# Malware = Malicious Software

- Accoring to NIST SP 800-83, 2013, malware is

  “A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim”

- Note that
  - Definition excludes coincidences, although their consequences may be similar
  - Owner of the system and the victim do not have to coincide

# Malware = Malicious Software

- Malicious code often masquerades as good software
- Some malicious programs need host programs
  - Trojan horses, logic bombs, viruses
- Others can exist and propagate on their own
  - Worms
- Many infection vectors and propagation methods
- Modern malware often combines several types of malware
  - E.g. a malware may combine trojan, rootkit, and worm functionality

# Trojan Horse

- Program with an
  - overt purpose (known to user) and a
  - covert purpose (unknown to user)
  - Often called a Trojan

- Example script on previous slide is a Trojan horse
  - Overt purpose: list files in directory
  - Covert purpose: create setuid shell

- In the classical sense, Trojans do not replicate themselves
  - Modern Trojans often come with worm-like functionality

# Spreading of Trojans

- Many Trojans are inadvertently installed by the user, e.g.
  - Trojan horses in purported hacking tools and free AV tools, other types of security software
  - Source Repositories that plant Trojan in popular packages
  - Third-party widgets that make sites "prettier" (e.g. calendars, visitor counters, etc.)
    - Example: free widget for keeping visitor statistics operates fine from 2002 until 2006
    - In 2006, widget starts pushing exploits on all visitors of pages linked to the counter
  - Website with thumbnails of adult videos
    - Clicking on a thumbnail brings up a page that looks like Windows Media Player and a prompt:
    - "Windows Media Player cannot play video file. Click here to download missing Video ActiveX object."
    - The "codec" is actually a malware binary

# How do we Avoid Installing Trojans

- Seemingly obvious solution
  - Install only trusted operating systems, applications, and tools
- But: how do we decide whether to trust an executable or not?
- Often claimed safe approach
  - Use only software with openly accessible source code
  - Compile source code yourself
- But:
  - Do you really check the source code?
  - And what about the compiler?