Lecture notes for Section 3.3 “Viruses and Worms”

- Malware
  - Malware is simply just code, needs to arrive on system (install) & execute
  - Usually installed and executed without or against user intent

- Effects
  - Anything user can do
  - Anything admin can do (if infection is via admin user)
  - Defacement, kill programs, delete files, activate microphone

- Types of malware
  - Viruses: spread by attaching to legit data
    - Legit data could be program or document w/ macros
  - Worms: self-propagating executables
    - Often spread over email
  - Trojans: apparent benign program with hidden malicious component
  - Trapdoor / backdoor: hidden feature triggered by specific input
  - Rootkits: hide itself & other malware on the system
  - Bot: malicious distributed system; sends spam, DDoSes

- Triggers
  - Date & time
  - Event (prog execution)
  - Observed input
  - Environment conditions (tracing / virtualization)

- Time to exploit
  - Critical events (attacker timeline, vendor timeline, user timeline)
    - attacker: discover vulnerability, launch exploit
    - vendor: discover vulnerability, announce vulnerability, distribute patch
    - user: learn of vulnerability, deploy mitigation, install patch
  - Zero-day exploit: exploit active before public disclosure

- Virus infection:
  - In program [Draw picture: box of virus code inserted before box of original prog code]
  - In boot sector (relocate orig bootloader to unused disk sector and chain to boot sector virus)

- Trojan installation:
  - Overwrite orig prog directly (if access)
  - Store in low-privilege location, alter user's path

- Worm execution:
  - Social engg: entice user to execute malicious file

- Malware needs to **execute**
  - Initial execution: exploit vulnerability, entice user to execute
  - Surviving reboot: alter registry so restarted by boot procedure

- White worms
  - Worms that repair flaws
  - Suggested by researchers, unlikely in the real-world
  - Bots often patch the vuln after installation to prevent competitors from acquiring machine

- Prevention
  - Remain disconnected from the outside world
  - Scan for known malcode
  - Test questionable software on isolated computer w/ monitoring tools
  - Keep backups of system, including data & progs

- Instances
  - Seagate shipped hard drives w/ viruses present
  - Windows .wmf vulnerability (design flaw: file format allowed executable code in file)
  - Malware distributed over napster et al.
  - 1988 Morris worm: UNIX, brute-forced passwords, buffer overflow in finger, sendmail debug
    - Dictionary attack used spell-check dictionary already on system
    - Password file split into user file and shadow file; only root can see shadow contents