Computer Security

Objectives

At the end of the lesson students should be able to

- State what is meant by malware
- Describe different type of Malware
- Give examples how hacking can compromise the computer system
- State what is social engineering
- Describe how online tracking done
- Describe methods to prevent online tracking

THREATS TO THE COMPUTER

Threats to the computer can be either **intentional or unintentional**.

Intentional threat is a deliberate act to destroy data, software or hardware

Unintentional threat is an accident act that destroy data, software or hardware.

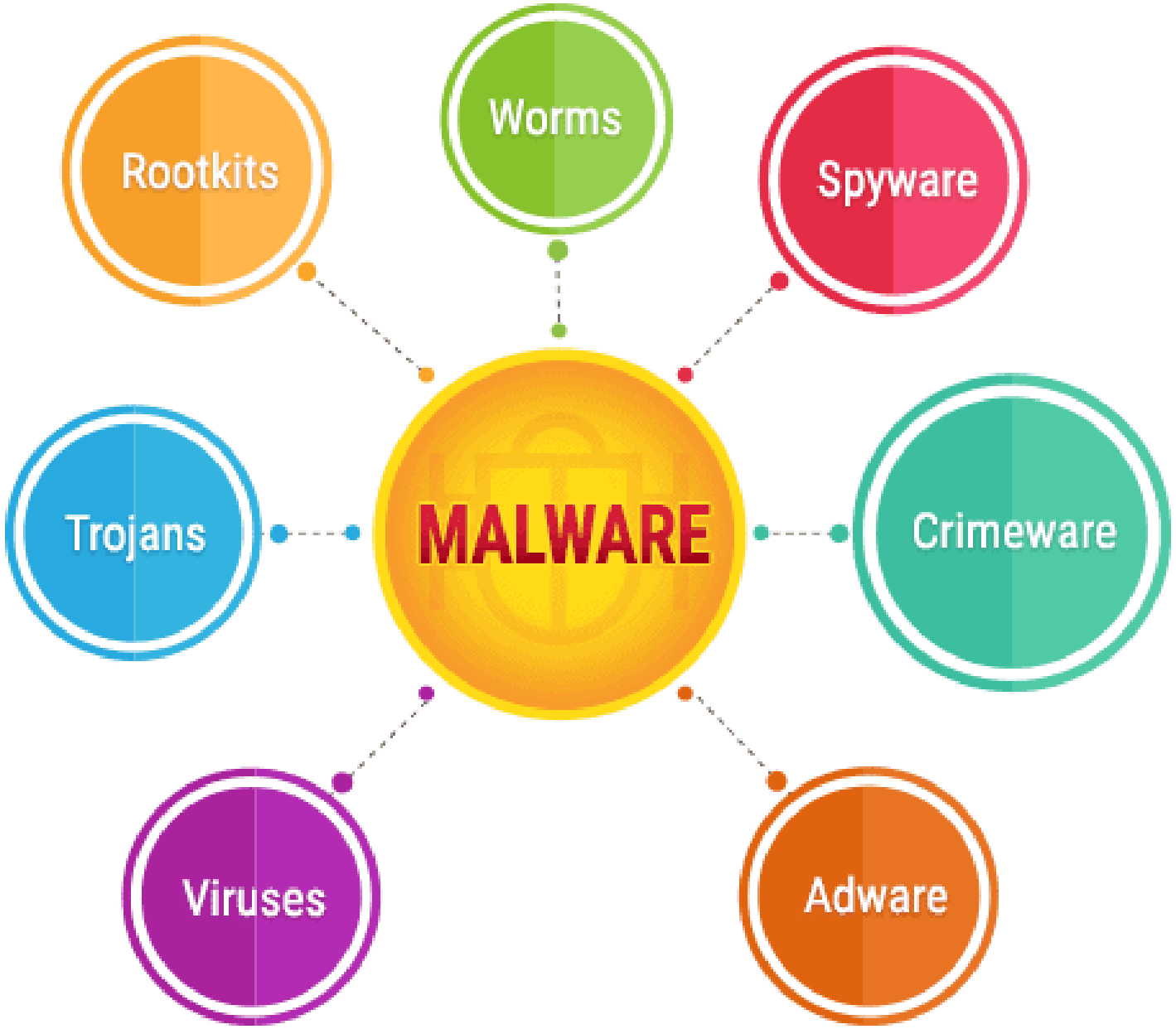
It destroys both hardware and software

Threats to the computer

MALWARE- is an abbreviated form of “malicious software.” This is software that is specifically designed to gain access to or damage a computer, usually without the knowledge of the owner.

There are various types of malware, including spyware, ransomware, viruses, worms, Trojan horses, adware, or any type of malicious code that infiltrates a computer

Types of Malware



Types of Malware

- **Worm**- Program that copies itself repeatedly in the memory or on a disk drive until no memory or disk space. It stays active in the computer memory and replicates itself over a network to infects machines.
- **Trojan -** **pretends** it will be a useful and safe program, when actually it will try to attack your device, such as a screen saver. Unlike a worm a Trojan horse does not replicate itself
- **Virus** A type of malware that spreads through **normal programs**. Once your device has a virus it may spread easily and quickly. A virus might just slow down your device - or it might be so severe you lose all your applications and documents!
- **Ransomware** is a form of malware in which the attacker encrypts the victims' files and demand payment to decrypt such. It has developed to include hacking of sensitive documents/pictures and demand for payment not to release these

Types of Malware

- **A rootkit** is a program that hides in a computer and allows someone from a remote location to take full control of the computer. Once the rootkit is, installed, the rootkit author can execute programs, change settings, monitor activity, and access files on the remote computer. Although rootkits can have legitimate uses, such as in law enforcement, their use in nefarious and illegal activities is growing rapidly.
- **Scareware** (false antivirus) is a malware that scare users to download fake, malicious or useless antivirus software.

Types of Malware

- **Spyware** is a program placed on a computer without the user's knowledge that secretly collects information about the user, often related to Web browsing habits. The spyware program communicates information it collects to an outside source while you are online.
- **Adware (advertising programmes)** is a program that displays an online advertisement in a banner or pop-up window on Web pages, e-mail, or other Internet services.

Other Types of Attacks

Other types of attack

- **Phishing** is a scam in which a perpetrator attempts to obtain your personal and/or financial information by sending out email to the users.
- **Pharming** is a scam, similar to phishing, where a perpetrator attempts to obtain your personal and financial information, except they do so via spoofing. You are redirected to a phony Web site that looks legitimate. The phony Web site requests you enter confidential information.
- DOS Attack -Denial of Service; This is an attack that floods a network especially a network server with many requests constantly and consistently until the server crashes because it cannot cope with so many requests.
- Hacking is an attempt to exploit a computer system or a private network inside a computer. It is the unauthorised access to or control over computer network security systems for some illicit purpose.
- Social engineering is the art of manipulating people so they give up confidential information.
- Online tracking is the practice of following, recording, storing, and repackaging your browsing history and habits in order to gather insights about what you do online or sell the data to third parties

It is the art of manipulating someone to divulge sensitive or confidential information, usually through digital communication, that can be used for fraudulent purposes.

The types of information these criminals are seeking can vary, they usually trick the victim into giving them passwords or bank information or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Online Tracking

Online tracking is the practice of following, recording, storing, and repackaging your browsing history and habits in order to gather insights about what you do online or sell the data to third parties.

For further reading

https://www.techlicious.com/blog/who-is-tracking-you-online/

Hacking

It is a process in which an individual uses a variety of techniques to compromise or gain access to a digital system.

This can be a computer, mobile phone or tablet, or an entire network.

Types of Hacking

White Hat Hacking- also called ethical hacking, white hat hackers are often employed or contracted by major companies to help them improve their security by identifying vulnerabilities in their system.

Black Hat Hacking often referred to as unethical.

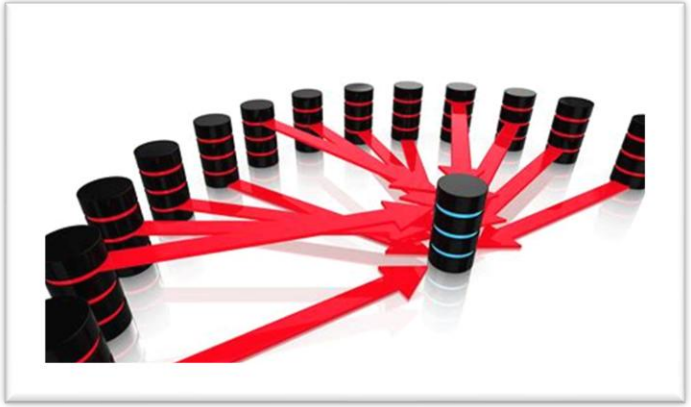
These are usually driven by personal or financial gain. They use phishing emails and compromised websites to download and install malicious software on potential victims' computers and use it to steal the victims' personal information.

Gray Hat Hacking. It lies between white and black hat

These hackers are never outright malicious, though some of their moves could be interpreted as such.

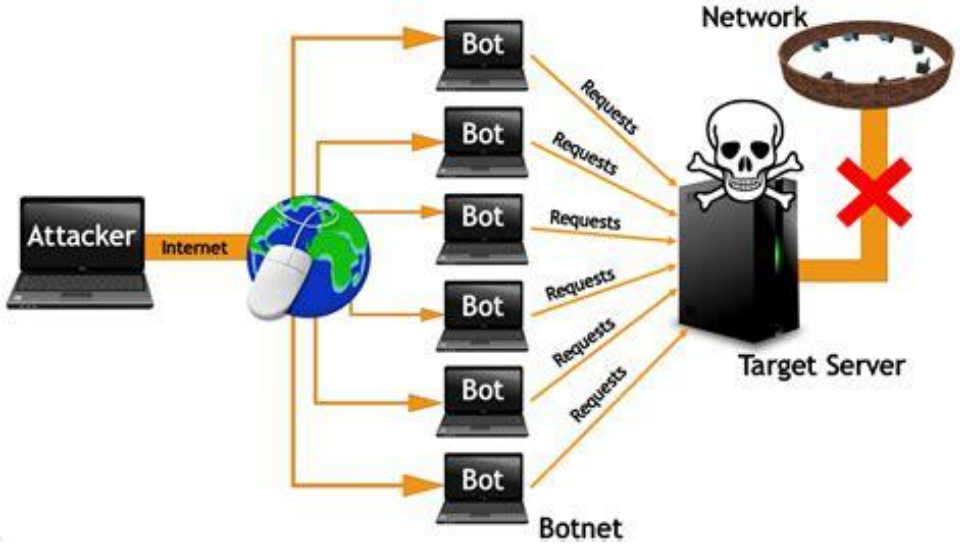
Denial of Service (DOS)

Denial of service attack (DOS) is an attack against computer or network which reduces, restricts or prevents accessibility of its system resources to authorized users.



The attack floods a network especially a network server with many requests constantly and consistently until the server crashes because it cannot cope with so many requests.

Distributed Denial of Service (DDoS) attack is an attack where multiple compromised systems simultaneously attack a single system; thereby, causing a DOS attack for the users of the target.



Physical Risks

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

The following list classifies the physical threats into three (3) main categories;

- **Internal**: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External**: These threats include Lightning, floods, earthquakes, etc.
- **Human**: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

Security Protection Measures

Antivirus

A special software that is used to find and delete malware. An anti-virus work by two methods

Virus definition a virus definition or virus signature is a known specific pattern of virus code. Once this pattern is seen by the antivirus it is deleted. Updating signature files downloads any new definition that had been added to the last update

File inoculation existing files; To inoculate a program file, the antivirus program records information such as the file size and file creation date in a separate inoculation file.

The antivirus then uses the information to detect if a virus tampers with the data describing the inoculated file.

Physical Security

It only prevent or deter user from getting physical access to the computer system.

Types of Physical security

- Locks and bolts-computer system can be kept in a locked room
- CCTV- cameras can be used to monitor who physically access a system
- Security guards/dogs- Guards are often employed as an extra level of security to help deter those users who do not have permission to access a computer system
- Cable straps
- Alarm system and video camera
- Dust covers
- Surge protectors
- UPS-(Uninterrupted Power Supply)
- Burglar bars

Protocols Secure

Secure Socket Layer

HTTPS makes use of this well-known protocol

It provides a secure environment for **online transaction and for sensitive data to be transmitted safely**. It provides encryption of all data that passes between a client and an Internet server

SSL requires the client to have a digital certificate.

Once the server has a digital certificate, the Web browser communicates securely with the client.

Web addresses of pages that use SSL typically begin with https and usually have a small padlock in the status bar

Protocols Secure

Transport Layer Security (TLS)

Works the same way as SSL but it is more secure as many security issues arose with SSL.

It is essentially designed to provide encryption, authentication and data integrity effectively

It's designed to prevent a third-party hacking into this communication.

TLS forms two layers

- ✓ **record protocol**: this part of the communication can be used with or without encryption (it contains the data being transferred over the internet).
- ✓ **handshake protocol:** this permits the website and the client (user) to authenticate each other and to make use of encryption algorithms (a secure session between client and website is established).

How do you know your computer is infected with malware or other risks

- Increased CPU usage.
- Slow computer or web browser speeds.
- Problems connecting to networks.
- Freezing or crashing.
- Modified or deleted files.
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)
- Strange computer behavior Emails/messages being sent automatically and without user's knowledge (a friend receives a strange email from you that you did not send).
- There seems to be a lot of network activity when you are not using the network.
- The available memory on your computer is lower than it should be.
- Programs or files appear or disappear without your knowledge.
- File names are changed