



# **Best Practices For Dealing With SpyWare/MalWare**

Service is the Solution



# What Is It?

## ▶ Spyware –

- Programs that secretly gather information about the user and relay it to advertisers or other interested parties.
  - Tracking cookies
  - Keyloggers
  - Programs that actively monitor and report on Internet surfing habits.

## ▶ Malware –

- Programs that perform malicious actions against the user or other parties.
  - Trojans/backdoors
  - Ad servers
  - DoS bots
  - Spam bots

Common Thread: Financial Gain!



# Symptoms of Infection

- ▶ Unusual pop-ups
  - Not associated with the site you're visiting
  - Often of an adult nature
  - Pop-ups when you're not even browsing the web
- ▶ Additional browser toolbars
  - Hot Bar
  - New Search Bars
- ▶ Settings are changed unexpectedly
  - Home page
  - Search page
  - Often can't be changed or revert back on restart
- ▶ Computer is sluggish or unusually slow
  - Increase in program crashes



# How Do I Get It?

- ▶ Piggyback Software Installation
  - Software installed along with a desired application
    - Grokster
      - 398 page license agreement, installs other programs and makes major changes, 134 "critical detections"
    - Comet Cursor
      - Toolbar, search bar, tracks usage
    - HotBar
      - tracks usage
- ▶ Drive-by Downloads
  - Software installed while browsing; possibly without user knowledge, often using ActiveX
    - 007 Arcade Games
    - Innovators of Wrestling
      - 27 other programs installed or major changes made, 153 "critical detections"
    - Tracking Cookies
- ▶ Exploitation of software vulnerability or 'feature'
  - Browser or OS bugs
  - Application bugs
    - JPEG library allowed for code execution just by looking at a picture.
  - Unusual use of application feature
    - Windows Media Digital Rights Management hole



# Statistics

It's a hostile world out there.

- ▶ Average Survival Time: 23 minutes.<sup>1</sup>
- ▶ 80% of home users have spyware or adware programs on their computer.<sup>2</sup>
- ▶ The average infected user has 93 spyware/adware components on their computer.<sup>2</sup>
- ▶ 89% didn't know the programs were on their computer.<sup>2</sup>
- ▶ 95% said they didn't give permission for the programs to be installed.<sup>2</sup>
- ▶ Nearly 92% of enterprises acknowledge a serious spyware problem.<sup>3</sup>

1. Source: dshield.org 3/30/2005

2. Source: National Cyber Security Alliance/AOL Study, Oct. 2004

3. Source: Web@Work, 2004



# How Can I Prevent It?

- ▶ There's no guaranteed solution.
- ▶ XP SP2 + built in firewall
- ▶ Maintain up to date anti-virus software.
- ▶ Use Windows Update regularly.
- ▶ Use a popup blocker like Google toolbar or one that's browser based.
- ▶ Use Spyware Guard and IE-SPYAD to add known spyware sites to I.E Restricted Sites list (8900+ sites).
  - Promising but questionable effectiveness
  - They do block known bad ActiveX controls which is good.
- ▶ Use Group Policies to lock down desktops and prevent installation of programs.
- ▶ Use an alternate browser like Firefox, Mozilla or Opera. They don't allow ActiveX and are often more secure than I.E.
  - Servers – I.E./Firefox
  - Teachers I.E./Firefox
  - Students: Firefox
- ▶ Block ActiveX controls. Tools, Internet Options, Security, Custom Level: set all ActiveX options to Prompt or Disable.
- ▶ Disable 'third party cookies'. Tools, Internet Options, Privacy, Advanced. Set 'First Party Cookies: Accept', 'Third Party Cookies: Block'



# How Can I Prevent It

- ▶ Keep browser/email usage to a minimum on servers.
- ▶ Teach safe browsing habits:
  - If unsure of a dialog don't say no, close the window with 'X'.
  - Create and enforce an Internet Acceptable Use Policy.
  - Have your teachers monitor students surfing; walk around, be visible.
  - Encourage students and teachers to ask if they have questions.
- ▶ If possible, use a non-Microsoft OS (labs or libraries for example).
  - K12LTSP or K12Linux
  - Knoppix (LiveCD)
  - Mandrake Move (LiveCD)
  - Linux
- ▶ If re-installing Windows, do so on a secure network with a slipstreamed CD (latest patches)
  - Use local SUS or update server
- ▶ Use DeepFreeze or similar program to quickly restore machine to original configuration.
- ▶ Firewalls and IDS provide limited protection because they operate at the network level; spyware is application level.