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*

Exfiltration and Control

How the malware can be exfiltrate data and/or be controlled remotely?

You either need

- **Data Exfiltration Channel** for a spyware (unidirectional)
- **Command & Control (C2)** for a bot (bidirectional)

- The goal is to prevent traffic from being detected
  - HTTP, SMTP, DNS tunneling
  - SSH tunnels, TOR
  - Remote drive, *Github*, *PasteBin*, *Twitter*, *Youtube*, *Reddit*
  - *Slack* Bots, *Telegram* bots, *Discord* WebHooks
  - Web3 (blockchain)