The first anti-virus softwares (end of 80's)

Virus scanner (detection)

- Signature based -
  Using a signature database of existing viruses
- Behavior based
  Looking for suspicious code patterns that can be used by viruses

Virus removal tools (sanitation)

- Cleaning the memory and the filesystem

Avoiding detection

Cascade (1987)

- The virus encrypts itself with a cryptographic key and changes this key when replicating itself

✓ Each instance of the virus does not look the same

➡ This is the emergence of polymorphic viruses