Malware Analysis

Introduction to Packers/Crypters

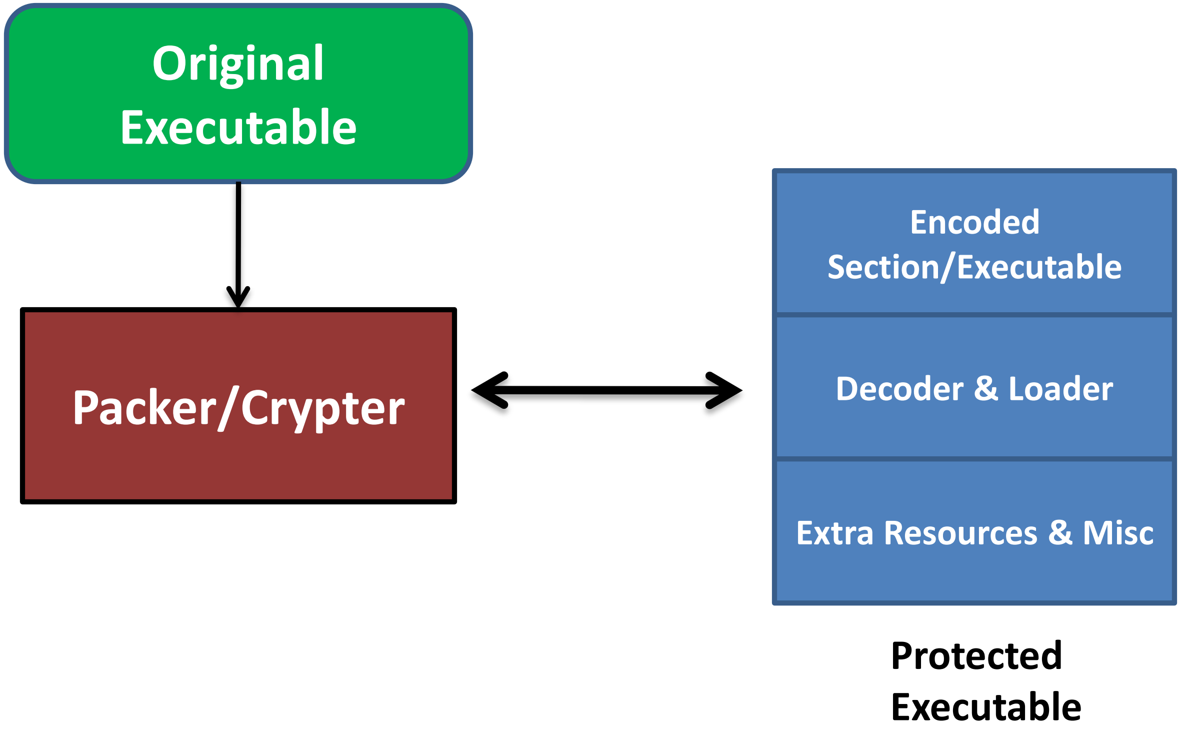
AV Technology

- Signature based
- Hash Based
- Behavior Based
  - HIPS
- Community Based
  - Reputation
  - Symantec Online Network for Advanced Response (SONAR)

A Packer/Crypter Role

- **Compress**
  - UPX
- **Protect**
  - VMProtect
- **Obfuscate** (AV Evasion)
  - Online-Crypter.com
- **Package**
  - WinRAR SFX
- **Licensing & Enforcement**
  - Themida
- …

A Typical Packers/Crypters



Original Executable

Packer/Crypter

Encoded Section/Executable

Decoder & Loader

Extra Resources & Misc

Protected Executable

- Decode original executable/sections.
- Map original executable.
- Process/Build IAT
- Process Relocation
- Transfer Control

Packer Functional Components

- Encryption/Encoding Algorithm
- Runtime Executable Loader
  - In-Memory Exec
  - Process Shuttle (LoadPE)
- Protection Engine
  - Code Obfuscator
  - Anti-Debugger
  - Anti-VM
  - Anti-Decompilation

Packers/Crypters

- UPX
- **ASPack**
- Armadillo
- Themida
- VMProtect
- …

Lets Get Real..

HANDS-ON