Malicious Software

- Malware: malicious software that exploit system vulnerabilities
- Two categories: those that need a host program and those that are independent (parasitic)
- May or may not replicate

Malicious Programs

- **Backdoor**: secret entry point into a program that allows someone to gain access. A **maintenance hook** is a backdoor inserted by a programmer to aid in testing and debugging.
- **Logic Bomb**: code embedded in a program that is set to go off when certain conditions are met.

Malicious Programs

- **Trojan Horse**: use program or command procedure that contains hidden code that when invoked performs some unwanted or harmful procedure. These may also be used for data destruction.
- **Mobile Code**: programs that can be shipped unchanged to a heterogeneous collection of platforms and execute identical semantics.

Malicious Programs

- **Viruses**: software that can *infect* other programs by modifying them. The infection may be passed onto other programs.
- Virus has three parts:
  -Infection mechanism
  -Trigger
  -Payload

Virus Phases

- **Dormant Phase**: virus is idle.
- **Propagation Phase**: virus places an identical copy of itself on other programs, each program will then place a copy into other programs
- **Triggering Phase**: virus is activated to perform the function for which it was intended.
- **Execution Phase**: the function is performed.

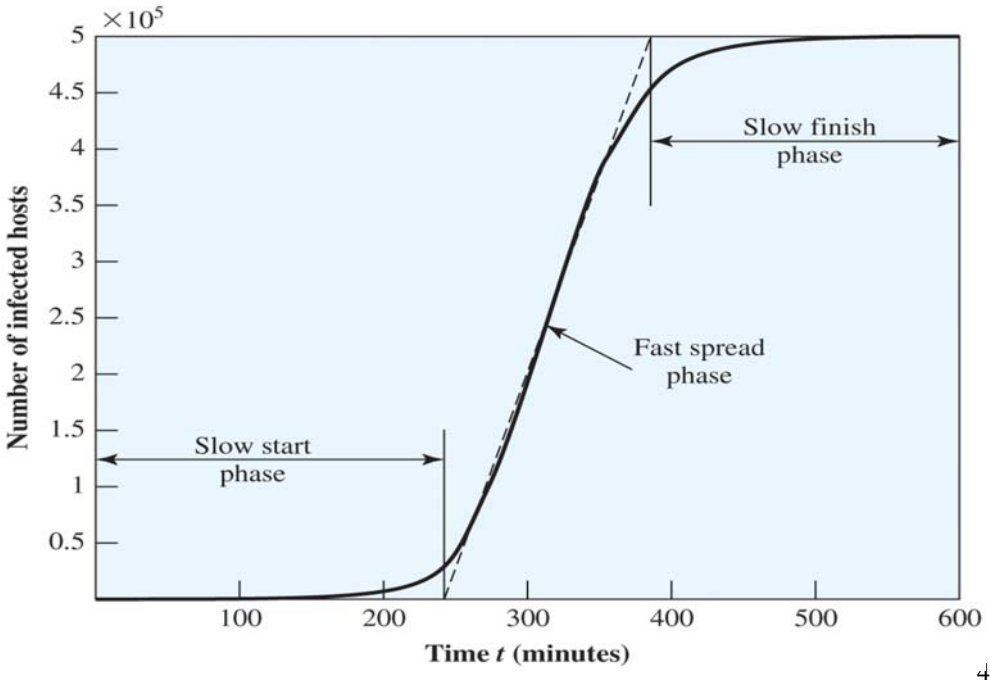
Virus Classifications

- By Target
  -Boot Sector Infector
  -File Infector
  -Macro Virus
- By Concealment Strategy
  -Encrypted Virus
  -Stealth Virus
  -Polymorphic Virus
  -Metamorphic Virus

Worms

- Worms replicate themselves and send copies from computer to computer across a network connection to perform some unwanted function.
- A network worm may also attempt to determine if a system has previously been infected before copying itself.

Worm Propagation Model



State of Worm Technology

- Multiplatform
- Multiexploit
- Ultrafast spreading
- Polymorphic
- Metamorphic
- Transport Vehicles
- Zero-day exploit

Bots

- Also know as a zombie or drone
- Program that secretly takes another Internet-attached computer, then uses it to launch attacks that are difficult to trace
- A **botnet** is a collection of bots capable of coordinating attacks

Uses of Bots

- Distributed denial-of-service attacks
- Spamming
- Sniffing traffic
- Keylogging
- Spreading new malware
- Installing advertisement add-ons and browser helper objects
- Attacking IRC chat networks
- Manipulating online polls/games

Constructing a Network Attack

- Software to carry out the attack must be able to run on a large number of machines and remain concealed
- The attack must be aware of a vulnerability that many system administrators have failed to notice
- A strategy for locating vulnerable machines must be implemented. This is known as **scanning** or **fingerprinting**.

Scanning Strategies

- Random
- Hit List
- Topological
- Local subnet