SandDroid User's Manual

SandDroid

SandDroid is an automatic Android application analysis system which combines static and dynamic analysis techniques. The home page shows as below.

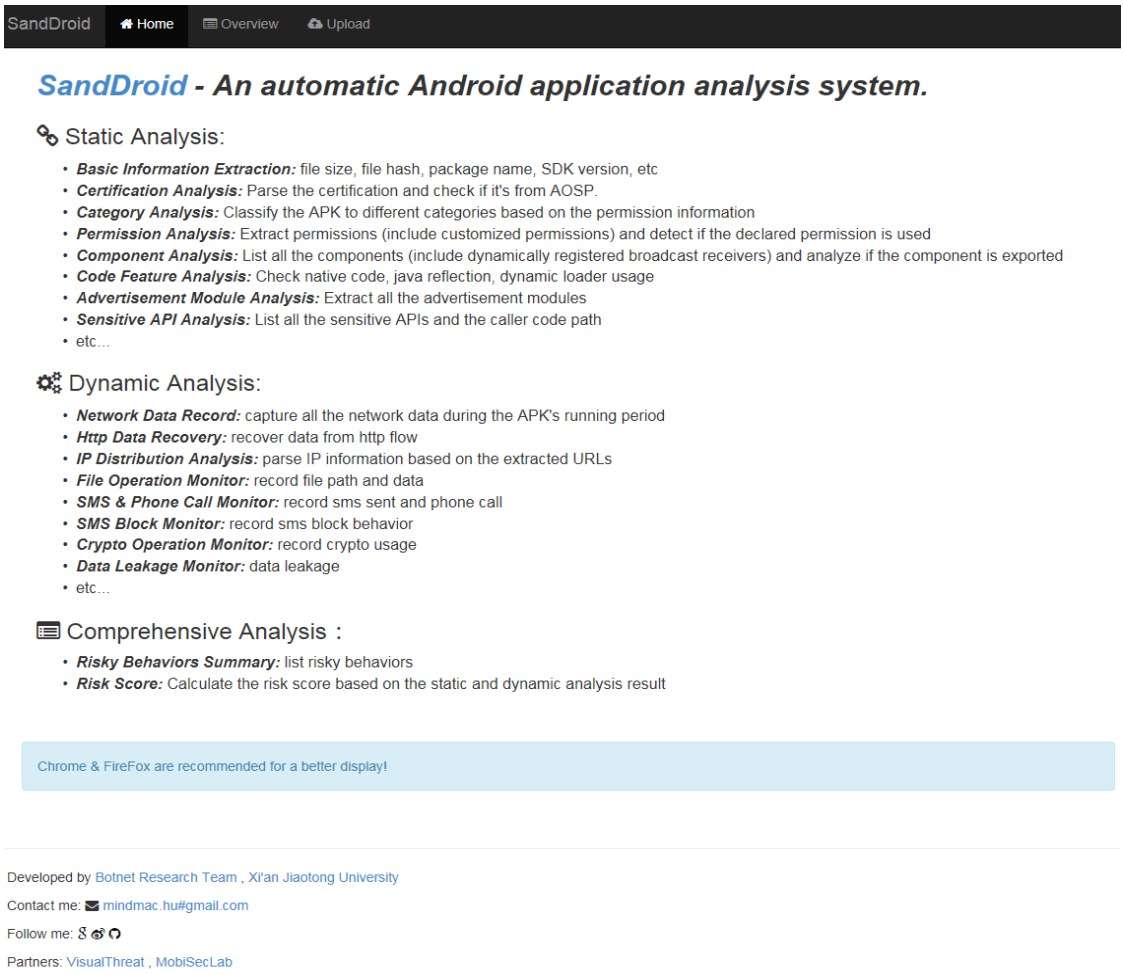


Figure 1 SandDroid home page

Overview

Click the ***Overview*** link in the navigation bar and you will see the over-view information of the analyzed Android applications.

Search

You can look for the Android applications in our database by using the *search* functionality.

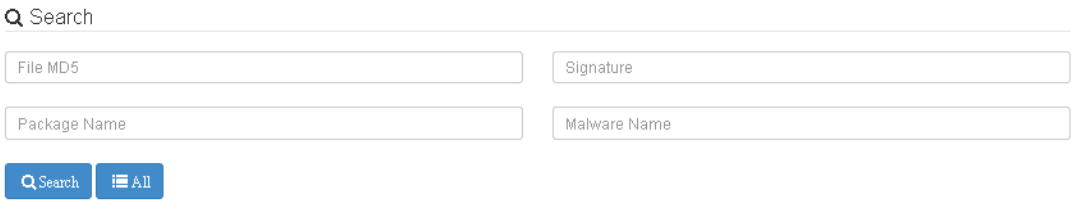


Figure 2 Search Form

How to *search*:

- File MD5: the MD5 value of the Android application;
- Signature: the SHA-1 value of the Android application's signature;
- Package Name: the package name of the Android application;
- Malware Name: the malware family name of the Android application.

Apk Information Table

The searched results will show in the table which displays the brief information about the analyzed Android applications. Click the "detail icon" to see the detail analysis report.

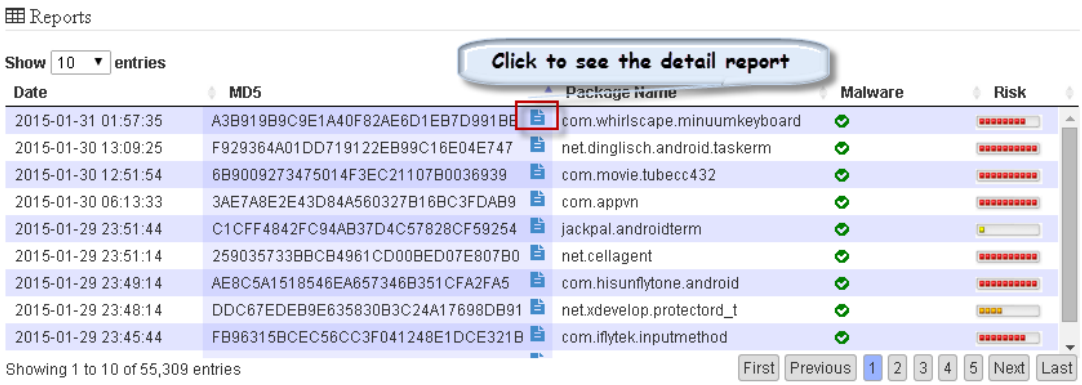


Figure 3 Apk Information Table

Explanation of the apk Information table's columns:

- Date: the date when starts to analyze the apk;
- MD5: the MD5 value of the apk;
- Package Name: the package name of the apk;
- Malware: the malware name of the apk;
- Risk: the risk level of the apk.

IP Distribution

The *ip distribution map* shows geographical distribution of ip addresses extracted from all the analyzed Android applications.

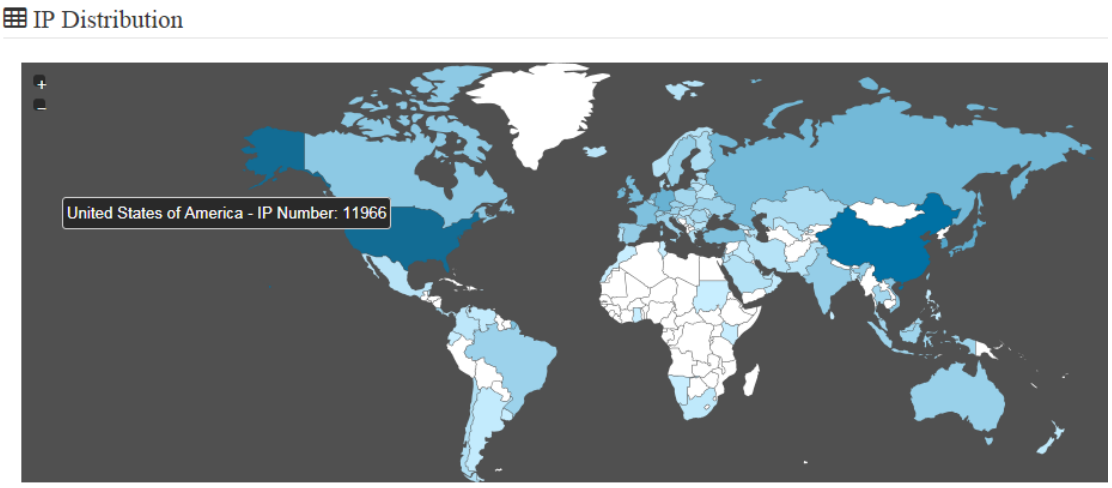


Figure 4 IP Distribution Map

Top 20 Used Permissions

The following chart shows top 20 used permissions in all the analyzed Android applications.

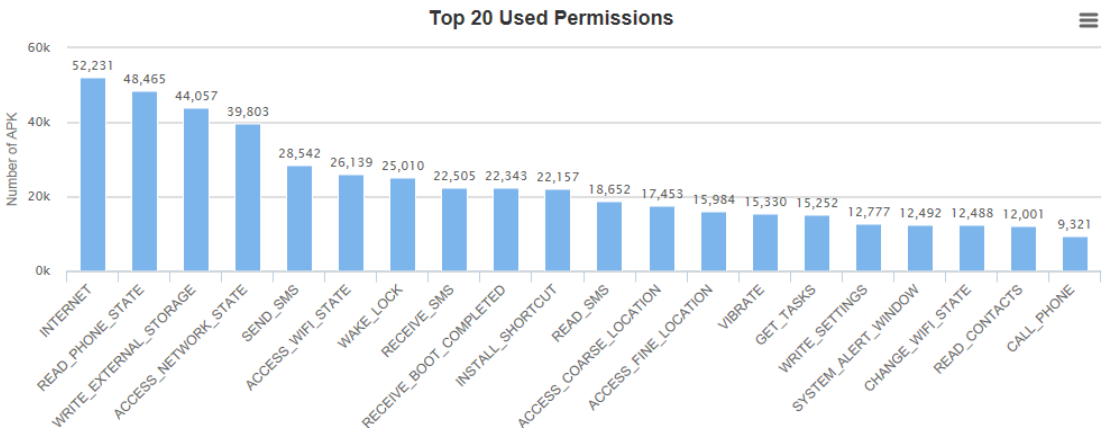


Figure 5 Top 20 Used Permissions

Top 20 Malware Families

The following chart shows top 20 malware families in all the analyzed Android applications.

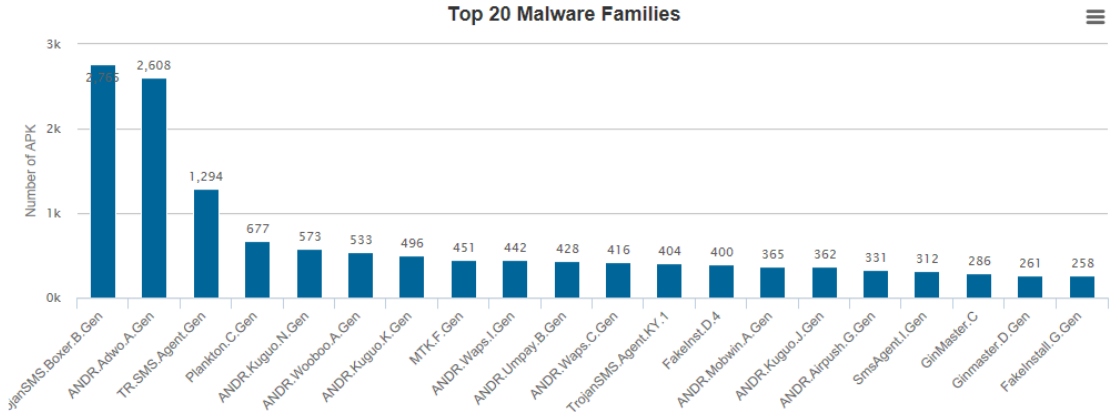


Figure 6 Top 20 Malware Families

Top 20 Advertisement Module Used

The following chart shows top 20 advertisement modules used in all the analyzed Android applications.

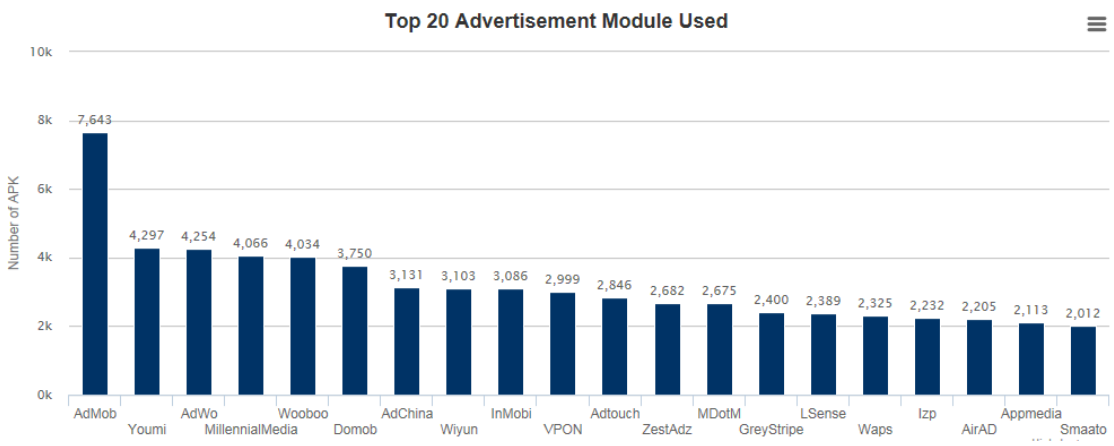


Figure 7 Top 20 Advertisement Module Used

Upload Page

You can upload an apk or a zip file on the *Upload* page and the file size limits to 50MB.

Detail Report

As shown in Figure 3, you can click the detail icon to see the detail analysis report.

General Information

The icon on the right is the Android application's icon. You can download the pcap file and log file captured during dynamic analysis.

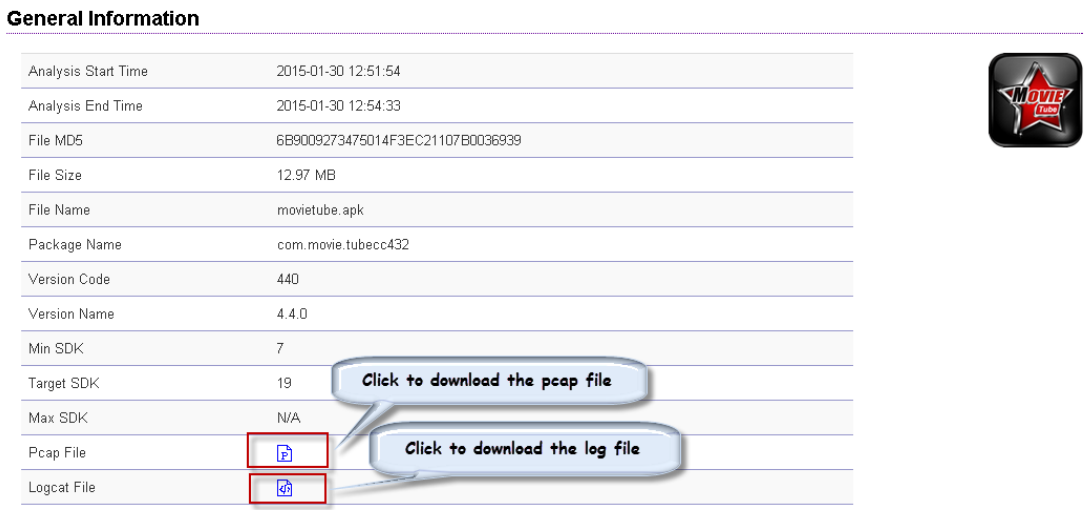


Figure 8 General Information

Risk Score

The risk score, between 0 and 100, represents the risk level. The higher the score is, the riskier the Android application is.

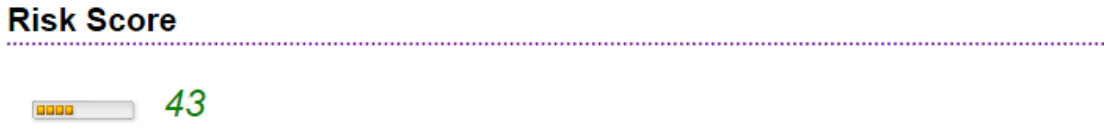


Figure 9 Risk Score

Risky Behaviors

As shown in **Figure 10**, Risky Behaviors table displays the suspicious embedded in this Android application.

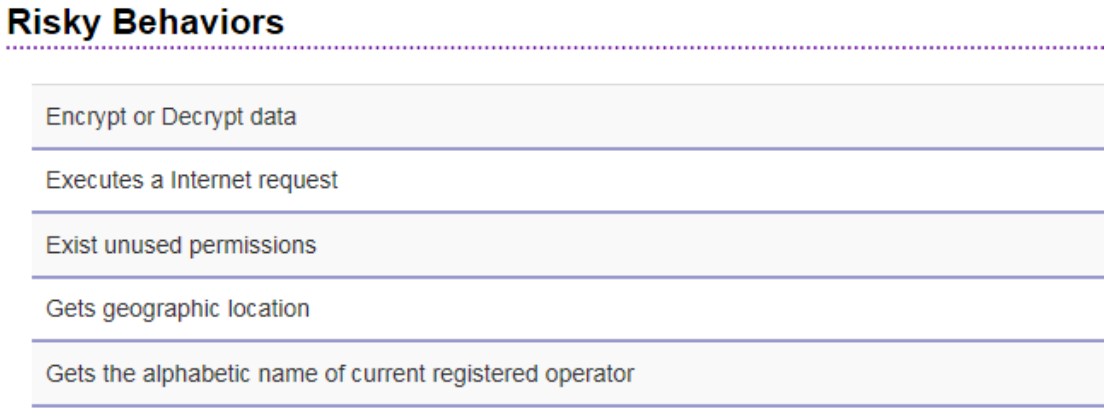


Figure 10 Risky Behaviors

Malware Detected by VirusTotal

The malware detection results are based on the VirusTotal.

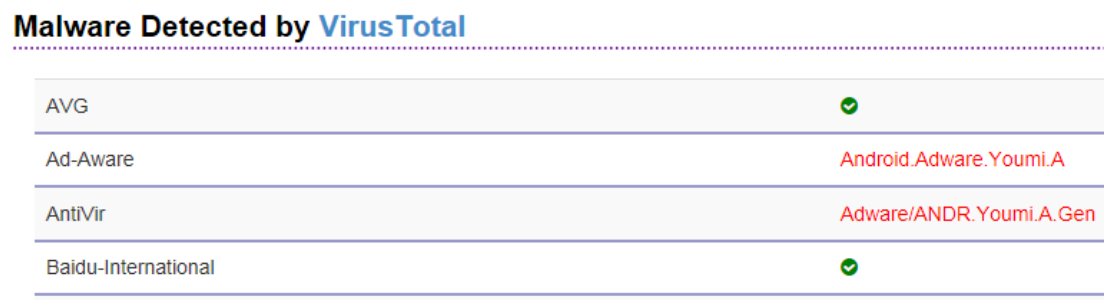


Figure 11 Malware Detected by VirusTotal

Certificate

The certification content is extracted from the META-INF/*.RSA of the Android application.

Certificate

Content	Owner: CN=YiKui, OU=K.U.I, O=K.U.I, L=ShenZhen, ST=GuangZhou, C=86 Issuer: CN=YiKui, OU=K.U.I, O=K.U.I, L=ShenZhen, ST=GuangZhou, C=86 Serial number: 4d6a5cef Valid from: Sun Feb 27 22:17:19 CST 2011 until: Mon Feb 14 22:17:19 CST 2061 Certificate fingerprints: MD5: F9:03:49:79:FE:8E:7F:8F:B5:6B:29:7B:8A:9A:8C:FB SHA1: 67:C8:F0:38:46:E1:79:13:A2:3C:D0:FA:64:1D:FB:9F:3D:4B:E5:CD SHA256: A8:87:A8:A8:2E:76:9C:06:24:C5:82:40:53:62:D5:D6:85:B3:CB:DB:18:39:84:F8:72:38:0C:AF:A9:FD:83:1B Signature algorithm name: SHA1withRSA Version: 3
Sha1	67C8F03846E17913A23CD0FA641DFB9F3D4BE5CD

Figure 12 Certificate

Classification

Classify this Android application based on permissions using ID3, NaiveBayes, Decision Table, J48 algorithms respectively and calculate the probability that which category the Android application belongs to.

Classification

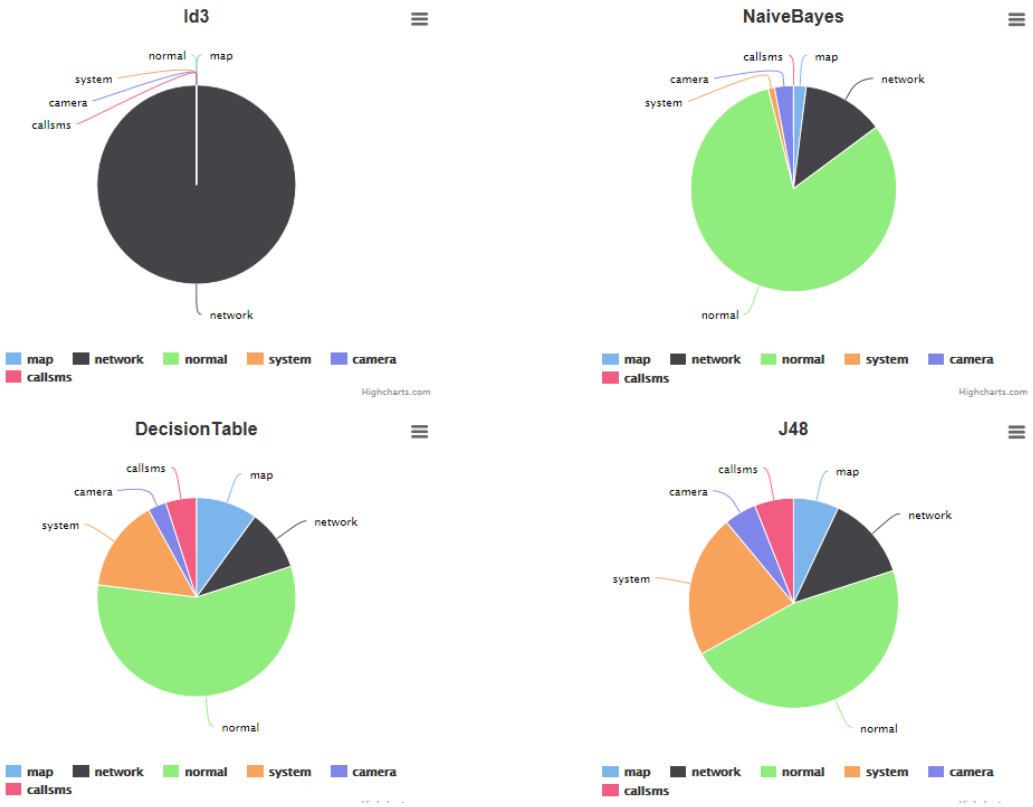


Figure 13 Classification

Code Features

As shown in **Figure 14**, Code Features table shows whether the Android application utilizes techniques including Native Code, Dynamic Loader, Java Reflection and Crypto.

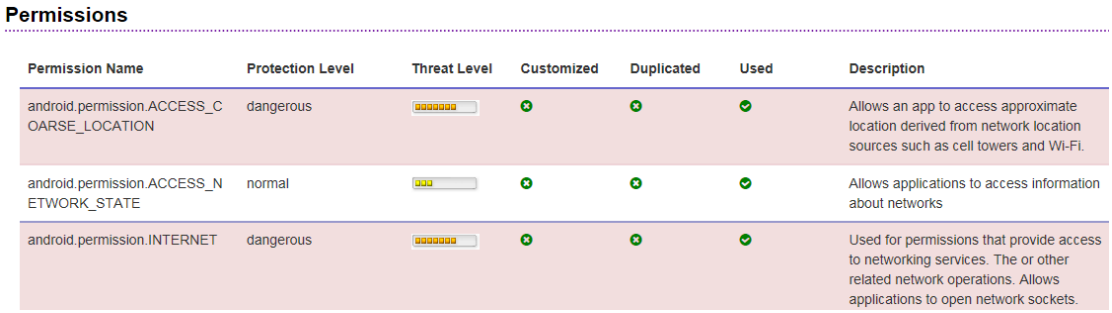
Code Features

Code Feature	Used
Native Code	✓
Dynamic Loader	✗
Java Reflection	✓
Crypto	✓

Figure 14 Code Features

Permissions

Display the permissions declared in the *AndroidManifest.xml*.



Permissions

Permission Name	Protection Level	Threat Level	Customized	Duplicated	Used	Description
android.permission.ACCESS_COARSE_LOCATION	dangerous		✗	✗	✓	Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal		✗	✗	✓	Allows applications to access information about networks
android.permission.INTERNET	dangerous		✗	✗	✓	Used for permissions that provide access to networking services. The or other related network operations. Allows applications to open network sockets.

Figure 15 Permissions

Components

Display the components declared in the Android application.

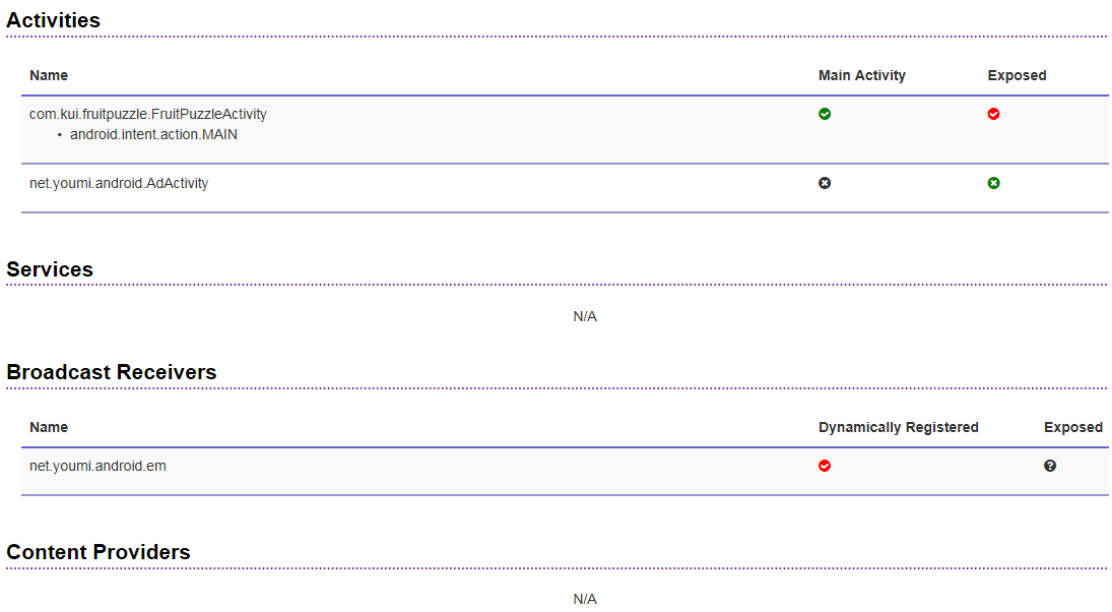


Figure 16 Components

Features

Display the features declared in the *AndroidManifest.xml*.

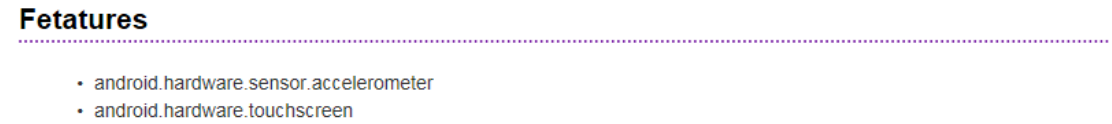


Figure 17 Features

Libraries

Display the libraries declared in the *AndroidManifest.xml*.

Figure 18 Libraries

Advertisement Modules

Display the advertisement modules used in this Android application.

Advertisement Modules

- AdColony
- AdMob
- Chartboost
- Domob
- Flurry
- HeyZap
- InMobi
- JumpTap
- MillennialMedia
- Mobclick

Figure 19 Advertisement Modules

IP Distribution

The geographical distribution of the ip addresses extracted from the Android application.

IP Distribution

Figure 20 IP Distribution

Urls

Display urls embedded in this Android applicaton and corresponding country name and ip address.

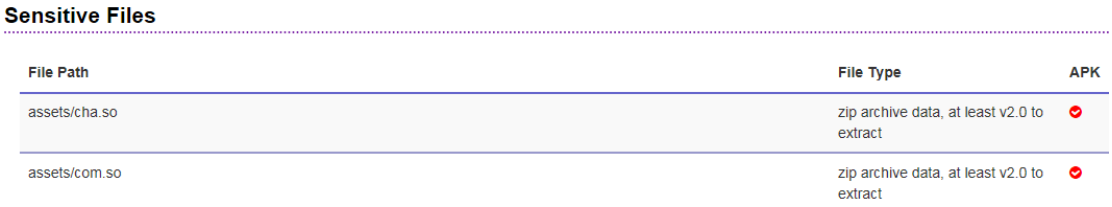
Urls

Country	Url	IP
Azerbaijan	https://www.facebook.com/dialog/feed?app_id=181821551957328&link=	37.61.54.158
Azerbaijan	http://twitter.com/home?status=	37.61.54.158
China	http://e.admob.com/imp?ad_loc=@gw_adlocid@&qdata=@gw_qdata@&ad_network_id=@gw_adnetid@&js=@gw_sdkver@&session_id=@gw_sessid@&seq_num=@gw_seqnum@&nr=@gw_adnetrefresh@&adt=@gw_adt@&aec=@gw_aec@	203.208.37.13

Figure 21 Urls

Sensitive Files

Display the sensitive files in this Android application.



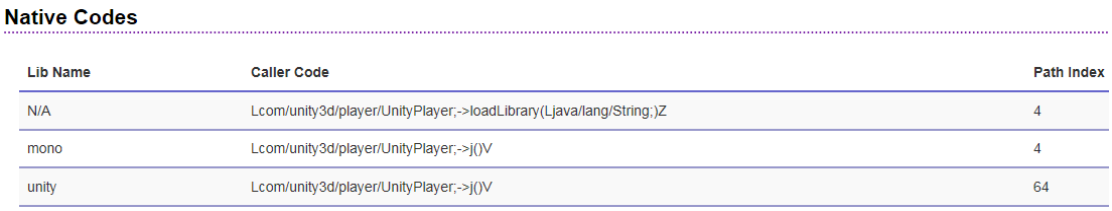
Sensitive Files

File Path	File Type	APK
assets/cha.so	zip archive data, at least v2.0 to extract	
assets/com.so	zip archive data, at least v2.0 to extract	

Figure 22 Sensitive Files

Native Codes

Display the information about calling native codes, such as library name, caller code, etc.



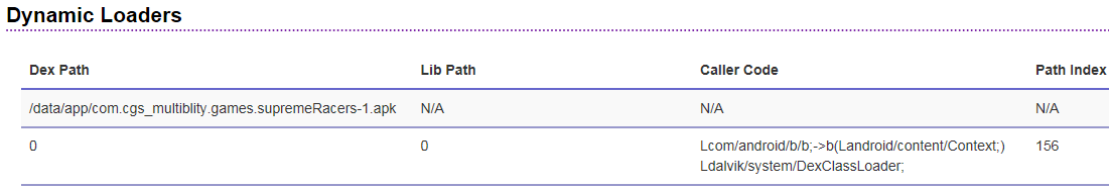
Native Codes

Lib Name	Caller Code	Path Index
N/A	Lcom/unity3d/player/UnityPlayer;->loadLibrary(Ljava/lang/String;)Z	4
mono	Lcom/unity3d/player/UnityPlayer;->j()V	4
unity	Lcom/unity3d/player/UnityPlayer;->j()V	64

Figure 23 Native Codes

Dynamic Loaders

Display the information about dynamic loaders in this Android application.



Dynamic Loaders

Dex Path	Lib Path	Caller Code	Path Index
/data/app/com.cgs_multiblity.games.supremeRacers-1.apk	N/A	N/A	N/A
0	0	Lcom/android/b/b;->b(Landroid/content/Context;)Ldalvik/system/DexClassLoader;	156

Figure 24 Dynamic Loaders

Crypto Operation

Display the information about crypto behavior in this Android application including algorithm used, plain text, cipher text, etc.

Crypto Operation

Operation	Algorithm	Key Encoded	Key Format	Plain Text	Cipher Text
encryption	AES/CBC /PKCS5Padding	33303231323130326469637564696162	RAW	357242043237511=37474F67E82E692AA949C9BAA90D2A9D	\xe1\x8f\xea\xa7\xe3\x96 \xc9\xee\xd4\xbb\x91q\xcf \xdbZ\x17\xb1'$\xb4%v \xe5\xb9>\xf1lP\xe9\xd3\xf1"' \xba\xdb\xf2N\x7f\x8e-\x98 \x9e\x12\x92\x8bw\xc8\x1c \x91\xe9\x96O\xec\x03`D \xfc\x1b0\xbbH\x14L_

Figure 25 Crypto Operation

Socket Connections

Display the socket connection information including remote address and remote port.

Socket Connections

Remote Address	Remote Port
claco.kicks-ass.net	9999
claco.kicks-ass.net	2641
claco.kicks-ass.net	9999
claco.kicks-ass.net	2965

Figure 26 Socket Connections

File Operations

Display the information about file operations during dynamic analysis.

File Operations

Operation	File Path	Data
write	/data/data/installer.com.rockstar.gta3/shared_prefs /PREFERENCE.xml	<?xml version='1.0' encoding='utf-8' standalone='yes' ?>\x0a<map>\x0a<boolean name="isFirstRun" value="fal

Figure 27 File Operations

DNS Query

Display DNS query information during dynamic analysis, such as QName, QType and ip addresses.

DNS Query

QName	QType	IPs
ads.net2share.com	A	216.158.77.154, 104.237.51.202
s.net2share.com	A	78.46.100.240

Figure 28 DNS Query

HTTP Data

Display information about HTTP Data generated during dynamic analysis.

HTTP Data

Method	Host	Path	Status Line
GET	ads.net2share.com	/config/1.0/ad.json?app=cw	HTTP/1.1 200 OK
GET	ads.net2share.com	/temporary_api/1.0/ad.json?type=app&incent=true	HTTP/1.1 200 OK
POST	s.net2share.com:8888	/beacon	HTTP/1.1 200 OK

Figure 29 HTTP Data

Files Recovered From Http

Display information about files recovered from http traffic produced during dynamic analysis.

Files Recovered From Http

Domain	File Name	File Type	Is APK
japp.apkshare.com	_api_i_php_cid_004003index.html	ASCII text, with very long lines, with no line terminators	⊗

Figure 30 Files Recovered From Http

Execute Shells

Display the shell commands executed by this Android application.

Execute Shells

- /system/bin/getprop
- /system/bin/getprop
- /system/bin/getprop

Figure 31 Execute Shells

Started Services

Display the information of started services.

Started Services

- Intent { act=com.google.app.DebugService.hfquewffhwuf83hasdf.ACTION_START cmp=installer.com.rockstar.gta3/com.adeco.adsdk.app.DebugService (has extras) }
- Intent { act=com.google.app.DebugService.hfquewffhwuf83hasdf.ACTION_START cmp=installer.com.rockstar.gta3/com.adeco.adsdk.app.DebugService (has extras) }

Figure 32 Started Services

May Send SMS

Extract SMS sending information through static analysis.

May Send SMS

Destination Number	Message Body	Caller Code	Path Index
N/A	N/A	Lcom/zplay/android/mm/d/a;->a(Landroid/app/Activity; Ljava/lang/String; Ljava/lang/String; Lcom/zplay/android/mm/d/g;)V	260
N/A	N/A	Lcom/zplay/android/mm/model/SmsMng;->a(J Ljava/lang/String; Ljava/lang/String;)V	108

Figure 33 May Send SMS

Send SMS

Display SMS sent information based on dynamic analysis.

Send SMS

Destination Number	Message Body
+79856842806	GNIM2A9pwttVZ0t657sBKNYLk/ZuOo66U+p96D1f8utlV3tK14sxGP04psFcDryKZ+p+6zhc8+p+FxkOso9ZS7lc0YIhDf7bEekrtGNbmO0lLj0W0/1xHaQg48daCrela+p96j5e8OI+V2BKzIpqA6NI+JgBTeCRFawgtC8orL8nCClex9RvCJNm5poPTuHIeO1i6SFY6et+Vw==

Figure 34 Send SMS

Block SMS

Display the information of the sms blocking behaviors.

Block SMS

Source Number	Message Body
null	
null	
null	
null	
null	http://glam-vids-nl.com/?cla=
null	http://glam-vids-nl.com/?cla=
null	FreeMSG
null	FreeMSG

Figure 35 Block SMS

Data Leakage

Display information about data leakage during dynamic analysis.

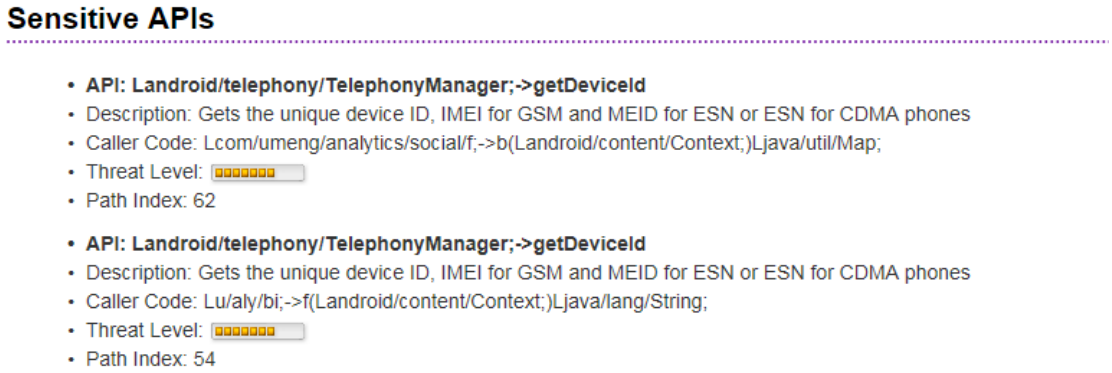
Data Leakage

Leak Type	Tag	Leak Data	Destination
File Write	TAINT_IMEI	<?xml version='1.0' encoding='utf-8' standalone='yes' ?>\x0a<map>\x0a<long name="session_end_time" value="	/data/data/com.brokenscreen.crackscreen /shared_prefs/umeng_general_config.xml
File Write	TAINT_IMEI	<?xml version='1.0' encoding='utf-8' standalone='yes' ?>\x0a<map>\x0a<long name="a_start_time" value="1417	/data/data/com.brokenscreen.crackscreen /shared_prefs/umeng_general_config.xml
File Write	TAINT_IMEI	\x1b\x02\xef\xbf\xbd\x0aandroid_id\x18\x10d091934bbabe6486\x16 \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdR\x15\x02\x00 \x04imei\x18\x0f357242043237511\x16 \xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbd\xef\xbf\xbdR\x15\x02\x00 \x19,\x18\x0aandroid_id(\x10d091934bba	/data/data/com.brokenscreen.crackscreen /files/umeng_it.cache

Figure 36 Data Leakage

Sensitive APIs

Display information about sensitive APIs.



Sensitive APIs

- **API: Landroid/telephony/TelephonyManager;->getDeviceId**
- Description: Gets the unique device ID, IMEI for GSM and MEID for ESN or ESN for CDMA phones
- Caller Code: Lcom/umeng/analytics/social/f;->b(Landroid/content/Context;)Ljava/util/Map;
- Threat Level:
- Path Index: 62

- **API: Landroid/telephony/TelephonyManager;->getDeviceId**
- Description: Gets the unique device ID, IMEI for GSM and MEID for ESN or ESN for CDMA phones
- Caller Code: Lu/aly/bi;->f(Landroid/content/Context;)Ljava/lang/String;
- Threat Level:
- Path Index: 54

Figure 37 Sensitive APIs

Permission Usage

In Android, if you want to call some special functions, you have to declare corresponding permissions in AndroidManifest.xml. As shown in **Figure 38**, it displays information about permission used in this apk, such as callee code correspond to permission.

Permission Usage

- **Permission Name: android.permission.ACCESS_NETWORK_STATE**
- Used Type: Api
- Caller Code: Landroid/support/v4/net/ConnectivityManagerCompat$GingerbreadConnectivityManagerCompatImpl;->isActiveNetworkMetered (Landroid/net/ConnectivityManager;)Z
- Callee Code: Landroid/support/v4/net/ConnectivityManagerCompatGingerbread;->isActiveNetworkMetered(Landroid/net/ConnectivityManager;)Z
- Path Index: 0

- **Permission Name: android.permission.ACCESS_NETWORK_STATE**
- Used Type: Api
- Caller Code: Landroid/support/v4/net/ConnectivityManagerCompat$HoneycombMR2ConnectivityManagerCompatImpl;->isActiveNetworkMetered (Landroid/net/ConnectivityManager;)Z
- Callee Code: Landroid/support/v4/net/ConnectivityManagerCompatHoneycombMR2;->isActiveNetworkMetered(Landroid/net/ConnectivityManager;)Z
- Path Index: 0

Figure 38 Permission Usage

Log Message

Display the logging messages during dynamic analysis.

Log Message

Tag	Message
Ads	Starting ad request.
Ads	Use AdRequest.Builder.addTestDevice("B3EEABB8EE11C2BE770B684D95219ECB") to g
Choreographer	Skipped 78 frames! The application may be doing too much work on its main thread.
Choreographer	Skipped 309 frames! The application may be doing too much work on its main thread.

Figure 39 Log Message

May Log Message

Display the information about log message extracted via static analysis.

May Log Message

Tag	Message	Caller Code	Path Index
ActionBarDrawerToggleHoneycomb	1	Landroid/support/v4/app/ActionBarDrawerToggleHoneycomb;->setActionBarDescription(Ljava/lang/Object; Landroid/app/Activity; I)Ljava/lang/Object;	78
ActionBarDrawerToggleHoneycomb	1	Landroid/support/v4/app/ActionBarDrawerToggleHoneycomb;->setActionBarUpIndicator(Ljava/lang/Object; Landroid/app/Activity; Landroid/graphics/drawable/Drawable; I)Ljava/lang/Object;	100
ActionBarDrawerToggleHoneycomb	1	Landroid/support/v4/app/ActionBarDrawerToggleHoneycomb;->setActionBarUpIndicator(Ljava/lang/Object; Landroid/app/Activity; Landroid/graphics/drawable/Drawable; I)Ljava/lang/Object;	136
ActionProvider(support)	2	Landroid/support/v4/view/ActionProvider;->setVisibilityListener (Landroid/support/v4/view/ActionProvider$VisibilityListener;)V	82

Figure 40 May Log Message

ScreenShots

The screenshots of the Android application's running on the Android

device.

ScreentShots

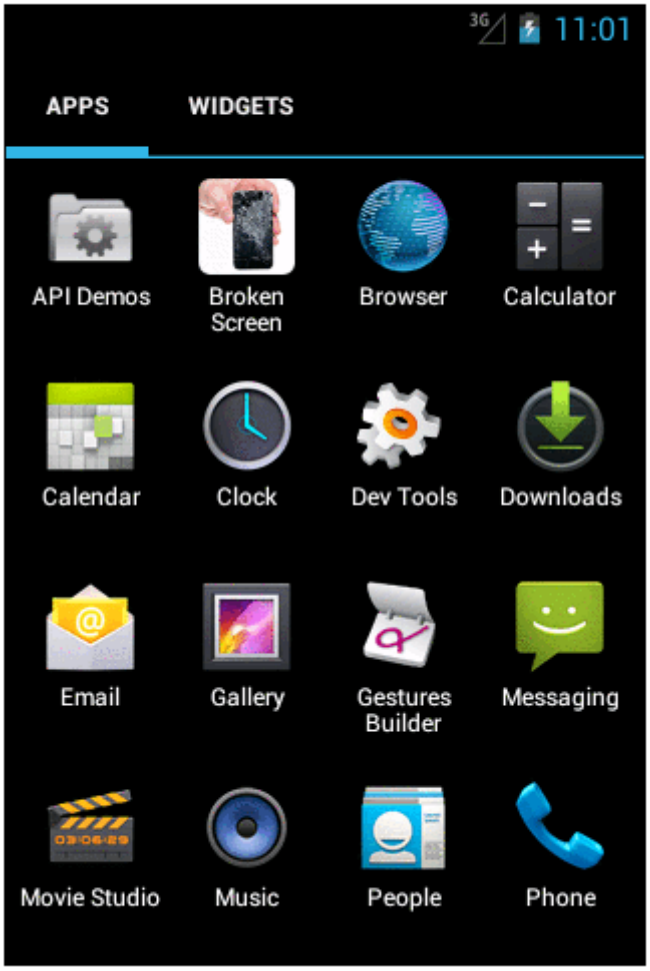


Figure 41 ScreenShots