

# Type of adversaries

## **Cybercrime-as-a-Service**

- The goal is to compromise machines at a large scale, build a botnet and rent such capability

## **Cybercrime Groups**

- The goal is to monetize attacks using ransomware, cryptominers and infostealers

## **Nation-State Groups**

- The goal is to infect targeted systems and remain undetected
- Often advanced and coordinated attacks

# **Payload** - What the malware do?

## **Backdoor**

- Allows the attacker to take control of a system

## **Wiper**

- Destroys data and take down services

## **Ransomware**

- Encrypts data and ask for a ransom paid in crypto

## **Cryptominer**

- Runs crypto-mining bots

## **Spyware** (including **keyloggers** and **infostealers**)

- Key logging, credential harvesting, file stealer, screen & camera capture, browsing monitoring, geo tracking,