Malware

- Hardware, software, or firmware that is intentionally included or inserted in a system for a harmful purpose
- Can be a logic bomb, Trojan horse, virus, worm
- Not all of the above are Malware

Computer Viruses

- **Computer viruses** are malicious programs that infect a computer system causing various problems with its use
- Viruses replicate and attach themselves to programs in the system
- There are more than 20,000 different computer viruses with the number growing daily
- [2004 statistics](#)

Virus Pests

- Number of disk viruses are going down while email and Internet type are going up.

Computer virus prevalence

<table>
<thead>
<tr>
<th>Year</th>
<th>Diskette</th>
<th>Email</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>50%</td>
<td>20%</td>
<td>30%</td>
</tr>
<tr>
<td>1997</td>
<td>40%</td>
<td>30%</td>
<td>30%</td>
</tr>
<tr>
<td>1998</td>
<td>30%</td>
<td>40%</td>
<td>30%</td>
</tr>
<tr>
<td>1999</td>
<td>20%</td>
<td>40%</td>
<td>40%</td>
</tr>
<tr>
<td>2000</td>
<td>10%</td>
<td>50%</td>
<td>40%</td>
</tr>
<tr>
<td>2001</td>
<td>0%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>2002</td>
<td>0%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>2003</td>
<td>0%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>2004</td>
<td>0%</td>
<td>50%</td>
<td>50%</td>
</tr>
</tbody>
</table>

How Virus Infections Spread

- Virus Infections spread by:
  - Inserting a disk with an infected program and then starting the program
  - Downloading an infected program from the Internet
  - Being on a network with an infected computer
  - Opening an infected e-mail attachment

Types of Viruses

- **File Infectors**
  - Most common type. Attach themselves to program files then spread to other programs on the hard drive
  - Melissa-distributed by e-mail attachments. If Outlook is used, sends first 50 people the attached virus

- **Boot Sector Viruses**
  - Attach to the boot sector of a hard drive
  - Execute each time the computer is started
  - May lead to the destruction of all data
  - One of earliest was the Stoned boot virus

Macro Viruses

- **Macro Viruses**
  - Infect the automatic command capabilities of productivity software
  - Attach themselves to the data files in word processing, spreadsheet, and database programs
  - Spread when the data files are exchanged between users
### Time Bombs

**Time Bombs** also called *logic bombs* are harmless until a certain date or time.

- **Michelangelo** – Destroys all data on HD on March 6. Mike’s birthday.
- **Jerusalem** – Deletes any program executed on any Friday the 13th.

### Logic Bombs

**Logic Bomb** - A software program that initiates destructive activity when certain conditions are met.

- 1. When a dismissed employee's record is deleted from the payroll. All records deleted
- 2. A Maryland library did not pay for a system that had many bugs. The software company said if they were paid they would tell where a logic bomb was located. Otherwise all records would be deleted.

### Denial of Service (DoS)

- A Denial of Service, or *DoS* is a malicious attack on a network. Essentially to bring a network to its knees by flooding it with useless traffic.
- In Feb 2000, Yahoo, Amazon.com, Ebay and Buy.com were taken down by DoS attacks. Millions of dollars lost.
- Jeffrey Lee Parson, 19 years old, wrote a variant of the Blaster worm and used it to attack 48,000 computers, was sentenced to 18 months in prison in January 2005, and may additionally have to pay a substantial fine.

### Trojan Horses

**Trojan Horses**

- Disguise themselves as useful programs/games but contain hidden instructions.
- May erase data or cause other damage.

**Example:** A chess game appeared, but in reality the hackers were going through files.

### Worms

- Resemble a virus but do not attach to a file.
- Spread from one computer to another independently.
- EXAMPLE: Bank computer transfers money to another account then deletes itself.
- **Pretty Park** once it is executed, after 30 minutes sends an email to everyone on your address list with attached prettypark.exe.

### Annoying Viruses

- **Cascade** - Text characters begin to fall in a pile at the bottom of the screen.
Other annoying viruses (not really!!)

- AT&T VIRUS: Every three minutes it tells you what great service you are getting
- MCI VIRUS: Every three minutes it reminds you that you are paying too much for the AT&T virus

Even More

- PAUL REVERE VIRUS: This revolutionary virus does not horse around. It warns you of impending hard disk attacks—once if by LAN, twice if by C:
- POLITICALLY CORRECT VIRUS: Never calls itself a "virus", but instead refers to itself as an "electric micro-organism"

And Finally

- CONGRESSIONAL VIRUS: The computer locks up, the screen splits erratically with a message appearing on each half blaming the other side for the problem.

Hoaxes

- Many people and companies receive spammed mail claiming virus attacks. Some of these are hoaxes

How do you protect your system

- INSTALL VIRUS PROTECTION and REMOVAL on your system
- Command antivirus
- Symantec antivirus
- McAfee antivirus

Spyware and Adware

- Spyware is a piece of software that collects and sends information (such as browsing patterns in more benign cases or credit card numbers in more malicious cases) about users or their activity,
- usually creates annoying popup advertising windows
- Both usually work and spread like Trojan horses.
- Free cleaners Spybot-Search & Destroy, Adaware, Microsoft AntiSpyware (beta version)
Phishing

• the act of tricking someone into giving them confidential information or tricking them into doing something that they normally wouldn’t do or shouldn’t do