How to automate malware analysis?

➡ Anti-malware tools combine static and dynamic analysis but use different approaches to make a decision

- **Signatures**
  Detect based on signatures database (known patterns)
  See *Yara* rules: https://yara.readthedocs.io/en/latest/

- **Machine learning**
  Detection based on similarities with a collection of known malware

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