

# How to create a new malware? 3 step process

1. Create the malware's payload

**2. Make the malware undetectable  
a.k.a packing a malware**

3. Spread the malware

# 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