Infection Vector

How the malware infects the system?

Social Engineering (the most common vector)

- Trick or convince the user to install the malware on the system

Credential Stuffing

- Use stolen credentials to get legitimate access to systems

Exploit

- Exploit a vulnerability on the system

Macros

- Embed malicious code into office documents

Supply Chain Attack

- Infect software libraries that will be embedded with software

Persistence Mechanism

How malware sticks to the system?

- Depends on the targeted system
  - **Windows** : registry keys, scheduled tasks, *DLL* hijacking, system services
  - **Linux** : cron jobs, *systemd* services, `LD_PRELOAD` tricks
  - **MacOS** : *LaunchAgents*