Finding the Developer's Code

Code in Binaries

STATICALLY LINKED LIBRARIES
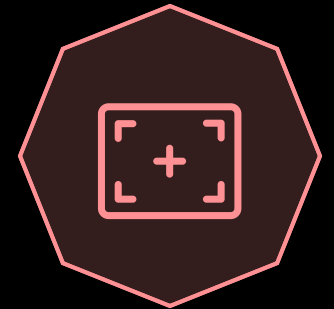
INCLUDED EXECUTION ENVIRONMENTS

- Wrappers
- Installers

INITIALIZATION CODE

ACTUAL MALWARE CODE

The code we are interested in
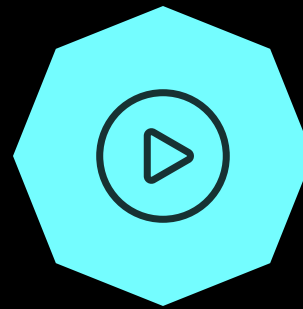
Code in Binaries
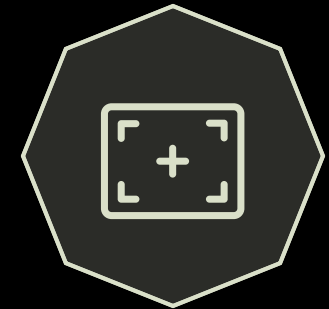
STATICALLY LINKED LIBRARIES

INCLUDED EXECUTION ENVIRONMENTS

- Wrappers
- Installers

INITIALIZATION CODE

ACTUAL MALWARE CODE

The code we are interested in

Code in Binaries

STATICALLY LINKED LIBRARIES

INCLUDED EXECUTION ENVIRONMENTS

- Wrappers
- Installers

INITIALIZATION CODE

ACTUAL MALWARE CODE

The code we are interested in