



Check Point®
SOFTWARE TECHNOLOGIES LTD.
SOFTWARE TECHNOLOGIES LTD.



Automated Android Malware Analysis
With Cuckoo Sandbox.

Idan Revivo - @idanr86 - idanr@checkpoint.com

Ofer Caspi - @shablolForce - oferc@checkpoint.com

<https://github.com/idanr1986/cuckoo-droid>

Abstract

- To combat the growing problem of Android malware, we present a new solution based on the popular open-source framework Cuckoo Sandbox to automate the malware investigation process. Our extension enables the use of Cuckoo's features to analyze Android malware and provides new functionality for dynamic and static analysis.

Problem - Too Many Malwares

- Manual malware analysis was always a slow process - taking days and even weeks per sample - rendering the task impractical even for a small sample pool.



Solution - Automation :-)

- Our solution is automating as much of the analysis process as possible - following the success of this approach for PC malware. The goal is to create a system that would take an app and produce a report describing exactly what it does when it's run, specifically pointing out anything "fishy", allowing us to perform initial analysis with no human intervention



Hello Cuckoo Sandbox

- Cuckoo Sandbox is an Open Source software for automating analysis of suspicious files.
- It uses custom components which monitor the behaviour of malicious processes while running in an isolated environment.
- Prior to our contribution, Cuckoo Sandbox supported Windows environment inspection of files such as PE, pdf, doc, etc.. and performs static and dynamic analysis on them.
- <http://cuckoosandbox.org>



Meet CuckooDroid

- CuckooDroid: an automated Android malware analysis framework – providing both static and dynamic APK inspection, as well as evading certain VM-detection techniques, encryption key extraction, SSL inspection, API call trace, basic behavioral signatures and many other features. The framework is highly customizable and extensible – leveraging the power of the large existing Cuckoo community.



ALL IN ONE Malware Analysis Framework

Static Analysis



Anti-Analysis
detection



Virtualization
Managers



Dynamic Analysis



Traffic Analysis



Intelligence Gathering



Behavioural Signatures



Static Analysis

- Static Data Gathering:

- Folder tree of all files MDS
- App activities
- App providers
- Main activity
- Package name
- App Receivers
- App services
- App permissions
- Data from google play
- Hardcoded strings



Static Analysis

- Static Api calls by decompiling the DEX of the application:
 - Used permissions Api calls
 - Used native code Api calls
 - Used dynamic code Api calls
 - Used reflection code Api calls



Dynamic Analysis

- Droidmon - Module based on Xposed Framework for Dalvik API Monitoring
- The monitoring Happen by hooking chosen Dalvik API calls for extracting behavioral information:
 - Crypto keys
 - Crypto plain text
 - Reflection calls
 - Sms messages
 - File accessed
 - Loaded Dex files
 - Fingerprinting
 - Accounts accessed
 - Shell Commands
 - SSL Traffic
 - Etc...



Virtualization Managers

- Cuckoo Supports many virtualization managers:

- Kvm

- Xen

- Virtualbox

- Esxi

- Vmware Workstation



- CuckooDroid adds a new type "avd" which is virtualization manager that supports Android Emulator

Traffic Analysis

- Cuckoo Supports many communication protocols parsing: http, tcp, udp, irc, dns, smtp, etc..
- CuckooDroid adds a new type "https" which by hooking the networking methods we are able to encrypted ssl traffic in clear text

```
POST https://ngpipes.mobage.com:443/pipes/r.2/bulk_record_stats HTTP/1.1
If-None-Match: 0
X-Ngpipes-API: 1.0
Accept: application/json
Accept-Encoding: gzip
```

```
{"sid": "GAME1uomorio7pk2a46msc6i7r8v1k4tfkphr46l7uk65pgi9i3e1lnvehfu4j3nlrmutghh71077g5a22sua2g7f62r17ng156o5l5v07q", "apiver": 5, "osrev": "Android 4.1.2", "avalue": {"TID": "351451208401216", "AID": "e437c41aa6b0bb13"}, "evid": "SST", "evcl": "PLUS", "netty": "WWAN", "arel": "6.0.9", "evts": 1423653857790, "srvc": "US", "hwty": "Nexus 5", "pltfmsku": "ANDROID", "udid": "351451208401216", "lang": "en", "asku": "BAHAMUTANDROID", "srcty": "PC", "tz": "Israel Standard Time", "carr": "CELLCOM", "seq": 1, "pver": "NDK-2.4.2-20130731-1059.0", "evpl": {"webviewurl": "http://webview.mobage.com/android/V4V", "distribution": "native_default_distribution"}, "hwrev": "", "seqdt": 193}
```







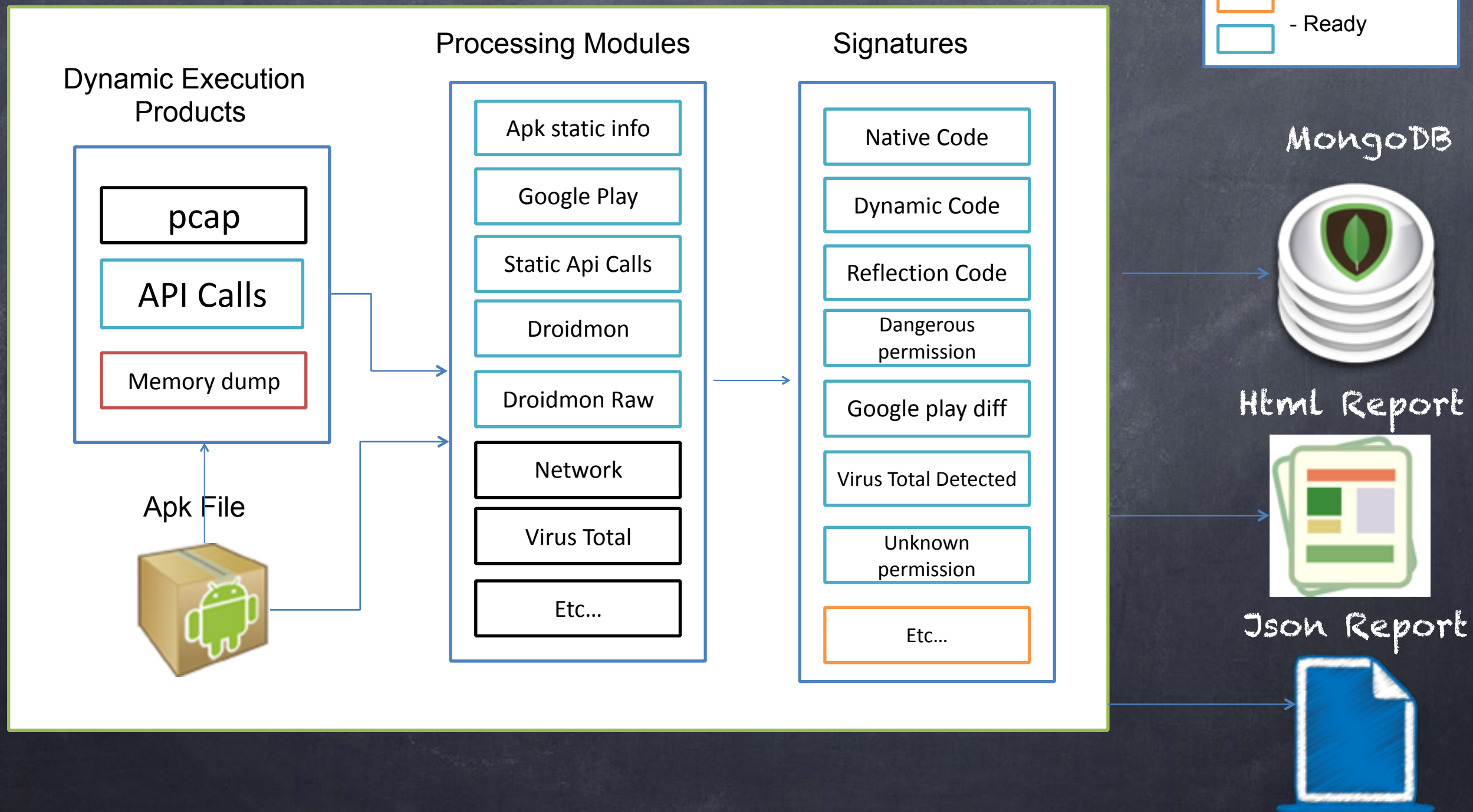
Behavioural Signatures

- App using dangerous permissions
- App using dynamic code
- App using reflection code
- App using native code
- App was identified by virus total by relevant AV's
- App Sent SMS
- App Queried sensitive information
- etc ...



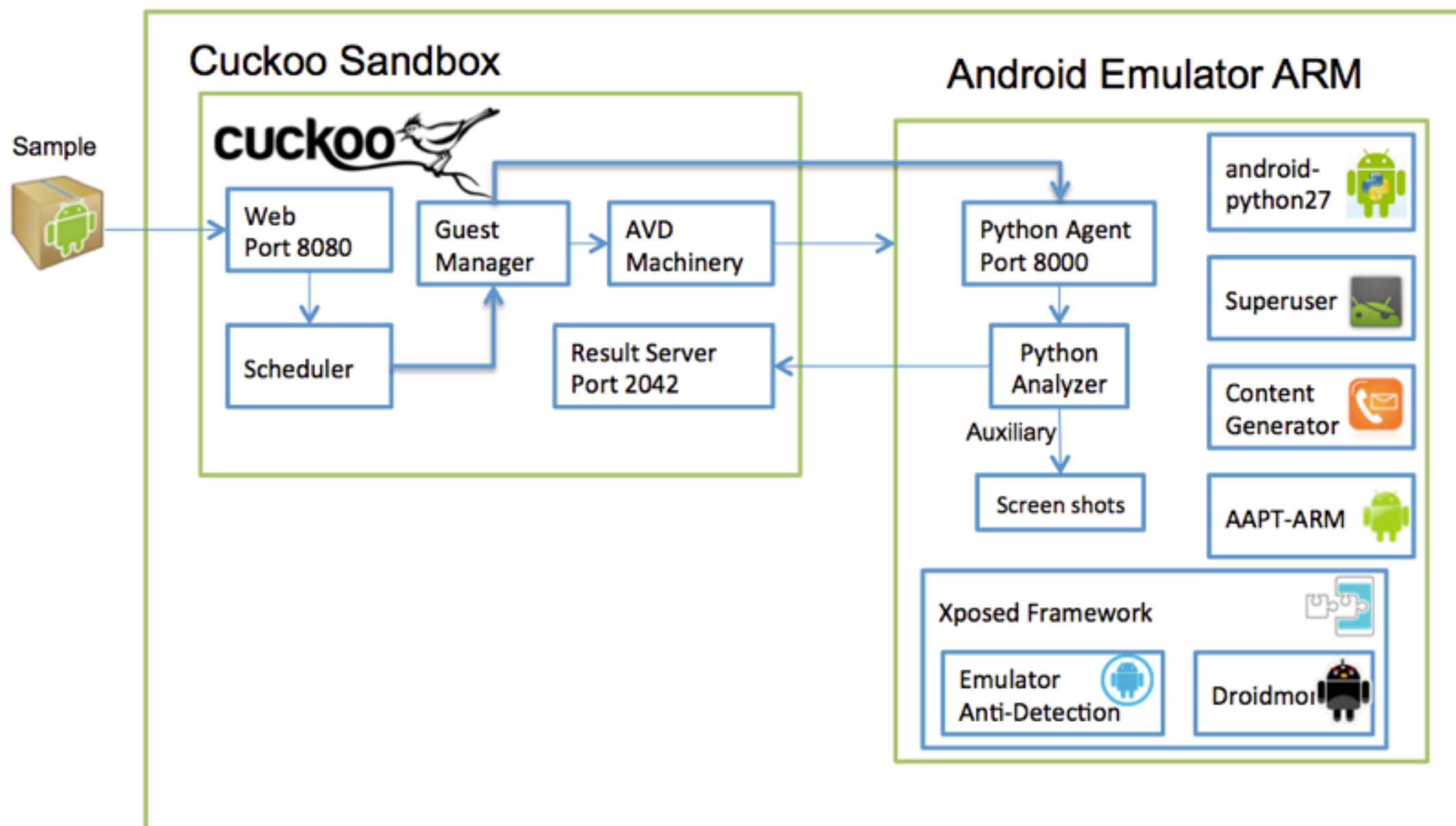
Analysis Flow

-  - Built in
-  - Planned
-  - Working
-  - Ready



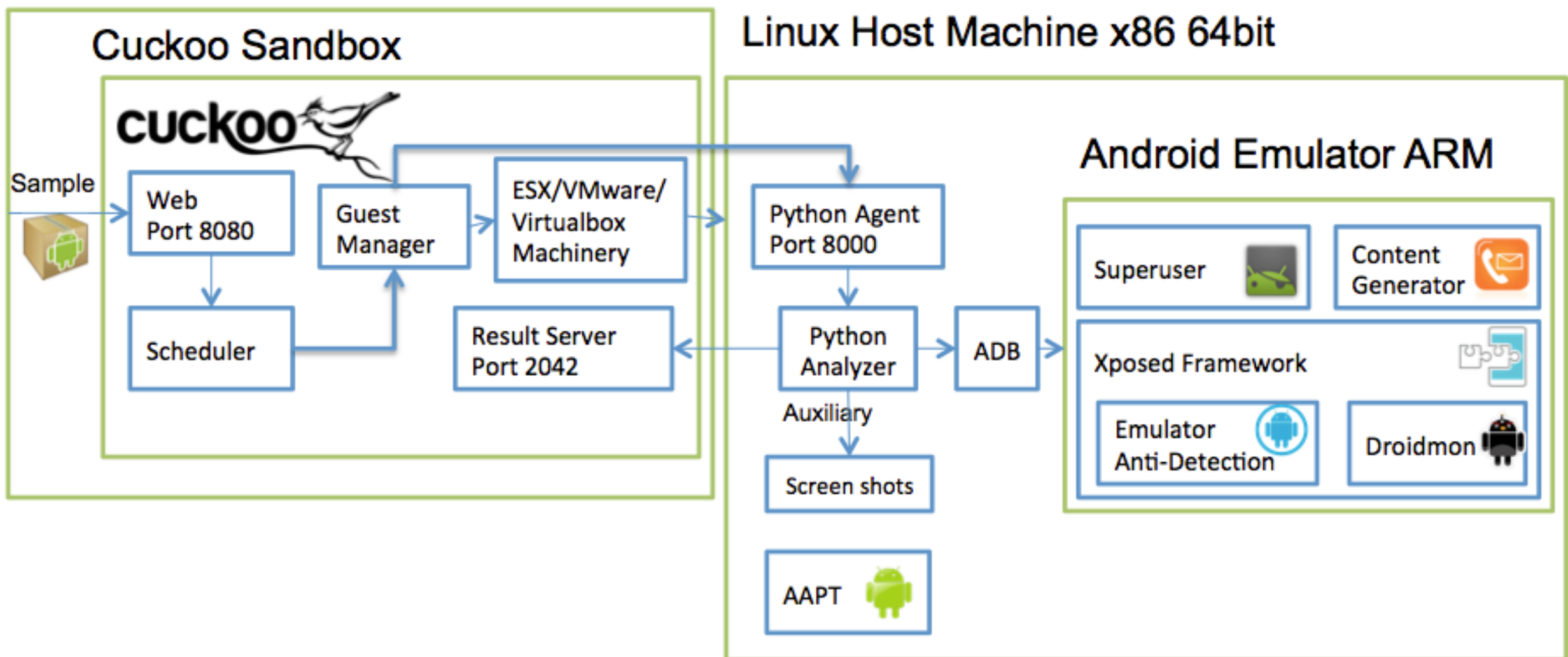
Android Emulator Setup

Linux Host Machine x86 64bit



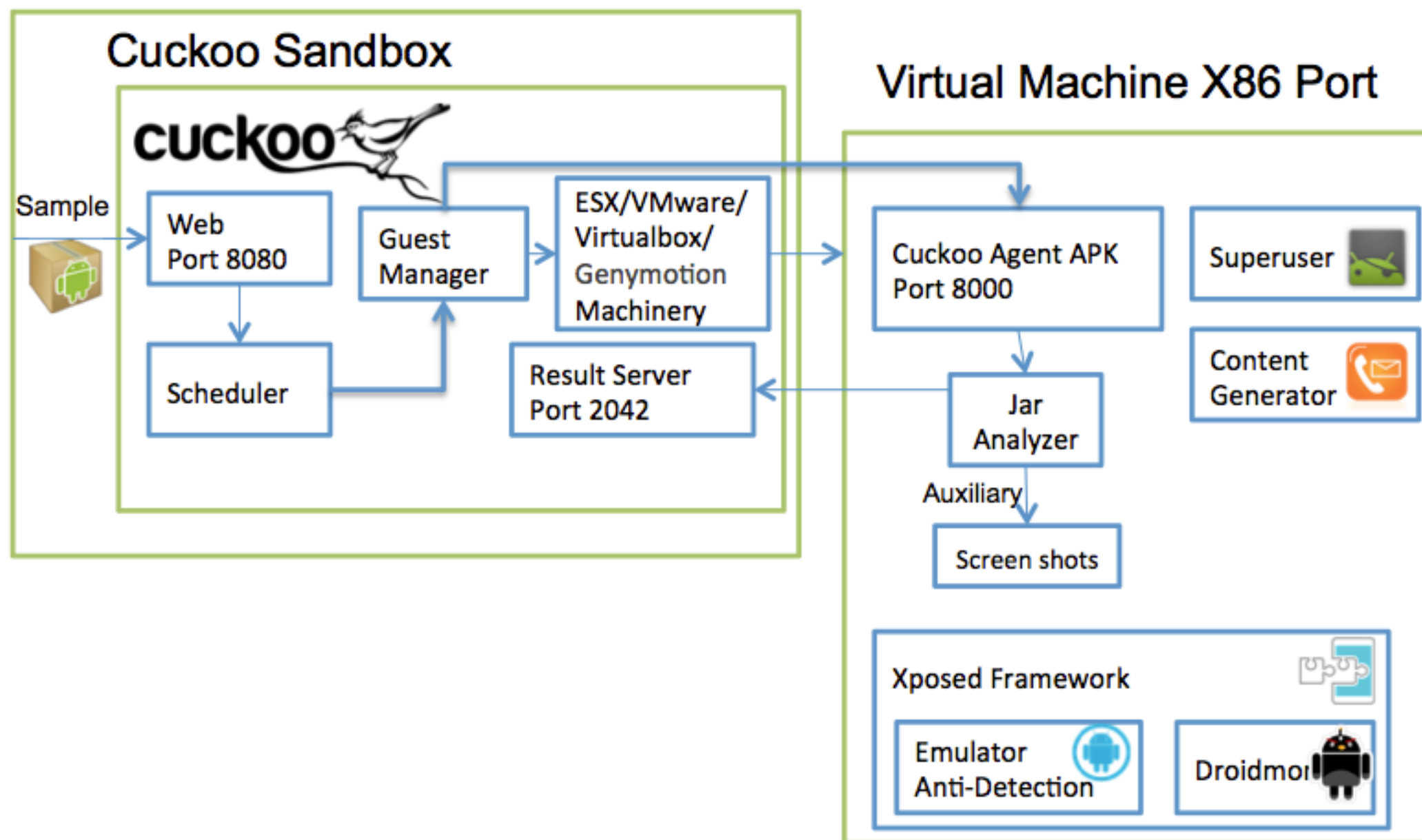
Android On Linux Setup

Linux Host Machine x86 64bit



Android x86 Port Setup

Linux Host Machine x86 64bit



Report - File Details

File Details

File name	CuckooTest.apk
File size	394209 bytes
File type	zip archive data, at least v2.0 to extract
CRC32	5959C612
MD5	378483362c34ddfca182a56e3ee640a5
SHA1	076128937c8373d68dbbd389b2ca08ca30f636e1
SHA256	9591b24ffb6d038c688e49ae4951e25412be7814138a2f1d4a423f5c0982c287
SHA512	8335e37dd67a7fb95cd7297d85fd0e78888a31fe35490619f0a85cedb650944383b3dd2e5d44c3dff143fab433a7d501dd44c0b7c12bca114c5386641bd5094e
Ssdeep	12288:HuFbkovvdCYgwsN7NVFX8kQYY2qY9pBw1X7u:HWtHde7jFXjQCLC7u
PEiD	None matched
Yara	None matched
VirusTotal	File not found on VirusTotal

Report - Application Info

Android Application Info

Package	vbkoxh.cswnpr
Main Activity	vbkoxh.cswnpr.vmbatqef

Activities

Services

Receivers

Permissions

android.permission.WRITE_EXTERNAL_STORAGE

android.permission.MOUNT_UNMOUNT_FILESYSTEMS

android.permission.ACCESS_NETWORK_STATE

android.permission.CHANGE_NETWORK_STATE

android.permission.INTERNET

android.permission.ACCESS_WIFI_STATE

android.permission.BROADCAST_STICKY

android.permission.READ_PHONE_STATE

com.android.launcher.permission.INSTALL_SHORTCUT

Report - Signature

Application Queried Phone Number (Dynamic)

Performs some HTTP requests (Traffic)

File has been identified by at least one AntiVirus on VirusTotal as malicious (Osint)

Application Registered Receiver In Runtime (Dynamic)

Application Asks For Dangerous Permissions (Static)

Application Uses Reflection Methods (Static)

File has been identified by more the 10 AntiVirus on VirusTotal as malicious (Osint)

Report - Behaviour Analysis

Android Dynamic Analysis



Shell Commands



Queried Accounts



Dynamically Loaded Files



Registered Broadcast Receivers



Crypto Keys



Encryption Plaintext



Intents



Reflection Calls



Fingerprints



Shared Preferences

Report - Behaviour Analysis

Android Dynamic Analysis



Dynamically Loaded Files

Library Name:skyforce ,Library Path:/data/app-lib/com.idreams.skyforce-1/libskyforce.so



Crypto Keys

HmacSHA1

Nr0BU0LVyb4v50hcwG4EiFqqecyaZGk76aIxCCWI&



Encryption Plaintext

/xp/devices+Nr0BU0LVyb4v50hcwG4EiFqqecyaZGk76aIxCCWI+POST+device%5Bos%5D=v4.4.2+%28eng.cwhuang.20140808.182504%29&device%5Bhardware%5D=p%28android_x86%29%2Fm%28VirtualBox%29&device%5Bprocessor%5D=family%28unknown%29+min%28unknown%29+max%28unknown%29&device%5Bscreen_resolution%5D=600x761+%280.812500+dpi%29&device%5Bidentifier%5D=android-id-d7fd32066ec0596d&of-version=1.9.2&platform=android&game_version=14&protocol_version=1.0

/xp/devices+Nr0BU0LVyb4v50hcwG4EiFqqecyaZGk76aIxCCWI+POST+device%5Bos%5D=v4.4.2+%28eng.cwhuang.20140808.182504%29&device%5Bhardware%5D=p%28android_x86%29%2Fm%28VirtualBox%29&device%5Bprocessor%5D=family%28unknown%29+min%28unknown%29+max%28unknown%29&device%5Bscreen_resolution%5D=600x761+%280.812500+dpi%29&device%5Bidentifier%5D=android-id-d7fd32066ec0596d&of-version=1.9.2&platform=android&game_version=14&protocol_version=1.0

/webui/manifest/android.embed.mdpi+Nr0BU0LVyb4v50hcwG4EiFqqecyaZGk76aIxCCWI+GET+

Report - Static Analysis

Android Static Analysis

Static Crypto Method Calls

Static Reflection Method Calls

Static ACCESS_NETWORK_STATE Method Calls

Api Call

```
1 Landroid/support/v4/net/ConnectivityManagerCompat;->getNetworkInfoFromBroadcast(Landroid/net/ConnectivityManager; Landroid/content/Intent; Landroid/net/NetworkInfo;)Landroid/net/NetworkInfo;
1 Landroid/support/v4/net/ConnectivityManagerCompatGingerbread;->isActiveNetworkMetered(Landroid/net/ConnectivityManager;)Z (0x2) --->
1 Landroid/support/v4/net/ConnectivityManagerCompatHoneycombMR2;->isActiveNetworkMetered(Landroid/net/ConnectivityManager;)Z (0x2) --->
1 Landroid/support/v4/net/ConnectivityManagerCompat$BaseConnectivityManagerCompatImpl;->isActiveNetworkMetered(Landroid/net/ConnectivityManager;)Z (0x2) --->
1 Landroid/support/v4/net/ConnectivityManagerCompat$BaseConnectivityManagerCompatImpl;->getActiveNetworkInfo()Landroid/net/NetworkInfo;
```

Static WAKE_LOCK Method Calls

Static SEND_SMS Method Calls

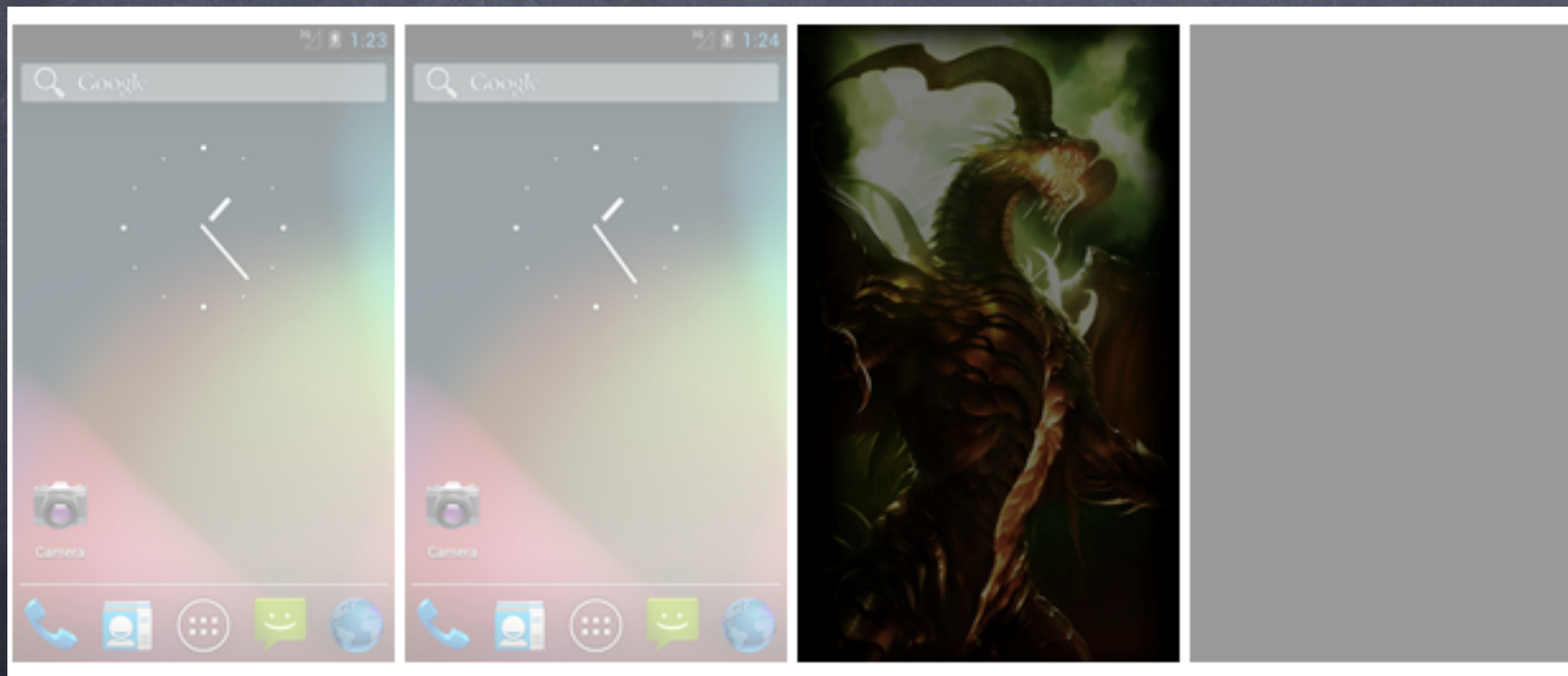
Static VIBRATE Method Calls

Static INTERNET Method Calls

Static READ_CONTACTS Method Calls

Static READ_PHONE_STATE Method Calls

Report - Screenshots



Network ssl

POST https://ngpipes.mobage.com:443/pipes/r.2/bulk_record_stats HTTP/1.1

If-None-Match: 0

X-Ngpipes-API: 1.0

Accept: application/json

Accept-Encoding: gzip

```
{"sid":"GAME1uomorio7pk2a46msc6i7r8v1k4tfkphr46l7uk65pgi9i3e1lnvehfu4j3nlrmutghh71077g5a22sua2g7f62r17ng156o5l5v07q","apiver":5,"osrev":"Android 4.1.2","avalue":{"TID":"351451208401216","AID":"e437c41aa6b0bb13"},"evid":"SST","evcl":"PLUS","netty":"WWAN","arel":"6.0.9","evts":1423653857790,"srvc":"US","hwty":"Nexus 5","pltfmsku":"ANDROID","udid":"351451208401216","lang":"en","asku":"BAHAMUTANDROID","srcty":"PC","tz":"Israel Standard Time","carr":"CELLCOM","seq":1,"pver":"NDK-2.4.2-20130731-1059.0","evpl":{"webviewurl":"http://webview.mobage.com/android/4"},"distribution":"native_default_distribution"},"hwrev":"","seqdt":193}
```


Summary

- We believe fighting the growing threat of Android malware should be an industry wide effort, so we are contributing CuckooDroid and all its logic and components into the open source realm.
- <https://github.com/idanr1986/cuckoo-droid>



Future Work

- full api call tracing
- android memory analysis with volatility
- Drozer integration - app penetrating automation
- Virtual machine introspection