Trojan Horses
Objectives

• Outline the evolution of the Trojan horse
• Name ways in which Trojans are deployed
• Identify risks associated with Trojans
Objectives (continued)

• Name some well-known Trojans
• List Trojan attack prevention measures
• List Trojan detection tools
Trojan Horses

- **Trojan horse**
  - Application that uses trickery to get a user to install it
  - Circumvents safety measures inherent in an operating system
    - That might make it difficult for a covert installation to operate
Trojan Horses (continued)

• Typical functions for a Trojan might include
  – Logging keystrokes, taking screen captures, accessing files on local and shared drives, or acting as a server where the client is the hacker
• Trojan horse applications are usually masqueraded as games, utilities, or other useful applications
• At this time, Trojans are not able to reproduce themselves like viruses or worms
Workings of Trojans

• For Trojans to be a threat
  – They must be installed by the user and activated
Installation

• Distribution vectors:
  – E-mail attachments
  – Scripts in HTML e-mails
  – Files on FTP servers
  – Scripts on spoofed Web sites
  – Scripts on hacked legitimate Web sites
  – Download opportunities on Web sites
  – Files offered on bulletin boards and forums
  – Social engineering
Installation (continued)

- Recent Trojan attacks have come disguised as a patch or package
- Always validate the checksum that legitimate download sites provide
Functions of a Trojan

• BO2K is a Trojan horse designed and used to make a horde of zombies
  – To do the hacker’s bidding

• **Zombies** are machines that have been unobtrusively “owned” by a hacker

• When a machine is **Owned**, the hacker can back door into it at any time
  – And perform actions from that machine as if she were sitting at its keyboard
Functions of a Trojan (continued)

• Tasks performed by Trojans include:
  – Sending and receiving files
  – Viewing cached passwords
  – Restarting the system
  – Launching processes
  – Modifying files
  – Sharing files
  – Modifying the registry keys
Famous Trojans

• This section describes the following Trojans:
  – PC-Write
  – AIDS
  – Back Orifice
  – Pretty Park
  – NetBus, SubSeven
  – BO2K
PC-Write (1986)

• First known Trojan horse
• Masqueraded as version 2.72 of the shareware word processor PC-Write by Quicksoft
• Wiped out the user’s FAT (file allocation table) and formatted the hard drive
• Was really a simple batch-file command, encoded as a binary .exe file
AIDS.exe/PC Cyborg (1989)

- Distributed through the postal mail in 1989
- Allegedly contained information about AIDS and HIV
- Actual payload was aids.exe, which would encrypt the hard drive
  - Prompted the user to pay a fee for the password needed to decrypt the hard drive
Back Orifice (1998)

- A remote administration server
  - Allows system administrators to control a computer from a remote location
- Designed by a group called the Cult of the Dead Cow
- Once installed, the server is intentionally difficult to detect
  - And it allows almost complete control over your computer by the remote attacker
Pretty Park (1999)

- The first Trojan to use a worm to propagate itself
- Once installed, this application would attempt to mail itself to anyone in your address book
- When PrettyPark.exe is executed, it may display the 3D pipe screen saver
  - And tries to connect to an IRC server and join a specific IRC channel
Pretty Park (1999) (continued)

- Pretty Park sends information to a pre-specified IRC every 30 seconds
  - Author or distributor of the worm can access information on your system
NetBus (2001)

• Written by Carl-Frederik Neikter
• Allows anyone running the client portion (the attacker) to connect
  – And control the server portion of the target computer
  – Using the same rights and privileges of the current user
NetBus (2001) (continued)

Figure 10-2  NetBus Client setup screen
SubSeven (1999)

• Enables unauthorized people to access your computer over the Internet without your knowledge
• Used a forged e-mail from Symantec to propagate itself
BO2K

- Possibly “gone legitimate” as an open source project
- Back Orifice 2000 is an interesting combination of fair and foul
  - And is appealing as a concept for a network administrator with at-risk remote users
- BO2K software allows you to use infected machines like a string of proxy servers
- Lets you set notifiers on the infected machines
  - Any client that wants to can log into your infected box
Detection and Prevention of Trojans

• The best way to deal with Trojans is to never get one
  – Never open an unverified executable file
  – Never accept attachments that are not expected
  – Never allow anybody on your network to operate with root or administrator privileges
  – Make sure the standard user does not have permission to load or install programs
  – Install a software firewall
Detection and Prevention of Trojans (continued)

• Object reconciliation
  – A widely used method that detects Trojans
  – Means “verification that things are the same”

• Can perform any or all of the following checks
  – Date and time
  – Size
  – Checksum
Detection and Prevention of Trojans (continued)

- Other methods for detecting Trojans
  - Compare your system binaries to the original install files from your installation media
  - Check the backup files for Trojan programs
  - Use the Message-Digest algorithm 5 (MD5), Tripwire, and other cryptographic checksum tools
  - Check for unauthorized services
  - Check and examine legitimate services that you have commented out with `# in /etc/inetd.conf` or `/etc/xinetd.conf`
Figure 10-3  Contents of inetd.conf
Detection and Prevention of Trojans (continued)

- Detecting Trojan Horses
- Tripwire Enterprise
- MDS
- Spybot Search & Destroy
- VirusBlokAda
- GMER
- MetaSploit
- Trojan Remover
- McAfee, Norton, Symantec
- Distributing Trojans
Summary

• Trojan horses use trickery to entice the user to install them
• To be a threat, Trojans must be installed by the user and activated
• Trojans act as remote administrative tools, and can be written to perform almost any task that a legitimate user can perform
• There are several distribution vectors in common use, including e-mail attachments
Summary (continued)

- Trojans can have many functions, such as logging keystrokes, taking screen captures, accessing files on local and shared drives, acting as a server, sending and receiving files, viewing cached passwords, restarting the system, launching processes, modifying and sharing files, and modifying registry keys.
- The first known Trojan horse was a fake version of PC-Write, developed in 1986.
Summary (continued)

• Famous Trojans include PC-Write, AIDS, Back Orifice, Pretty Park, NetBus, SubSeven, and BO2K
• To prevent receiving a Trojan, never open an executable file that you have not verified
  – Or open unexpected attachments
• Trojans can be detected by various means, including software firewalls, IDS systems, some antivirus software, commercial programs, object reconciliation, and registry checkers