Packers

Packers and Packed Files

PACKER

Program that takes a target file as input, modifies it, and puts it into a software envelope, the stub

PACKED FILE

Consists of a stub and the compressed or encrypted target file. The stub is responsible for decrypting/decompressing the target file, loading it and running it in memory.

Types of Packers

COMPRESSOR

- purpose: shrink size
- legitimate packers (UPX)
- compress file

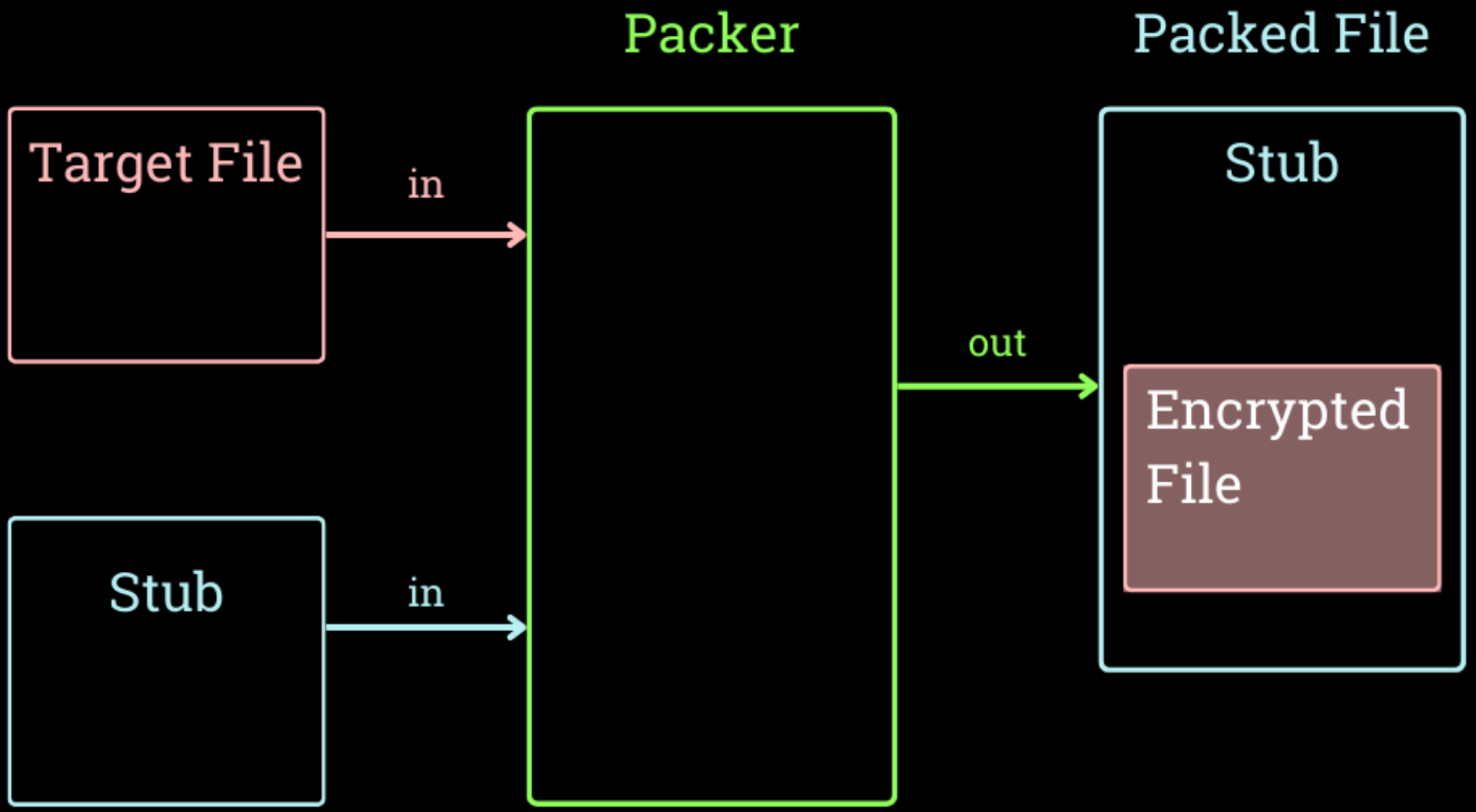
CRYPTER

- purpose: evade antivirus
- malware packers
- encrypt file

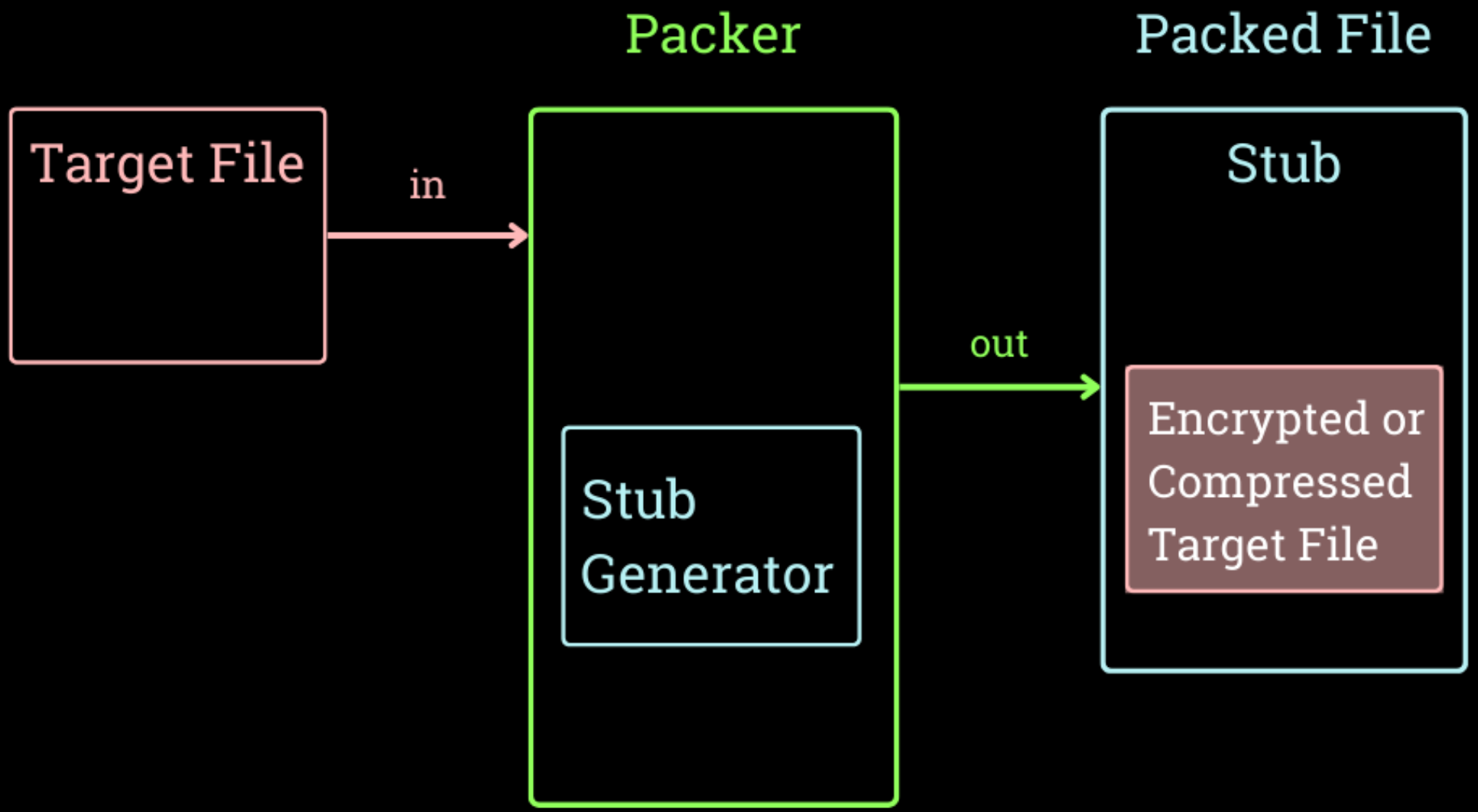
PROTECTOR

- purpose: prevent reverse engineering
- usually legitimate packers (VMProtect)
- compress & encrypt, or virtualize

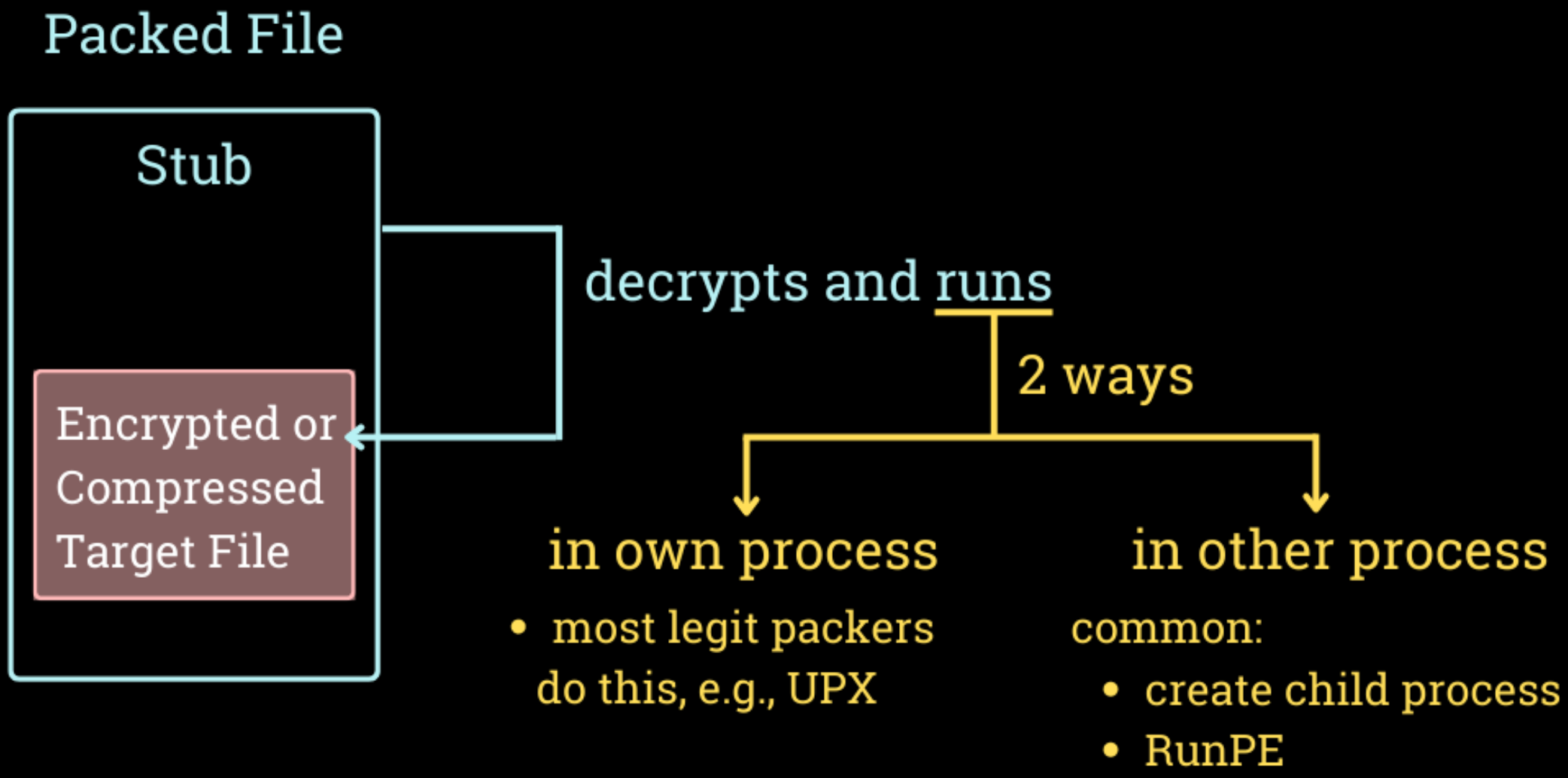
PACKING


Packer
Packed File
Target File
in
Stub
Stub
Encrypted File
in
out

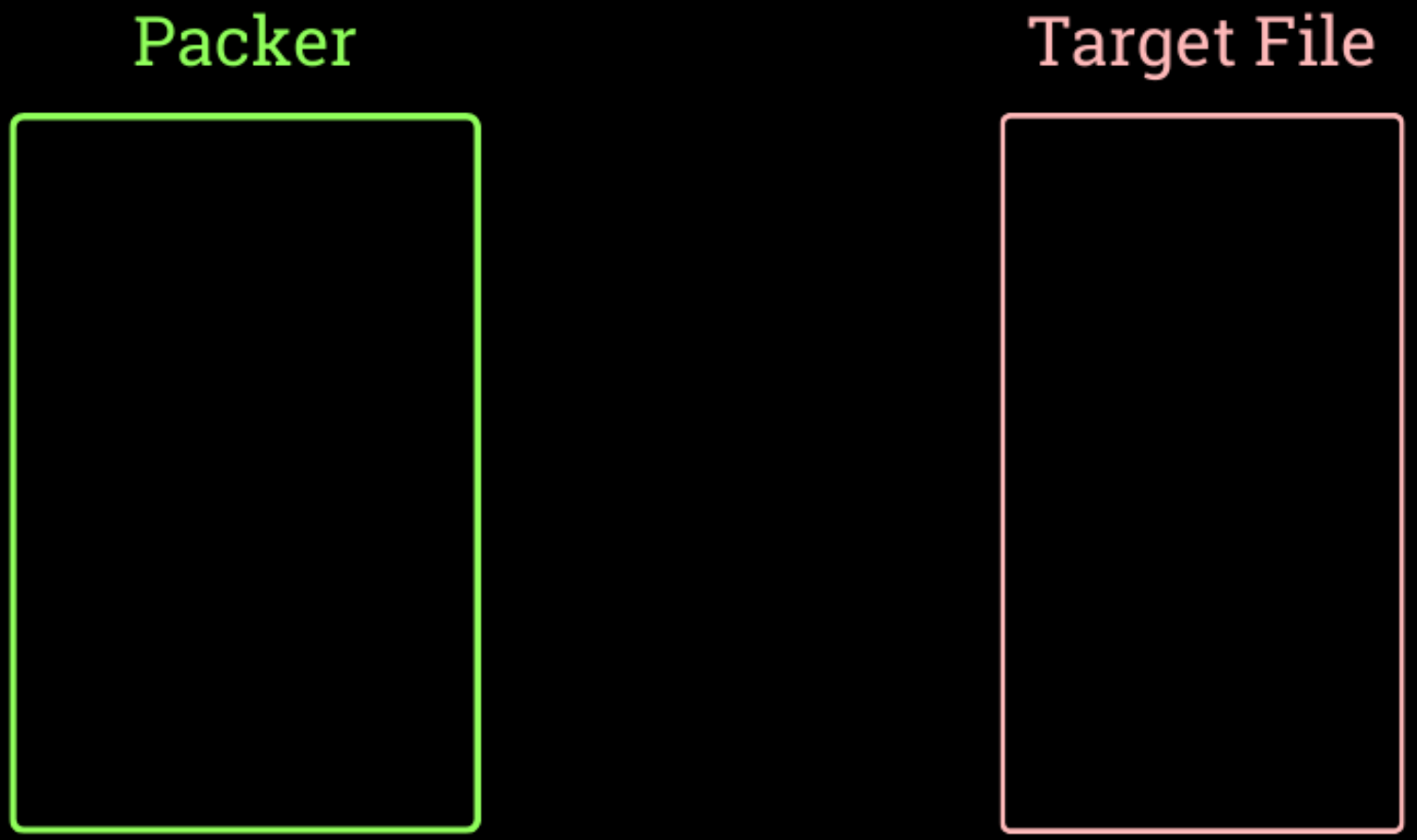
PACKING


Packer
Packed File
Target File
in
Stub
Generator
out
Stub
Encrypted or
Compressed
Target File

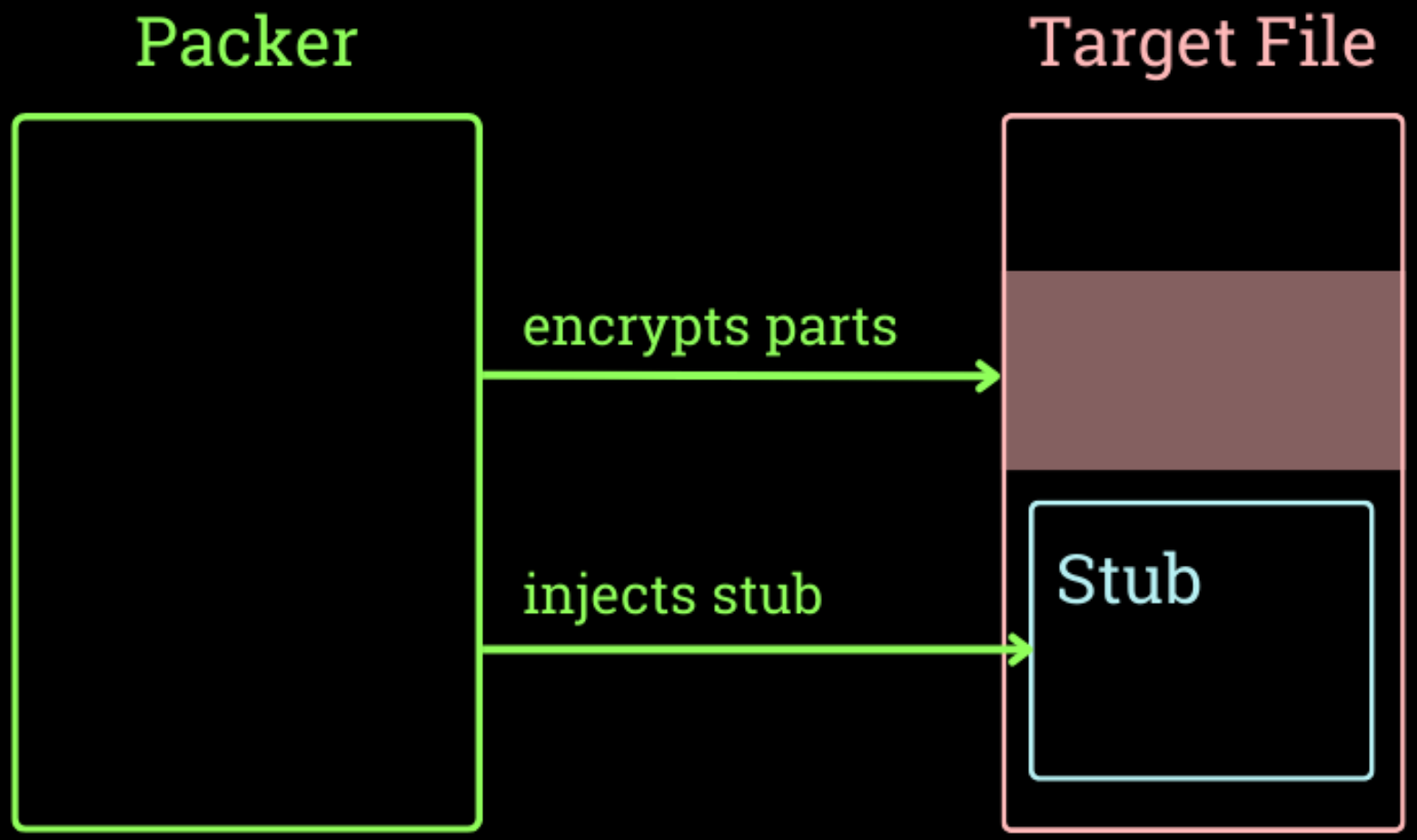
PACKED FILE AT RUNTIME



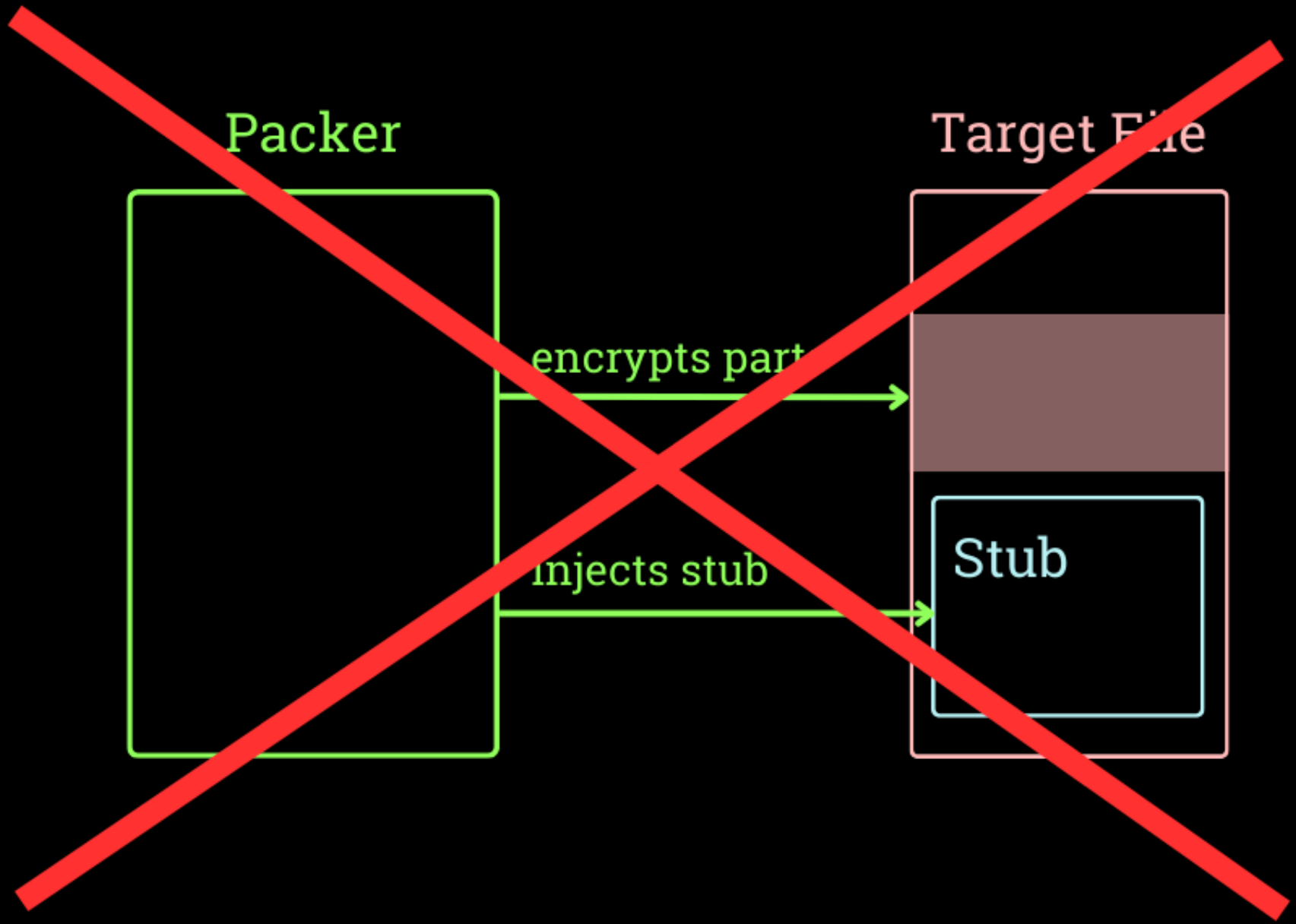
MISCONCEPTION



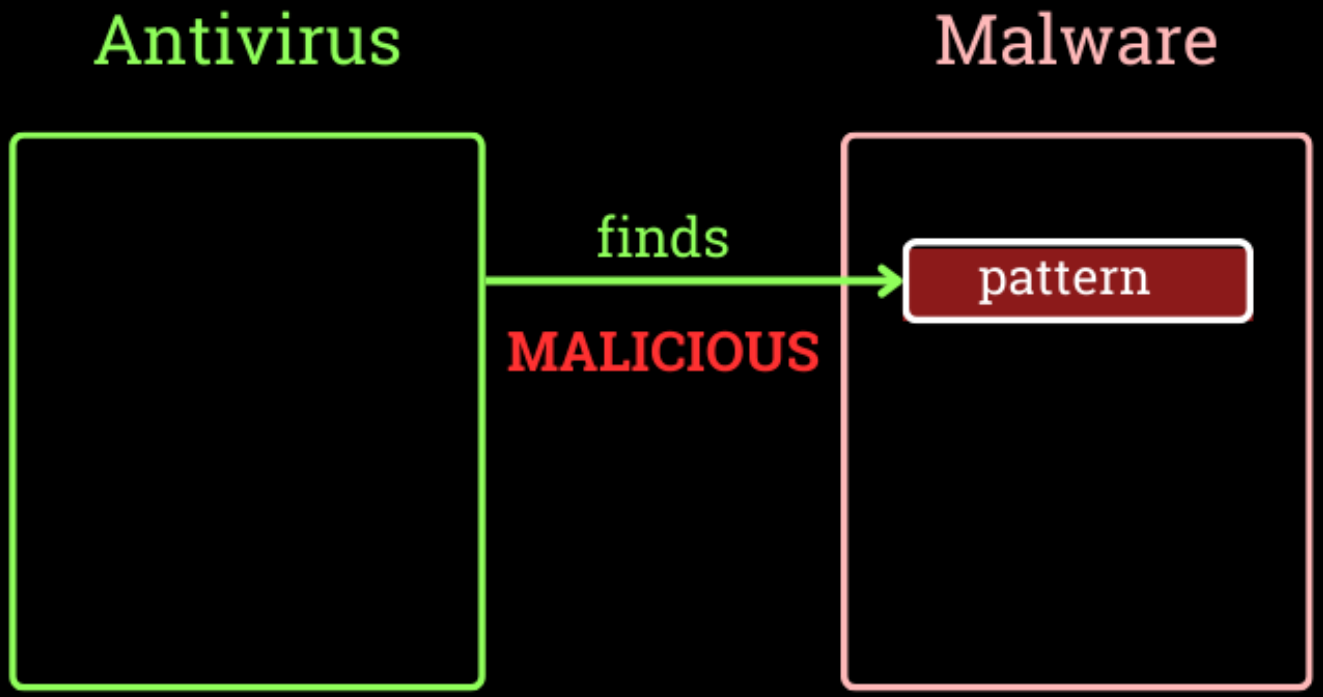
MISCONCEPTION



MISCONCEPTION



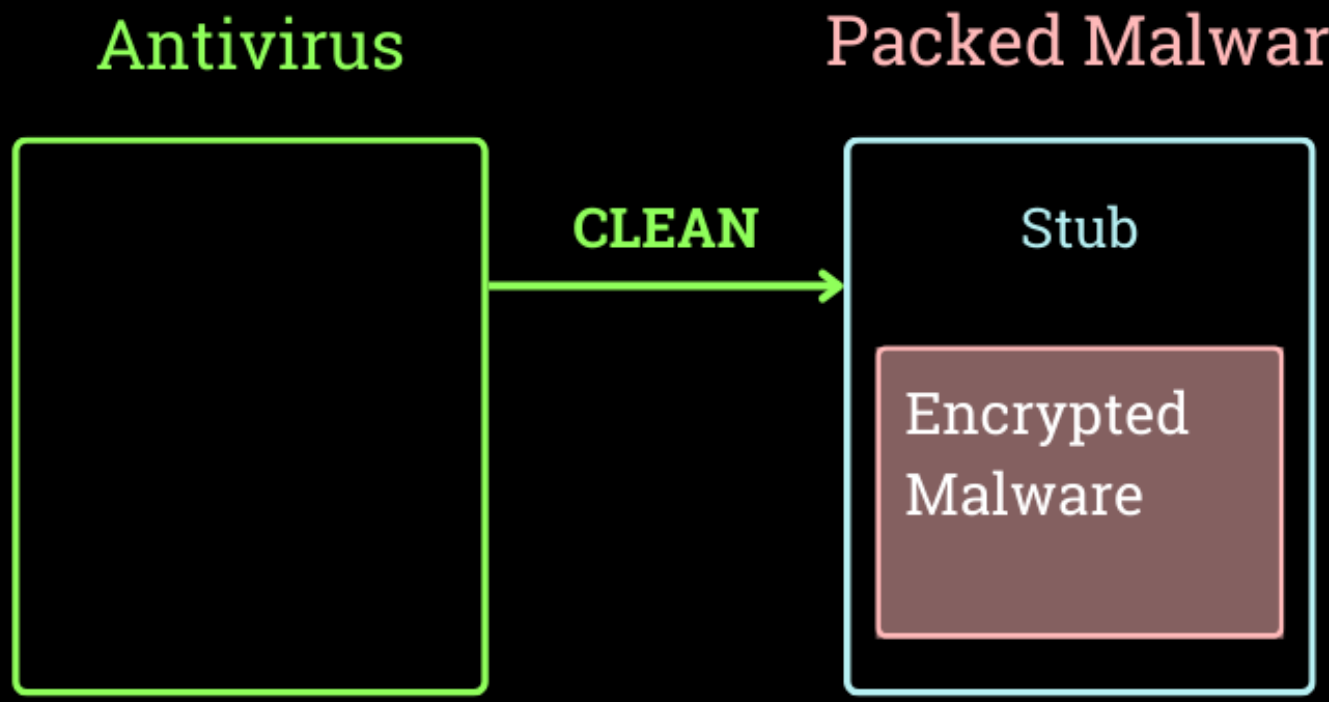
ANTIVIRUS EVASION



pattern = byte sequence, often with wildcards

example: CA FE BA BE ?? FE BA BE

ANTIVIRUS EVASION



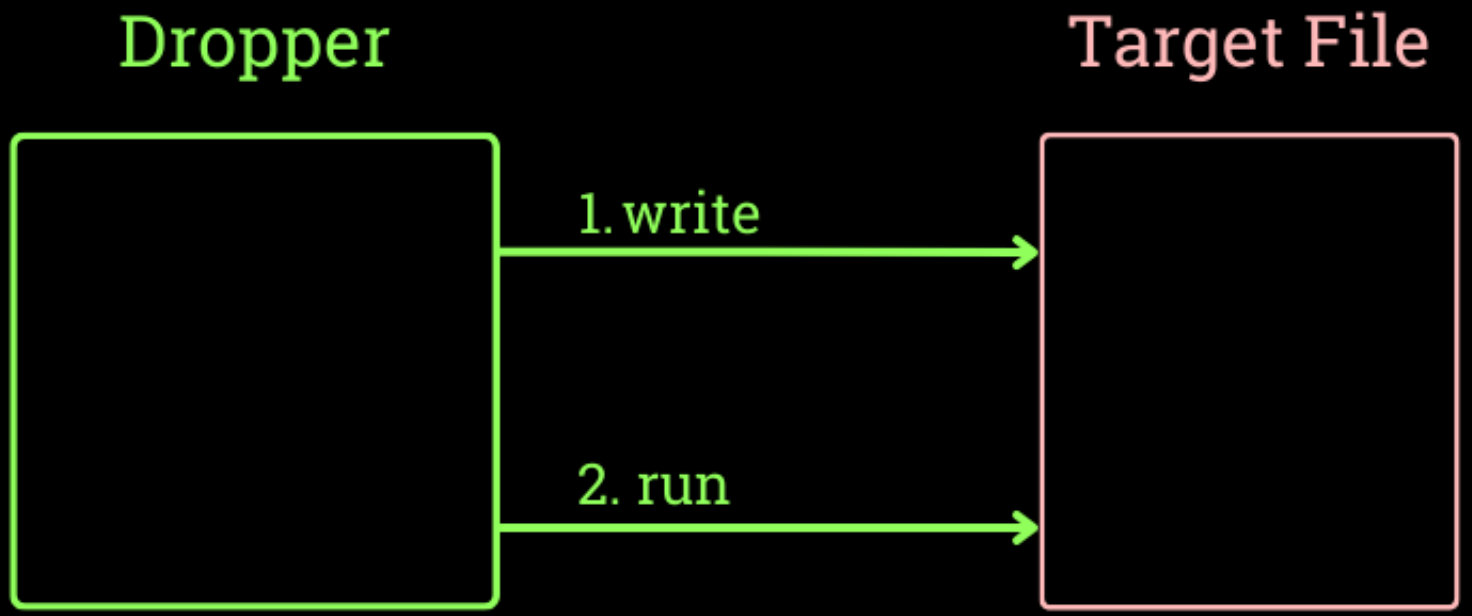
MISCONCEPTION

"Scantime Crypter" == Packer

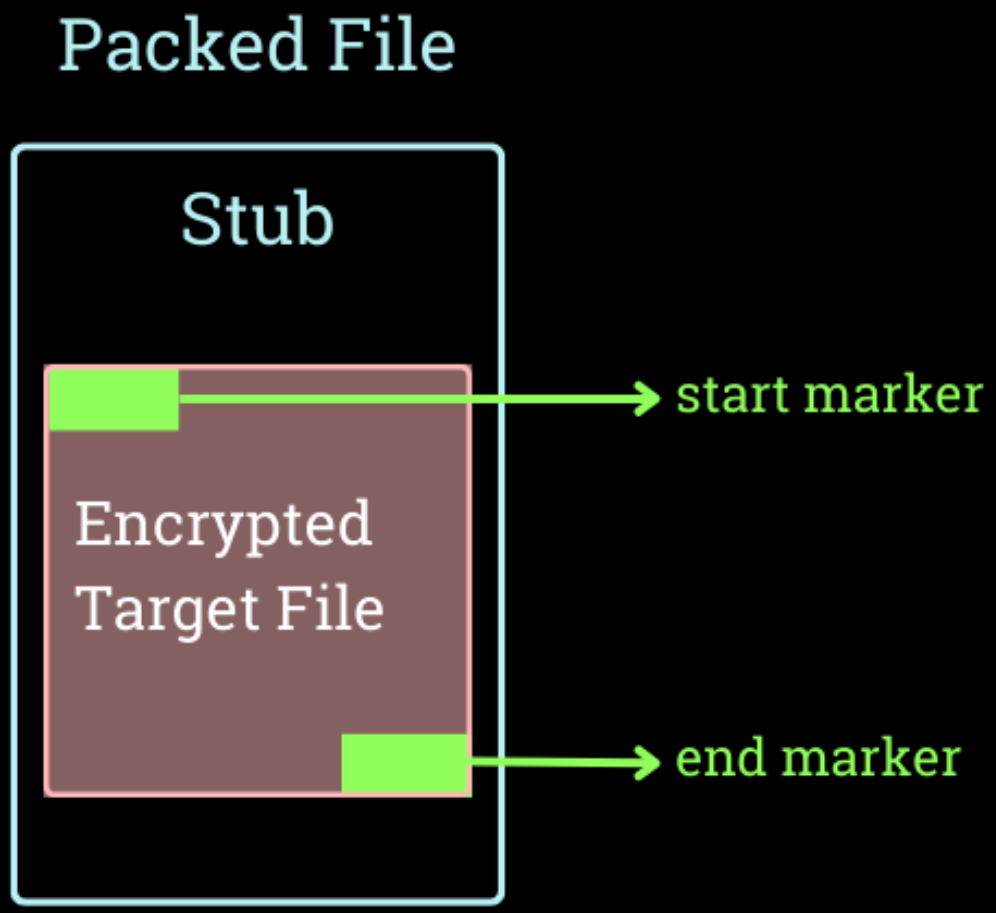
MISCONCEPTION

"Scantime Crypter" == ~~Packer~~

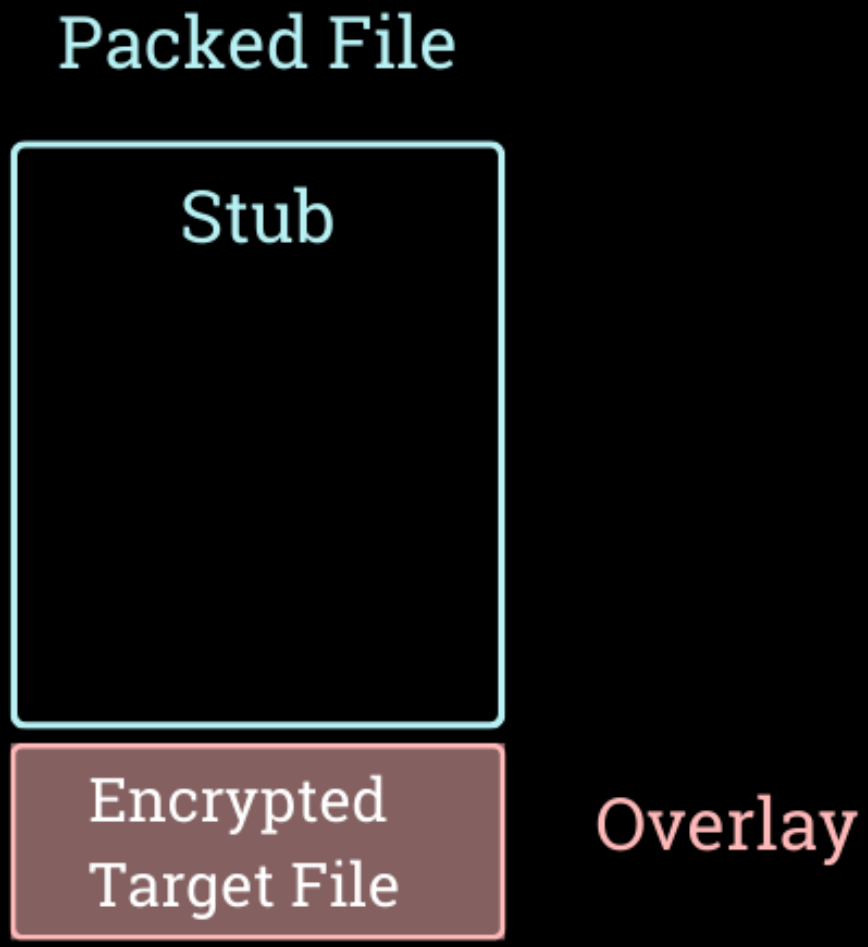
== Dropper Builder



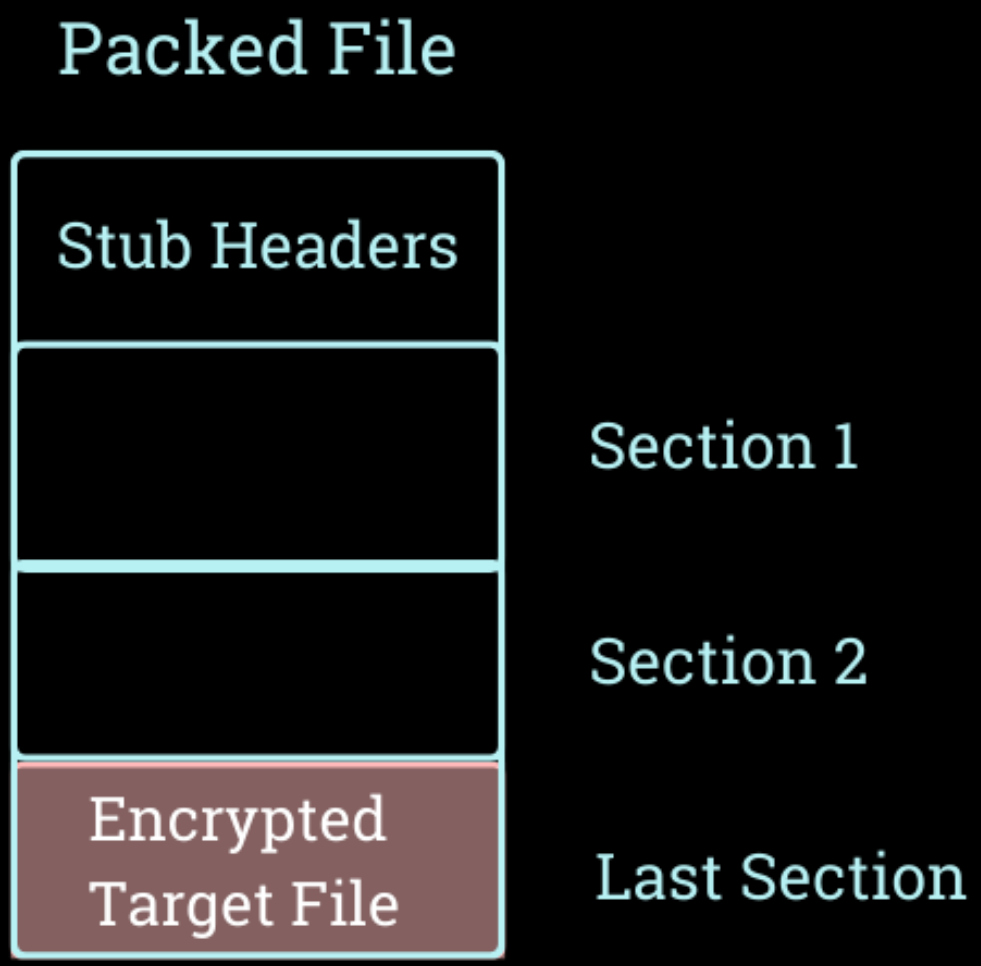
TARGET LOCATION - MARKERS



TARGET LOCATION - OVERLAY



TARGET LOCATION - LAST SECTION



TARGET LOCATION - RESOURCES