTenREVIEWS.com

# MONITORING SOFTWARE REVIEW

We Do the Research So You Don't Have To™

**Concerned about what your family or employees are doing online?**

Have you ever wanted to know who is saying what in chat rooms, emails, or Instant Messaging? Have you ever wanted to know where your children are surfing and what they are seeing without the restrictions of an Internet filter? Have you ever wanted to know what your employees are spending their time doing on the Internet? This site, Monitoring Software Review, is a tool to help you better assess your needs for being able to monitor and record every activity your spouse, children, or employees do online.

Click to read "What makes a great Monitoring Software solution?"

**2005 MONITORING SOFTWARE REPORT** [EMAIL TO A FRIEND](#)

Click on a product name to read our review

■■■■ Excellent  
 ■■■□ Very Good  
 ■■■□ Good  
 ■□□□ Fair  
 □□□□ Poor

Rank	GOLD	SILVER	BRONZE	4	5	6	7	8	9	10
Overall Rating	■■■■	■■■■	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□
<b>Ratings</b>										
Feature Set	■■■■	■■■■	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□
Ease of Use	■■■■	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□
Ease of Installation/Setup	■■■■	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□
Monitoring Effectiveness	■■■■	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□
Help/Documentation	■■■■	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□	■■■□
<b>Purchase</b>										

[Spector Pro](#)  
[SpyAgent](#)  
[IamBigBrother](#)  
[eBlaster](#)  
[Golden Eye](#)  
[Guardian Monitor](#)  
[Invisible Keylogger](#)  
[007 Spy Software](#)  
[SpyBuddy](#)  
[Keylogger Pro](#)

[Definitions of Features](#)  
[What is Spyware?](#)  
[Monitors vs. Filters - Which One is Right?](#)  
[Internet Safety Tips](#)  
[Tricks Pornographers Play](#)  
[P2P Pornography— Kids Know! Do Mom/Dad?](#)  
[Pornography Statistics](#)

Advertisement

**INTERNET FILTERS**

TOP TEN INTERNET FILTER SOLUTIONS REVIEWS

[Click here](#)

<http://www.monitoring-software-review.toptenreviews.com//index.html?ttreng=2&trkey=key+logger&OVRAW=Key%20logger&OVKEY=key%20> Internet

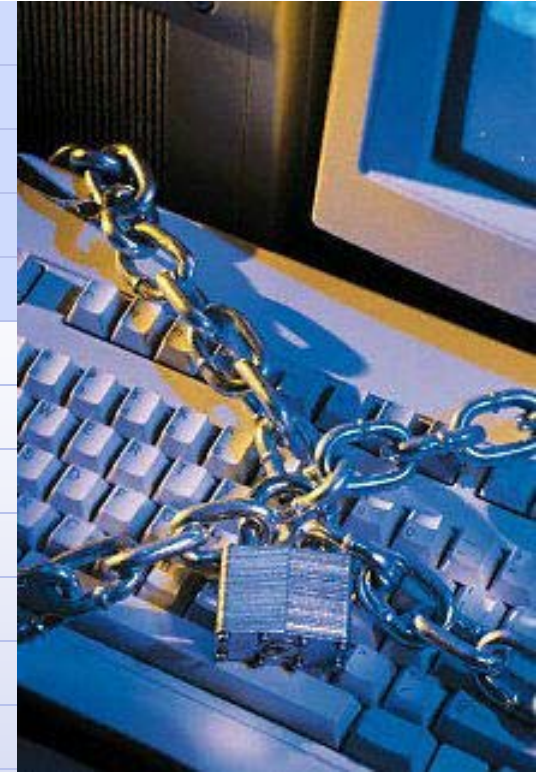
# Top reviewed spyware

- ◆ Specter Pro
- ◆ SpyAgent
- ◆ IAmBigBrother
- ◆ eBlaster
- ◆ GoldenEye



# Anti-spyware software

- ◆ There is no silver bullet
- ◆ 2-3 programs recommended
- ◆ Volatile market –
- ◆ Recommendations change every few months
- ◆ You can still get spyware
- ◆ You must scan periodically
- ◆ Safe computing is still important










## McAfee AntiSpyware



### 18 programs detected

AntiSpyware detected the following program(s) on your computer.

To remove a program from your computer, select the program and choose 'Remove'. To avoid future detections, select the program and choose 'Trust'. For details on the detected components, select a program and choose 'Details...'.

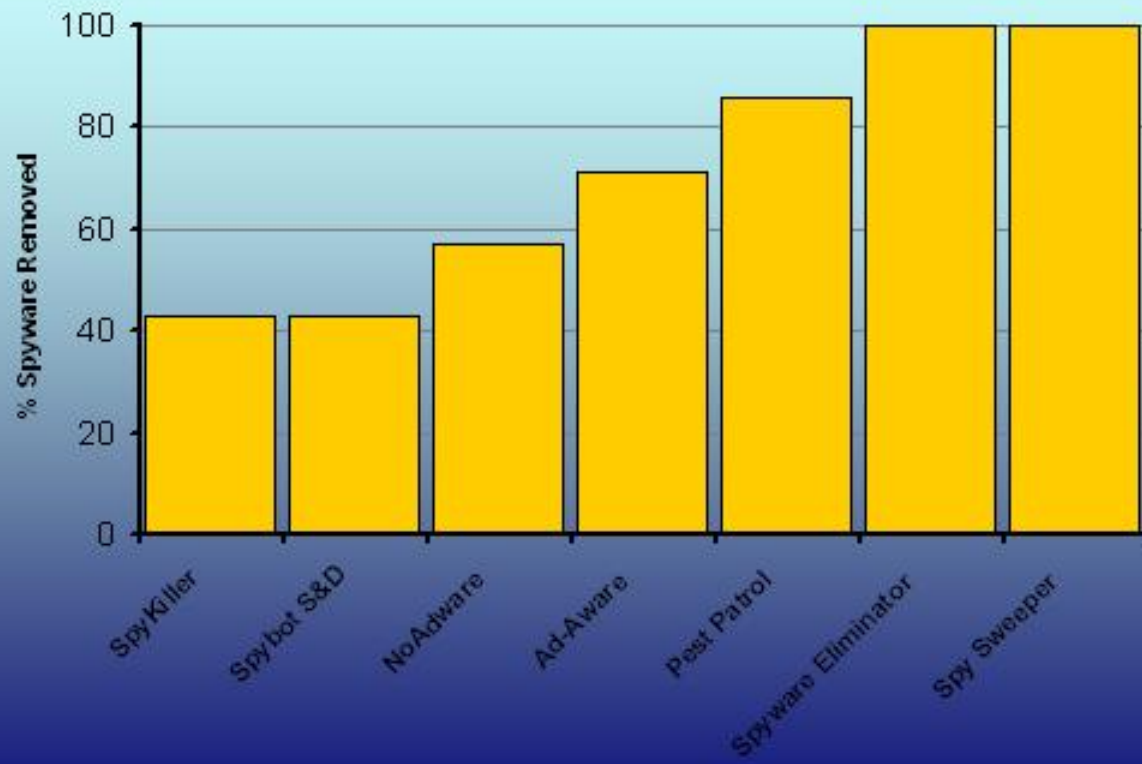
Program	Type	Status
 BargainBuddy	Adware	Detected
 CommonName	Adware	Detected
 Ezula	Adware/Web Browser Plug-in	Detected
 GAIN - Gator Advertising Inform...	Adware	Detected
 ISTBar	Adware/Web Browser Plug-in	Detected
 My Search	Adware/Web Browser Plug-in	Detected
 ...	...	...

Details... Trust Remove...

OK

Help

## Gooroo Spyware Removal Test Results August 2004



Webroot Software - Spy Sweeper, Window Washer, Pop Up Washer and more. - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print PageRank 2298 blocked AutoFill e Options

Address http://www.webroot.com/ Go Links

Google Search Web PageRank 2298 blocked AutoFill e Options

webroot SOFTWARE, INC. shopping cart | sitemap | contact us | privacy policy United States

products purchase downloads support company

home :

# Webroot Software

Privacy. Protection. Peace of mind.

Stop spyware, pop-ups, privacy intrusions, identity thieves and hackers.  
Take control of your online world with Webroot Software.

## For the Corporation



Corporate anti-spyware solution that provides comprehensive protection to eradicate spyware across the enterprise.

[Learn more about Spy Sweeper Enterprise](#)

*"Webroot's Spy Sweeper Enterprise proved itself the best anti-spyware tool in our tests, winning a Clear Choice Award."*



## For the Home



Award-winning anti-spyware software that effectively detects and safely removes spyware and adware from your PC.

*"Webroot Spy Sweeper ... a superior choice."*

-c|net download.com



[Learn more about Spy Sweeper](#)

- Free Spyware Scan
  - [Spy Audit](#)
  - Find out if you have spyware with this quick and easy scan
- Spyware Information Center
  - [Learn More about Spyware](#)
- More Products
  - [Window Washer](#)
  - [Spam Shredder](#)
  - [Pop Up Washer](#)
  - [Accelerate](#)
  - [Phish Net](#)
- Partners
  - [Join forces with Webroot to deliver proven solutions](#)

RADIO LISTENERS  
CLICK HERE



Microsoft Internet Explorer window: Spy Sweeper - Spyware Removal Software and Spyware Protection by Webroot Software

Address: http://www.webroot.com/products/spysweeper/?rc=1651

Navigation: products, purchase, downloads, support, company

United States

- Spy Sweeper
  - Spy Sweeper Enterprise
- Window Washer
  - Pop-Up Washer
  - Spam Shredder
- My Firewall Plus
  - Private Surfing
  - Phish Net
- Accelerate
  - My Personal Favorites
- MacWasher X
  - MacWasher



# webroot® Spy Sweeper

Stop spyware from monitoring your online activities and reducing PC performance.

**New in Version 3.5**

- ▶ Improved sweep time - now up to 30% faster
- ▶ Defeats CoolWebSearch, a notorious home page hijacker

**buy now!**  
Subscribe today - \$29.95



## Why you need spyware protection

<p>🕒 It's everywhere</p> <p><b>Supporting Statistics</b></p> <ul style="list-style-type: none"> <li>▶ 9 out of 10 Internet-connected PCs are infected with spyware and adware</li> <li>▶ A recent study found an average of 26 spyware and adware traces per scan.</li> </ul> <p><a href="#">Learn more about spyware</a></p>	<p>🕒 It's annoying</p> <p><b>Common Symptoms</b></p> <ul style="list-style-type: none"> <li>▶ Increased pop-up ads</li> <li>▶ Slow computer performance</li> <li>▶ Unexplained home page change</li> <li>▶ Mysterious web search results</li> </ul> <p><a href="#">Learn more about effects</a></p>	<p>🕒 It's a threat</p> <p><b>Real Consequences</b></p> <ul style="list-style-type: none"> <li>▶ Corrupt hard drive</li> <li>▶ Exposure of private information</li> <li>▶ Stolen usernames and passwords</li> <li>▶ Identity theft</li> </ul> <p><a href="#">Learn more about risks</a></p>
---	---	--



September 7, 2004  
Spy Sweeper 3.0

*"Spy Sweeper is the most effective standalone tool for detecting, removing and blocking spyware."*

[home](#) : [products](#) : [spysweeper](#) : [enterprise](#)

<p> <b>Spy Sweeper</b>            Spy Sweeper Enterprise         </p>		<p> <input type="button" value="buy now"/> </p> <p> <b>Spy Sweeper Enterprise - NEW v2.0</b> </p>
<p>           Window Washer            Pop-Up Washer            Spam Shredder         </p>		<p> <b>What is Webroot Spy Sweeper Enterprise?</b>            Webroot Spy Sweeper Enterprise is a centrally-managed, comprehensive spyware and adware solution for corporations. Using a client / server architecture, Spy Sweeper Enterprise proactively detects and removes all forms of spyware, adware and other unwanted programs within the organization. Spy Sweeper Enterprise effectively manages the corporate spyware threat by reducing security risks, minimizing support requests and reestablishing computing and network performance.         </p>
<p>           My Firewall Plus            Private Surfing            Phish Net         </p>	<p>           Webroot Spy Sweeper Enterprise provides         </p> <ul style="list-style-type: none"> <li>▶ Centralized management via the admin console</li> <li>▶ Manual or automated deployment of definition updates and product upgrades</li> <li>▶ Advanced desktop-level protection with Active Shields to prevent new infections</li> <li>▶ Customizable protection and security policies</li> <li>▶ Definition updates and sweep schedule retention for laptop and mobile users while away from network</li> <li>▶ Fully customizable reporting</li> <li>▶ Most comprehensive detection and elimination of spyware, adware and other unwanted programs available</li> </ul>	<p> <b>Evaluation and Information</b> </p> <ul style="list-style-type: none"> <li>▶ <a href="#">Download a 30-day trial</a></li> <li>▶ <a href="#">Submit an electronic information request</a></li> </ul>
<p>           Accelerate            My Personal Favorites         </p>	<p> <b>Spyware Threat to the Corporation</b>            Spyware poses a significant threat to corporations such as:         </p>	<p> <b>Sales and Support</b> </p> <p> <b>Contact Sales</b>            Telephone: 1-800-870-8102            E-mail: <a href="mailto:enterprise@webroot.com">enterprise@webroot.com</a>            Online: <a href="#">Information request form</a>            International: <a href="#">International Contacts</a> </p> <p> <b>Request Support</b>            Telephone: 1-800-870-8102            Online: <a href="#">Trouble-ticket form</a>            E-mail: <a href="mailto:esupport@webroot.com">esupport@webroot.com</a> </p>
<p>           MacWasher X            MacWasher         </p>		

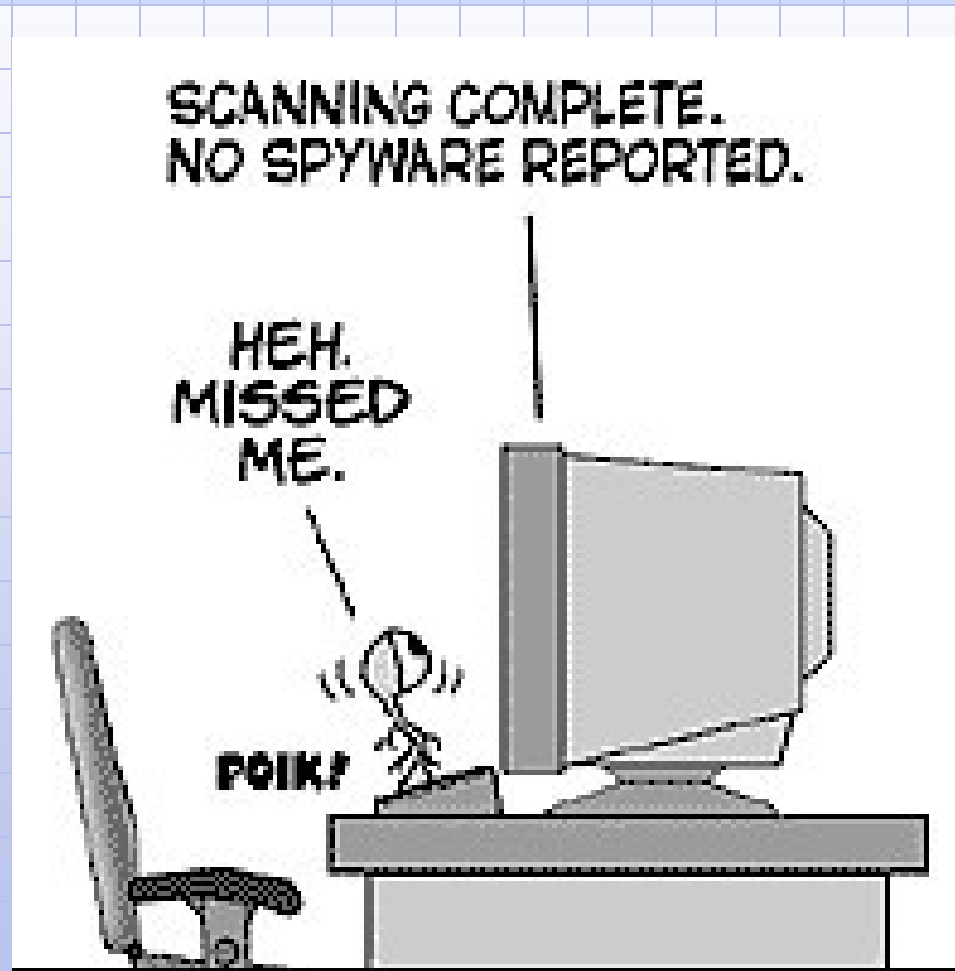
# Blocking Pop-Ups, Spyware, Adware

- ◆ Free Google toolbar to block pop-ups
- ◆ <http://toolbar.google.com>
- ◆ Ad-aware, free for personal use
- ◆ <http://www.lavasoftusa.com/software/adaware/>
- ◆ PestPatrol - \$29.95 (download)
- ◆ <http://www.pestpatrol.com>
- ◆ SpySweeper - \$29.95 (download)
- ◆ <http://www.webroot.com>

# Corporate Anti-Spyware Solutions

- ◆ Ad-Aware Professional - \$39.95
- ◆ PestPatrol Corporate - \$34.99 (2-14)
- ◆ PestPatrol Corporate - \$30.99 (15-24)
- ◆ SpySweeper Enterprise - \$31.96 (10-24)
- ◆ SpySweeper Enterprise - \$29.96 (25-99)

# Best Practice: Two or more anti-spyware packages



# Federal law

- ◆ Use of wiretap laws largely unsuccessful
- ◆ Law based on old technology
- ◆ SPY ACT overwhelming passed House in 2004, didn't get through Senate
- ◆ Securely Protect Yourself Against Cyber Trespass Act
- ◆ Passage of this law, or something similar, expected this session

# U.S. v. Councilman

- ◆ 1<sup>st</sup> Cir. June 2004
- ◆ Offered customers e-mail accounts
- ◆ Read their e-mail from Amazon.com
- ◆ Charged with violating ECPA (Electronic Communications Privacy Act)
- ◆ E-mail in RAM when copied, therefore not intercepted. In storage, not transit.
- ◆ Ruling vacated and will be heard en banc

# U.S. v. Ropp

- ◆ C.D. Cal. Oct 2004
- ◆ Hardware keystroke logger did not violate ECPA
- ◆ Transmission of keystrokes from keyboard to computer does not affect interstate commerce
- ◆ Not within statute's purview

# State Anti-spyware law

- ◆ California and Utah have laws
- ◆ Legislation pending in Michigan, Pennsylvania, New York, and Iowa
- ◆ VA has computer trespass and computer privacy laws that apply
- ◆ Ditto for Kansas, Tennessee, Rhode Island, Washington and North Carolina

# Software monitoring employees

- ◆ Legal everywhere
- ◆ Connecticut and Delaware require that employees be given notice before e-mail or Net access monitored

Want to know if there's  
spyware on your computer?

Take the free systems audit at:

[www.webroot.com](http://www.webroot.com)

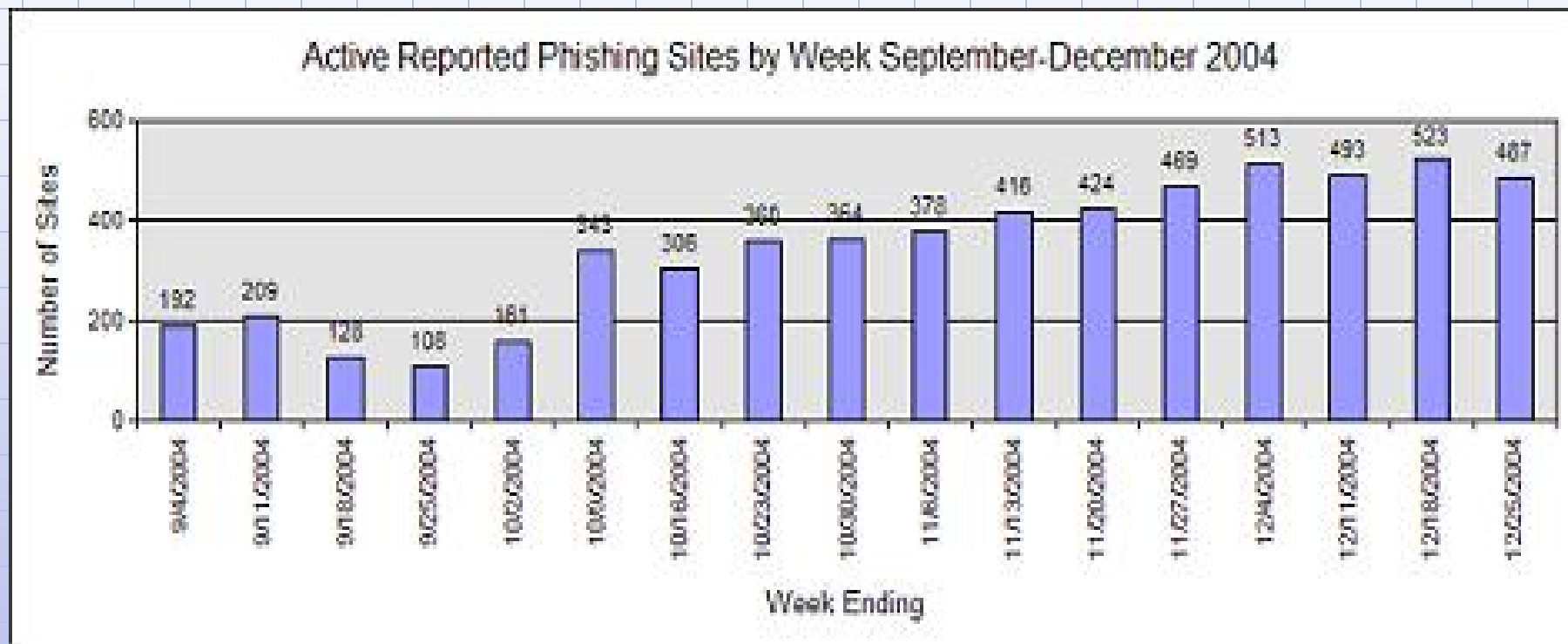
Or the corporate audit at:

[http://www.webrootdisp.net/entaudit/  
start.php](http://www.webrootdisp.net/entaudit/start.php)

# Phishing

- ◆ Hackers commonly replace “f” with “ph”
- ◆ They fish for financial info and credit cards in the sea of Internet users
- ◆ “Phishing” is also a tribute to “phreaking” , the original hacker’s term for hacking, used by “phone phreakers” hacking phone companies with blue boxes

# Anti-Phishing Working Group



Anti-Phishing Working Group: Phishing Archive - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address [http://www.antiphishing.org/phishing\\_archive.html](http://www.antiphishing.org/phishing_archive.html)

Google phishing Search Web PageRank 2300 blocked AutoFill Options phishing

# Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud [register](#)

**APWG**





[report phishing - click here](#)

## Phishing Archive

Below are examples of phishing attacks submitted to antiphishing.org:

Date	Company	E-mail
08-Feb-05	KeyBank	'SECURE YOUR ACCOUNT NOW'
02-Feb-05	Huntington Bank	'Huntington - Urgent Security Notification'
31-Jan-05	Amazon.com	'Account Verification Notice'
27-Jan-05	MSN	'Warning Message'
25-Jan-05	M&I Marshall & Ilsley Bank	'Banking Online customer Report'
21-Jan-05	Washington Mutual Bank	'Re-Submit: wamu.com Urgent requirementvu'
19-Jan-05	TCF Bank	'TCF express checking card alert'
14-Jan-05	Paypal	'New email address added to your account'
12-Jan-05	Citizens Bank	'Important Online Banking Alert'
11-Jan-05	eBay	'Account Verification'
10-Jan-05	AOL	'You've Got (2) Pictures@AOL.com'
07-Jan-05	KeyBank	'Keybank Internet Banking Account Suspension Notice!'
23-Dec-04	AOL	'Verify your account'
22-Dec-04	U.S. Bank	'Customer service'
21-Dec-04	VISA	'Notice from VISA'
04-Dec-04	eBay	'Update or verify your account informations'
03-Dec-04	America Online	'Notice : Your account will be suspended !'
02-Dec-04	Earthlink	'Earthlink payment is cancelled'
30-Nov-04	Suntrust	'Security Alert on Microsoft Internet Explorer'
29-Nov-04	Washington Mutual	'WARNING: CONFIRM YOUR ONLINE BANKING ACCOUNT'
24-Nov-04	Bank One	'Bank One security upgrade'
19-Nov-04	eBay	'Account Suspension Notice - Section 9'
17-Nov-04	Citibank	'Your online activity confirmation'
16-Nov-04	Suntrust	'Internet Banking with Bill Pay Fees Waived'
15-Nov-04	People's Bank	'New Mail from People'
10-Nov-04	Citibank	'Citibank Alert Service'

**RESEARCH PARTNER:**

Internet



Dear Amazon user,

During our regular update and verification of the accounts, we couldn't verify your account information. Either your information has changed or it is incomplete.

Please update and verify your information below.

[Sign in using our secure server](#)

Sincerely,  
Amazon Security Department

---

#### Updating Subscriptions and Communication Preferences

You can access your New for You subscriptions, Special Occasion Reminders, Available to order notifications, and other communication preferences directly through [Your Account](#).

When logging in, remember to enter the e-mail address and password currently associated with your account. If you do not have a customer account, we'll ask you to create one first. Simply enter your e-mail address, indicate that you are a new customer, and click the Sign in using our secure server button. On the next page, we'll ask you to enter your name and select a password.

#### Forgot Your Password?

We cannot tell you your current password, but we can certainly help you acquire a new one by sending a personalized link to your e-mail address. This way, you can securely change your password to whatever you want. If you visit us from a computer you have not used before, we will ask for complete verification of your account information before proceeding with the password change. [Reset your password now.](#)

#### Changing Your 1-Click Settings

Your 1-Click settings allow you to ship all of your 1-Click orders efficiently in the way you decide is best. You are always welcome to change the credit card account, shipping address, and shipment method associated with your 1-Click settings. Any changes you make, however, will affect only future 1-Click orders. If you want to change the particulars of an order you've already placed, visit [Your Account](#).

# Fighting phishing

- ◆ Don't click on pop-up boxes or e-mail requesting personal info – legitimate inquiries won't be made this way
- ◆ Keep anti-virus and anti-spyware software up to date
- ◆ Don't send financial/personal info via e-mail
- ◆ Do Net orders only through secure sites with known vendors

# The Can-Spam Act

- ◆ a/k/a “The I Can Spam” Act
- ◆ Compliance under 3%
- ◆ Growth exceeds 3%
- ◆ No gain
- ◆ Best current solutions
  - Blacklists, filters and whitelists
- ◆ Coming solutions
  - Caller ID for e-mail
  - “Black Penny” day

# Voice Communications

- ◆ Voice Mail
- ◆ Answer Machines
- ◆ PBX Routing
- ◆ VoIP

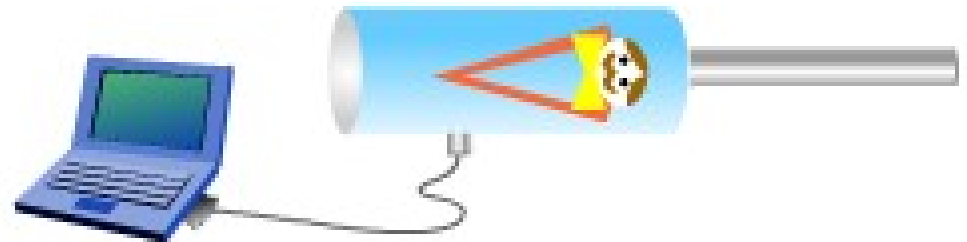
# VoIP

- ◆ Secure Logs
- ◆ Do Not Use Shared Media Devices
- ◆ Periodic Audits
- ◆ Encrypt
- ◆ Network Redundancy
- ◆ 911 Services
- ◆ VoIP Aware Firewalls

# Wireless Networks

- ◆ Default Values
- ◆ Drive By
- ◆ War Chalking
- ◆ Wi-Fi Wardriving
- ◆ RSA Security: 63% of surveyed networks are left at default values
- ◆ Used by Spammers

# Wi-Fi Wardriving



Using a Pringles® Can Antenna to extend wireless range of a WiFi network

# Wireless APs



# Linksys Wireless

◆ <http://www.freenetworks.org/moin/index.cgi/SSIDDefaults>

LINKSYS Product Families:

LINKSYS WAP-11 802.11 DS AP, reportedly supports repeater mode

Default SSID: linksys Default Channel: 6 Default WEP key one: 10 11 12 13 14 15 Default WEP key two: 20 21 22 23 24 25 Default WEP key three: 30 31 32 33 34 35 Default WEP key four: 40 41 42 43 44 45

Extended WEP key pattern: 10 11 12 13 14 15 16 17 18 1a 1b 1c ...

20 21 22 23 24 25 26 27 28 2a 2b 2c ... 30 31 32 ... until the input fields are full

Default SNMP Write: No Authentication

# Metadata

◆ Data About Data

◆ Word

◆ WordPerfect

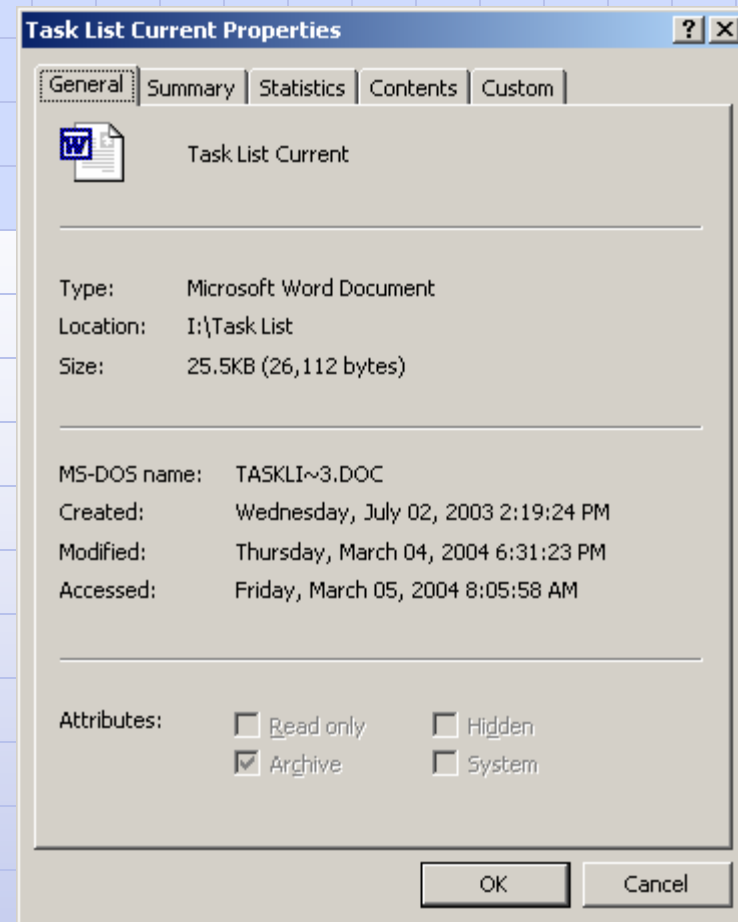
◆ Excel

◆ PowerPoint

◆ Scrubbers

- Metadata Assistant

- RFT



**Task List Current Properties** [?] [X]

General | Summary | **Statistics** | Contents | Custom

Created: Monday, November 10, 2003 8:32:00 AM  
Modified: Thursday, March 04, 2004 6:31:23 PM  
Accessed: Friday, March 05, 2004 8:05:58 AM  
Printed: Thursday, March 04, 2004 6:27:00 PM

---

Last saved by: Sharon Nelson  
Revision number: 571  
Total editing time: 23173 Minutes

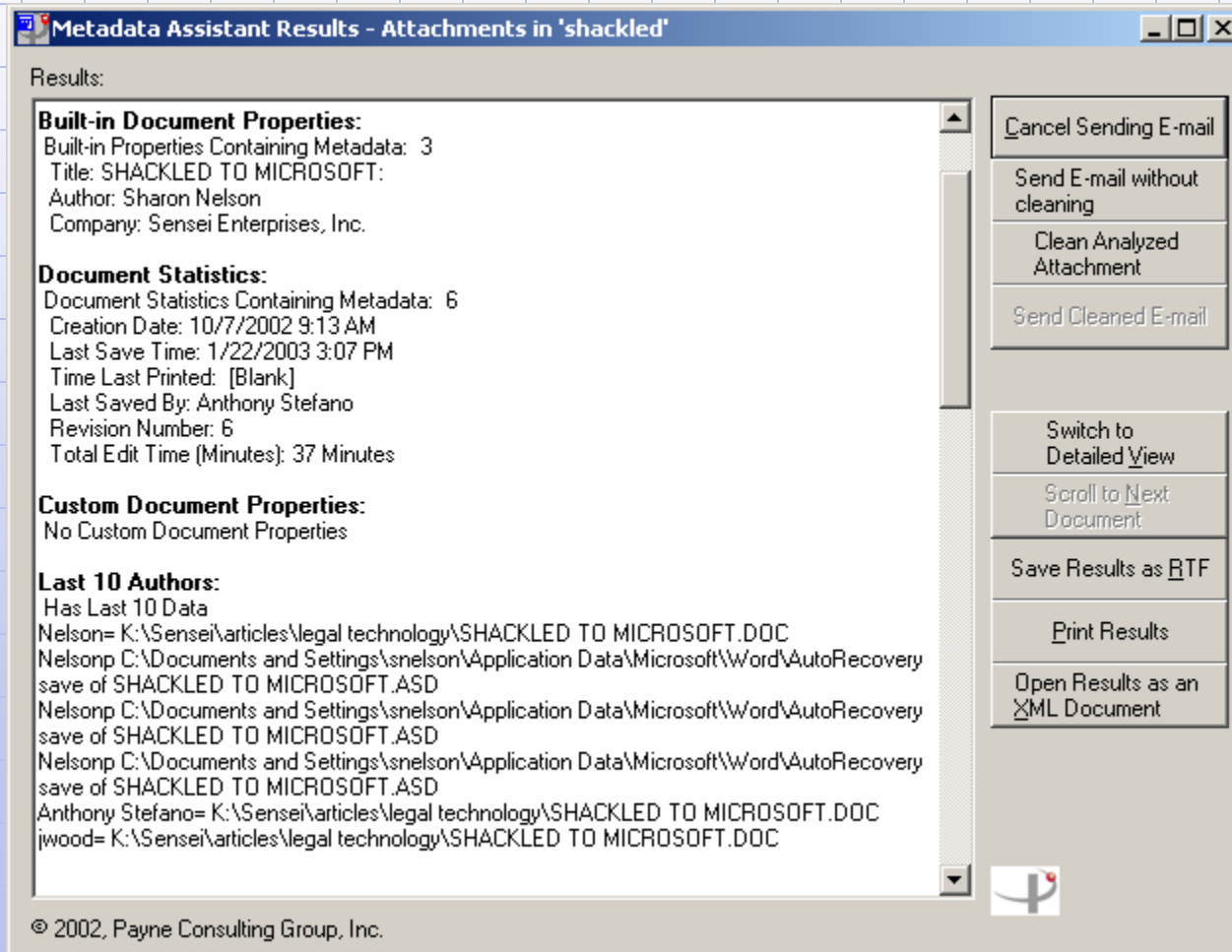
---

Statistics:

Statistic name	Value
Pages:	1
Paragraphs:	83
Lines:	94
Words:	361
Characters:	1915
Characters (with spaces):	2220

OK Cancel

# Metadata Assistant



Metadata Assistant Results - Attachments in 'shackled'

Results:

**Built-in Document Properties:**  
Built-in Properties Containing Metadata: 3  
Title: SHACKLED TO MICROSOFT:  
Author: Sharon Nelson  
Company: Sensei Enterprises, Inc.

**Document Statistics:**  
Document Statistics Containing Metadata: 6  
Creation Date: 10/7/2002 9:13 AM  
Last Save Time: 1/22/2003 3:07 PM  
Time Last Printed: [Blank]  
Last Saved By: Anthony Stefano  
Revision Number: 6  
Total Edit Time (Minutes): 37 Minutes

**Custom Document Properties:**  
No Custom Document Properties

**Last 10 Authors:**  
Has Last 10 Data  
Nelson= K:\Sensei\articles\legal technology\SHACKLED TO MICROSOFT.DOC  
Nelsonp C:\Documents and Settings\snelson\Application Data\Microsoft\Word\AutoRecovery  
save of SHACKLED TO MICROSOFT.ASD  
Nelsonp C:\Documents and Settings\snelson\Application Data\Microsoft\Word\AutoRecovery  
save of SHACKLED TO MICROSOFT.ASD  
Nelsonp C:\Documents and Settings\snelson\Application Data\Microsoft\Word\AutoRecovery  
save of SHACKLED TO MICROSOFT.ASD  
Anthony Stefano= K:\Sensei\articles\legal technology\SHACKLED TO MICROSOFT.DOC  
jwood= K:\Sensei\articles\legal technology\SHACKLED TO MICROSOFT.DOC

© 2002, Payne Consulting Group, Inc.

Buttons on the right side of the window:

- Cancel Sending E-mail
- Send E-mail without cleaning
- Clean Analyzed Attachment
- Send Cleaned E-mail
- Switch to Detailed View
- Scroll to Next Document
- Save Results as RTF
- Print Results
- Open Results as an XML Document

CERT Coordination Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Copy Paste

Address <http://www.cert.org/> Go Links

Google spyware Search Web PageRank 2247 blocked AutoFill Options spyware

Carnegie Mellon Software Engineering Institute

**CERT® Coordination Center**

Home Site Index Search Contact FAQ

vulnerabilities, incidents & fixes | security practices & evaluations | survivability research & analysis | training & education

Options search  GO customize...

**Vulnerabilities, Incidents & Fixes**

**Security Practices & Evaluations**

**Survivability Research & Analysis**

**Training & Education**

**Help Protect the Future of Technology**

Employment opportunities available in Pittsburgh and DC

Established in 1988, the CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the [Software Engineering Institute](#), a federally funded research and development center operated by [Carnegie Mellon University](#).

**What's New** more

**January 27, 2005**  
[Preliminary System Dynamics Maps of the Insider Cyber-threat Problem](#)  
 This paper (pdf) was published in the Proceedings of the 22nd International Conference of the System Dynamics Society, July 2004

**January 24, 2005**  
[CERT/CC Statistics](#)  
 The statistics have been updated to include information from the last quarter of 2004.

**January 12, 2005**  
[Resources for enterprises](#)  
 Significant information pertaining to insider threats, Enterprise Security Management (ESM), and Mission Assurance Analysis Protocol (MAAP) has been added to the [Security Practices and Evaluations](#) section of the web site.

**Related**

[CERT Contact Information](#)

[CERT Statistics](#)

[Meet the CERT/CC](#)

[CERT/CC Overview and Intruder Trends](#)

[CERT Annual Reports](#)

[Publications by CERT/CC Staff](#)

[Presentations by CERT/CC Staff](#)

**React to Today's Problems** more

**Advisories & Incident Notes** all  
[advisories](#) | [incident notes](#)

**US-CERT Technical Cyber Security Alert**  
 TA05-026A  
[Multiple Denial of Service Vulnerabilities in Cisco IOS](#)

**US-CERT Technical Cyber Security Alert**  
 TA05-012B  
[Microsoft Windows HTML Help ActiveX Control Cross-Domain Vulnerability](#)

**US-CERT Technical Cyber Security Alert**  
 TA05-012A  
[Multiple Vulnerabilities in Microsoft Windows Icon and Cursor Processing](#)

**US-CERT Vulnerability Notes** [US-CERT vulnerability notes database](#)

**New and Notable Vulnerabilities:**

- [LDAP buffer overflow](#)
- [Microsoft Windows LoadImage API integer overflow](#)
- [IE DHTML Edit Control cross-domain vulnerability](#)
- [Windows XP SP2 HTML Help Local Machine Zone Lockdown bypass](#)

**US-CERT Current Activity** [Latest Version:](#)  
 Mon Feb 7 16:53:21 EST 2005

Internet

# Incidents Reported

**1988-**

**1989**

Year	198	198
Incident	6	132

s

**1990-**

**1999**

Year	199	199	199	199	199	1995	199	199	199	199
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,174	3,734	9,899

**2000-**

**2003**

Year	2000	2001	2002	2003
Incident	21,756	52,658	82,094	137,529

s

6

8

4

9