Unit -2

Zombies and Trojan Horses: Working of Zombies and Bot Networks, Working of Trojan Horses, Zombie Money Trail, Working of Zombie and Trojan Protection

Security Dangers in Browsers: Hackers exploit Networks, Protection against browser based attacks

Worms and viruses: Working of viruses and worms, antivirus software

Malware

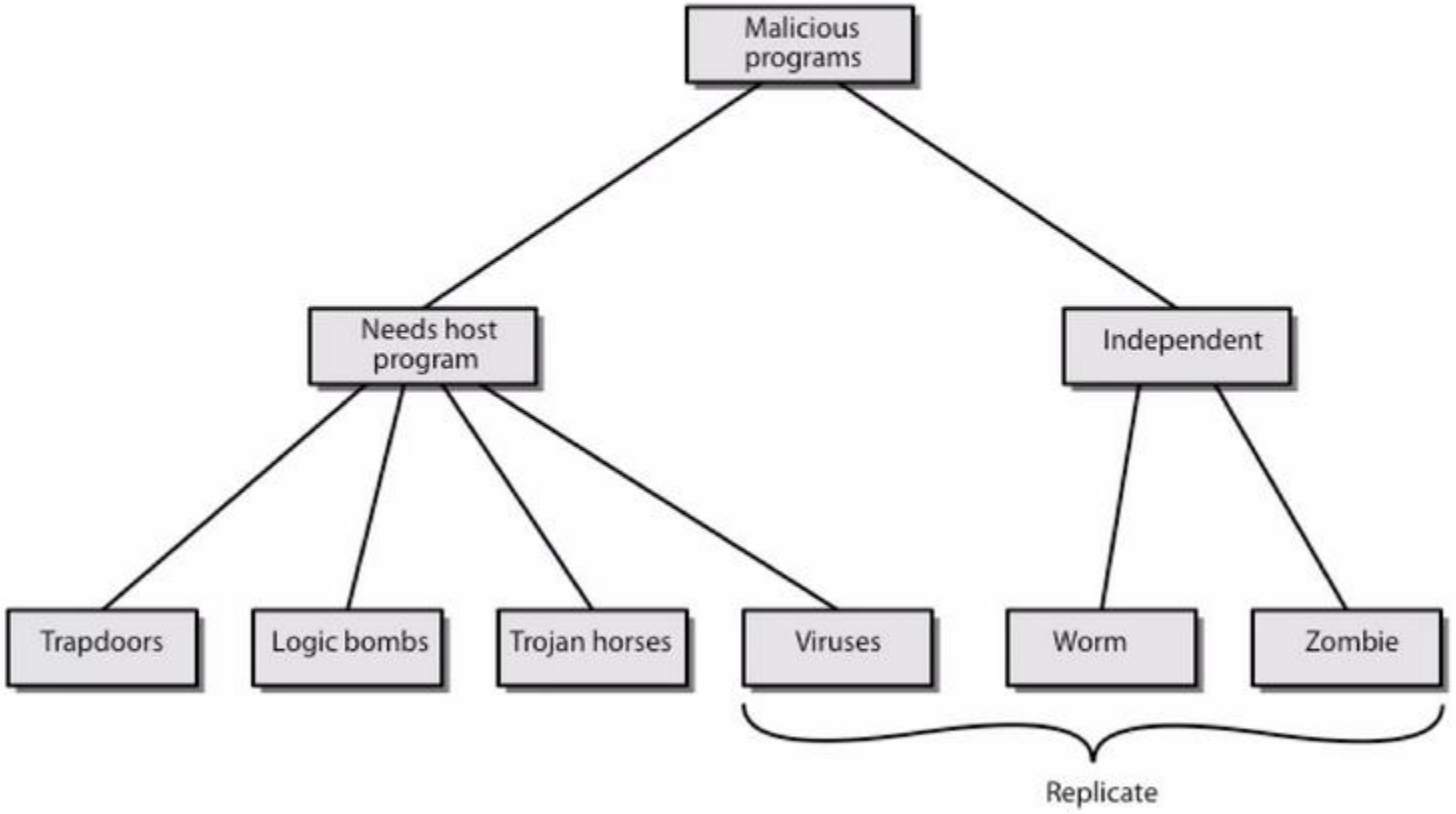
What is a Malware ?

- Malware = Malicious + Software
- A Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.

Types of malware

- Virus
- Backdoor
- Trojan horse
- Rootkit
- Scareware
- Adware
- Worm

Malware according to spreading



Trojan Horse

- Agenda
  - Introduction of Trojan Horse
  - Objectives of Trojan Horse
  - Types of Trojan Horses
  - Trojan Horse Techniques
  - Implementation with an example
  - Prevention Methods

Trojan Horse Definition

- A Trojan describes the class of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the victim computer

Trojan Horse : Introduction

- A Trojan Horse program is a unique form of computer attack that allows a remote user a means of gaining access to a victim's machine without their knowledge.

- Trojan Horse initially appears to be harmless, but later proves to be extremely destructive.

- Trojan Horse is not a Virus.

Objectives of Trojan Horse Programs

Trojan horses can exploit your system in various and creative ways including:

- **Creating a "backdoor" that allows remote access to control your machine**
- **Recording keystrokes to steal credit card or password information**
- **Commandeering your system to distribute malware or spam to other computers**
- **Spying on your activities by sending screenshots of your monitor to a remote location**
- **Uploading or downloading files**
- **Erasing or overwriting data**

Types of Trojan Horses

The EC Council groups Trojan horses into seven main types

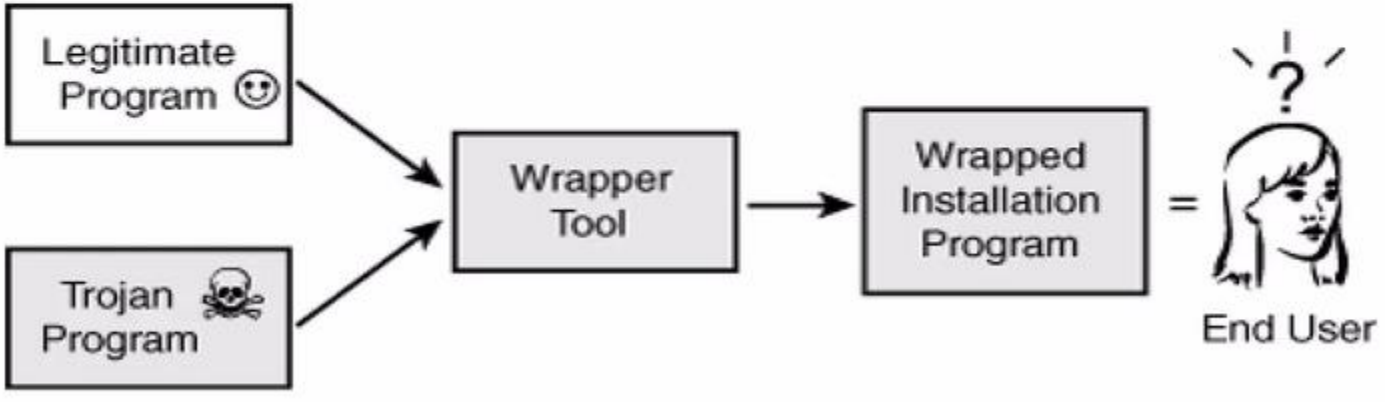
- Remote Access Trojans
  - Subseven
- Data Sending Trojans
  - Eblaster
- Destructive Trojans
  - Hard Disk Killer
- Proxy Trojans
  - Troj/Proxy-GG
- FTP Trojans
  - Trojan.Win32.FTP Attack
- security software disabler Trojans
  - Trojan.Win32.Disabler.b
- denial-of-service attack (DoS) Trojans
  - PC Cyborg Trojan

Trojan Horse Techniques

- Alter name of malicious code on system.
- Create a file name to obscure the file's type.
  - just_text.txt.exe
- abcd.shs where by default the shs file will not be displayed in the system"

Trojan Horse Techniques

- Create another file and process with same name eg. UNIX init process.
- Combine malicious code with an innocuous program



Prevention of Trojan Horse Programs

- Install latest security patches for the operating system.
- Install Anti-Trojan software.
  - Trojan Hunter
  - A- Squared
- Install anti-virus software and update it regularly
- Install a secure firewall
- Do not give strangers access (remote as well as physical) to your computer.
- Do not run any unknown or suspicious executable program just to "check it out".
- Scan all email attachments with an antivirus program before opening it.

Prevention of Trojan Horse Programs

- Do regular backup of your system.
- Do not use the features in programs that can automatically get or preview files.
- Do not type commands that others tell you to type, or go to web addresses mentioned by strangers.
- Never open instant message (IM) attachments from unknown people.
- Do not use peer-to-peer or P2P sharing networks, such as Kazaa, Limewire, Gnutella, etc. as they do not filter out malicious programs hidden in shared files.
- Educate your coworkers, employees, and family members about the effects of Trojan Horse.
- Finally, protection from Trojans involves simple common sense