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 analyze malware?

➡ Understand what a program does by looking at system calls, library calls, IO operations and so on

Two complementary approaches:

1. **Static Analysis**
   Analyze binary code and infer its behavior (control flow and data flow approaches)

2. **Dynamic Analysis**
   Run program in a sandbox and observe its behavior