

# Analyse App: Monkey

Patrick Kainz

Folgende Informationen waren herauszufinden:

- developer (=signed by)
- capabilities
- entitlements
- (localisable) strings
- app group / bundle ID
- all input fields, remote servers (urls), ...
- functionality <= check used libraries, method(s)

## Developer

Der Team Identifier ist ES542PV7SE und der App Identifier HackyEaster.Monkey

Kommandos:

```
codesign -vd Monkey.app
```

## Capabilities

Device Capabilities: armv7

App Capabilities werden laut Doku als Entitlements gespeichert.

Kommandos:

```
less Info.plist
```

## Entitlements

Keychain Access für ES542PV7SE.HackyEaster.Monkey

Kommandos:

```
less archived-expanded-entitlements.xcent
```

## Strings

Interessante Strings:

```
thisIStheKEYyoyo, monkeyluv$Banana
```

Text auf Inputs:

- Enter the MonKey!
- Decrypt

Bilder:

- egg\_gray.png

Kommandos:

```
strings Monkey.app/Monkey | less
strings Base.lproj/Main.storyboardc/BYZ-38-t0r-view-8bC-Xf-vdC.nib | less
strings Base.lproj/Main.storyboardc/UIViewController-BYZ-38-t0r.nib
```

## App Group / Bundle ID

HackyEaster.Monkey

Kommandos:

```
less Info.plist
```

## All Input Fields, Remote Servers (Urls), ...

Text auf Inputs:

- Enter the MonKey!
- Decrypt

Bilder:

- egg\_gray.png

Keine URLs

Kommandos:

```
strings Monkey.app/Monkey | less
strings Base.lproj/Main.storyboardc/BYZ-38-t0r-view-8bC-Xf-vdC.nib | less
strings Base.lproj/Main.storyboardc/UIViewController-BYZ-38-t0r.nib
```

## Functionality

Es handelt sich scheinbar um keine Cross Platform App sondern nur um eine Swift / Objective-C ab, da keine für ein Cross Platform Framework benötigten Ressourcen beim Unzip gefunden werden konnten.

Die Sprache ist Englisch.

Laut den Strings in den Storyboards wird etwas laut einem Key entschlüsselt (es werden auch Entschlüsselungsfunktionen verwendet). Da es sich um eine HackyEaster App handelt, war die Aufgabe wahrscheinlich den Key zu finden.

Kommandos:

```
unzip Monkey.ipa
strings Monkey.app/Monkey | less
strings Base.lproj/Main.storyboardc/BYZ-38-t0r-view-8bC-Xf-vdC.nib | less
strings Base.lproj/Main.storyboardc/UIViewController-BYZ-38-t0r.nib
```