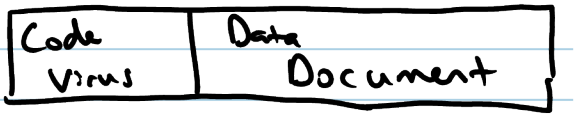
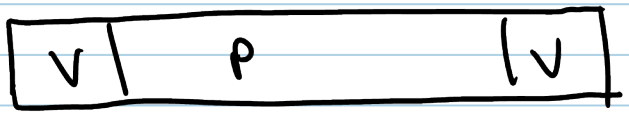
Malware Terminology & Basics

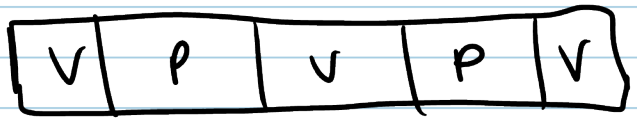
Thursday, July 25, 2013
9:05 AM

Terminology
- Virus
- Worm
- Trojan Horse
- Logic Bomb
- Time Bomb
- Trapdoor / Backdoor
- Rabbit
- Web Bug

Virus: usually embed their code into a document or program







Also can locate themselves in protected portions of memory, but need to have a way to run again if the machine reboots (memory resident malware)

"Boot Sector"
portion of hard drive / USB drive used to load OS

Anti-Virus & Anti-Malware Software
Can look at both disk files & memory
limitation: mostly looks for known malware w/ its signature database
"zero day" attacks are hard for it to detect