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

[Bonus] A Malware Story (2014)