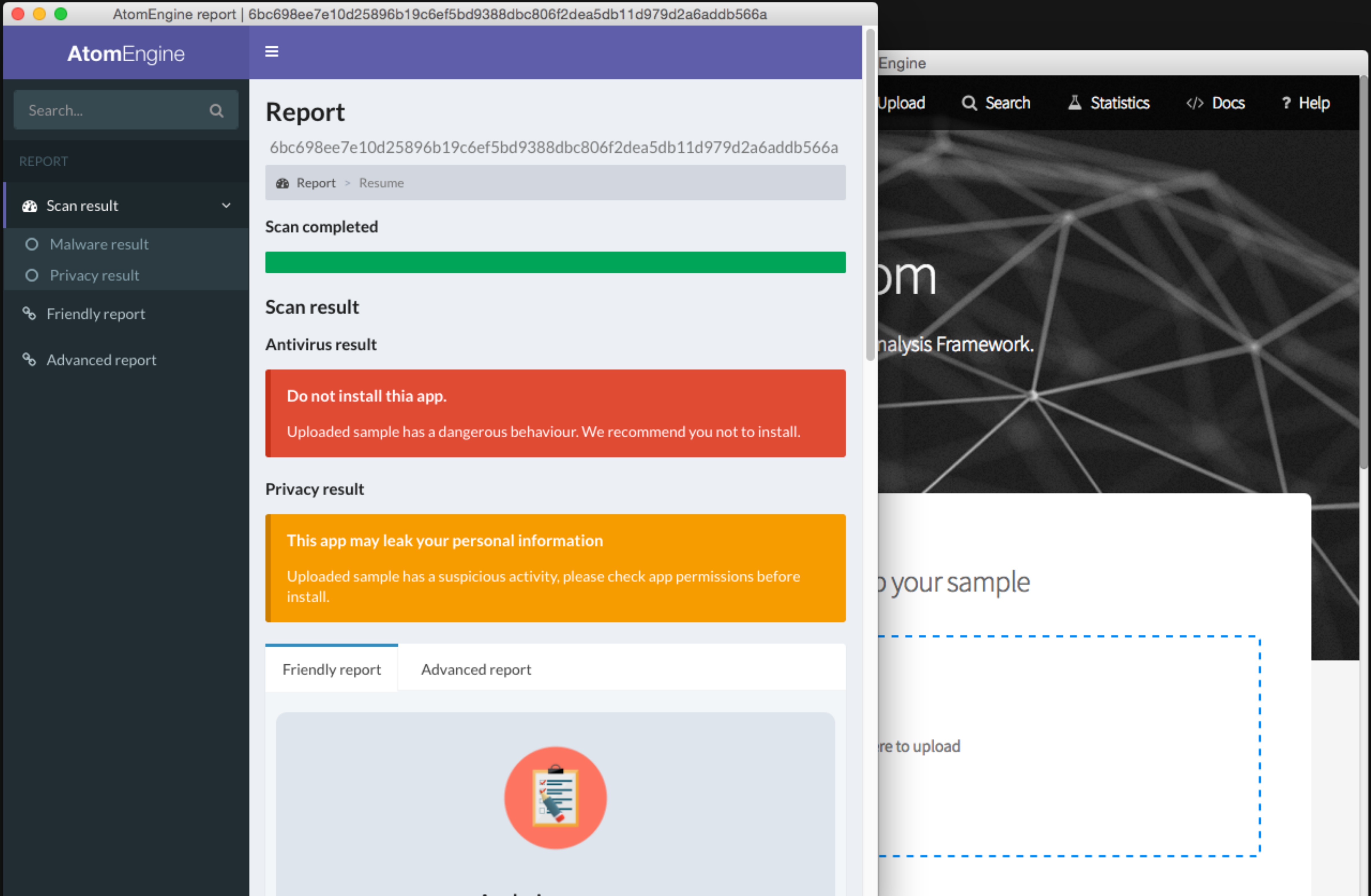
apkr:

ANALYSIS THROUGH SIMULATED RUNTIME OBSERVATION



AtomEngine report | 6bc698ee7e10d25896b19c6ef5bd9388dbc806f2dea5db11d979d2a6addb566a

Report

6bc698ee7e10d25896b19c6ef5bd9388dbc806f2dea5db11d979d2a6addb566a

Report > Resume

Scan completed

Scan result

Antivirus result

Do not install thia app.

Uploaded sample has a dangerous behaviour. We recommend you not to install.

Privacy result

This app may leak your personal information

Uploaded sample has a suspicious activity, please check app permissions before install.

<reason/>

2010

REASON

Android.FakePlayer

First Android malware discovered in **2010** which sends **SMS** messages to certain numbers

2010

REASON

Android.FakePlayer

First Android malware discovered in **2010** which sends **SMS** messages to certain numbers

still online, available, infecting mobile devices.

FEW ‘DAYS’ AGO

REASON

275 million Android phones imperiled by new code-execution exploit

FEW ‘DAYS’ AGO

REASON

275 million Android phones imperiled by new code-execution exploit

Unpatched **"Stagefright"** vulnerability gives attackers a road map to hijack phones.

FEW ‘DAYS’ AGO

REASON

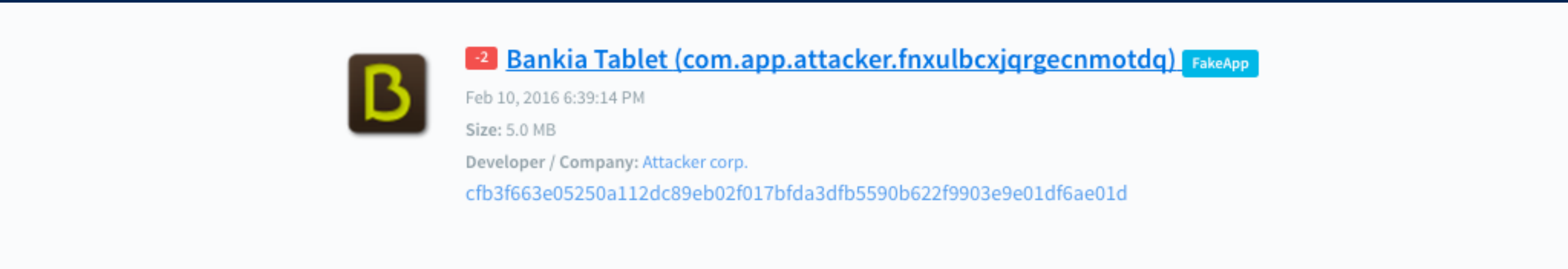
275 million Android phones imperiled by new code-execution exploit

Unpatched **"Stagefright"** vulnerability gives attackers a road map to hijack phones.

Google

TODAY

REASON



-2 Bankia Tablet (com.app.attacker.fnxulbcxjqrgecnmotdq) FakeApp

Feb 10, 2016 6:39:14 PM

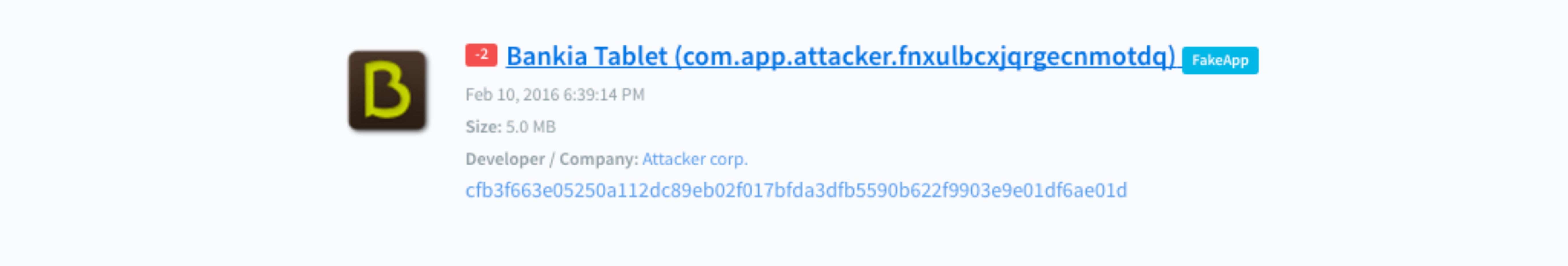
Size: 5.0 MB

Developer / Company: Attacker corp.

cfb3f663e05250a112dc89eb02f017bfda3dfb5590b622f9903e9e01df6ae01d

TODAY

REASON



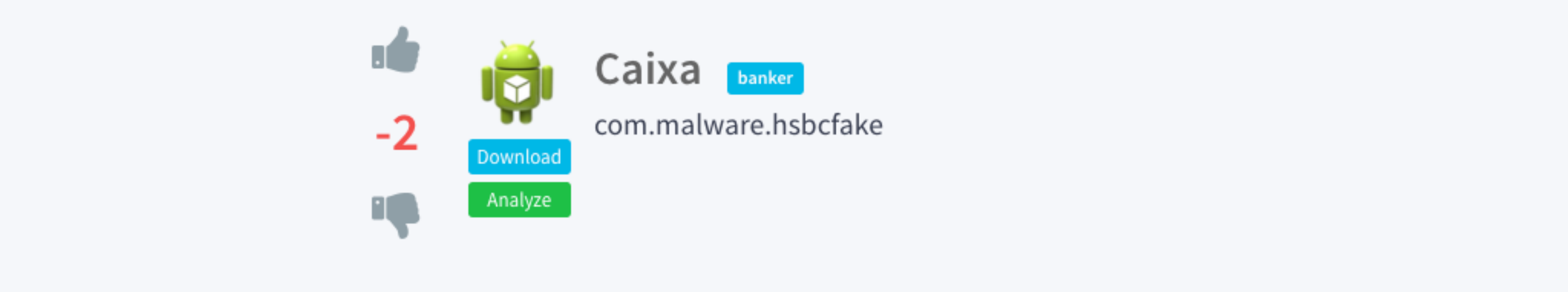
-2 Bankia Tablet (com.app.attacker.fnxulbcxjqrgecnmotdq) FakeApp

Feb 10, 2016 6:39:14 PM

Size: 5.0 MB

Developer / Company: Attacker corp.

cfb3f663e05250a112dc89eb02f017bfda3dfb5590b622f9903e9e01df6ae01d



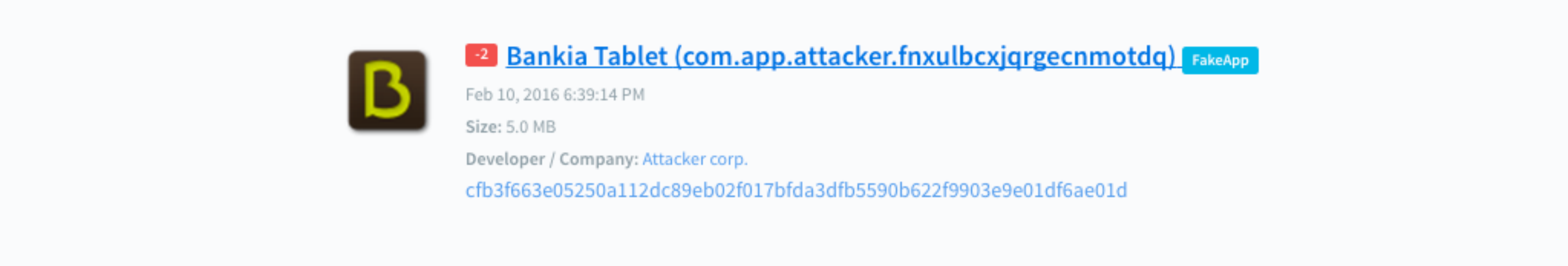
-2

Caixa banker

com.malware.hsbcfake

TODAY

REASON



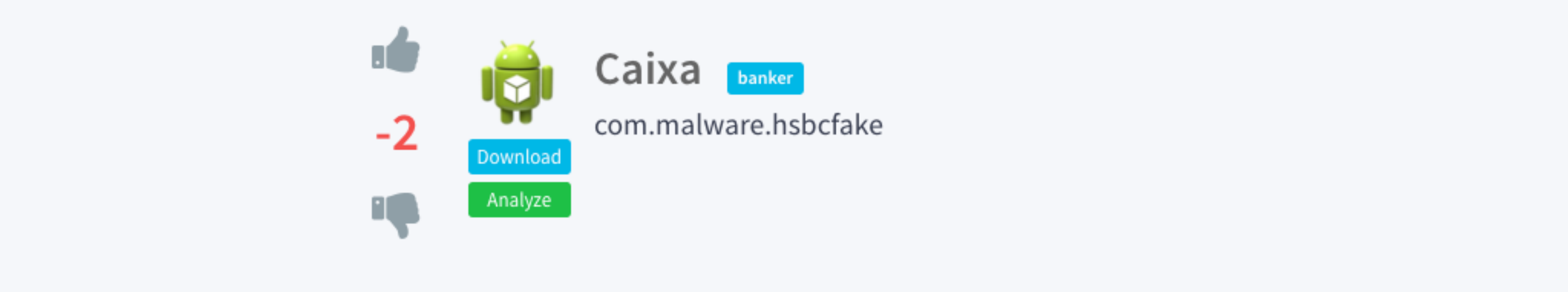
-2 Bankia Tablet (com.app.attacker.fnxulbcxjqrgecnmotdq) FakeApp

Feb 10, 2016 6:39:14 PM

Size: 5.0 MB

Developer / Company: Attacker corp.

cfb3f663e05250a112dc89eb02f017bfda3dfb5590b622f9903e9e01df6ae01d



-2

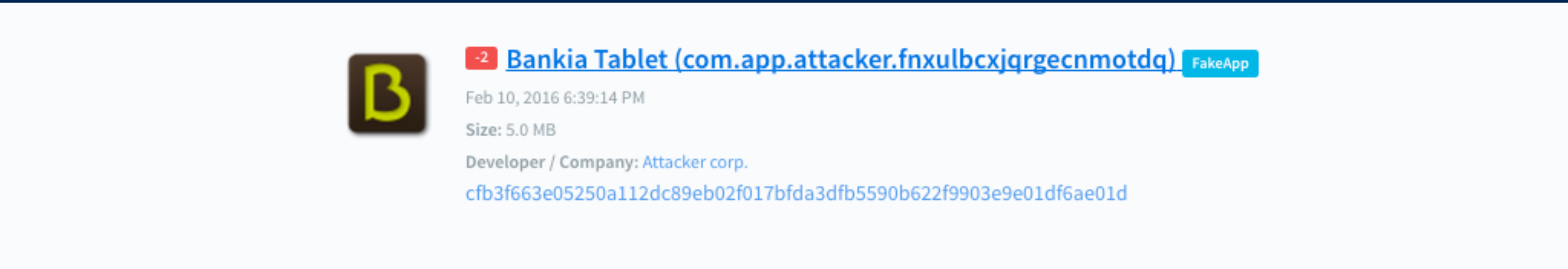
Caixa banker

com.malware.hsbcfake

Android malware masquerading as fake bank app

TODAY

REASON

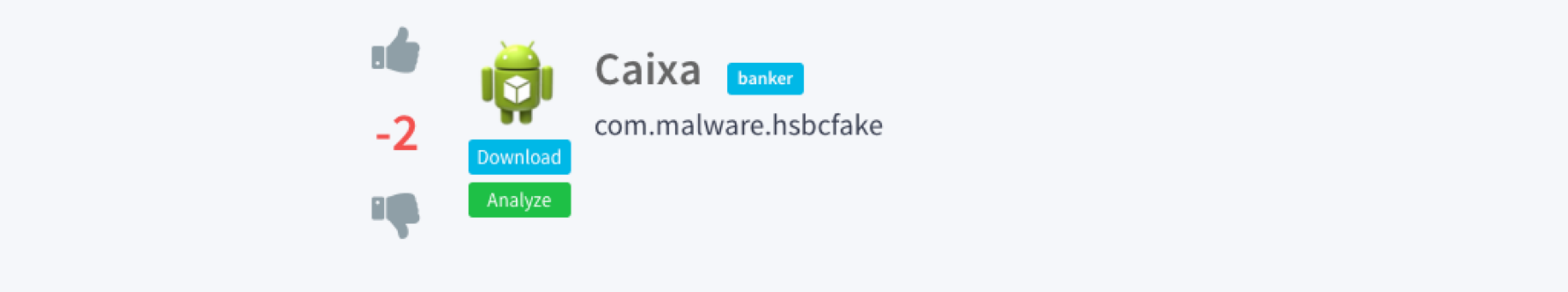

-2 Bankia Tablet (com.app.attacker.fnxulbcxjqrgecnmotdq) FakeApp

Feb 10, 2016 6:39:14 PM

Size: 5.0 MB

Developer / Company: Attacker corp.

cfb3f663e05250a112dc89eb02f017bfda3dfb5590b622f9903e9e01df6ae01d


Caixa banker

com.malware.hsbcfake

-2

Android malware masquerading as fake bank app

acts in a illegitimate way, running against user interests.

<background/>

BACKGROUND

There are hundreds of websites working as **SAAS**

virustotal

KOODOUS

Dexter

JOESandbox Cloud BASIC

AndroidSandbox*

nviso
SECURITY. RESEARCH. RISK.

AVCaesar

Anubis*

AVC UnDroid

* Discontinued software
SAAS: Software as a Service

BACKGROUND

There are hundreds of websites working as **SAAS**

…and many others

BACKGROUND

Each of them using their own analysis tools

Each of them using their own analysis tools

- **Unpackers**: apktool, axml, etc.

BACKGROUND

Each of them using their own analysis tools

- **Unpackers**: apktool, axml, etc.
- **Static analysis:** dexter, androguard, etc.

Each of them using their own analysis tools

- **Unpackers**: apktool, axml, etc.
- **Static analysis:** dexter, androguard, etc.
- **Dynamic Analysis:** virustotal, kodoous, droidbox, Hooker, etc.

BACKGROUND

Each of them using their own analysis tools

- **Unpackers**: apktool, axml, etc.
- **Static analysis:** dexter, androguard, etc.
- **Dynamic Analysis:** virustotal, kodoous, droidbox, Hooker, etc.
- **Big data & Data correlation:** tacyt*.

Tacyt

* https://www.elevenpaths.com/es/tecnologia/tacyt/index.html

<project/>

UNPACKER + STATIC + X = ANALYSIS ENGINE

UNPACKER + STATIC + X = ANALYSIS ENGINE

🤔 Start thinking, looking for similar project, libraries that could help, etc.

UNPACKER + STATIC + X = ANALYSIS ENGINE

🤔 Start thinking, looking for similar project, libraries that could help, etc.

😝 But rather than reusing other’s tools, I selected to build my own.

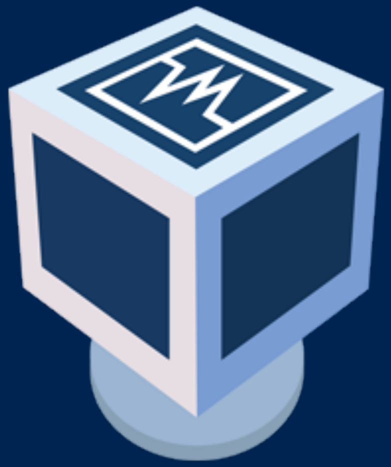
UNPACKER + STATIC + X = ANALYSIS ENGINE

🤔 Start thinking, looking for similar project, libraries that could help, etc.

😝 But rather than reusing other’s tools, I selected to build my own.

😭😭😭 idea: **virtual machine**

UNPACKER + STATIC + X = ANALYSIS ENGINE



UNPACKER + STATIC + X = ANALYSIS ENGINE

X = (Oracle VM VirtualBox | my thing)

PROJECT

UNPACKER + STATIC + X = ANALYSIS ENGINE

X = (Oracle VM VirtualBox | my thing)

X = my thing

UNPACKER + STATIC + X = ANALYSIS ENGINE

X = (Oracle VM VirtualBox | my thing)

X = my thing

my thing = Dalvik virtual machine

<development/>

DEVELOPMENT

CLIENT

nw.js

dropzone JS

5

3

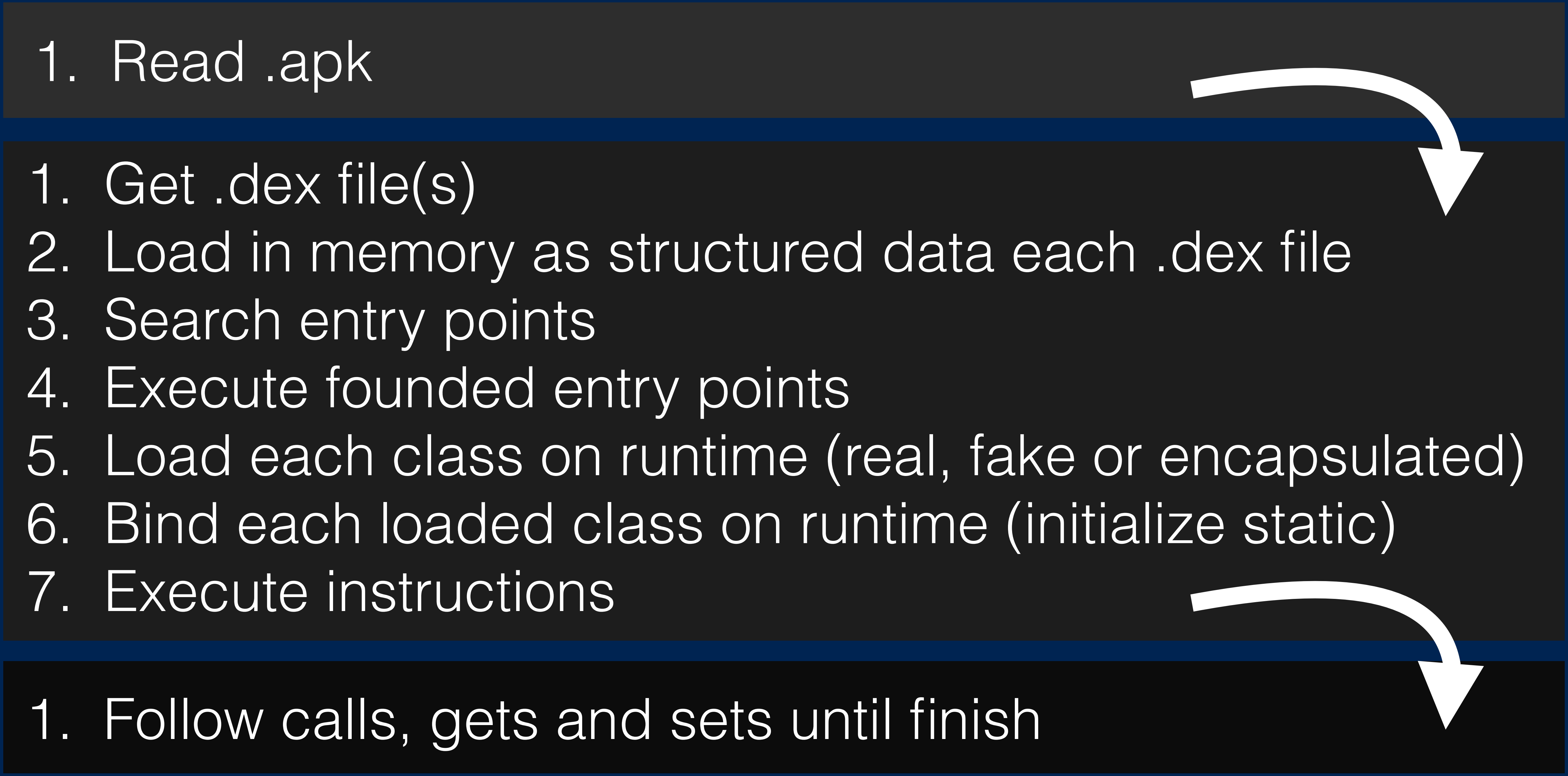
SERVER

Java

WEKA

APK TOOL

OBSERVATION MACHINE

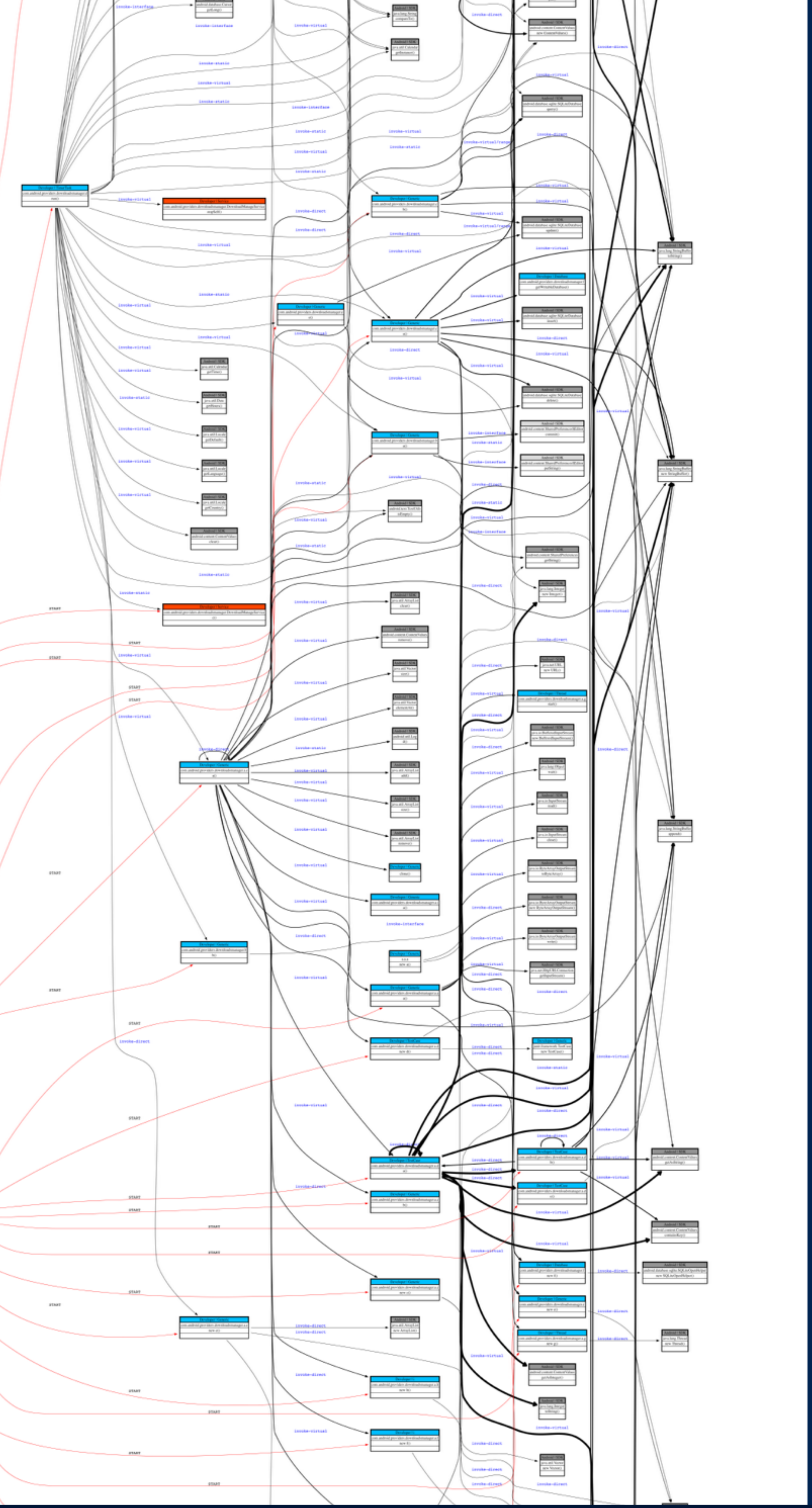


1. Read .apk

1. Get .dex file(s)
2. Load in memory as structured data each .dex file
3. Search entry points
4. Execute founded entry points
5. Load each class on runtime (real, fake or encapsulated)
6. Bind each loaded class on runtime (initialize static)
7. Execute instructions

1. Follow calls, gets and sets until finish

<results/>



RESULTS

- UNPACKER
- DECODER
- FILE ENUMERATION
- FILE CLASSIFIER
- RESOURCE FUZZING & HASHING
- NATIVE CODE DUMP
- CERTIFICATE PARSING
- DEBUG CERTIFICATE DETECTION
- OPCODE ANALYSIS
- UNUSED OPCODE DETECTION
- DALVIK BYTECODE FLOW ANALYSIS

RESULTS

CFG GENERATION

SIMPLE REFLECTION RESOLVER

LITERAL STRING CLASSIFICATION

PERMISSIONS BASED ML MODEL

<future/>

FUTURE WORK

ADD MULTIDEX SUPPORT

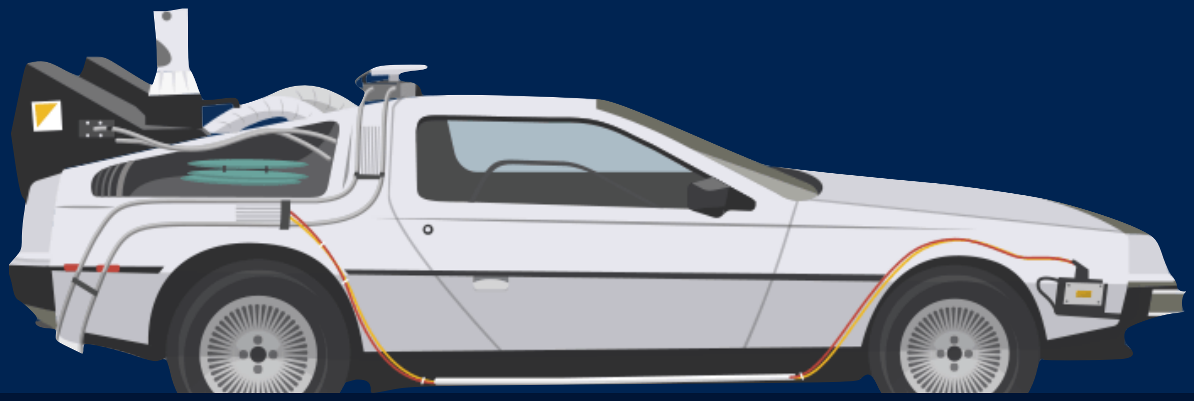
STORE DATA IN NOSQL DB FOR CORRELATION

ANALYZE OBJDUMP OUTPUT

IMPROVE REFLECTION RESOLVER

IMPROVE OBSERVATION MACHINE

ETC



<demo/>

THANKS

FSOCIETY

END