How antiviruses detect malware? 2 techniques

1. **Static Analysis**

➡ Scan program comparing it to a collection of signatures

How to bypass it ? encryption and code obfuscation

2. **Dynamic Analysis**

➡ Run program in a sandbox and infer from its behavior

How to bypass it? detect the sandbox environment and employ trigger based behaviors

DIY packing - make the code undetectable yourself

Pro

- ➡ Free
- ➡ Personalized

Cons

- ➡ Time consuming
- ➡ Requires good expertise of cryptography, code obfuscation and execution environment