Malicious Software:

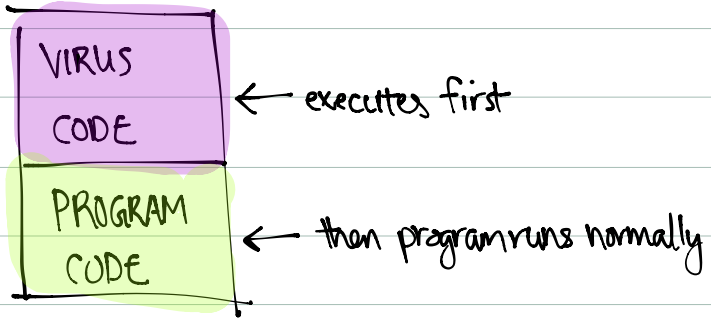
- software with malicious intent
- needs to be executed to do harm

↳ can run by:

- email
- Removable media
- web page
- exploiting buffer overflows

Viruses

- infects other files
  - do not only infect executables, also documents as well
- when virus runs, it tries to infect other files



- To infect host, virus duplicates itself to top of other programs
- copy itself as a macro to documents

Virus Code:

- Try to infect other programs
- may infect host operating system

↳ add itself to startup / boot sector
- evade detection } later
- execute payload }

Worm spreads on its own - Virus requires user action to spread

Virus - needs a host program / file

Payload
- To evade detection by disabling anti-virus
- actual malicious activity

Virus History
- Initial viruses were proof-of-concepts
- 1980s - removable storage
↳ boot sector viruses

Kenzero
- 2010
- Spread through P2P
- ransomware

Flame
- 2012
- toolkit

- cyber espionage
- related to Stuxnet