How antiviruses 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

Malware Crypter

- Encryption
- Code obfuscation
- Stealth mode to detect and bypass sandbox