# 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)

# How to detect malware? 2 techniques

1. **Static Analysis**

➡ Scan program comparing it to a collection of signatures

2. **Dynamic Analysis**

➡ Run program in a sandbox and infer from its behavior

✓ See *Yara* Rules
https://yara.readthedocs.io/en/latest/