Data Security

Chapter 2

Malware

LEARNING OBJECTIVES

1. Understand the term malware.
   a. Recognize different ways that malware can be concealed (Trojans, rootkits, backdoors).
   b. Recognize types of infectious malware (viruses, worms).
   c. Recognize types of data theft, profit generating/extortion malware (adware, spyware, botnets, keystroke logging, dialers).
2. Protection and Resolving
   a. Understand how anti-virus software work & its limitations, and the importance of updates.
   b. Scan drives, folders, files using anti-virus software. Schedule scans using anti-virus software.
   c. Understand the term quarantine and the effect of quarantining infected/suspicious files.

WHAT IS MALWARE?

- The term malware is short for malicious software, designed to infiltrate & install itself on a computer without the owner's permission.
- The purpose of malware is to damage a computer or its content, mobile device, network or to take full or partial control over the operations.

DIFFERENT WAYS MALWARE CAN BE CONCEALED

- **Trojan –** Short for Trojan horse; is a destructive program that hide & pretend to be friendly.
  - Pretend to be any kind of file, such as a document, image, audio, video & even online games.
  - Create a backdoor for criminals.
  - Trojans can also for example, record keyboard activities, monitor Internet usage & collect personal information.

DIFFERENT WAYS MALWARE CAN BE CONCEALED

- **Rootkit –** Stealthy type of software, difficult to detect as they are activated before the operating systems.
- **Backdoors –** A method used to bypass system security, securing remote access to another device without the owner knowledge, and installing malicious software.
  - A software developer may sometimes install a backdoor for troubleshooting purposes.

TYPES OF MALWARE

- **Viruses –** Called so as they share some of the biological viruses' traits, passing from computer to computer.
  - A piece of computer code or application
  - Almost all viruses are attached to an executable file, which means that the virus may exist on the PC but it cannot infect it unless you run or open the malicious application.
  - Viruses spread through sharing files and sending emails with viruses as attachments.

TYPES OF MALWARE

- **Worms –** Similar to a virus by design and is considered to be a sub-class of a virus.
  - unlike a virus, worms has the capability to travel without any human action.
  - Worms are self-replicating malicious applications, which try to multiply as many times as possible.

TYPES OF MALWARE (Cont'd)

- **Types of Data Theft, Profit Generating/ Extortion Malware**
  - **Adware –** Short for *advertising supported software*, a free software supported by advertisement.
    - They are free to use, but require you to watch advertisements as long as the programs are open.
    - Some adware are created with malicious intent.
  - **Spyware –** When adware becomes seriously malicious it is known as spyware.
    - Spyware is usually a separate program that enters a computer as the result of installing another application.

    Technically adware and spyware are not viruses, worms, or Trojans.

TYPES OF MALWARE (Cont'd)

- **Types of Data Theft, Profit Generating/ Extortion Malware (Cont'd)**
- **Botnets –** Bot is short for Robot, which can turn the computer into a bot, also known as zombie.
  - Criminals tries to infect large numbers of computers, which form a network, or botnet also known as zombie army, in order to spread viruses and attack computers.
- **Keystroke Logging –** Can be a hardware device or small program that monitors each keystroke on a user keyboard.
  - Criminals use these programs to steal online banking passwords for instance.
  - However, it can be a useful tool for large companies to monitor user's movements.

TYPES OF MALWARE (Cont'd)

- **Types of Data Theft, Profit Generating/ Extortion Malware (Cont'd)**
- **Dialers –** Are malicious software that attempts to dial and make as many long distance calls as possible.
  - Dialers affect only computers that use modem to connect to the Internet; it modifies & changes the phone number & modem configuration, from locally charged rates, to long distance rates.
  - Fortunately, this is becoming out of fashion as old-fashioned dial-up modems are phasing out.

ANTI-VIRUS SOFTWARE

- A computer program that uses scans to detect, prevent and take action to disarm, remove or block malicious software, preferably before it infects the system.
- Anti-virus software normally uses two different techniques to accomplish this:
  - **Examining Files** to look for known malware by means of virus dictionary.
  - **Identifying Suspicious Behavior** from any computer program that might indicate infection.
  - The anti-virus can then either delete or quarantine the file.

ANTI-VIRUS SOFTWARE (Cont'd)

- Anti-Virus Limitations
  - New viruses are constantly being released.
  - To be successful, the virus dictionary must be updated at least on a weekly basis.
  - Unable to detect even old viruses, because users forget to update their virus database.
  - Frequent scans are rarely performed, which can be scheduled on a regular basis

ANTI-VIRUS SOFTWARE (Cont'd)

- **QUARANTINE FILES AND THE EFFECTS**
- When an infected file, such a virus is quarantined, it is moved to a safe location on the hard drive that is managed by the anti-virus software. It can be seen as a high-security jail for malware.
- When quarantined, a file is deleted from its original location and it cannot do any further harm.
- When removing a virus the infected file must be deleted, and since anti-viruses does not know if a file is important or not. Therefore, before deleting important files, it rather move them to a safe place and let you decide if the file must be deleted, ignored, or restored.