

Anatomy of Modern Malware

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 info stealers

Nation-State Groups

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