Module IV

Malware: Viruses, Worms and Trojans. Topological worms. Internet propagation models for worms.

MALWARE

Malicious software is software that is intentionally included or inserted in a system for a harmful purpose. Malicious software can be divided into two categories: those that need a host program, and those that are independent. The former, referred to as **parasitic**, are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program. Viruses, logic bombs, and backdoors are examples. Independent malware is a self-contained program that can be scheduled and run by the operating system. Worms and boot programs are examples.

- It is a software written into intentionally cause undesirable effect
- Can do anything that a normal program can do
- Designed to damage a computer system without owners concern
- Gets installed in your device and perform unwanted tasks
- Mainly designed to transmit information about your web browsing.
- It comes from different sources such as website, email, physical media etc
- In some cases it spreads itself to other computers though email or infected discs.

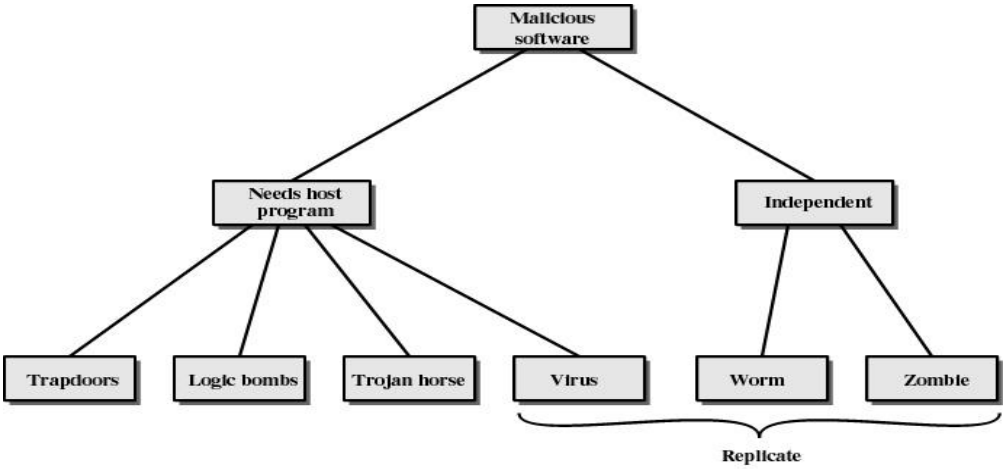


Figure 15.7 Taxonomy of Malicious Programs

VIRUSES

- A *computer virus* is a program that inserts itself into one or more files and then performs some action.
- A computer virus is a piece of software that can "infect" other programs by modifying them; the modification includes injecting the original program with a routine to make copies of the virus program, which can then go on to infect other programs.
- A virus can do anything that other programs do. The difference is that a virus attaches itself to another program and executes secretly when the host program is run.

- Once a virus is executing, it can perform any function, such as erasing files and programs that is allowed by the privileges of the current user.
- Purpose is to infect the computer system, gain admin control and steal user information
- It spread through emails- opening attachment, visiting infected website, USB devices etc.
- The first phase, in which the virus inserts itself into a file, is called the *insertion phase*. The second phase, in which it performs some action, is called the *execution phase*.
- The following pseudocode fragment shows how a simple computer virus works.

Symptoms

- Slow response and slow program execution
- Random hard drive crashes and restarts
- Inability to open files with existing passwords
- Distorted graphics and text
- Make some programs faulty and corrupt

```
beginvirus:
    if spread-condition then begin
        for some set of target files do begin
            if target is not infected then begin
                determine where to place virus instructions
                copy instructionns from beginvirus to endvirus into target
                alter target to execute added instructions
            end;
        end;
    end;
perform some action(s)
goto beginning of infected program
endvirus:
```

As this code indicates, the insertion phase must be present but need not always be executed.

A computer virus has three parts

• **Infection mechanism:** The means by which a virus spreads, enabling it to replicate. The mechanism is also referred to as the **infection vector**. A virus has a search routine, which locates new files or new disks for infection.

• **Trigger:** The event or condition that determines when the payload is activated or delivered.

• **Payload:** What the virus does, besides spreading. It is the actual data that perform purpose of virus.

Phases or Lifecycle of a virus

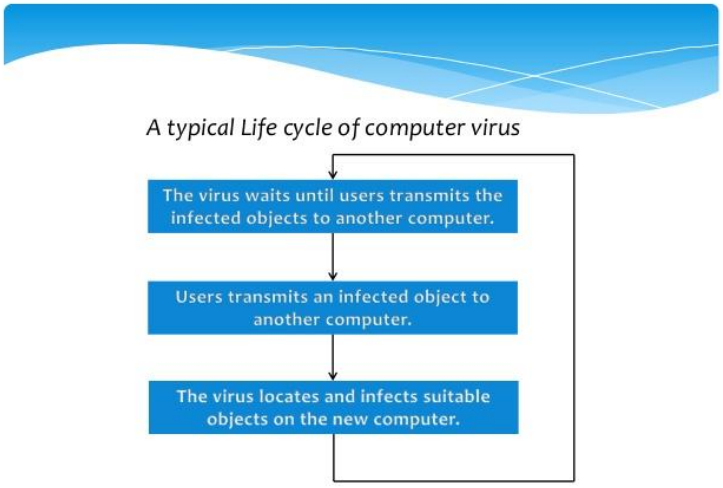
During its lifetime, a typical virus goes through the following four phases:

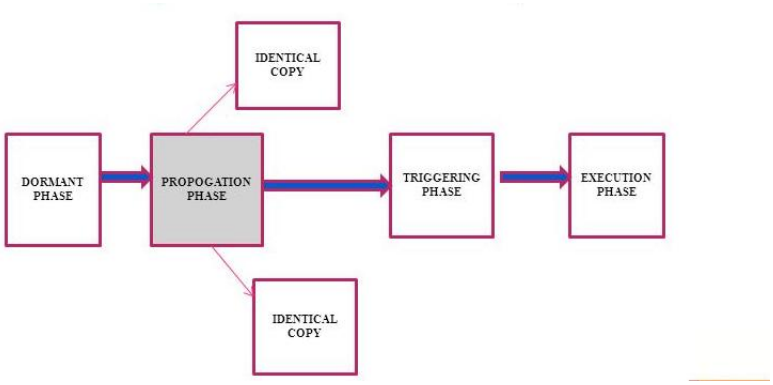
• **Dormant phase:** The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

• **Propagation phase:** The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

• **Triggering phase:** The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

Execution phase: The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.





Viruses Classification

 File Virus: This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called **Parasitic virus** because it leaves no file intact but also leaves the host functional.

 Boot sector Virus: It infects the boot sector of the system, executing every time system is booted and before operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory virus** as they do not infect file system

 Macro Virus : Unlike most virus which are written in low-level language(like C or assembly language), these are written in high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, macro virus can be contained in spreadsheet files.

 Source code Virus: It looks for source code and modifies it to include virus and to help spread it.

 Polymorphic Virus: A **virus signature** is a pattern that can identify a virus (a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of virus remains same but its signature is changed.

Stealth Virus: It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of virus becomes very difficult. For example, it can change the read system call such that whenever user asks to read a code modified by virus, the original form of code is shown rather than infected code.

Executable Infectors

An *executable infector* is a virus that infects executable programs.

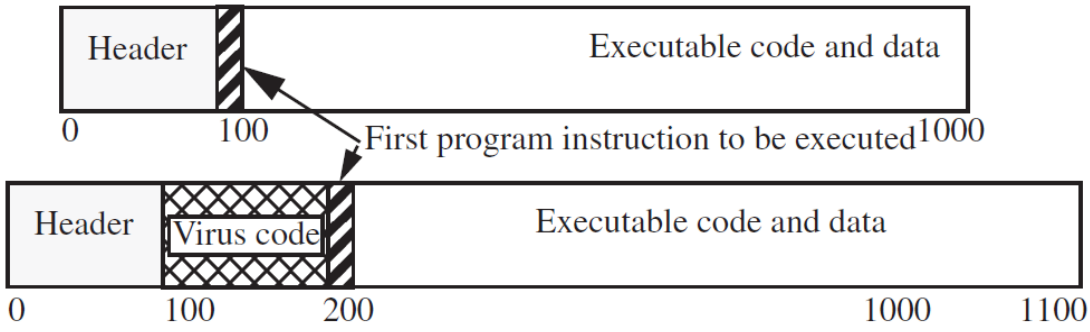


Figure 19–1 How an executable infector works. It inserts itself into the program so that the virus code will be executed before the application code. In this example, the virus is 100 words long and prepends itself to the executable code.

Web Scripting Virus

These viruses come from the programming used for a site's display. The image placement, videos, links and layout of a site are all constructed with coding. This can be altered with the intent of infecting your computer when you click links or watch videos on a malicious site. A site may unknowingly host malicious codes added by a third party, so be careful about visiting any sites. Good security programs have features that detect malicious sites while you browse the Internet.

Memory Resident Virus

This form of computer virus is very destructive. It embeds itself in the computer's memory to carry out operations. This means whenever you run your operating system, the virus is working. It has varying effects, but it will clear up space on your computer for its own use by corrupting and deleting your files.

Browser Hijacker

Imagine typing in an internet address and automatically bouncing through several different sites. When this happens, a browser hijacker is responsible for the incident. Unfortunately, hijackers are usually attached to appealing toolbars, programs and other free downloads you choose. They often have the word "search" in their names. A good security program can detect nearly all of these.

Counter Measures of virus

Some Anti-virus Software

1.Norton Anti-virus: Norton Antivirus Is a product of symantec cooperation founded in 1982.

Norton checks following program:

I. Boot records.
II. Programs(all the time you used them)
III. All local Hard Disk.
IV. Files download from internet.
V. Usb (when in use)

2. MaCFee Virus Scan

MacAfee is an antivirus software and computer security company head quartered in santa Clara, California. It markets MacAfee virus scan and related security products and services, including the intercept and found stone brands. .

3.Kaspersky Anti-virus

• Kaspersky is product of kaspersky lab.
• A Russian computer security company.
• Co-founded by Natalya Kaspersky antivirus, do the following thing.
• Invite virus scan by opening the Kaspersky Antivirus window.

If virus And Worms Attack on our Computer it disturb our System, corrupts data, Some time deletes data and make harm to our computer. Hence, we need to keep safe our computer or any device by using various antivirus software's. Do smart surfing on the Internet For better and Safe computation Anti-Virus software¬ should be installed and be helpful for global network system.

WORM

A network worm is a kind of virus which propagates using computer networks. These might directly exploit a vulnerability in software running on computers which have network connections to cause themselves to be installed and to run on the vulnerable computer. Alternatively end users may be tricked into running the worm program when they receive it via a network, e.g. by double clicking on an executable file attached to email.

- Is a self-replicating program that is harmful to networks.

- Worm uses the network to duplicate its code to the hosts on a network, often without any user intervention.

- Different from the virus because the worm does not need to attach to a program to infect the host.

- It harms networks because it consumes bandwidth.

Virus v/s Worm

Virus	Worm
· Attaches itself to OS or the programs	• Do not Attaches itself to OS
· Need user action to abet their propagation.	• Self propagates across a network exploiting security in widely used services.
· Damages caused is mostly local to the machine	• It harms the network and consumes n/w bandwidth.
· Spread quite slowly	• Spread much more rapidly Ex. SQL Slammer worm 75,000 victims within ten minutes.

A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function. An e-mail virus has some of the characteristics

of a worm because it propagates itself from system to system. However, we can still classify it as a virus because it uses a document modified to contain viral macro content and requires human action. A worm actively seeks out more machines to infect and each machine that is infected serves as an automated launching pad for

attacks on other machines.

The concept of a computer worm was introduced in John Brunner's 1975 SF novel *The Shockwave Rider*. The first known worm implementation was done in Xerox Palo Alto Labs in the early 1980s. It was nonmalicious, searching for idle systems to use to run a computationally intensive task.

Network worm programs use network connections to spread from system to system. Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions.

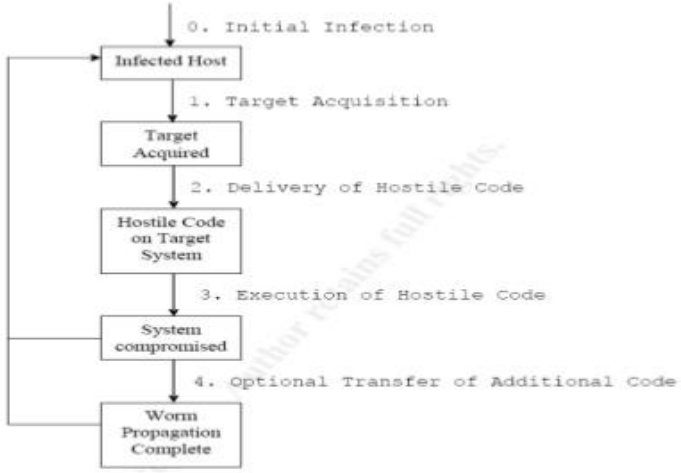
To replicate itself, a network worm uses some sort of network vehicle. Examples include the following:

• **Electronic mail facility:** A worm mails a copy of itself to other system, so that its code is run when the e-mail or an attachment is received or viewed.

• **Remote execution capability:** A worm executes a copy of itself on another system, either using an explicit remote execution facility or by exploiting a program flaw in a network service to subvert its operations.

• **Remote login capability:** A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other, where it then executes.

Mechanism of Operation



Symptoms : Worms

- Shows Error Messages.
- System performs slowly.
- Network Traffic.
- Program Malfunctions.
- Unexpected Restarts.

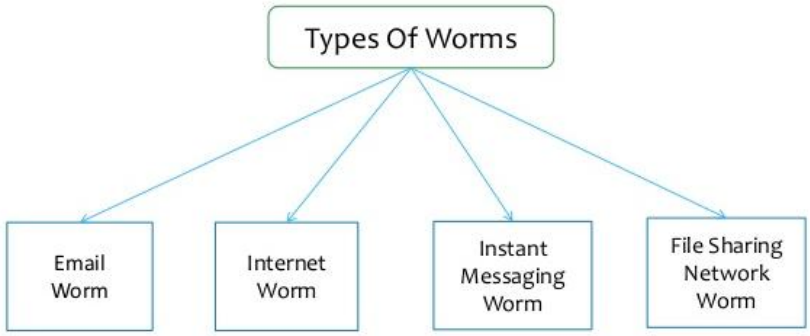
Prevention and Cure

- Regularly update the program.
- Open E-mail attachment files only if you are expecting the attachment files, or the sender is known and has confirmed sending the files.
- Try to avoid downloading and installing the illegal software from the Internet.
- Install only registered copies of software the system.
- Install an Antivirus Software.

Phases of worm

(Same as virus)

Types of Worm



Email Worms: Email Worms spread through infected email messages as an attachment or a link of an infected website.

An email worms uses a PC's email client to spread itself. It will either send a link within the email that, when clicked, will infect the computer, or it will send an attachment that, when opened, will start the infection. Once the worm is installed, it will search the host computer for any email addresses contained on it. It will then start the process again, sending the worm without any input from the user. A well-known example of this type of worm is the "ILOVEYOU" worm, which infected millions of computers worldwide in 2000

• **Instant Messaging Worms:** Instant Messaging Worms spread by sending links to the contact list of instant messaging applications.

These work in a similar way to email worms. The infected worm will use the contact list of the user's chat-room profile or instant-message program to send links to infected websites. These are not as effective as email worms as the recipient needs to accept the message and click the link. They tend to effect only the users of the particular program.

• **Internet Worms:** Internet worm will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. If a computer is found vulnerable it will attempt to connect and gain access to them.

Internet worms are completely autonomous programs. They use an infected machine to scan the Internet for other vulnerable machines. When a vulnerable machine is located, the worm will infect it and begin the process again. Internet worms are often created to exploit recently discovered security issues on machines that haven't installed the latest operating-system and security updates.

• **File-sharing Networks Worms:**File-sharing Networks Worms place a copy of them in a shared folder and spread via P2P network.

File-sharing worms take advantage of the fact that file-sharers do not know exactly what they are downloading. The worm will copy itself into a shared folder with an unassuming name. When another user on the network downloads files from the shared folder, they will unwittingly download the worm, which then copies itself and repeats the process. In 2004, a worm called "Phatbot" infected millions of computers in this way, and had the ability to steal personal information, including credit card details, and send spam on an unprecedented scale.

Worm Propagation Model

Worm propagation process

- Find new targets
  - IP random scanning
  - Send TCP/SYN or UDP packet
- Compromise targets
  - Exploit vulnerability
- Newly infected join infection army

It describes a model for worm propagation based on an analysis of recent worm attacks.

The speed of propagation and the total number of hosts infected depend on a number of factors, including the mode of propagation, the vulnerability or vulnerabilities exploited, and the degree of similarity to preceding attacks.

For the latter factor, an attack that is a variation of a recent previous attack may be countered more effectively than a more novel attack. Figure shows the dynamics for one typical set of parameters. Propagation proceeds through three phases. In the initial phase, the number of hosts increases exponentially.

To see that this is so, consider a simplified case in which a worm is launched from a single host and infects two nearby hosts. Each of these hosts infects two more hosts, and so on.

This results in exponential growth. After a time, infecting hosts waste some time attacking already infected hosts, which reduces the rate of infection. During this middle phase, growth is approximately linear, but the rate of infection is rapid.

When most vulnerable computers have been infected, the attack enters a slow finish phase as the worm seeks out those remaining hosts that are difficult to identify.

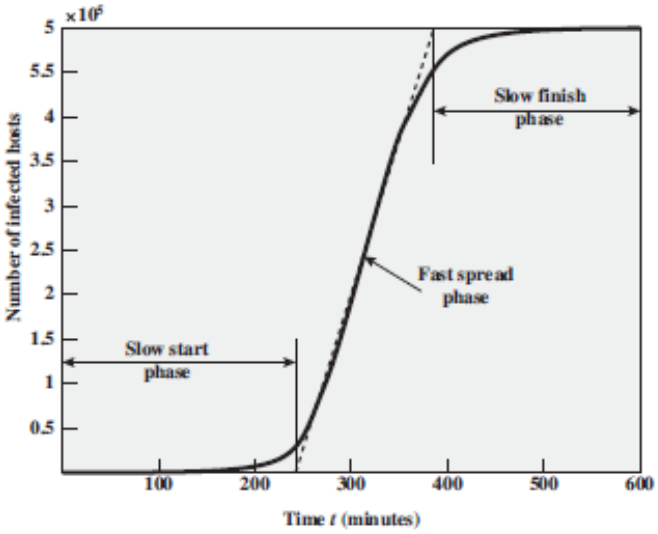
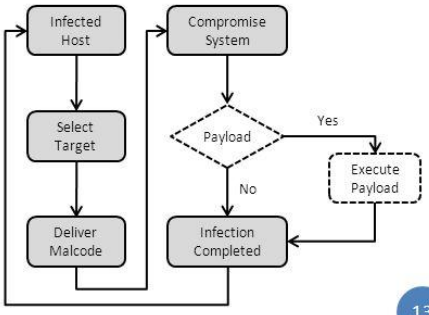


Figure 21.6 Worm Propagation Model

Generalized Worm Propagation Model

- In the first stage the infected host searches for vulnerable targets
- When the target is found, the infected host tries to deliver malcode to the selected target
- Executing the malcode, the target host would be comprimised
- Once the system is compromised, some malware can perform additional tasks
  - Payload refers to those additional tasks by a worm (DoS, install backdoors, self-replicate)



13