Lecture 16: Anti-Malware Programs

Date: October 25, 2013

Homework Due: Nov. 1 at 5:00pm
Midterm: Nov. 4 *in class*

1. Midterm: questions, review
2. Review of types of malware
   a. Trojan horses
   b. Computer viruses
      i. Stealth
      ii. Encrypted
      iii. Polymorphic
      iv. Metamorphic
   c. Computer worms
   d. Bacteria, rabbits
3. Signature detection
   a. What a signature is: hash, patterns
   b. How to look for it
   c. When to look for it: at boot time, on file open, at execution
   d. Scanning disks
4. Behavioral analysis
   a. Execute in contained environment
   b. Simulate execution