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,

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