Malicious Software

By
Assist. L. Mohamed A. Abdul-Hamed
Computer Scenes and information Technology collage
University of Basra
Computer Science Department

Learning objectives

- Introduction
- What is a computer virus.
- The anatomy of a computer virus.
- What is a computer Worms.
- Viruses VS. Worms.
- Different types of viruses.
- Some Solution to protect your PC.

Introduction

- Malware (malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network.
- While software that causes unintentional harm due to some deficiency is typically described as a Software Bug.
- A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware

What is a virus?

- **A Computer Virus**
- It is one of the malware.
- It is computer program that spreads or replicates by copying itself.

The main parts of a virus' code are :-

- The replication routine.
- The payload routine.

life-cycle of a computer virus

- **The typical life-cycle of a computer virus takes place in four stages**;

1. The dormant phase (خامل),
2. The propagation phase (التكاثر),
3. The triggering phase (الانطلاق),
4. And the execution phase (التنفيذ).

Note: During the dormant phase, the virus has accessed its victim's computer or software, but it does not do anything yet.

The Anatomy of a viruses

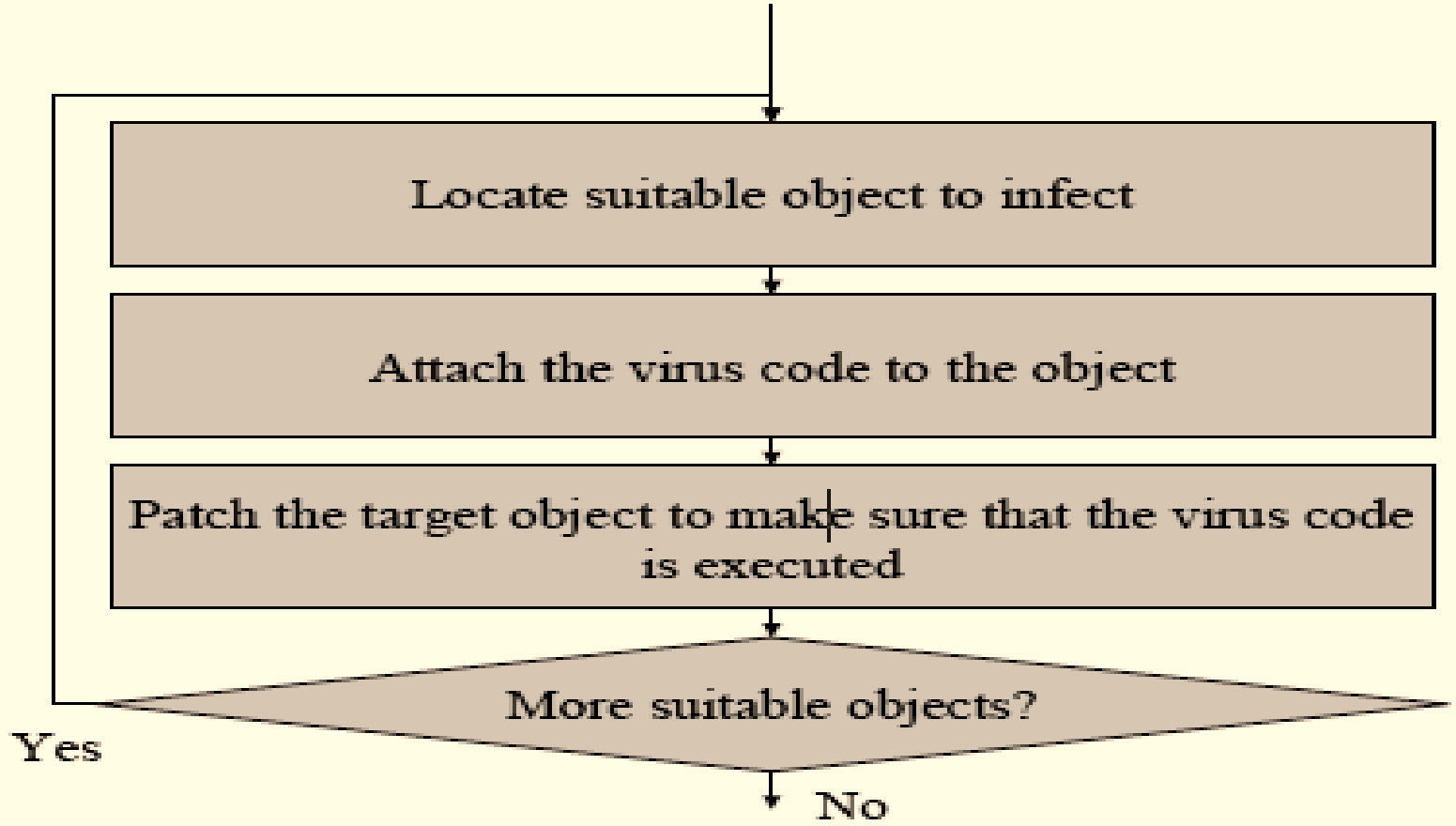
1. **The replication routine**:-

- This mechanism is the most important part of the virus.
- It is infection mechanism (also called 'infection vector'), is how the virus spreads or propagates.
- A virus typically has a Search routine, which locates new files or new disks for infection. So that this part of the virus code locates suitable objects to attach the virus to and copies the virus to these objects.
- A large number of various techniques have been used for this purpose.

The problems of work the replication routine

- **The first problem** the replication routine must solve is how to find suitable objects.
- A virus is always written so as to work attached to a certain type of carrier object, such as a **program file** or **text document**.
- This can be done by searching through the computer, file by file.
- A more elegant approach is for the virus to remain in memory and monitor system activity.
- This enables the virus to infect files when they are used.

- **The second problem** that the replication mechanism must solve is how to attach the virus to the carrier object.
- This step is done using totally different techniques for different types of viruses.
- However, one common requirement is that the virus' code be executed when the object is used.



Functions performed by a typical replication mechanism

The Anatomy of a viruses

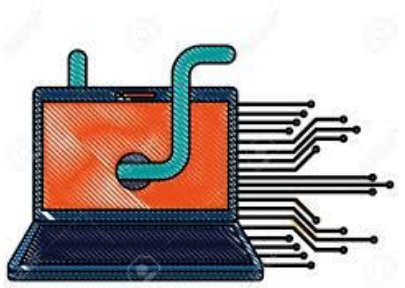
2. **The payload routine**:-

- The **payload** is the actual body or data that performs the actual malicious purpose of the virus.
- payload routine is not a mandatory part of a virus. It does not take part in the replication of the virus in any way.
- Some viruses also lack a payload routine altogether.
- **The payload routines can be divided into two groups, malicious and non-malicious.**

a- **Malicious payloads**, for example, delete files, modify data, plant backdoors in the system or reveal confidential data.

b- **Non-malicious payloads** may play music, show pictures or animations, and promote something … etc.

A Computer Worm



- A computer worm is a type of malicious software program whose primary function is to infect other computers while remaining active on infected systems.
- A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers.
- Worms often use parts of an operating system that are automatic and invisible to the user.
- It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Viruses VS. Worms

- The difference between these two groups may not be obvious to the computer user who encounters a virus or worm, but the difference is significant from a technical point of view.

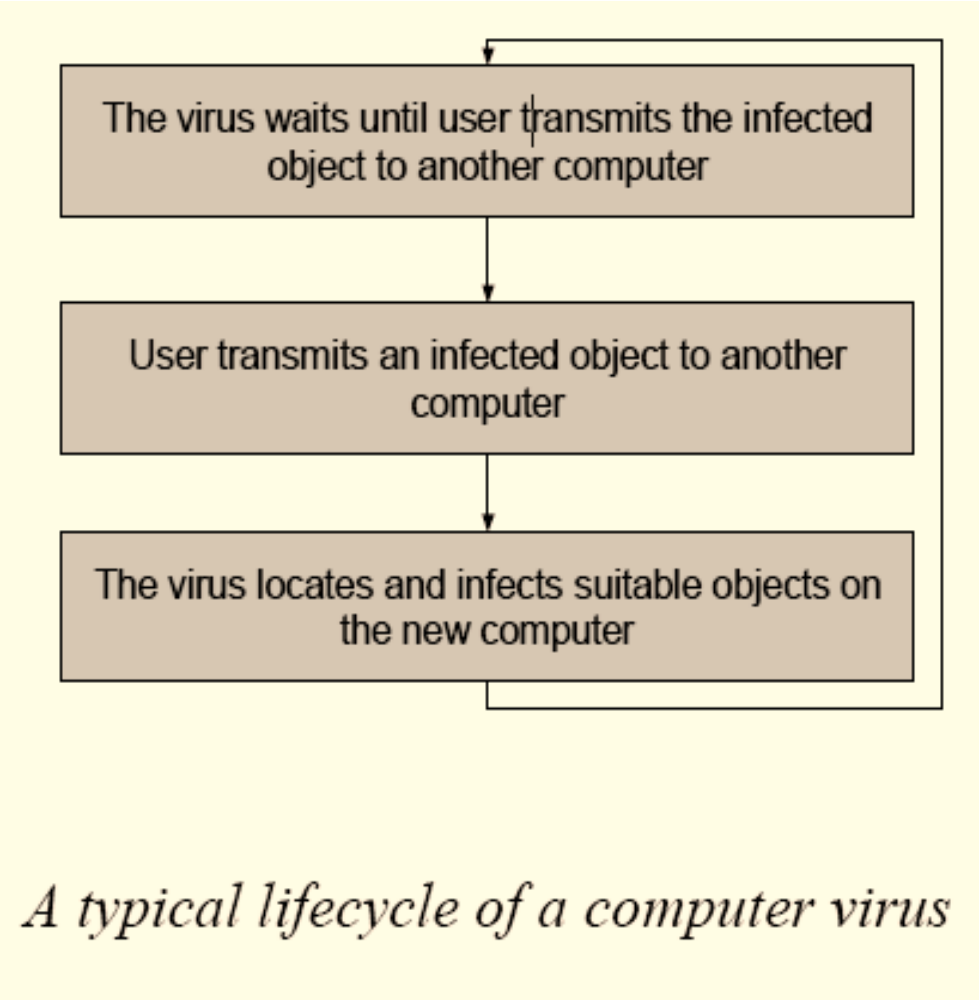
❖ A **worm**, is able to use services provided by a modern networked environment much more efficiently than a virus. This results in an advantage that enables worms to spread much faster than viruses.

❖ **Viruses** attach to a carrier object and wait for the object to be transmitted to another computer. Once transmitted, they activate and start looking for other objects to infect.

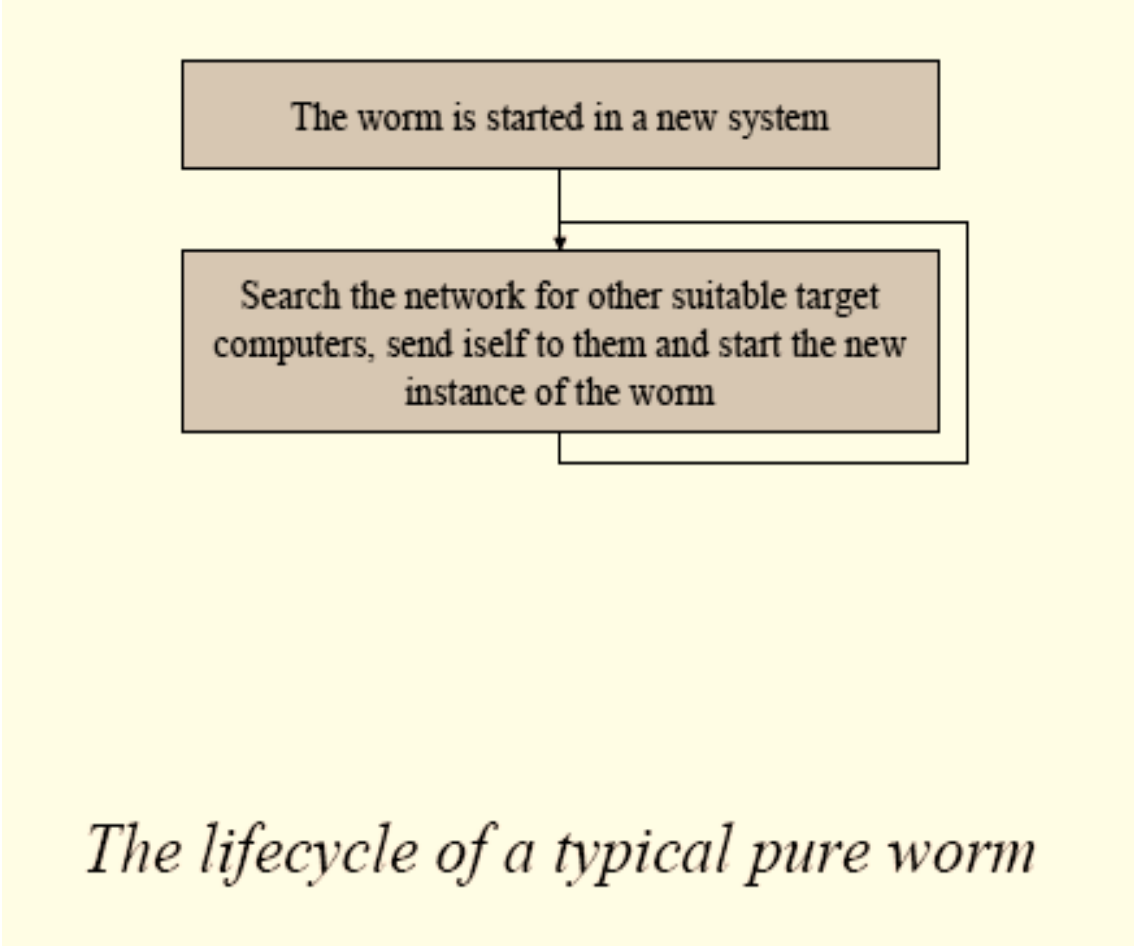
Viruses VS. worms

- Computer worms are self-replicating programs that spread with no human intervention after they are started.
- In contrast, viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems.
- After a computer worm loads and begins running on a newly infected system, it will typically follow its prime directive: to remain active on an infected system for as long as possible, and to spread to as many other vulnerable systems as possible.

Viruses VS. worms



A typical lifecycle of a computer virus



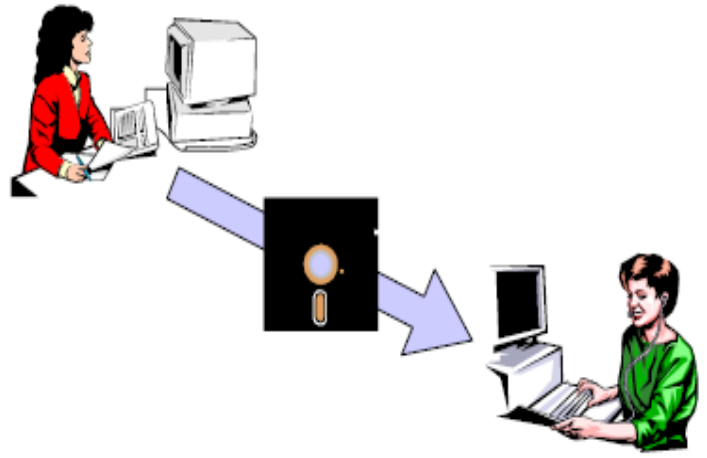
The lifecycle of a typical pure worm

Types of viruses

Different types of viruses

1. **Boot sector viruses**

- A boot sector virus infects the boot sector of floppy disks or hard drives.
- These blocks contain a small computer program that participates in starting the computer.
- A virus can infect the system by replacing or attaching itself to these blocks.

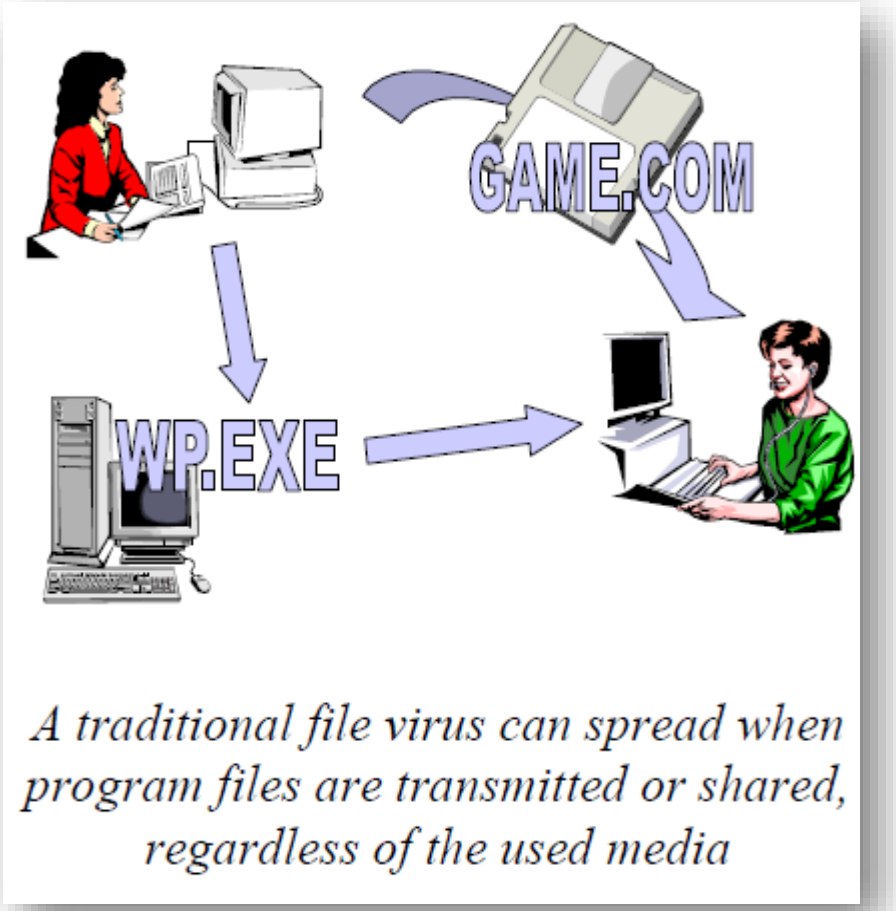


A boot sector virus spreads when data or programs are transferred to another computer using diskettes

Different types of viruses

2. Traditional file viruses

- This group of viruses replicates when attached to MS-DOS program files with the EXE or COM extensions.
- They cannot infect 32-bit EXE files used by newer versions of MS Windows.
- The Traditional file viruses were made for 16-bit program files used by MS-DOS.

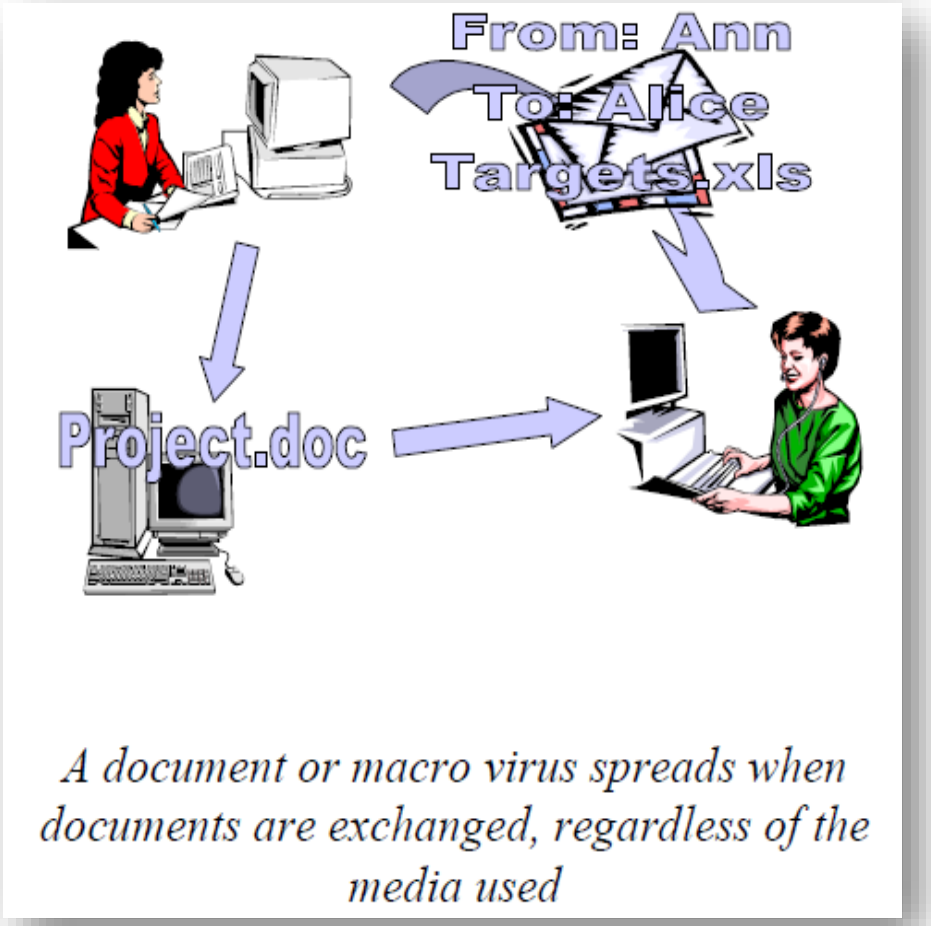


A traditional file virus can spread when program files are transmitted or shared, regardless of the used media

Different types of viruses

3- Document or macro viruses

- written in a macro language, Such languages are usually included in advanced applications such as word processing and
- spreadsheet programs.
- The vast majority of known macro viruses
- replicate using the MS Office program suite, mainly MS Word and MS Excel.

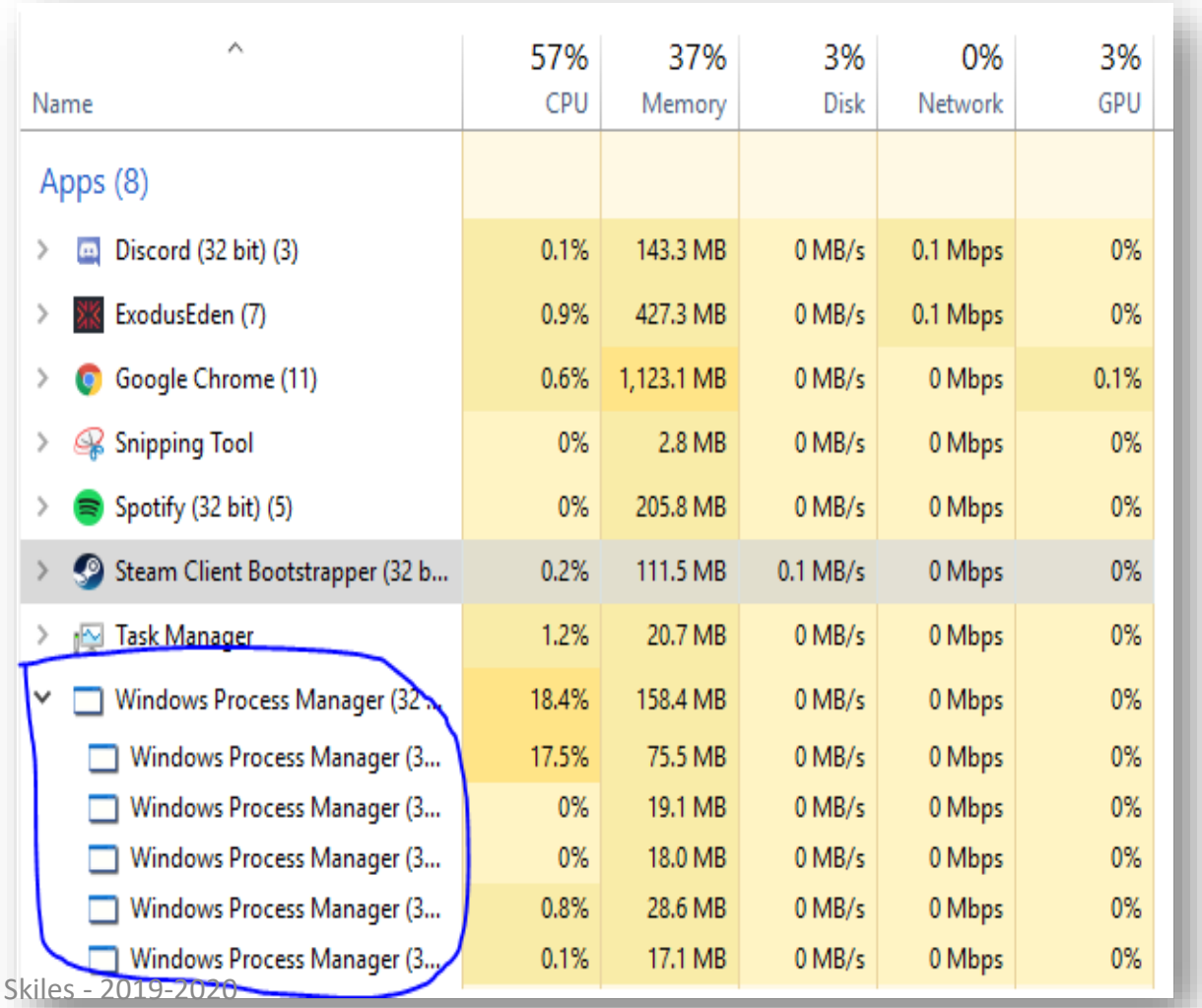


A document or macro virus spreads when documents are exchanged, regardless of the media used

Different types of viruses

4- 32-bit file viruses

- The 32-bit versions of Windows, such as Windows 95, 98 and NT, use a different and more complex format for the program files.
- Traditional files viruses cannot infect these files.



Different types of Malware

5- **Worms**

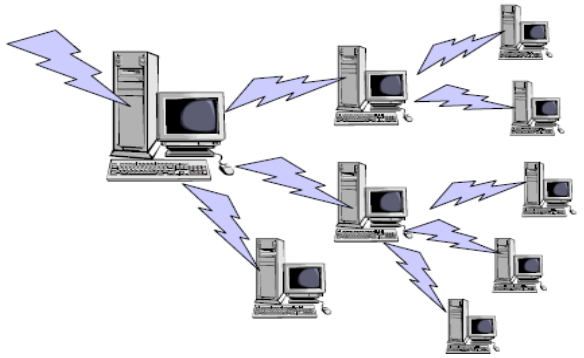
A. mail worm

is carried by an email message, usually as an attachment but there have been some cases where the worm is located in the message body. The recipient must open or execute the attachment before the worm can activate.

An e-mail worm sends a large number of messages automatically when the user has activated the worm

B. Pure worms

A worm is a replicating program that works independently without a host file and without user intervention. Pure worms have the potential to spread very quickly because they are not dependent on any human actions.



A pure worm locates and infects other machines on the same network without user interventions

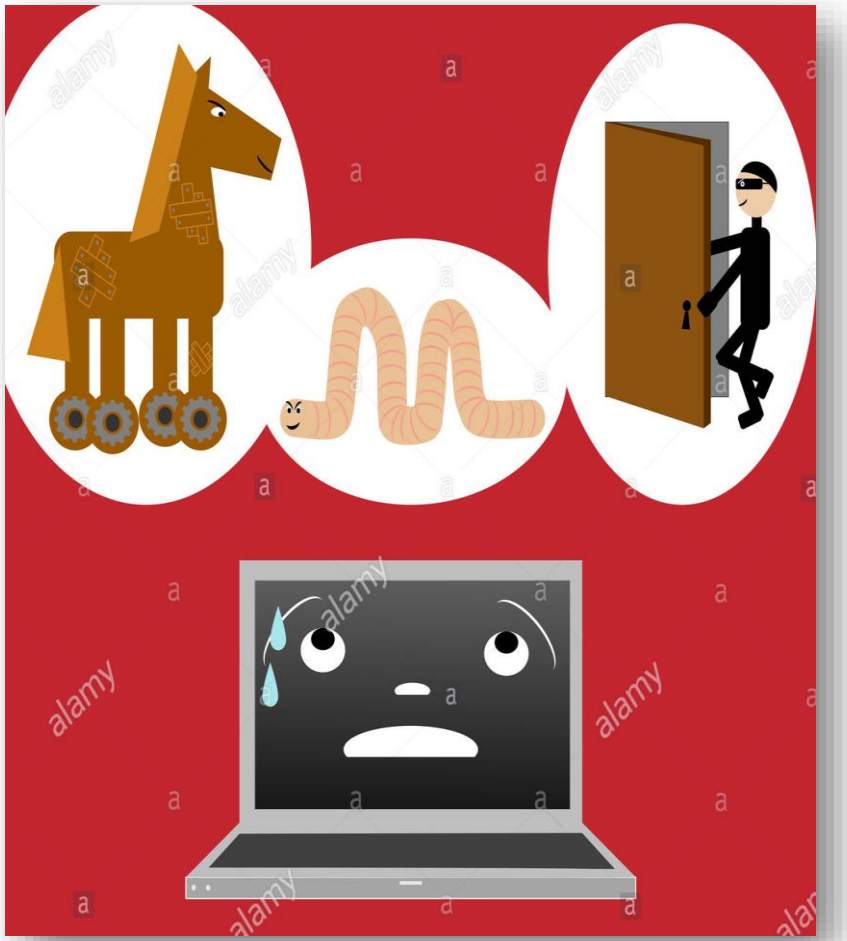
6- Other kinds of malware

A. Trojan horses

- In the computer world the term refers to a program that contains hidden malicious functions.
- The program may look like something funny or useful such as a game or utility, but harms the system when executed.

B. Backdoor Trojans

- are a special kind of Trojan that grant unauthorized access to computer systems.
- This type of Trojan is rather common and can pose a significant threat to business users.



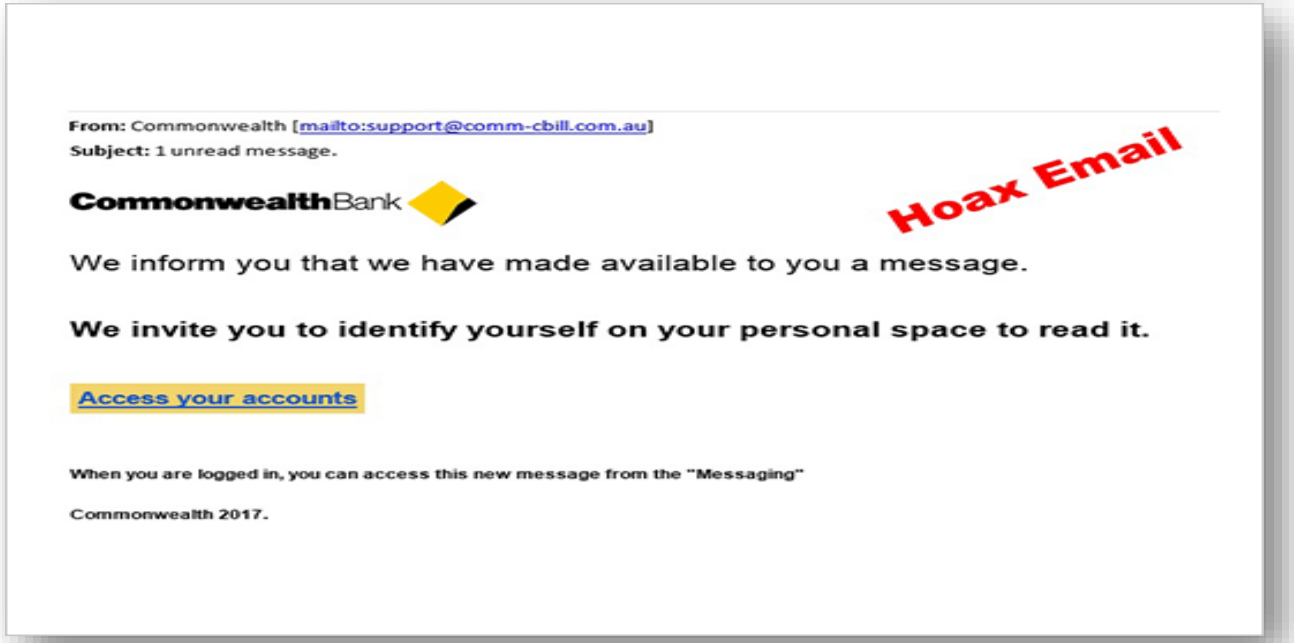
Other kinds of malware

C. Jokes

- A joke program does something funny or tasteless, but does not harm the computer environment. The effect may be music or sounds, video or animation.

D. Hoaxes

- A hoax is a chain letter that is usually circulated as an email message. These chain letters may have any content and are actually not related to computer viruses in any way.



Other kinds of malware

E- Rogue software : are forms of Internet fraud using computer malware to trick users into revealing financial and social account details or paying for bogus products.

F- Scareware software : is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software.

- Scareware is part of a class of malicious software that includes rogue security software, ransomware and other scam software that tricks users into believing their computer is infected with a virus, then suggests that they download and pay for fake antivirus software to remove it.

Some Solution to protect your PC

- With dangerous viruses on the network, what can computer users do to protect their systems?

- Be sure to install an anti-virus software program to guard against virus attacks.
- Also, be sure you turn on the scanning features. It can't protect you if it's not enabled.
- Practice caution when working with files from unknown or questionable sources.

Some Solution to protect your PC

- Do not open e-mail attachments if you do not recognize the sender (though you may also receive viruses from people you know).
- Scan the attachments with anti-virus software before opening them.
- Download files only from reputable Internet sites, and be wary when exchanging diskettes or other media with friends.
- Scan your hard drive for viruses monthly.


Thank
you