Advanced Network Security

Spyware

Amir Mahdi Sadeghzadeh, Ph.D.

Most slides have been adapted from Mehdi Kharrazi, CE40-817, Sharif University of Technology, 2015

What is Spyware?

- Spyware is a broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of the machine's user

Threats

- As of 2006, spyware has become one of the leading security threats to computer systems running Microsoft Windows operating-systems

Threats

- Webroot Software, makers of Spy Sweeper, said that 9 out of 10 computers connected to the internet are infected and 86% of those surveyed suffered a monetary loss due to spyware

Types of Spyware

- Adware
- Collectware
- Tracking Cookies
- Keyloggers
- Browser Hijackers

Adware

- Advertising-supported software, any software package which automatically displays, plays or downloads advertising material to a computer after the software is installed on it or while the application is being used

- Types of adware
  - Legitimate adware
    - Legitimate adware is downloaded with the user's express consent. Users download this form of adware knowingly and will usually get something (discount or free software) in return.
  - Malicious adware
    - Deceptive or abusive adware makes it difficult for the user to refuse consent or uses deceptive means to gain the user's consent.

Adware

- Adware is not always spyware
- It is spyware when information about the user's activity is tracked, reported, and often re-sold, usually without the knowledge or consent of the user

Adware

- Also considered shareware
  - Different from other types of shareware because it is primarily advertising-supported
- User's may have the option to pay for a "registered" or "licensed" copy of the software to do away with advertisements
- Example: WeatherBug

Collectware

- Tracks web surfing habits and transmits statistical data to the hacker
- The information later gets sold to advertisement companies

Tracking Cookies

- Tracking cookies are cookies that are either set on a user's web browser by the website they are on or by a third party.
  - track the user's online behavior i.e. collect their data
    - clicks, shopping preferences, device specifications, location, and search history.
- targeted advertising
- First-party tracking cookies
  - used to track the visitor's surfing behavior on the website, to remember user activity over multiple visits etc.
- Third-party tracking cookies
  - created by an external server via a piece of code loaded on the website you are browsing.
  - Third-party cookies are usually created by advertisers etc.

Keyloggers

- Keystroke logging is a diagnostic used in software development that captures the user's keystrokes
- Measure employee productivity and certain clerical tasks
- Have been used in espionage and can obtain passwords, encryption keys or account numbers

Browser Hijackers

- Software that tends to hijack the computer operator's browser's web connections to do their own purposes
- Often changes the user's homepage or when doing a search in Google, will hijack your search request and send it to another search engine

How Computers Become Infected with Spyware

The User Installs it

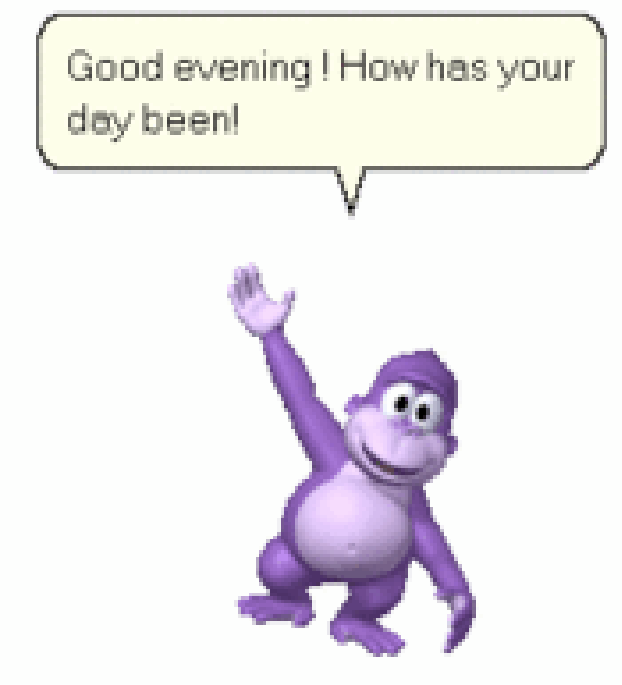
- Piggybacking
  - refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.
- The spyware is included with wanted software, most commonly P2P applications.
- Free programs such as Kazaa bundle spyware with their software
- They usually disclose this in their End User License Agreement (EULA)
  - Have you ever read an EULA?

The User Installs it (con't)

- Smuggle spyware in, disguised as useful software
- Examples:
  - FunWebProducts: supposed to install funny icons, but its main purpose is to trick users into installing tons of spyware

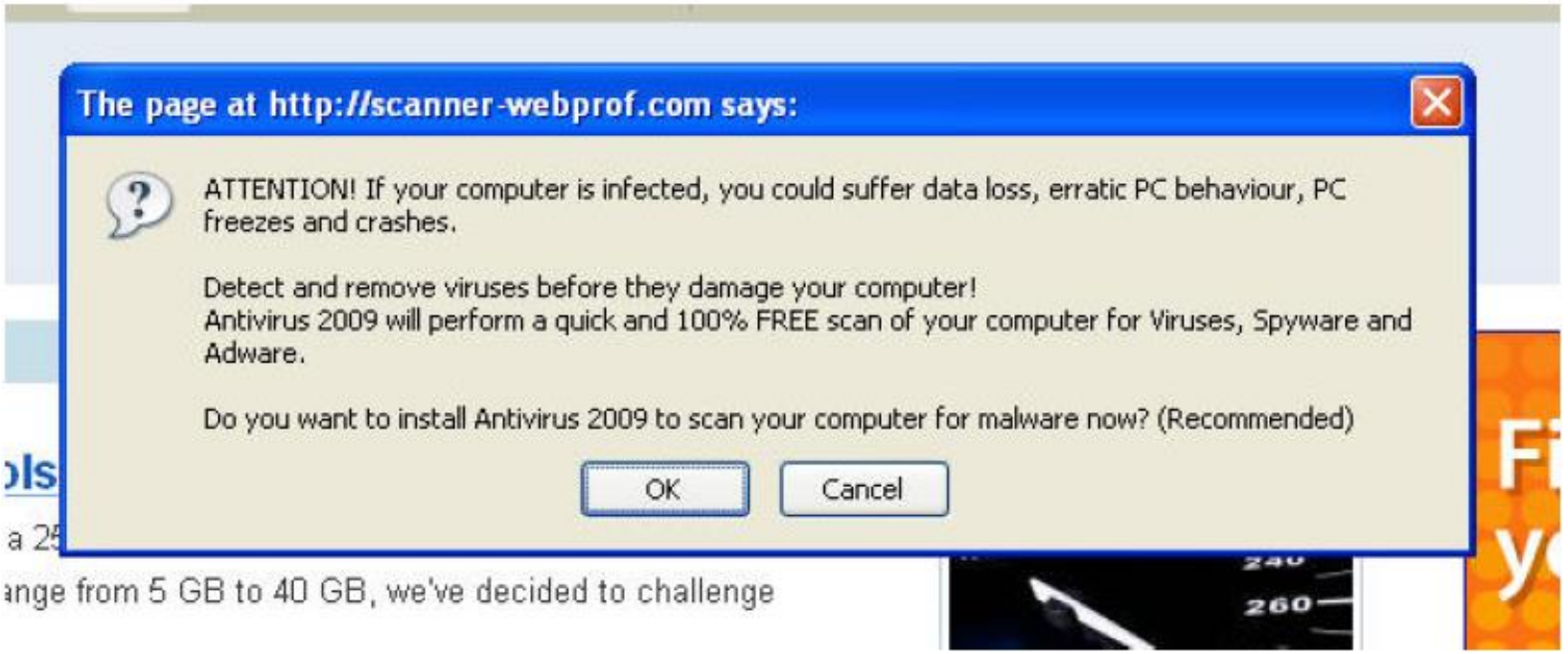
Examples

- Bonzi Buddy: targets children. Kids are enticed to download this “online sidekick”
- Collects users information, resets homepages without clients permission, and displays pop-ups



Pop-ups

- Pop-ups disguised as windows error messages trap users into clicking on a button inside the pop-up. This triggers an automatic download without the users knowledge or consent

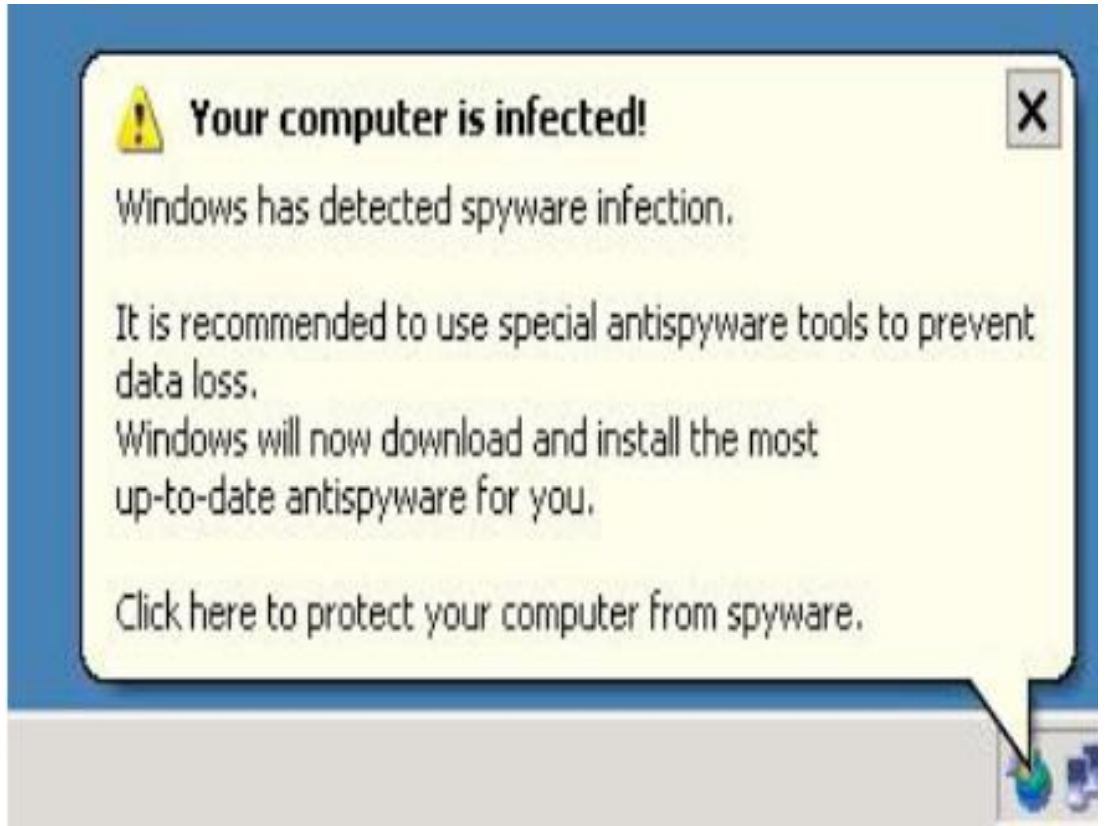


Drive-by downloads

- Occur when spyware automatically downloads through security holes in a Web browser
- Malicious websites will download spyware as soon as someone navigates to it
- These sites will either bait search engines or have domain names that are misspellings of popular websites

Rogue anti-virus software

- This software actually installs spyware
- Antivirus Gold Family - variants include:
  - Adware Delete
  - SpyAxe
  - Antivirus Gold
  - SpywareStrike



Can be delivered by a virus or worm

- A worm can help a criminal to remotely gain control in installing spyware and more malware
- Worms or viruses may lower security settings on the computer allowing a “backdoor” for spyware to enter

Legal Issues

- Unauthorized access to a computer is illegal under the United States Computer Fraud and Abuse Act.
- Companies distributing spyware claim that they have authorization because of their EULAs

Legal Issues

- Federal Trade Commission (FTC) vs. Seismic Entertainment Productions, Inc., SmartBot, Inc., and Sanford Wallace
- SmartBot and Wallace barred from spyware-related activity, pay $4 million, in settlement, Lansky and OptinTrade ordered to pay $227,000, barred from spyware-related activity

Effects of Spyware

- Decreases Performance
  - Unwanted behavior
- System Wide Crashes
- User unaware of spyware
  - Blame Hardware, Installation, or Virus
- Disable fire-walls and Anti-virus software
  - Multiple spyware
  - Opportunistic infections (infect the infected)
  - Disable competing spyware

Effects of Spyware

- Annoying pop-ups
- Affiliated Fraud
  - Redirects Revenues
  - If you direct a customer to eBAY, and he makes a purchase, then you get a commision

A Crawler-based Study of Spyware on the Web

A. Moshchuk, T. Bragin, S.Gribble, H. Levy, NDSS06

Why measure spyware?

- Understand the problem before defending against it
- Many unanswered questions
  - What's the spyware density on the web?
  - Where do people get spyware?
  - How many spyware variants are out there?
  - What kinds of threats does spyware pose?

Approach

- Large-scale study of spyware on the Web
  - Crawl "interesting" portions of the web
  - Download content
  - Determine if it is malicious
    - Use virtual machines
- Two strategies:
  - Executable study
    - Find executables with known spyware
  - Drive-by download study
    - Find web pages with drive-by downloads

Analyzing Executables

- Web crawler collects a pool of executables
- For each:
  - Clone a clean virtual machine
    - 10-node VM cluster, 4 VMs per node
  - Automatically install executable
  - Run analysis to see what changed
    - Currently, an anti-spyware tool (Ad-Aware)
  - Average analysis time – 90 sec. per executable

Analyzing Drive-by Downloads

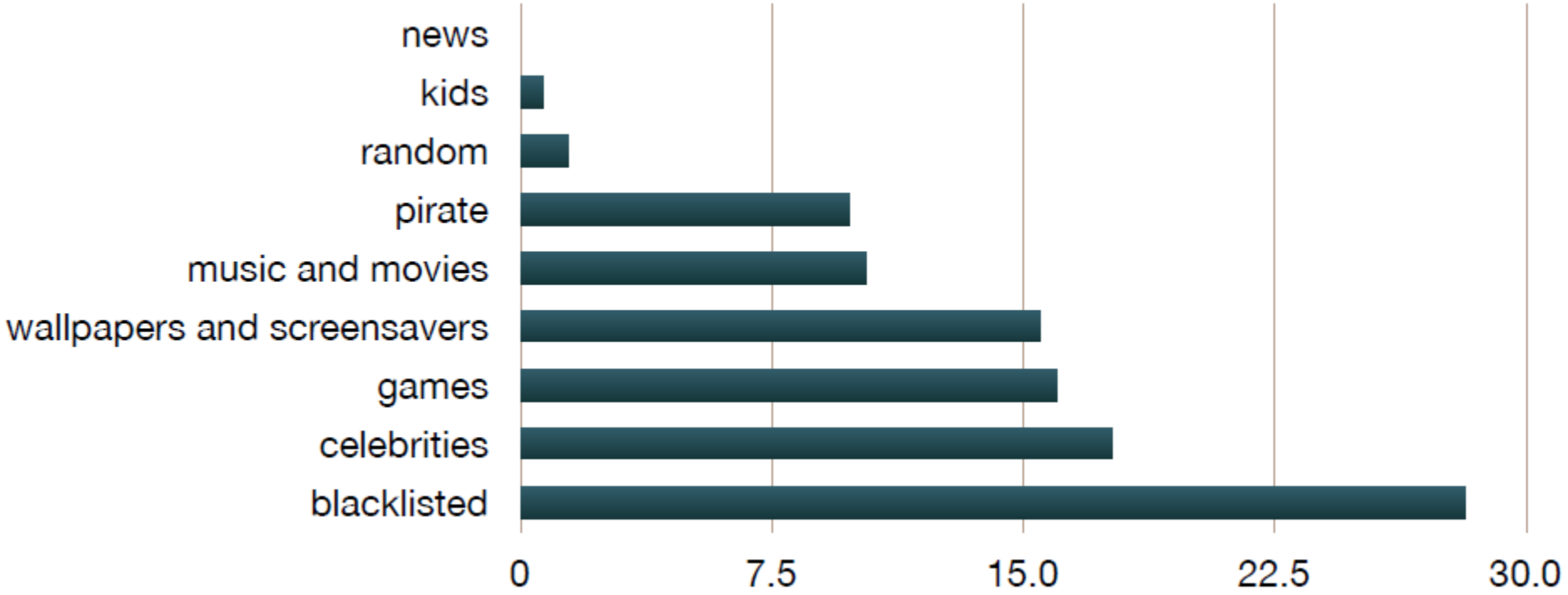
- Evaluate the safety of browsing the web
- Automatic virtual browsing
  - Render pages in a real browser inside clean VM
    - Internet Explorer
  - Define triggers for suspicious browsing activity
    - Process creation
    - Files written outside browser temp folders
    - Suspicious registry modifications
  - Run anti-spyware check only when trigger fires

Executable Study Results

- Crawled 32 million pages in 10000 domains
- Downloaded 26,000 executables
- Found spyware in 13.5% of them
  - 6% installed three or more spyware variants
  - 142 unique spyware threats
    - Only 29 found more than 20 times

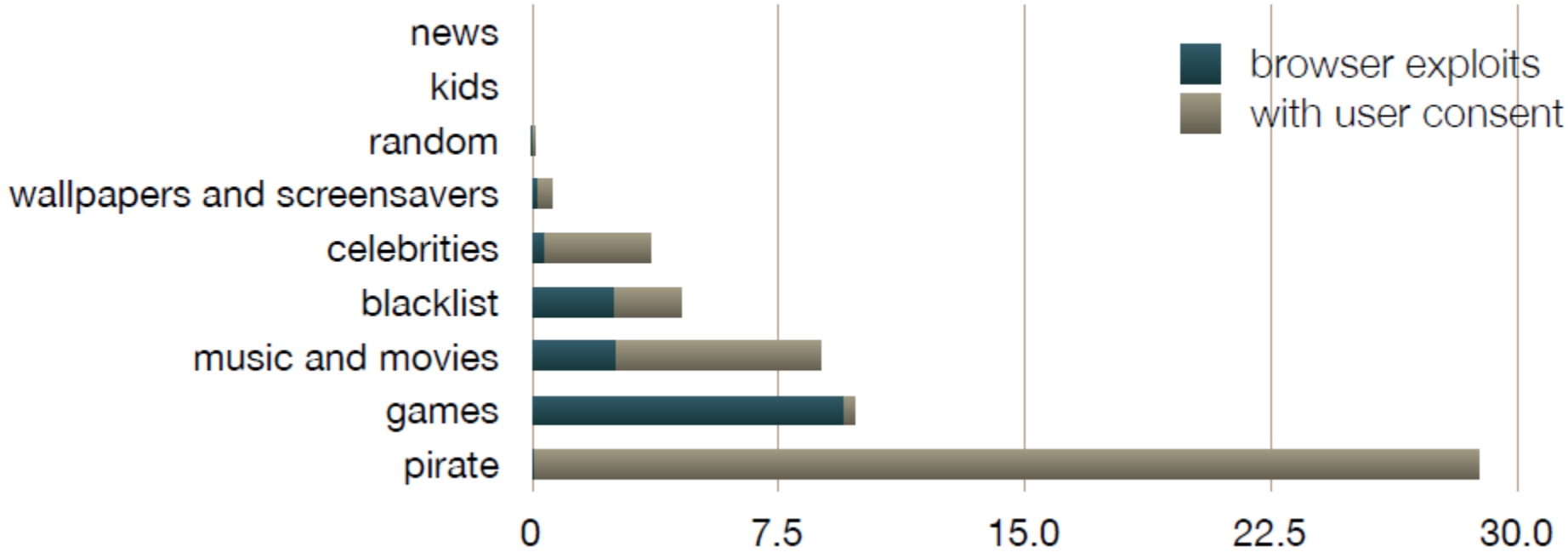
Infection of Executables

- Visit a site and download a program
- What's the chance that you got spyware?



Drive-by Download Results

- 5.5% of pages we examined carried drive-by downloads
  - 1.4% exploit browser vulnerabilities



Summary

- Lots of bad stuff on the web
  - 1 in 8 programs is infected with spyware
  - 1 in 18 web pages has a spyware drive-by download
- Most of it is just annoying (Adware)
  - But a significant fraction poses big risks
- Spyware companies target specific popular content
- Few spyware variants are encountered in practice

Acknowledgments/References

- [Caviness] Spyware, Johanna Caviness, Jamie Johnson, Carolyn Ruthstrom, and Christy Pace, CIS 3330 - Sections 01 and 04, West Texas A&M University, Fall 2006.
- [Moshchuk] A Crawler-based Study of Spyware in the Web, Alexander Moshchuk,CSE 2005-06 Annual Industrial Affiliates Meeting, University of Washington.