CE 817 - Advanced Network Security
Spyware

Lecture 14

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology

Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, when the content is fully obtained from another source. Otherwise a full list of references is provided on the last slide.

What is Spyware?

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

History

- First recorded use of the term spyware occurred on October 17, 1994
- Later came to refer to espionage equipment
- In early 2000 the founder of Zone Labs, Gregor Freund, used the term in a press release for the ZoneAlarm Personal Firewall

History

- 2000, Steve Gibson, of Gibson Research, suspected that advertising software that had been unintentionally installed on his computer was stealing personal information
- Determined it was adware components from the companies Aureate and Conducent
- In 2000, Gibson released the first anti-spyware program, OptOut

Threats

- As of 2006, spyware has become one of the leading security threats to computer systems running Microsoft Windows operating-systems
- Users of Internet Explorer are particularly targeted

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
- Dialers
- Keyloggers
- Browser Hijackers

Adware

- Or 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

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

Dialers

- Install themselves to the user’s dial-up settings and dials numbers without the user’s knowledge
- Often dials out of country numbers that charge while being connected to the internet

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: 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
  - Have you ever read an EULA?

Kazaa

- Kazaa has been bundling spyware with its file-sharing software since its inception.
- The spyware automatically installs when a user installs Kazaa
- Users will have their surfing habits tracked by corporations such as Claria and Altnet, and targeted pop-up ads will display
- Also, users will be redirected to InstaFinder's search engine anytime they misspell a URL

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

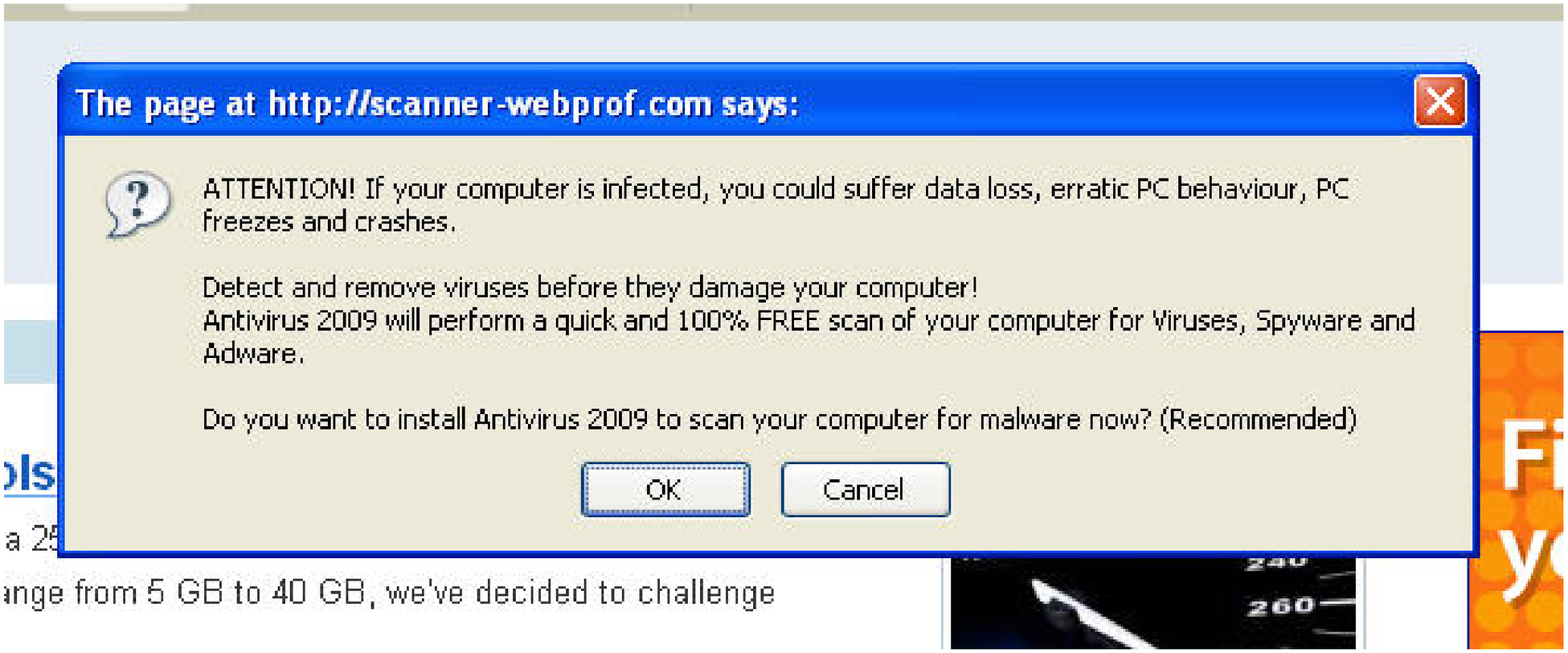
Examples

- 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

Example

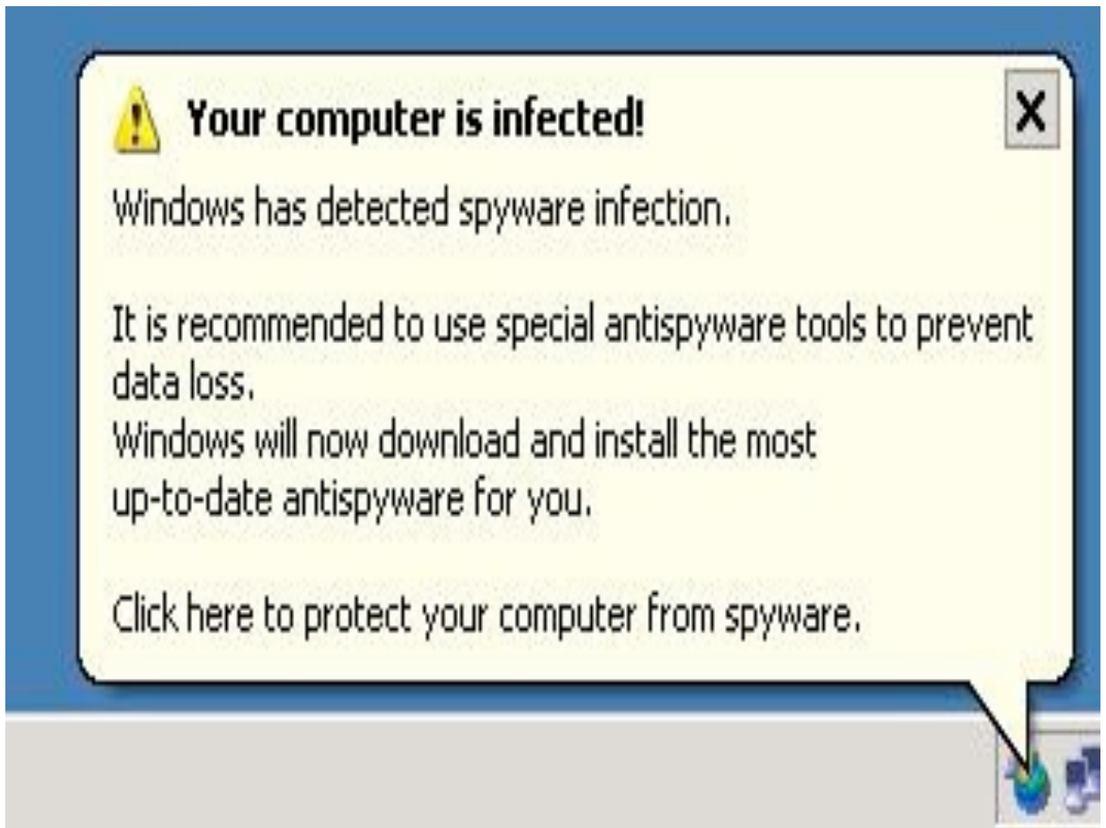

The page at http://scanner-webprof.com says:
ATTENTION! If your computer is infected, you could suffer data loss, erratic PC behaviour, PC freezes and crashes.
Detect and remove viruses before they damage your computer!
Antivirus 2009 will perform a quick and 100% FREE scan of your computer for Viruses, Spyware and Adware.
Do you want to install Antivirus 2009 to scan your computer for malware now? (Recommended)
OK
Cancel
ange from 5 GB to 40 GB, we've decided to challenge
240
260

“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 with Spyware

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

- FTC v. 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

Effects of Spyware

- Identity Theft
  - TRANSMIT
    - Chat Sessions
    - User Names
    - Passwords
    - Bank Information

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

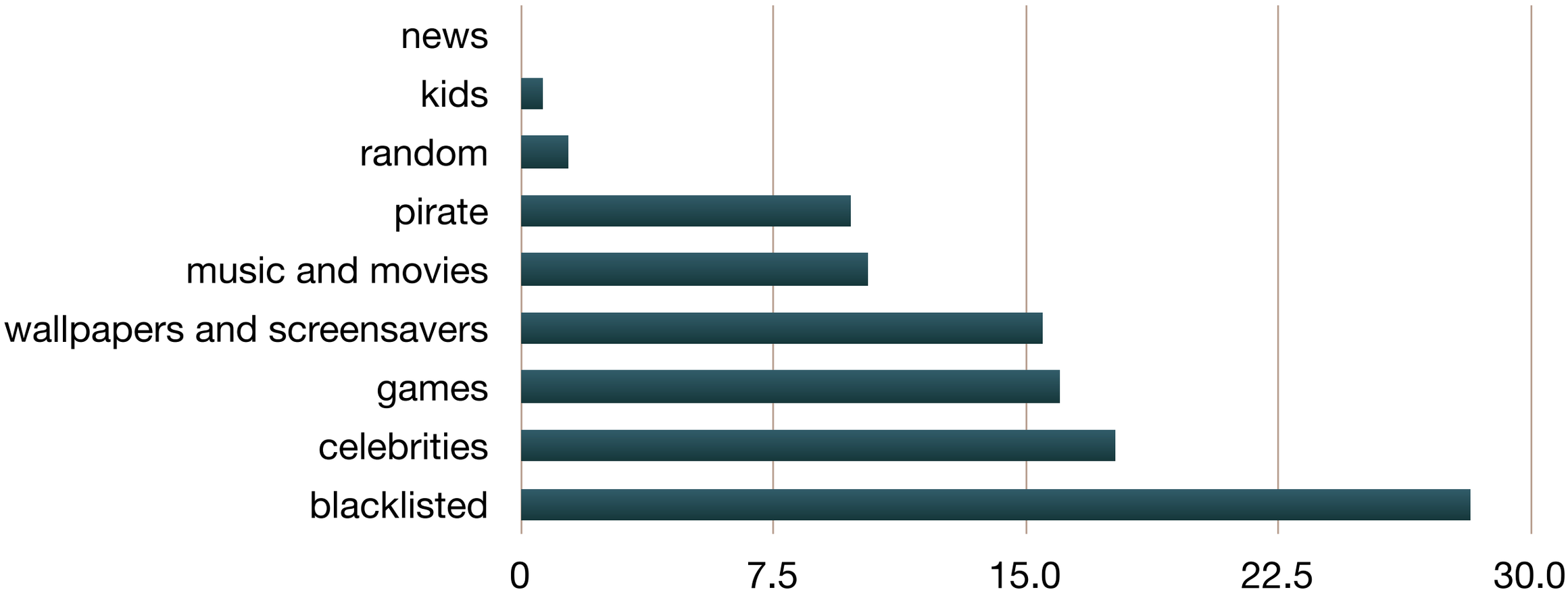
- Evaluate the safety of browsing the web
- Automatic virtual browsing
  - Render pages in a real browser inside clean VM
    - Internet Explorer
  - Define triggers for suspicious browsing activity
    - Process creation
    - Files written outside browser temp folders
    - Suspicious registry modifications
- 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?



Number of installs

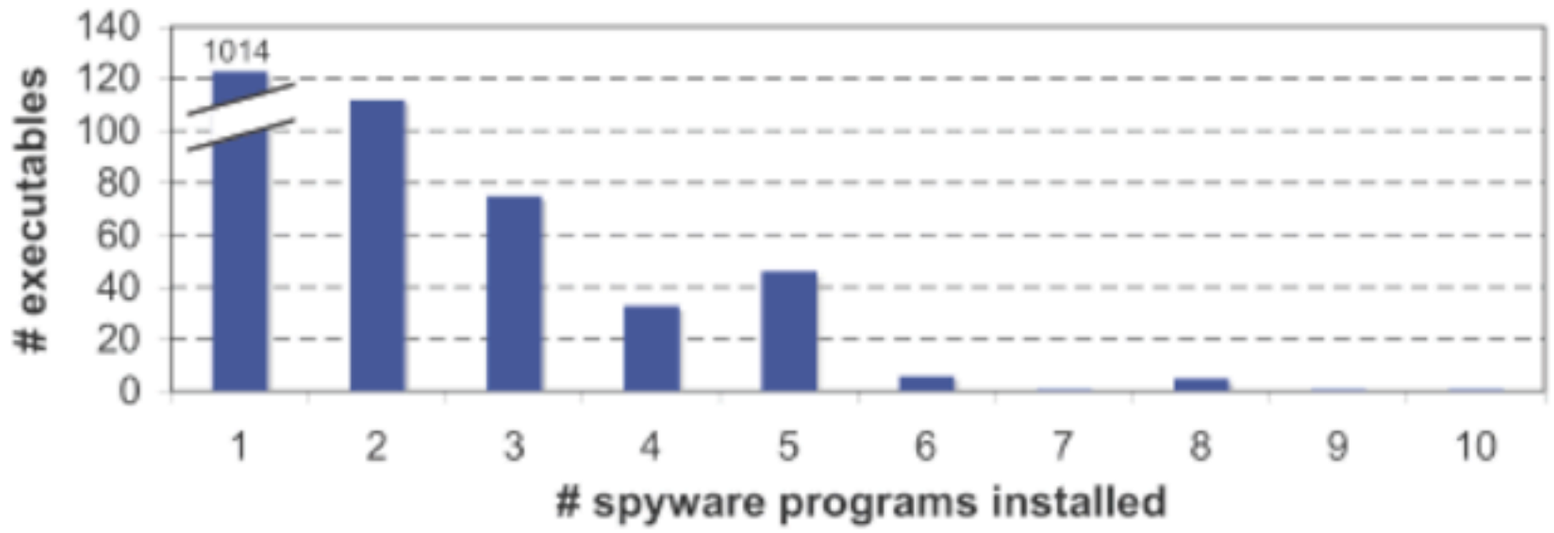
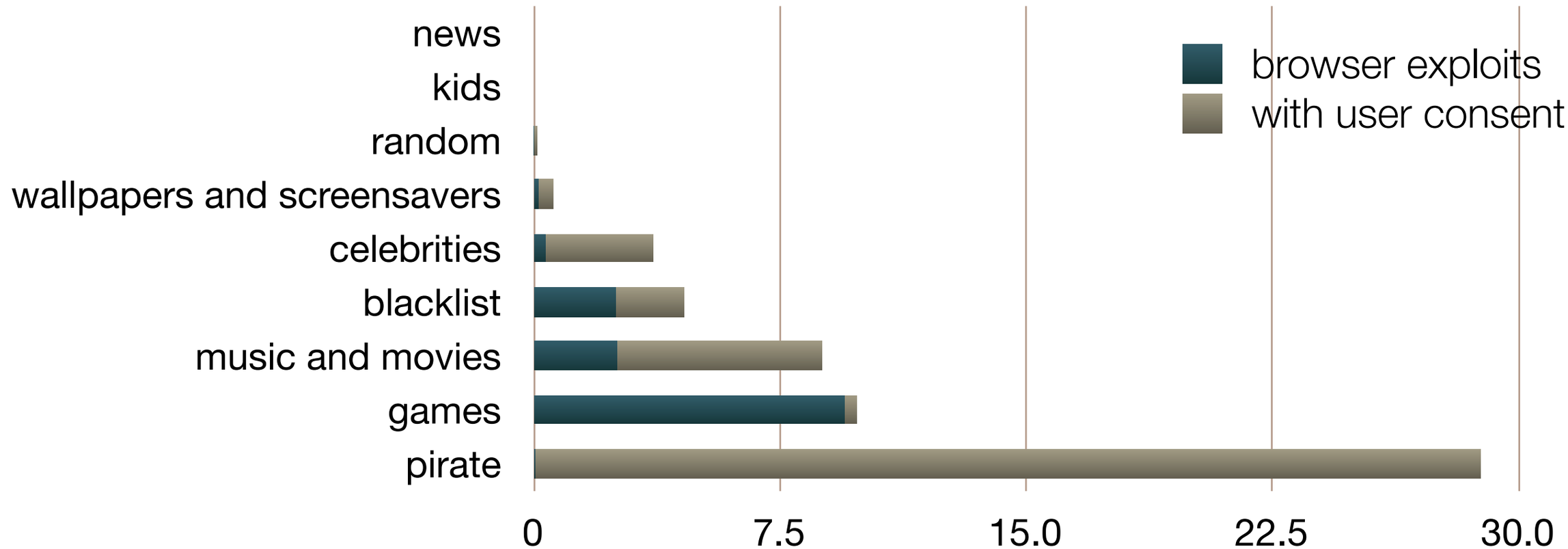


Figure 2: Number of programs installed. The number of spyware programs installed per executable, for the October 2005 crawl data. Most infected executables install only one or two spyware programs, but some install many.

Drive-by Download Results

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



Types of spyware

- Quantify the kinds of threats posed by spyware
- Consider five spyware functions
- What's the chance a spyware program contains each function?

	Executables	Drive-by Downloads
Keylogger	0.05%	0%
Dialer	1.2%	0.2%
Trojan Downloader	12%	50%
Browser hijacker	62%	84%
Adware	88%	75%

IE Browser Configuration

- Security-related IE dialog boxes

		May 2005	October 2005 (recrawl May URLs)	October 2005 (new URLs)
URLs crawled		45,000	45,000	45,000
domains crawled		1,353	1,353	1,420
unique spyware programs found		48	26	36
say yes to prompts ("cfg_y")	infectious URLs	2,675 (5.9%)	1,548 (3.4%)	186 (0.4%)
	infectious domains	46 (3.4%)	27 (2.0%)	23 (1.6%)
say no to prompts ("cfg_n")	infectious URLs	690 (1.5%)	37 (0.1%)	92 (0.2%)
	infectious domains	16 (1.2%)	5 (0.4%)	9 (0.6%)

IE vs Firefox Security

- Internet Explorer v6
  - 186 - cfg_y
  - 92 - cfg_n

- Firefox v1.0.6
  - 36 - cfg_y
  - 0 - cfg_n

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
- More details:
  - A Crawler-based Study of Spyware in the Web – NDSS06

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.