CSC427
Malware Investigation

Brandon Frendo
Gabriel Tan-Chen

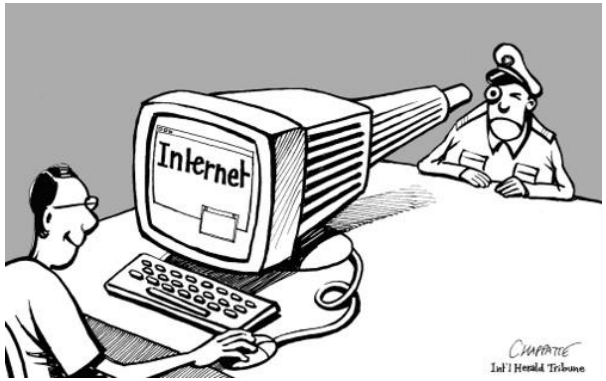
What is malware?

- Encompasses a variety of forms of hostile or intrusive software

- Often disguised in “non-malicious” files
  - Executable Files
  - PDF and Word documents
  - Images

What is malware used for?

- Stealing information
- Spying
- Causing harm to infected computers
- Encrypting files to demand payment (ex: CryptoLocker)



How does malware get onto your machine?

- Everyday computer users:
  - Drive-by downloads
  - E-mails
    - Attachments
    - Links

- Vulnerable Machines
  - Systems with vulnerable software
  - Large networks with vulnerable machines

Preventing Malware Infections

- Install anti-malware/anti-virus software
  - Preferably multiple kinds (layered security)
- Keep software up to date
- Use a firewall to limit traffic to your system
- Be careful when running executable files
  - Proper training

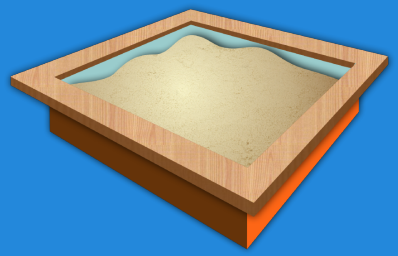
How to discover malware

- File integrity monitoring
  - Validating the integrity of operating system and application software files
  - *Tripwire Enterprise/File Integrity Manager*
  - *CimTrak*
- Process monitoring
  - Monitoring the performance of processes
  - Real-time or log based
  - *Process Explorer*
- Network monitoring
  - Monitoring a computer network for suspicious activity
  - *Wireshark*

Once you've discovered malware

- It is not enough to simply find and delete the malicious file
- You must investigate the effects that the malware had on a system
- To do this, execute the malware in a safe environment (a sandbox) to determine exactly what it does

Sandbox



- A sandbox is a secure environment used to run and observe untrusted programs
- No processes within the sandbox environment can interact with any external files or processes
- No permanent changes are made to the system
- Can be set up using virtual machines on a host or a network of physical machines
- MUST be isolated from the production environment

Malware Analysis Tools

- Online
  - Malwr (www.malwr.com)
  - Anubis
  - ThreatExpert
  - Comodo
  - ThreatTrack ThreatAnalyzer
- Standalone
  - Cuckoo
  - Sandboxie
  - Remnux
  - Zero Wine Tryout

Cuckoo Sandbox

- Free malware analysis system
- Allows suspected data to be queued up (tasks) and then inspected
- Generates reports on the inspected malware
- Report information can include
  - Native libraries used by the malware
  - Registry and file changes
  - Communicated domains/IP addresses
  - Programs accessed

Cuckoo Sandbox

Demo