

# CS 410 : Malware

<http://thefengs.com/wuchang/work/courses/cs410>

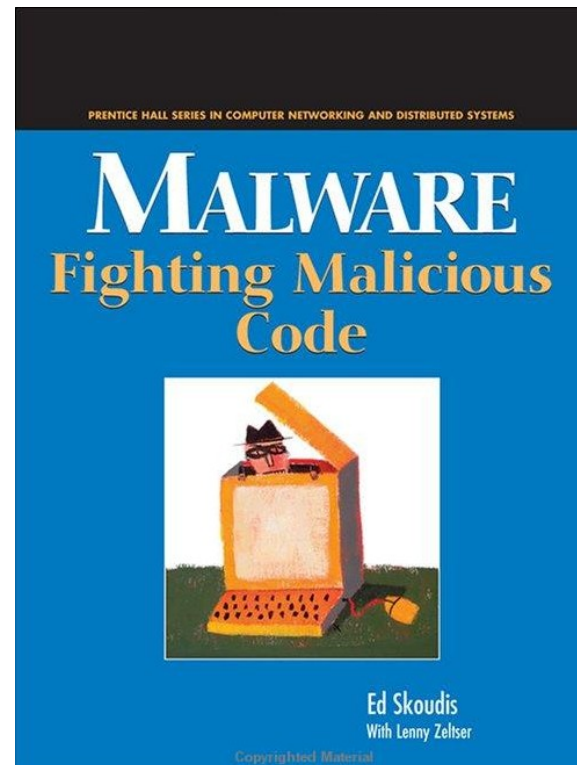
# Textbook

**Optional:**

**Malware – Fighting Malicious**

**Code, Ed Skoudis**

**ISBN: 0131014056**



# Ethics

## Exploring malware

**Do it on your own computer, or somewhere you have permission to**

**Don't run vulnerability scanners on other people's machines**

# What is Malware?

**Malware – set of instructions that run on your computer and make your system do something that an attacker wants it to do**

- Delete files to render your computer inoperable
- Infect other systems (worms, viruses)
- Monitor activity (webcams, keystroke loggers)
- Gather information on you, your habits, web sites you visit
- Provide unauthorized access (trojans, backdoors)
- Steal files (credit card data)
- Store illicit files (copyrighted material)
- Send spam or attack other systems
- Stepping stone to launder activity (frame you for a crime)
- Hide activity (rootkits)

# Why make malware?

**For kicks**

**For profit**

- **Commercial-grade malware**

# Why is it so prevalent?

**Unprecedented Connectivity**

**Huge clueless userbase**

**Increasingly generic software**

**Homogeneous architectures**

**Mature toolkits**

**Data/Instruction mix (.. more)**

# Mixing Data & Code

**What's the difference between code and data?**

- Data is information that your CPU acts on
- Code tells your CPU to take action (danger!)

**To a computer, what's the difference between code and data?**

**.... Not much \***

**Data & code are intermixed these days**

- ELF, .exe, .html, .doc ....

# Mixing Data & Code

## Developers do it because

- **Cool** – Dynamic, interactive environment (eg HTML)
- **Flexible** – Extended functionality (eg .doc)
- **Efficient** – Flexible software building blocks (eg .js)
- **Market share** – Features increase usage

# Types of malware

**Viruses**

**Worms**

**Malicious mobile code**

**Backdoors**

**Trojans**

**Rootkits (user & kernel level)**

# Viruses

**Infects a host file**

**Self-replicates**

**Spreads via secondary storage or network**

**Human interaction usually required**

**Examples**

- Michelangelo, stoned, CIH

# Worms

**Spreads across a network**

**Self-replicates**

**Human interaction not usually required**

**Examples**

- **Morris Worm, Code Red, SQL Slammer**

# Malicious Mobile Code

**Lightweight**

**Downloaded and executed locally**

**Human interaction minimal**

**Javascript, VBScript, Java, ActiveX, Flash**

**Examples**

- **Cross Site Scripting, Drive-by downloads, Cross-site Request Forging**

# Backdoor

**Bypasses normal security controls to give an attacker access**

**Can have dual uses (for good and evil)**

## Examples

- Netcat, VNC, Back Orifice

# Trojan Horse

**Disguised as useful file/program**

**Performs malicious purpose such as launching other programs or capturing user information**

- **Eg. Setiri, Hydan**

# Rootkits

**Tools to hide presence of attacker/other malware on system**

## **User-level rootkit**

- Replaces utilities on host system

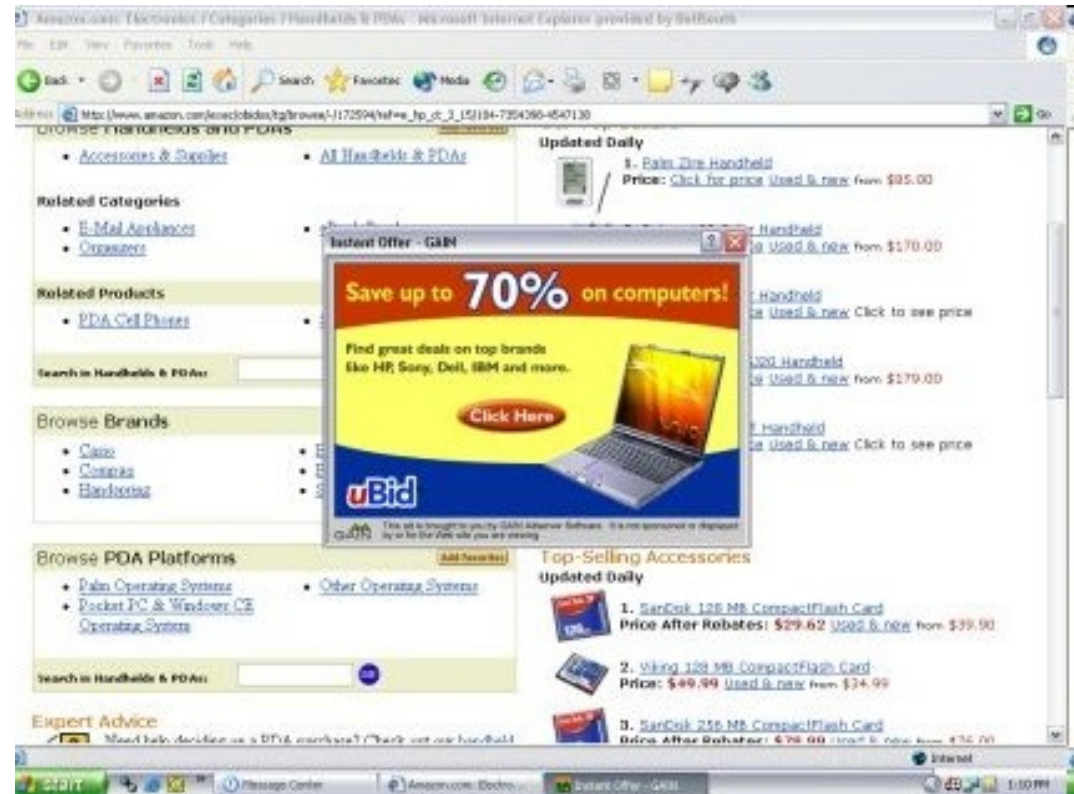
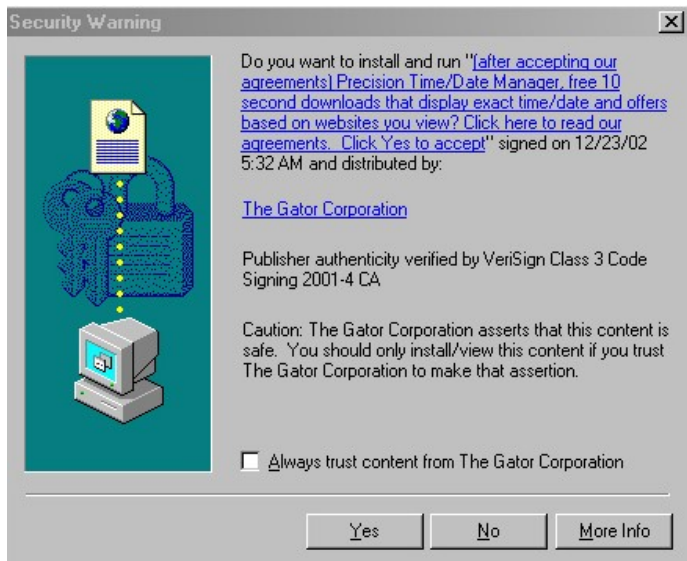
## **Kernel-level rootkit**

- Manipulates operating system directly

# Others

## Spyware

- Monitors a system's activity and reports it to attacker



# Others

## Adware

- Software to continually display advertisements to users

The image displays a dense collection of advertisements and pop-ups, illustrating the concept of adware. The ads include:

- Xerox:** "Enter to WIN! WIN an \$11,000 Business Upgrade Package or a Xerox Phaser™ 8400 Color Printer. World's fastest color printer for under \$1,000. Phaser 8400 Color Printer \$999".
- AOL:** "Before you go, did you know.... You can add AOL® for Broadband to any high-speed cable or DSL connection! Works with and enhances any basic high-speed connection. Built-in protection for you and your family. The best on-demand and exclusive programming online. GET A FREE TRIAL! Upto 45 days FREE. Click here for details".
- Insurance:** "INSWEB Lower your insurance costs. 15 FREE POWER GUIDES".
- Travel:** "TRAVELZOO This Week's Top 10 on the Internet Released APRIL 14. Song CheapCaribbean.com".
- Home Loans:** "Home-Owners Click Here AMERIQUEST MORTGAGE COMPANY®. Rates are...".
- Other:** "BT Make power to you", "ReliaQuote A better way to buy life insurance", "HomeLoanCenter".

# Others

## Scareware

- Software that scares users to purchase or install software they do not want or need

