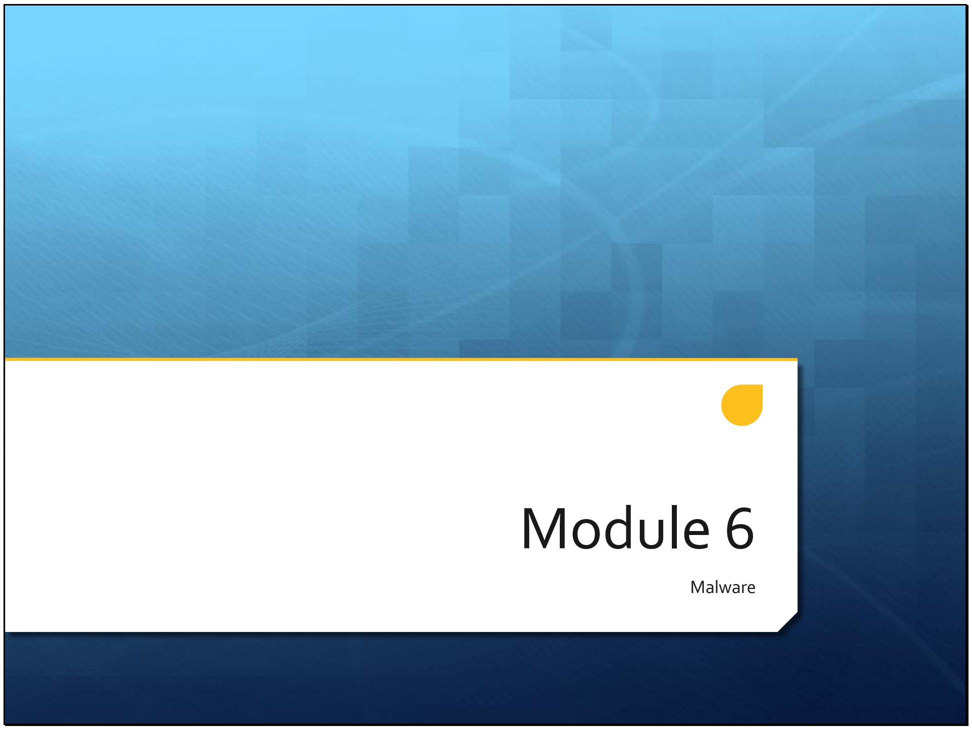
Security Awareness

Module 06 – Malware

WORKBOOK

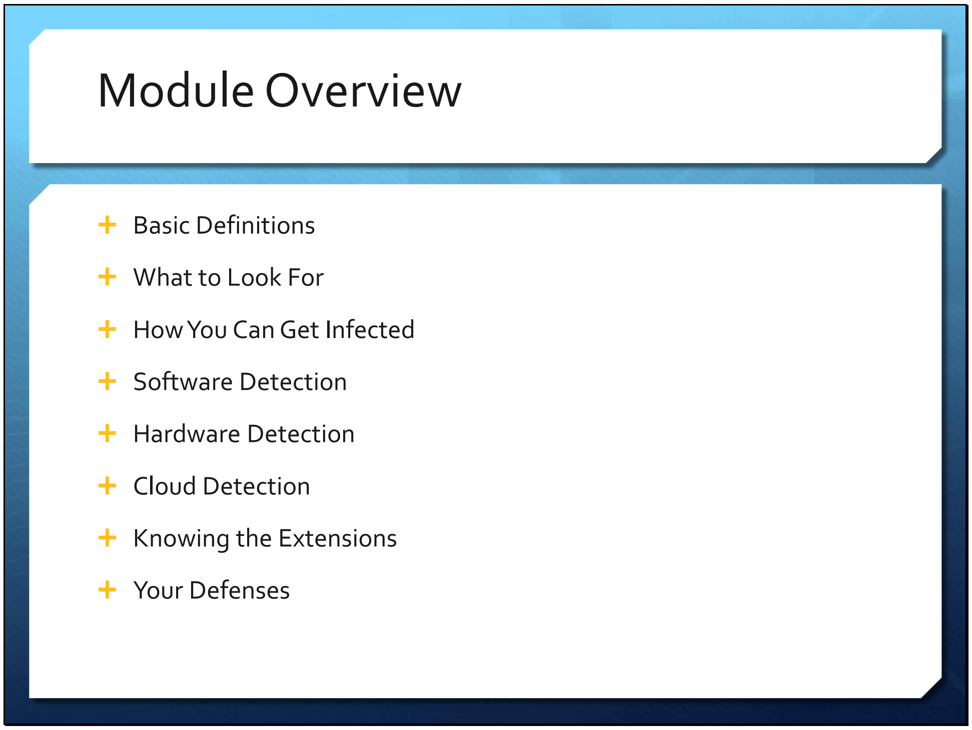
Slide 1



Module 6

Malware

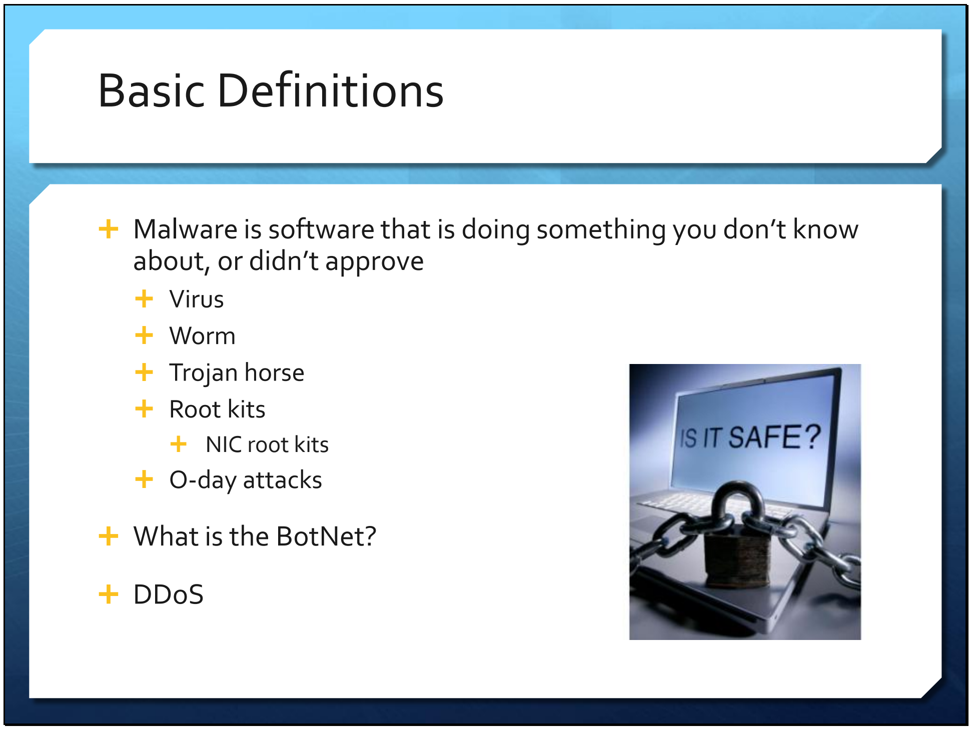
Slide 2



Module Overview

- Basic Definitions
- What to Look For
- How You Can Get Infected
- Software Detection
- Hardware Detection
- Cloud Detection
- Knowing the Extensions
- Your Defenses

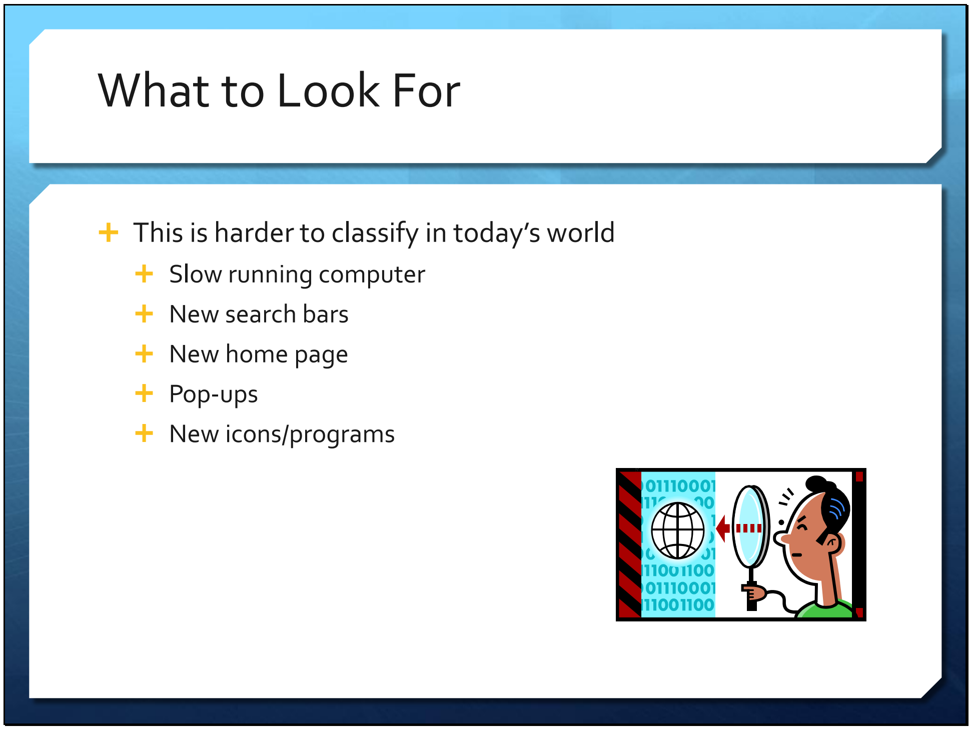
Slide 3



Basic Definitions

- Malware is software that is doing something you don't know about, or didn't approve
  - Virus
  - Worm
  - Trojan horse
  - Root kits
    - NIC root kits
  - O-day attacks
- What is the BotNet?
- DDoS

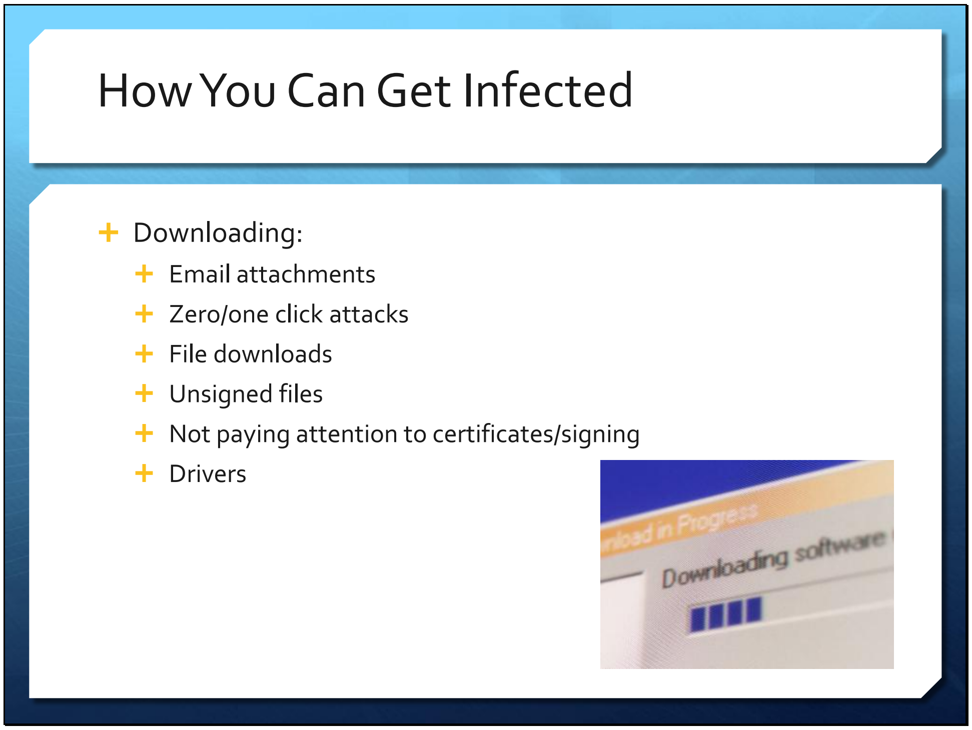
Slide 4



What to Look For

- This is harder to classify in today's world
  - Slow running computer
  - New search bars
  - New home page
  - Pop-ups
  - New icons/programs

Slide 5

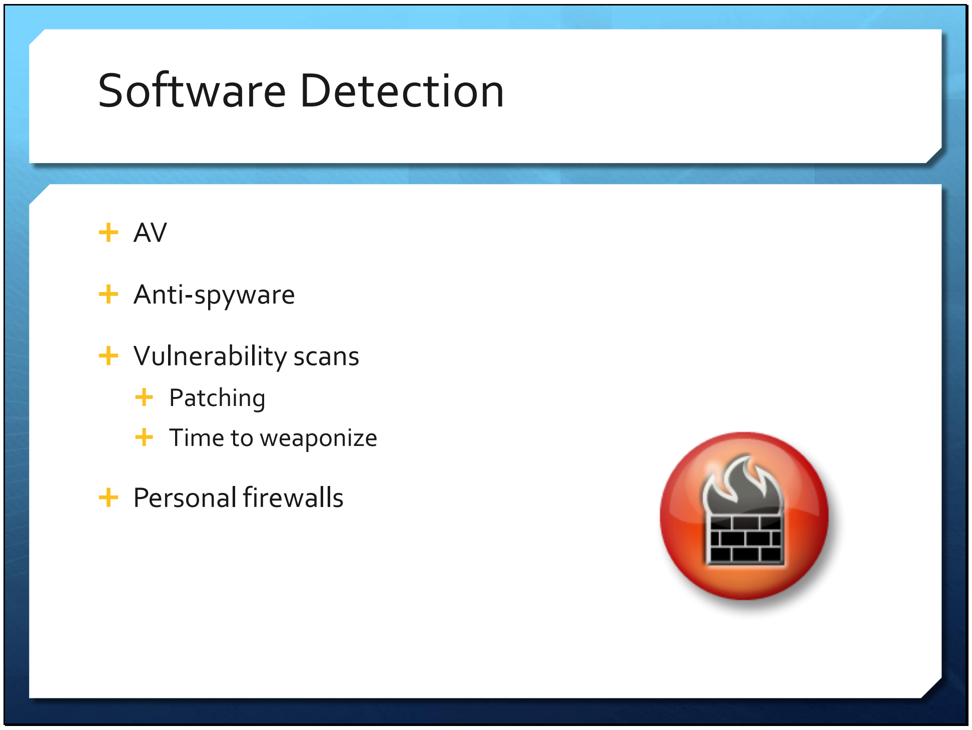


How You Can Get Infected

- Downloading:
  - Email attachments
  - Zero/one click attacks
  - File downloads
  - Unsigned files
  - Not paying attention to certificates/signing
  - Drivers

nload in Progress
Downloading software

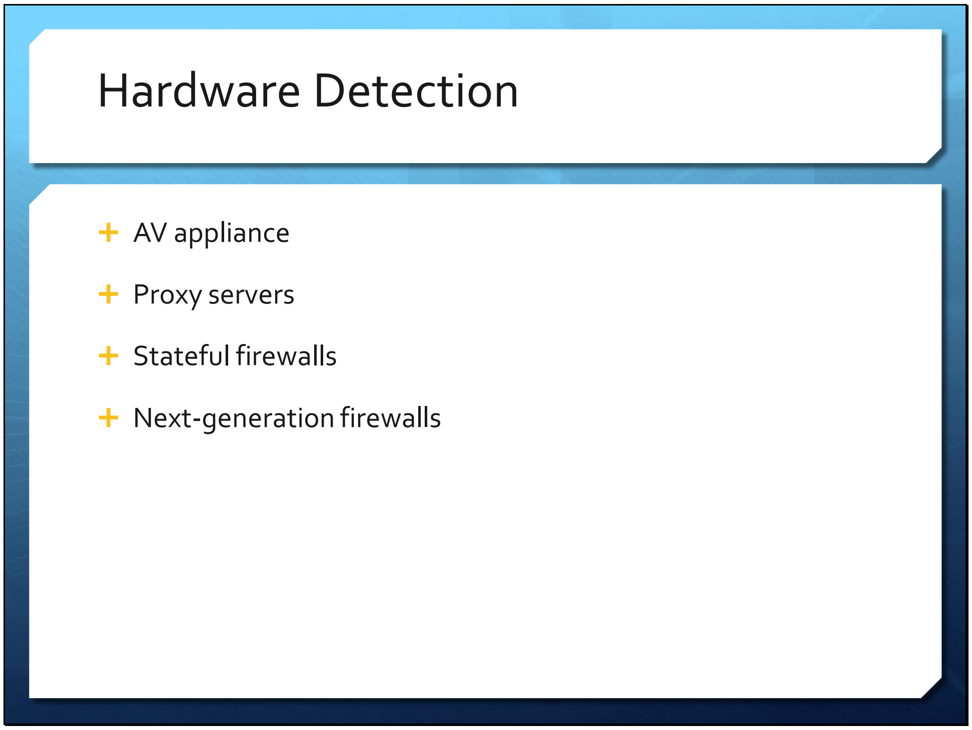
Slide 6



Software Detection

- AV
- Anti-spyware
- Vulnerability scans
  - Patching
  - Time to weaponize
- Personal firewalls

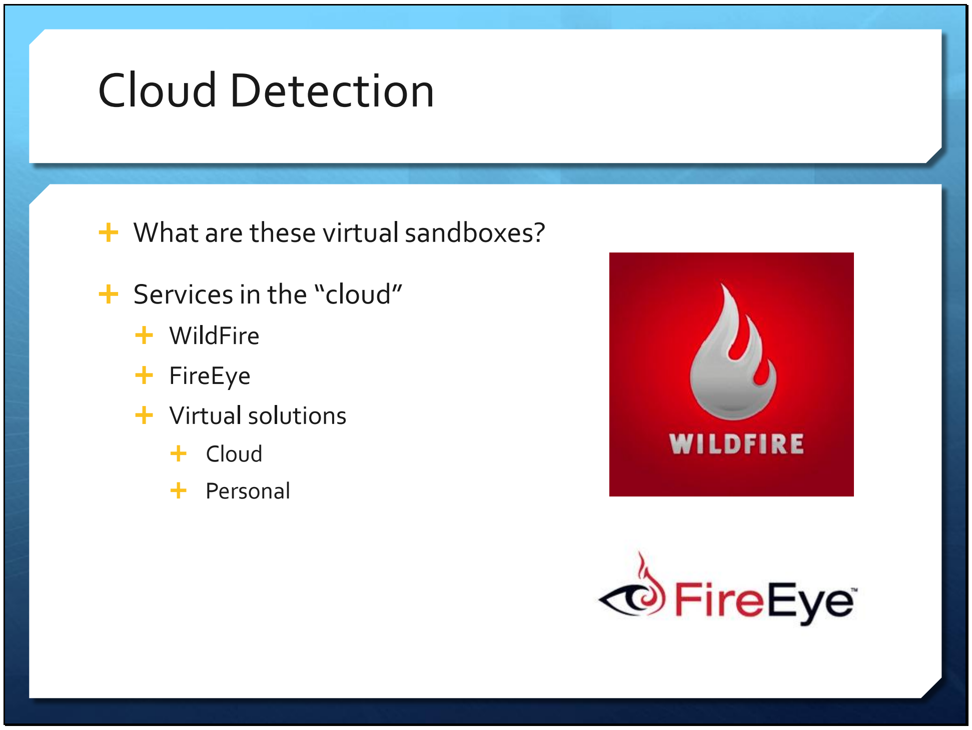
Slide 7



Hardware Detection

- AV appliance
- Proxy servers
- Stateful firewalls
- Next-generation firewalls

Slide 8

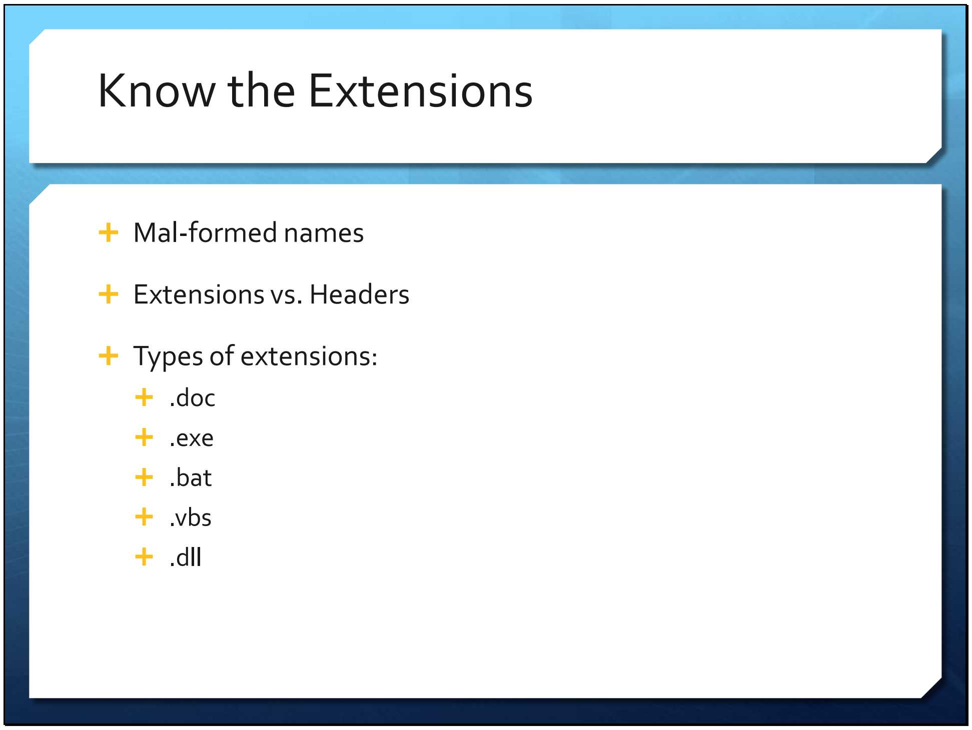


Cloud Detection

- What are these virtual sandboxes?
- Services in the "cloud"
  - WildFire
  - FireEye
  - Virtual solutions
    - Cloud
    - Personal

WILDFIRE
FireEye

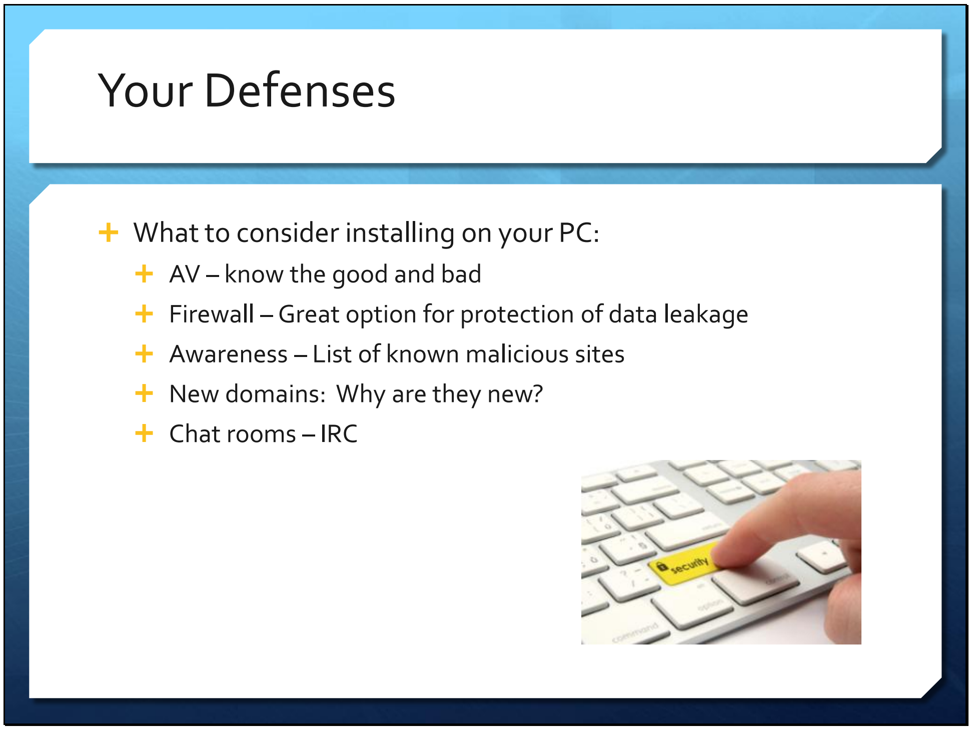
Slide 9



Know the Extensions

- Mal-formed names
- Extensions vs. Headers
- Types of extensions:
  - .doc
  - .exe
  - .bat
  - .vbs
  - .dll

Slide 10



Your Defenses

- What to consider installing on your PC:
  - AV – know the good and bad
  - Firewall – Great option for protection of data leakage
  - Awareness – List of known malicious sites
  - New domains: Why are they new?
  - Chat rooms – IRC

QUESTIONS and ANSWERS

Review Questions:

1. What type of malware can propagate itself?
    A. Virus
    B. Worm
    C. Trojan horse
    D. Bot net

2. What type of malware attaches itself to a host in order to be spread from system to system?
    A. Virus
    B. Worm
    C. Trojan horse
    D. Bot net

3. What type of malware disguises itself as a helpful or wanted program?
    A. Virus
    B. Worm
    C. Trojan horse
    D. Bot net

4. Malware that is unknown to vendors or inspection mechanisms is referred to as what?
    A. Virus
    B. Worm
    C. Trojan horse
    D. 0-day

5. Which of the following methods could be used to deliver malware?
    A. E-mail
    B. Zero-click attacks
    C. File downloads
    D. All of the above

6. What type of firewall can give you visibility to all of the traffic, including which applications are running?
    A. Statefull
    B. Packet filter
    C. Proxy server
    D. Next-generation

Answer Key:

1. B
   A worm can "crawl" or propagate itself to other victims.

2. A
   A virus attaches itself to a file, which is then spread by the distribution of that file.

3. C
   A Trojan horse is known as a way of disguising malware as a usually helpful program.

4. D
   0-day is malware that a vendor doesn't know about, or has no signature to detect it.

5. D
   All of these methods could deliver malware onto your system.

6. D.
   A next-generation firewall is capable of looking into the data layer of the packets and can determine the applications that are running.