How to 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

✓ See *Yara* Rules
https://yara.readthedocs.io/en/latest/

Evasion Technique - How the malware stays undetectable and/or hard to analyze?

Living-Off-The-Land (LOLbins)

- Reuse legitimate tools for payload, exfiltration and C2

Malware Packing

➡ The goal is to evade common detection techniques

- Encryption
- Code obfuscation
- Rewrite engines
- Stealth mode to detect and bypass VMs and sandboxes

Generative AI (newest trend)

- Use AI to dynamically generate payload or rewrite itself