Malicious Software
Malware

- a malicious software.
- includes the program that exploits the vulnerabilities in computing system.

Purpose –

- to harm a system or steal the information from the system.
Characteristics of Malwares

- **Self-replicating:**
  - actively attempts to propagate by creating new copies, or instances, of itself.
  - may also be propagated passively, by a user copying it accidentally (not self-replication).

- **Population growth:**
  - the overall change in the number of malware instances due to self-replication.
  - Malware that doesn’t self replicate will always have a zero population growth,
  - but malware with a zero population growth may self-replicate.

- **Parasitic:**
  - requires some other executable code (including boot block code) in order to exist.
Trojan Horse

- Self-replicating: no; Population growth: zero; Parasitic: yes
- a program which purports to do some benign task, but secretly performs some additional malicious task.
  - E.g. a password-grabbing login program which prints authentic-looking “username” and “password” prompts, and waits for a user to type in the information.
  - When this happens, the password grabber stashes the information away for its creator, then prints out an “invalid password” message before running the real login program.
  - The unsuspecting user thinks they made a typing mistake and re-enters the information
Logic Bomb

- Self-replicating: no, Population growth: zero, Parasitic: possibly
- The oldest type of malicious software.
- This program is embedded with some other program.
- When certain condition meets, the logic bomb will destroy the system.
- e.g. system may crash at particular date which is fixed by attacker:

  E.g. legitimate code:
  
  ```python
  if date is Friday the 13th:
    crash_computer
  ```

  legitimate code

- Or, if some antivirus trying to delete or clean the logic bomb. The logic bomb will destroy the pc.
Back Door or Trap Door

- Self-replicating: No, Population growth: zero, Parasitic: possibly
- any mechanism which bypasses a normal security check.
- can be placed into legitimate code or be standalone programs
- e.g.
  - username = read_username()
  - password = read_password()
  - if username is “133th4ck0r”: return ALLOW_LOGIN
  - if username & password are valid: return ALLOW_LOGIN
  - Else: return DENY_LOGIN

- One special kind of back door is a RAT, which stands for Remote Administration Tool or Remote Access Trojan, depending on who’s asked
  - These programs allow a computer to be monitored and controlled remotely;
Virus

- Self-replicating: yes, Population growth: positive, Parasitic: yes
- A malware, when executed, tries to replicate itself into other executable code;
  - when it succeeds, the code is said to be infected.
  - The infected code, when run, can infect new code in turn.
  - This self-replication into existing executable code is the key defining characteristic of a virus.

Types of Virus

- Parasitic virus:
  - Traditional and common virus.
  - will be attached with EXE files and search for other EXE file to infect them.
- Memory Resident Virus:
  - Present in your system memory as a system program.
  - from here onwards it will infects all programs that execute.
- Boot Sector Virus:
  - Infects the boot record and spread when the system is booted from the disk containing the virus.
- Stealth Virus:
  - virus hides itself from detection of antivirus scanning.
**Worm**

- Self-replicating: yes, Population growth: positive, Parasitic: no
- shares several characteristics with a virus
- worms are self-replicating too, but self-replication of a worm is distinct from virus in two ways:
  - worms are standalone, and do not rely on other executable code.
  - worms spread from machine to machine across networks.

**Zombies**

- Computers that have been compromised can be used by an attacker for a variety of tasks, unbeknownst to the legitimate owner;
- most common tasks for zombies are sending spam and participating in coordinated, large-scale denial-of-service attacks.
**Rabbit**

- Self-replicating: yes, Population growth: zero, Parasitic: no
- Rabbit is the term used to describe malware that multiplies rapidly. Also called bacteria
- Two kinds of rabbit:
  - First kind, a program which tries to consume all of some system resources, like disk space.
    - A “fork bomb,” a program which creates new processes in an infinite loop, is a classic example of this kind of rabbit.
    - Tends to leave painfully obvious trails pointing to the perpetrator, and are not of particular interest.
  - Second kind of rabbit is a special case of a worm.
    - A standalone program which replicates itself across a network from machine to machine,
    - But deletes the original copy of itself after replication.
    - In other words, there is only one copy of a given rabbit on a network; it just hops from one computer to another.
- Rabbits are rarely seen in practice.
Spyware

- Self-replicating: yes, Population growth: zero, Parasitic: no

- A software which collects information from a computer and transmits it to someone else.

- The exact information spyware gathers may vary, but can include anything which potentially has value e.g.
  - Usernames and passwords.
    - might be harvested from files on the machine, or by recording what the user types using a key logger.
    - A keylogger differs from a Trojan horse in that a keylogger passively captures keystrokes only; no active deception is involved.
  - Email addresses, which would have value to a spammer.
  - Bank account and credit card numbers
  - Software license keys, to facilitate software pirating
Adware

- Self-replicating: no, Population growth: zero, Parasitic: no

- similar to spyware in that both are gathering information about
  - the user and their habits.

- more marketing-focused, and may pop up advertisements or redirect a user’s web browser to certain web sites in the hopes of making a sale.

- Some adware will attempt to target the advertisement to fit the context of what the user is doing.
  - for example, a search for “Calgary” may result in an unsolicited pop-up advertisement for “books about Calgary.”

- Adware may also gather and transmit information about users which can be used for marketing purposes.

- As with spyware, adware does not self-replicate.