Anti-virus Evasion

Overview of how to develop Trojans that can evade AVs

Problems with Anti-virus for malware developers

- Virustotal or any online scanner will have copy of your sample and may eventually tag it as malware
- Windows Defender or locally installed AV will quarantine your sample

The solution

- Use Yara

Where to get Yara?

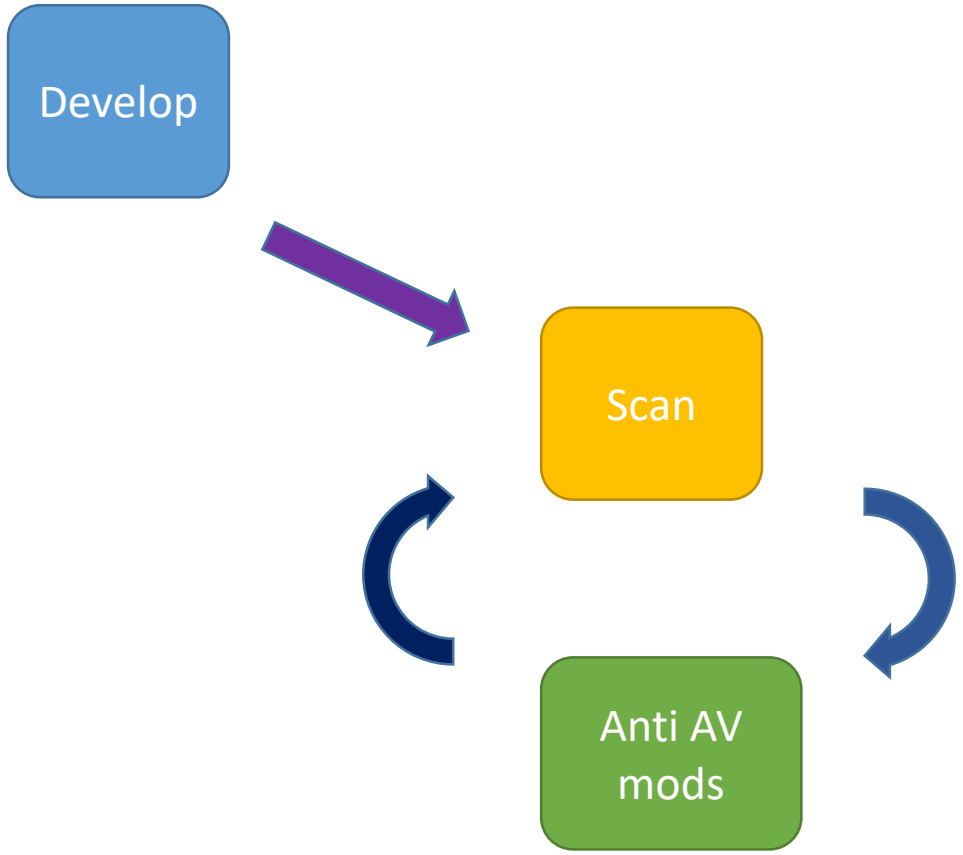
- Download yara:

  https://virustotal.github.io/yara/

Download yara rules:

https://github.com/Yara-Rules/rules

Trojan development Life Cycle



Anti-virus evasion techniques (Anti-AV Mods)

- Function hiding
- Encryption of string parameters, or, payload bytes
- Encoding of string parameters, or, payload bytes

Thank you