Chapter 14
Computer Threats

Contents:

---

1 Introduction(Viruses,Bombs,Worms)

A virus is a computer program that executes when an infected program is executed.

A virus reproduces its own code by attaching itself to other executable files in such a way that the virus code is executed when the infected executable file is executed.

It attaches itself to some form of host such as legitimate, executable program. Virus lives within the program, which is said to be 'infected'. Execution of the host program implies execution of the virus. It may or may not damage the infected program.
A virus is able to replicate and it creates (possibly modified) copies of itself. It needs to have some form of distribution such as via disks or a computer network.

- Examples: W95.CIH (Chernobyl), Sampo and Hare

1.1 History of Viruses:

There are several stories of the first computer virus. The Pakistani Brain Virus (1986): is the first widely spread IBM Compatible virus. This is commonly mistaken for the first virus. The Apple Virus 1 (1981): It's a Boot sector infecting virus; it was possibly created for pirated games. The Animal (1975) (Univac): "Guess an animal" game is copied to other users' home directories when run.

2. Classifying Viruses: categories

2.1 The Computer Viruses are generally classified as follows:

- Boot Sector
- TSR (Terminate and stay resident)
- Multipartite

- Macro
- Companion
- Polymorphic

(a) Boot Sector Viruses:

Boot sector viruses are those that infect the boot sector (or master boot record) on a computer system. They first move or overwrite the original boot code, replacing it with infected boot code. They will then move the original boot sector information to another sector on the disk, marking that sector as a bad spot on the disk so it will not be used in the future. Boot sector viruses can be very difficult to detect since the boot sector is the first thing loaded when a computer is starts. In effect, the virus takes full control of the infected computer.

About three out of every four virus infections reported are boot sector viruses. The only way that a system can become infected with a boot sector virus is to boot using an infected floppy disk. This is most commonly done when a user leaves a floppy disk in a drive and reboots the system (with the drive door closed). Good anti-virus software will look for an infected floppy disk when a user boots from the floppy drive and before the boot strap is loaded.

(b)File infecting viruses

File infecting viruses are, unsurprisingly, viruses that infect files. Sometimes these viruses are memory resident. However, they will commonly infect most, if not all of the
executable files (those with the extensions .COM, .EXE, .OVL and other overlay files) on a system. Some file infecting viruses will only attack operating system files (such as COMMAND.COM), while others will attack any file that is executable.

Some of these viruses act like boot sector infectors. They replace the “program load” instructions in an executable file with their own instructions, and move the original program load instructions to a different part of the file. This usually increases the file’s size, making detection a little easier. Other file infecting viruses work by using companion files. They rename all files with .COM extensions to .EXE, then write a file with the same name and a .COM extension. This new file will usually have the “hidden” attribute, making it difficult to detect with ordinary file handling commands. By default, MS-DOS executes the .COM file before the .EXE file so that the .COM file is executed first, loading the virus.

(c) TSR (Terminate and stay resident)

A TSRS virus is a virus that stays active in memory after the application (or bootstrapping, or disk mounting) has terminated.TSR viruses can be boot sector infectors or executable infectors. The Brain virus is a TSR virus.

(d) Multipartite

A multipartite virus is a virus that can infect either boot sectors or executables. Such a virus typically has two parts, one for each type. When it infects an executable, it acts

as an executable infector. When it infects a boot sector, it works as a boot sector infector.

(e) Macro

A macro virus is a virus composed of a sequence of instructions that is interpreted rather than executed directly. Macro viruses can infect either executables (Duff's shell virus) or data files (Highland's Lotus 1-2-3 spreadsheet virus).
Eg. Duff's shell virus can execute on any system that can interpret the instructions

This is Piece of self-replicating code written in an application's macro language. A macro virus requires an auto-execute macro one which is executed in response to some event e.g opening or closing a file or starting an application , once the macro virus is running, it can copy itself to other documents delete files, etc.

(f) Polymorphic

Polymorphic viruses change their appearance with each infection. Such encrypted viruses are usually difficult to detect because they are better at hiding themselves from anti-virus software. That is the purpose of the encryption.

Polymorphic viruses take encryption a step further by altering the encryption algorithm with each new infection. Some polymorphic viruses can assume over two billion different guises. This means anti-virus software products must perform algorithmic scanning, as opposed to standard string-based scanning techniques that can find simpler Viruses

3. Types of Viruses

3.1 Viruses can be of the following types:

- Worms
- Trojan Horse
- Bombs

(a) Computer Worm:

This is a ***self-replicating*** computer program, similar to a computer virus. Unlike a virus, it is ***self-contained*** and does not need to be part of another program to propagate itself. This is often designed to exploit computers' file transmission capabilities. A worm could be stated as a program or algorithm that replicates itself over a computer network or through e-mail and sometimes performs malicious actions such as using up the computer and network resources and possibly destroying data.
Examples: Klez, Nimda, Code Red
In addition to replication, a worm may be designed to: delete files on a host system, send documents via email, and carry other executables as a payload

(b) Trojan

A Trojan Horse is a destructive program that has been disguised (or concealed in) an innocuous piece of software.Indeed, worm and virus programs may be concealed within a Trojan Horse. Trojan Horses are not viruses because they do not reproduce themselves and spread as viruses do.
A program may seem both attractive and innocent, inviting the computer user to copy (or download) the software and run it. Trojan Horses may be games or some other software that the victim will be tempted to try.

They can be programmed to self-destruct, leaving no evidence other than the damage they have caused. A Trojan Horse is particularly effective for the common banking crime known as 'salami slicing' in which small sums unlikely to be noticed are sliced off a number of legitimate accounts and moved to a secret account being operated by the thief.

(c) Logic Bomb

Writing a logic bomb program is similar to creating a Trojan horse. Both also have about the same ability to damage data, too. Logic bombs include a timing device so it will go off at a particular date and time. The Michelangelo virus is embedded in a logic bomb, for example. Other virus programs often include coding similar to that used in logic bombs, but the bombs can be very destructive on their own, even if they lack the ability of the virus to reproduce.

Logic bombs are usually timed to do maximum damage.

4. How do viruses work? (Characteristics)

Once a virus gains access to a computer, its effects can vary.
Possible attacks include:

- Replicating itself
- Interrupting system/network use
- Modifying configuration settings
- Flashing BIOS
- Format hard drive/destroy data
- Using computer/network resources
- Distribution of confidential info
- Denial of Service attacks

(a) The Typical methods of infection

- Removable media or drives
- Downloading Internet files
- E-mail attachments
- Unpatched software and services
- Poor Administrator passwords
- Poor shared passwords

5. Computer Security

Different organizations have different styles of operation. This fact extends to the ways they set up their computer networks and operating procedures. That makes it impossible for any document to set down a detailed set of procedures that can be used to cover each and every organization
subject to virus attack. In any case some of the procedures that could be followed are listed below:

5.1 Virus prevention

Virus prevention can be done in any of the ways listed below:

- Patching the operating system
- Patching services
- Patching client software
- Passwords
- Antivirus software
- Firewalls

(a) Passwords

As discussed earlier when talking about Trojans, strong passwords are a vital part of keeping your systems free of infection. Antivirus software does not catch the majority of the Trojans. These Trojans are typically legitimate networking tools that were never intended to be used as a Trojan. Having strong passwords will deter most worms and scanners that attempt to crack passwords as a means of entry.

The Administrator account and those users who have Administrator privileges are at the greatest risk, but all users on the network should follow the same password policy.

(b) Virus Detection (Antivirus software)

The primary method of detection of antivirus software is to check programs and files on a system for virus signatures. However, good antivirus software uses many methods to search the system for viruses.
Antivirus Software Consideration: While choosing antivirus software the following features could be considered:

- Cost (per workstation/server)
- Frequency of updates
- Ease of update installation
- Server administration
- Certification

Some of the Antivirus software options are:

- Aladdin Knowledge
- Alwil Software
- AVG Antivirus
- Central Command
- Command Software
- Computer Associates
- Data Fellows Corp.
- Dr. Solomon's Software

- ESET Software
- Finjan Software

(c) Cleaning viruses

Cleaning viruses depends entirely on your local antivirus solution. The virus must be identified before it can be removed, so it makes sense to try your antivirus scanner first.
If your software identifies, but can't remove the virus, check the manufacturer's website for manual removal instructions.

(d) Perform Basic Computer Safety Maintenance

Use an Internet "firewall", Update your computer, Use up-to-date antivirus software

1.Use an Internet Firewall

A firewall is software or hardware that creates a protective barrier between your computer and potentially damaging content on the Internet or network. The firewall helps to guard your computer against malicious users, and also against malicious software such as computer viruses and worms. Commercial hardware and software firewalls may also be used

2. Update" Your Computer

Download service packs and updates. Especially important for Windows XP users: "SP2".Use Up-to-date Antivirus Software.McAfee and Symantec are prominent vendors. **Make certain to keep "virus definitions" up-to-date.**

Summary:

The chapter details the meaning of computer viruses and their different features. It summaries the different preventive mechanisms for viruses.