Chapter 4

A Horse of a Different Color

Malicious Code

• Attack?
  – Execution of malicious code

• Threat?
  – Malicious code:
    • Virus
      – Transient
      – Resident
    • Trojan horse
    • Worm
Malicious Code
– Malicious code:
  • Rabbit
  • Logic bomb
  • Time bomb
  • Dropper
  • Hostile mobile code agent
  • Bot
  • Zombie
  • Script attack

Malicious Code
– Malicious code:
  • Browser hijacker
  • Rootkit
  • Trapdoor/backdoor
  • Tool/toolkit
  • Scareware

Zero-day exploits?
Malicious Code History

• 1982 Elk Cloner, First virus, target is Apple II computers
• 1985 Brain, First virus to attack IBM PC
• 1988 Morris worm, Allegedly accidental infection disabled large portion of the ARPANET, precursor to today’s Internet
• 1989 Ghostballs First multipartite (has more than one executable piece) virus

• 1990 Chameleon, First polymorphic (changes form to avoid detection) virus
• 1995 Concept, First virus spread via Microsoft Word document macro
• 1998 Back Orifice, Tool allows remote execution and monitoring of infected computer
• 1999 Melissa, Virus spread through email address book
Malicious Code History

• 2001 Code Red, Virus propagates from 1st to 20th of month, attacks whitehouse.gov web site from 20th to 28th, rests until end of month, and restarts at beginning of next month; resides only in memory: undetected by file-searching antivirus products

• 2001 Code Red II, Like Code Red, but also installs code to permit remote access to compromised machines

Malicious Code History

• 2001 Nimda, Exploits known vulns.; reported to have spread through 2 million machines in a 24-hour period

• 2003 Slammer worm, Attacks SQL servers; has unintended DoS impact due to massive amount of traffic it generates

• 2003 SoBig worm, Worm propagates by sending itself to all email addresses it finds; can fake From: field; can retrieve stored passwords
Malicious Code History

• 2004 MyDoom worm, Mass-mailing worm with remote-access capability
• 2004 Bagle or Beagle worm, Gathers email addresses to be used for subsequent spam mailings; SoBig, MyDoom, and Bagle seemed to enter a war to determine who could capture the most email addresses

• 2008 Rustock.C, Spam bot and rootkit virus
• 2008 Conficker, Virus believed to have infected as many as 10 million machines; has gone through five major code versions
• 2010 Stuxnet, Worm attacks SCADA (supervisory control and data acquisition) automated processing systems; zero-day attack
Malicious Code

- Consider four aspects of malicious infections:
  - Harm: how they affect users/systems
  - Transition/propagation: how they spread
  - Activation: how they gain control
  - Stealth: how they hide themselves

Malicious Code

- Harm:
  - Non-destructive (hoaxes)
  - Destructive
  - Commercial/criminal intent

- Harm to user:
  - Hiding cursor, displaying text, opening/closing programs, sending email, Deleting/modify (system) files, stealing info
Malicious Code

• Harm to system:
  – Hide file, attach to crucial system file, replace non-crucial system file, hide copies of executable, modify system registry
• Harm to world:
  – Infecting as many as possible PCs across the world, harming productivity etc.

Malicious Code

• Transmission/propagation
  – Setup/installer program
  – Attached file in email
  – Download from web
  – Document viruses
  – Malicious scripts
  – Autorun
  – Drive-by download
  – Appended/surround/integrated
FIGURE 4-1 Virus Attachment

From Analyzing Computer Security by Charles P. Pfleeger and Shari Lawrence Pfleeger (ISBN: 0132789469) Copyright © 2012 Pearson Education, Inc. All rights reserved.

FIGURE 4-2 Surrounding Virus

From Analyzing Computer Security by Charles P. Pfleeger and Shari Lawrence Pfleeger (ISBN: 0132789469) Copyright © 2012 Pearson Education, Inc. All rights reserved.
Malicious Code

- Activation
  - Embedding: appealing to build malware that:
    - Is hard to detect
    - Is not easily destroyed/deactivated
    - Spreads infection widely
    - Can infect home program or others
    - Is easy to create
    - Is machine/OS independent
  - One-time execution
  - Boot-sector viruses
  - Memory-resident
**FIGURE 4-4 Virus V Replacing Target T**

From *Analyzing Computer Security* by Charles P. Pfleeger and Shari Lawrence Pfleeger
(ISBN: 0132789469) Copyright © 2012 Pearson Education, Inc. All rights reserved.

**FIGURE 4-5 Boot or Initialization Time Virus**

From *Analyzing Computer Security* by Charles P. Pfleeger and Shari Lawrence Pfleeger
(ISBN: 0132789469) Copyright © 2012 Pearson Education, Inc. All rights reserved.
Malicious Code

• Stealth
  – Detection “signature”
  – Installation stealth
  – Execution stealth
  – Storage stealth

• Vulnerabilities
  – Voluntary introduction
  – Unlimited privileges
  – Stealthy behaviour

Malicious Code

• Countermeasure: Hygiene
  – Use commercial software from known/reputable source
  – Test new software in isolated computer
  – Open attachments only known to be safe
  – View all websites as potentially harmful
  – Backup system image/executable files
Malicious Code

• Countermeasures
  – Detection tools
    • Antivirus: Virus signatures(patterns):
      – Code analysis
      – Storage patterns
      – Execution patterns
      – Transmission patterns
      – Polymorphic
      – Fake antivirus tools! (often freeware)
    • Anti malware/spyware
    • Suites

FIGURE 4-6 The Compilation Process: (a) Compilation; (b) Decompilation
Malicious Code

• Countermeasures
  – Error detection and error correcting codes
    • Error codes (parity bits)
    • Hash codes (message digest)
    • Cryptographic hash codes
    • Tripwire
Malicious Code

• Countermeasures
  – Memory separation
    • Physical (different devices)
    • Temporal (different times)
    • Logical (OS vs User space)
    • Cryptographic
  – Basic security principals
    • Least privilege by default
    • Complete mediation

Malicious Code

• Conclusions
  – Why is computer crime hard to define?
    • Not everybody are enthusiastic computer sci.
    • Not everybody knows the law
    • Changing laws takes time
  – Why is computer crime hard to prosecute?
    • Lack of understanding, lack of physical evidence, lack of recognition of assets, lack of political impact, complexity of cases, Age of defendant