College of Information Studies

University of Maryland Hornbake Library Building College Park, MD 20742-4345

Malware

Session 11

INST 346

Agenda

- Malware
- Delivery
- Prevention
- Exam 1

Malware

- Software that acts with nefarious intent
- Examples:
  - Slow down your computer (e.g., mining bitcoin)
  - Erase or encrypt your hard drive (e.g., ransomware)
  - Root kit (i.e., an operating system virus)
  - Sends private information (spyware)
  - Uses the network on behalf of the attacker (botnet)
  - Replicates itself (virus)

Why Malware?

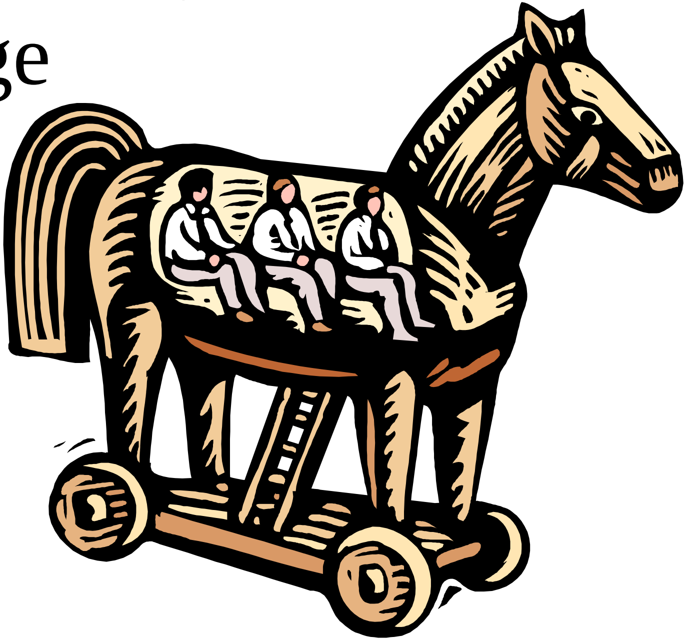
- Hackers
- Theft (identity, secrets, money, …)
- Damage (data, service, damage hardware)
- Profit (botnets, credentials, credit cards, …)

Delivery

- You install it
  - Masquerading as software you wanted
  - Phishing
  - Link following (e.g., fake ads)
- It installs itself
  - Embedded code (Trojan horse, macros, …)
  - Zero-day exploit (e.g., buffer overflow attack)
- Someone else puts it there
  - Access control compromise
  - Trapdoor

Trojan Horse

- Malicious program with undesired capabilities
  - Log key strokes and sends them somewhere
  - Create a “back door” administrator logon
- Spyware: reports information about your activity without your knowledge
- Doesn’t (necessarily) replicate



Prevention

- Keep software current
  - Antivirus “definition” updates
  - Operating system updates
  - Application updates
- Change default settings
  - Userids, passwords, file sharing permission, …
- Separate systems for different functions
- Counter social engineering attacks
  - Training, storytelling, …

Exam 1

- Wednesday Feb 21
- 50 minutes (full class period)
- Online or paper, your choice
- Either 5 or 20 points
- 4-ish questions
- Open book, notes, Web, Panopto, …
- No communication with anyone until exam **period** ends
- Exam review on Monday