Malware Terminology & Basics

Terminology

Virus
Worm
Trojan Horse
Logic Bomb
Time Bomb
Trap door / Backdoor
Rabbit
Web Bug

Viruses usually embed their code into a document or program:

\[ \text{Virus} \quad \text{Program} \quad \text{Code} \quad \text{Document} \]

\[ V | P | V \]

\[ V | P | V | P | V \]

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