

Spyware and Adware – What's in Your Computer?

Part 1

Disclaimer

- This course is designed for **Windows** operating system clients
- This course is not relevant for Mac OS clients

Objectives

- Definitions
- Purpose
- How Do You Know?
- Pop-Ups
- Peer-to-peer Network Sharing
- Installation Methods
- Prevention
- Resources

“State of Spyware” Report

- Nine out of 10 PCs connected to the Internet are infected with spyware or adware
- 88% of consumer computers had some form of unwanted program (Trojan, system monitor, cookie or adware)
- 87% of corporate PCs had some form of spyware

Definition - Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.

Spyware – What Is Its Purpose?

- Tracks your computer usage
- Collects personal information
- Reports on web sites visited
 - Builds a marketing profile for the user to sell “targeted” advertisements
 - Results in targeted e-mails sent to the user
- Installs components that affect your system performance or take up bandwidth
- Violates your privacy

Symptoms of Spyware – How Do You Know if You Have It?

- Computer crashes
- Home page has changed
- New toolbar installed automatically
- Browser settings have changed
- Large number of pop-up ads display – even when not in the browser
- Decreased system performance
- Something “new” on system
- Unidentified toll charges on phone bill

Spyware Example: Bonzi Buddy



Spyware Example: Bonzi Buddy

- Spyware program targeted at children
 - Children often install the software – looks like a fun toy
- Computer speed, privacy, ease of use all adversely affected by installing

Note: The Bonzi Buddy site was discontinued in 2004

Definition - Adware

Software that goes beyond the reasonable advertising that one might expect from freeware or shareware.

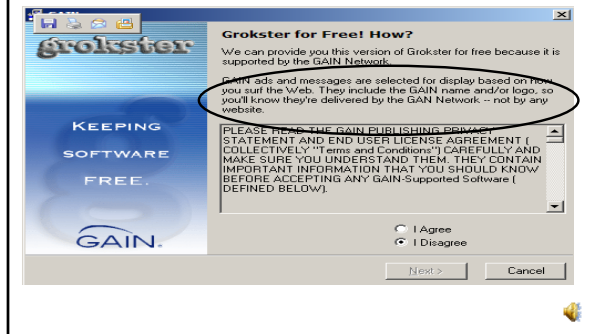
Adware – What Is Its Purpose?

- Advertising-supported software
- Frequently “free” software comes with adware
 - Alternative to paying registration fees
 - Bombarded with advertisement pop-ups
- Runs in the background
 - Acts as a “mole”
 - Information is logged and used to create a user profile

End User License Agreement

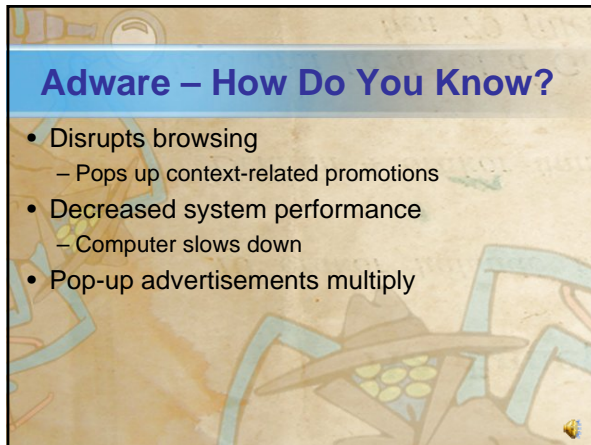
- EULA = End User License agreement
- Read the license agreement!
- Examples:
 - Claria's Gator EULA when installing as part of a bundle with Kazaa:
 - 56 on-screen pages
 - 5,541 words
 - WhenU (Bear Share)
 - 45 on-screen pages

Grokster – EULA First Page



Adware – How Do You Know?

- Disrupts browsing
 - Pops up context-related promotions
- Decreased system performance
 - Computer slows down
- Pop-up advertisements multiply





ShopAtHome - Adware Example

- Can silently download, install and run new software
 - Includes updates of its software
- Monitors Internet usage and displays pop-up advertisements
- Modifies browser settings

Pop-Ups

- Ads – want to sell something
- Clicking anywhere on pop-up may trigger installation of spyware
 - Program downloaded without your consent or knowledge

Pop-Ups



Pop-Up Example



Peer-to-Peer Networking

- File-sharing software available freely on the Internet
- Allows computers to connect with each other and directly access files from one another's hard drive
 - Exchange files from one another
 - Allows for sharing of music files **as well as personal files**

File Sharing Scenario 1

- Mary downloads free version of file-sharing program (i.e. Kazaa, Limewire, Morpheus)
 - Mary uses her new file-sharing program to download music files
 - The music file that Mary downloads also contains key logging spyware which installs itself on her computer and captures her every keystroke

File Sharing Scenario 2

- John unknowingly saves a copy of his recent loan application to the "shared folder" on his computer
 - Now, John's personal information is available to anyone on the file-sharing network via his loan application
 - Once the information has been exposed, it's difficult to know how many people have accessed it

Peer-to-Peer Networking Risks identified by US-CERT

- Installation of malicious code
- Exposure of sensitive/personal information
- Susceptibility to attack
- Denial of service
- Prosecution

Popular Adware/Spyware Programs

- Weatherbug
- Gator
- iMesh
- BargainBuddy
- eDonkey
- Morpheus
- Grokster
- Comet Cursor
- Kazaa (paid version free of adware)
- Limewire (paid version free of adware)
- Complete list:
http://www.spywareguide.com/creator_list_full.php

Record Course Completion

- Click the following link to have this course added to your training record:

<http://survey.uakron.edu:2929/2wV3GFE/Link.html>

NOTE: Failure to click the link and complete the necessary information will result in your course completion being unrecorded!

Part 1 Conclusion

To advance to Part 2 click the link below:

<http://video.uakron.edu:82/train/Security/Spyware/SpywarePart2.htm>

Questions?
pstrain@uakron.edu
