**CHAPTER 5: MALICIOUS SOFTWARE**

1. Malware
2. Overview
   * + - 1. Types
     + Need a host program
     + Independent, self-contain
     + Sophisticated threat
       - 1. Terms
3. Virus
4. Features
   * + Modify programs to include virus
     + Execute automatically when the program run
     + Taking advantages of OS weaknesses & vulnerabilities
       - 1. Phases of operation
     + Dormant,
     + Propagation,
     + Triggering,
     + Exec
       - 1. Structure
     + Components (infection mechanism, Trigger, Payload)
     + Prepended/Post-pended/Embedded
       - 1. Categories
     + Parasitic
     + Memory-resident
     + Macro
     + Boot sector
     + Polymorphic
5. Worms
   * + What is worm?
     + Morris worm
     + Others
     + State of worm technology
6. Malware prevention & detection approaches
   * + Approaches (Prevention, Detection, Removal)
     + Generation of AV software
7. Modern Malware

Advanced capabilities

Malware in the past

Modern Malware

1. Botnet
   1. Bot & Botnet
   2. Botnet Command & Control (C&C)
   * Mechanism
   * Problem
   1. Botnet C&C Design
   2. DNS based botnet C&C
   3. How to detect & stop botnet C&C
2. APT
3. Malware Analysis
   * + 1. Goal
       2. Techniques (Static, Advanced)
       3. Basic Static Analysis
       4. Basic Dynamic Analysis

Review questions

1. What are three broad mechanisms that malware can use to propagate?
2. What characteristics of an advanced persistent threat give it that name?
3. What are typical phases of operation of a virus or worm?
4. What is the difference between machine executable and macro viruses?
5. What means can a worm use to access remote systems to propagate?
6. What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware?
7. Malware analysis techiques?