Installers

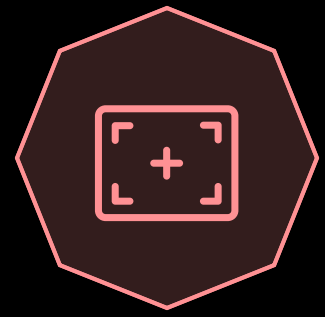
Code in Binaries

STATICALLY LINKED LIBRARIES

INCLUDED EXECUTION ENVIRONMENTS

- Wrappers
- Installers

INITIALIZATION CODE



ACTUAL MALWARE CODE

The code we are interested in

Code in Binaries

STATICALLY LINKED LIBRARIES

INCLUDED EXECUTION ENVIRONMENTS

- Wrappers
- Installers

INITIALIZATION CODE

ACTUAL MALWARE CODE

The code we are interested in

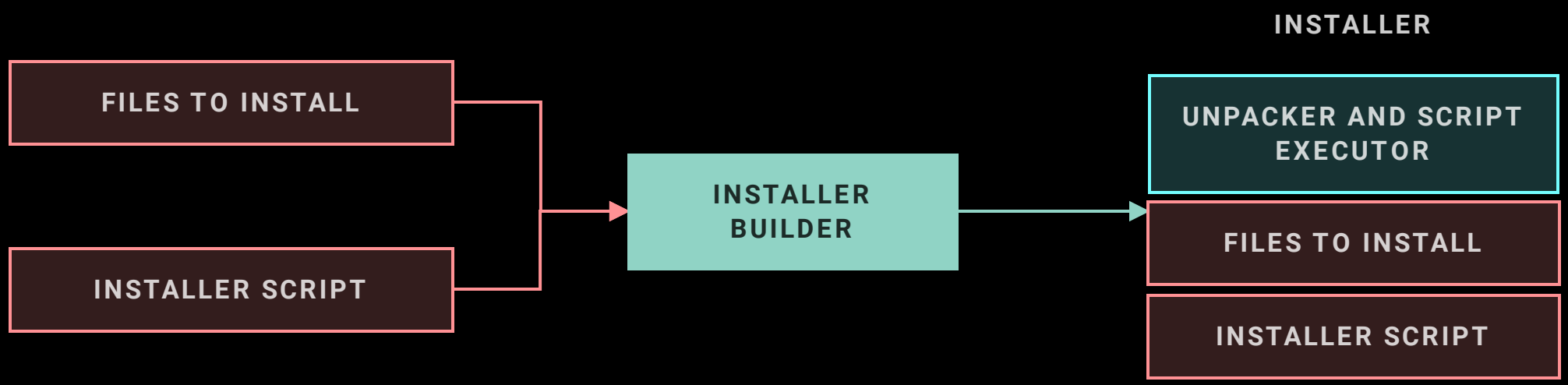
Installers

- installer builders are an easy way to create custom installers
- usually have their own scripting language
- resulting installer carries binaries and instructions how to install them
- examples: Nullsoft Scriptable Install System (NSIS), Inno Setup, Advanced Installer

Installers

- the installer embedded binaries might be all you need
- but sometimes you also need the install script

Installers


FILES TO INSTALL
INSTALLER SCRIPT
INSTALLER BUILDER
INSTALLER
UNPACKER AND SCRIPT EXECUTOR
FILES TO INSTALL
INSTALLER SCRIPT

Obtaining installed files

UNARCHIVERS

- most installed files are just archives
- just try and use 7zip on the installer

DYNAMICALLY

- run the installer
- monitor file write calls
- obtain the extracted files

INSTALLER EXTRACTORS

- identify installer with DiE
- search for specific extractor

Obtaining the installer script

INSTALLER EXTRACTORS

- identify installer with DiE
- search for installer-specific extractor
- in most cases such extractors exist already

CUSTOM SOLUTION

- analyze the installer code
- some installers compile their script to an intermediate language, some just pack it
- it helps to build your own installer with different scripts and see what changed