

## Types

### Virus

Program borne by a disk or file which replicates  
Attaches to files, memory, boot or partition sector, or registry

#### Classification: how spread

Boot sector, loads with OS, spreads by infecting disks  
File infector adds itself to programs  
Macro spreads from infected Office type files using scripts  
Multi-partite may use multiple means

#### Classification: how they hide

Armored hide intent  
Polymorphic changes each time it spreads  
Stealth  
Companion appears to run from a different file

### Worms

Replicated on the same computer, or over a network  
Spread by buffer overflow, port flooding, and compromised passwords  
Many open back doors to allow computer access

### Trojan Horse

Usually resides in a desirable program  
May open back doors

### Common locations from which loaded

Autoexec.bat or inittab  
initialization scripts or ini files  
Bootloaders  
Kernel

## Methods

### Executable methods

Exe com bat  
Bin cgi pl

### Boot and Partition sector Methods

Formatting creates MBR, which starts loading the OS by directing to partition, then boot loader  
Fix with fdisk or fixmbr

### Macro Methods

Infect templates, spread when macro run  
Disabled by default  
Digital signatures

### eMail methods

attachments

### Software Exploitation

Network  
Database  
Buffer overflow

### Spyware

Cookie snarfing

---

## Protecting the OS

Watch boot process  
Updates: patches, service packs  
Digital signatures /Scanners: locate, remove, inoculate  
Backup and Repair/Policies p. 74