Chapter 2: Malware

→ Malware Definition and Function

- Malware = MALicious soFtWARE
- Purpose:
  - Infiltrate and install itself on computer/device without owner's permission
  - → Target mobile devices, networks
  - → Take full/partial control over operations
  - → Damage Computer / steal content

→ Malware concealment (إخفاء) methods

1) Trojan

- Pretends to be friendly (document, image, audio, video, games ...)
- Cannot replicate themselves
- run silently and secretly
- Create a backdoor for criminals to access system
- record keyboard activities
- monitor internet usage
- collect personal information

2) Rootkit

- Difficult to detect
- Activated before the operating systems completes booting
- Creates deep system access holes

3) Backdoors

- Bypass normal system security
- Allows remote access to malicious software
- used for troubleshooting (legitimate) or hacking (malicious)

→ Types of Malware

1) Viruses

- Piece of code or app written for damaging softwares, files, or hardwares
- Can't infect unless we run the application
- Require human action to spread

2) Worms

- Sub Class of virus
- Travel without human action
- Replicate and send itself to another computer
- Spread through email with viruses as attachement

→ Data Theft and Profit Malware

1) Adware
- Advertising supported software
- Free to use (require watching ads)
- Can be safe or malicious

2) Spyware
- When adware becomes seriously malicious
- Program that enters when installing another app
- Monitor activity on internet/ gather info about, emails, passwords, credit cards

Adware and Spyware are not viruses, worms or Trojans

3) Botnets (Robot)
- Infect large nb. of computers
- Known as zombie army
- Spread viruses and attack computers

4) Keystroke Logging
- Hardware device / Small program
- Record each keystroke made on a keyboard

5) Dialers
- Malicious software installed without user knowledge
- Attempt to dial using modem, DSL, or VoIP connection
- Become out-of-fashion

→ Anti-Virus
- Computer program that uses scans to detect, prevent and take action to disarm / remove or block malicious software.

- Detection Methods → Examining Files (using virus dictionary)
  → Identifying Suspicious Behavior

- Can delete or quarantine (isolate) infected files

- Limitations
  - ↳ New viruses released constantly
  - ↳ Virus dictionary must be updated
  - ↳ Frequent scans are rarely performed

- Quarantine Process
  1) Infected file detected
  2) Move to safe location on hard drive
  3) Managed by anti-virus software
  4) File deleted from original location