



大金牙麻将 2.3.5.APK 分析报告



APP名称:

大金牙麻将

包名: com.leyou.ruianmahjong

域名线索: 35条

URL线索: 29条

邮箱线索: 2条

分析日期: 2025年6月21日

分析平台: [摸瓜APK反编译平台](#)

文件名: o_1ipp0oqklo9ofein19p531i7va.apk
文件大小: 124.57MB
MD5值: 5927c0616f6a4249b75663fe8e424428
SHA1值: 21efb737992bd33e45a43892725b0eae6353a577
SHA256值: c7d4b553fddcd1fb3afe83a01641fa4a4d40af46dda508b06bb2bea4bd8a1a67

i APP 信息

App名称: 大金牙麻将
包名: com.leyou.ruianmahjong
主活动Activity: org.cocos2dx.lua.AppActivity
安卓版本名称: 2.3.5
安卓版本: 235

🔍 域名线索

域名	服务器信息
www.browserleaks.com	IP: 104.236.69.55 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
mobilegw.stable.alipay.net	没有服务器地理信息.
bugzilla.mozilla.org	IP: 34.110.178.183 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568

mobilegw.aaa.alipay.net	没有服务器地理信息.
m.alipay.com	IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
cgicol.amap.com	IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
dualstack-arestapi.amap.com	IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mta.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
long.open.weixin.qq.com	IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948

mcgw.alipay.com	IP: 111.202.5.210 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
paygate-yf.meituan.com	IP: 103.37.152.89 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
xmlpull.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
example.com	IP: 23.192.228.80 所属国家: United States of America 地区: California 城市: Santa Clara 纬度: 37.354111 经度: -121.955490
mobilegw.alipaydev.com	IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
wappaygw.alipay.com	IP: 111.202.5.209 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

	经度: 116.397102
mta.oa.com	IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
valve.github.io	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
dualstack-a.apilocate.amap.com	IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
pingma.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 60.29.240.104 所属国家: China 地区: Tianjin

rqd.uu.qq.com	城市: Tianjin 纬度: 39.142181 经度: 117.176102
mobilegw.alipay.com	IP: 203.209.243.27 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
stats.magicwindow.cn	IP: 118.31.214.104 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mclient.alipay.com	IP: 116.142.235.203 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
lbs.amap.com	IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
apilocate.amap.com	IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

adiu.amap.com	IP: 110.253.189.147 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
sites.google.com	IP: 199.16.158.12 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
h5.m.taobao.com	IP: 60.9.1.94 所属国家: China 地区: Hebei 城市: Hengshui 纬度: 37.732220 经度: 115.701157
abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.opensource.org	IP: 172.67.26.198 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
android.bugly.qq.com	IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221

	经度: 123.432877
restsdk.amap.com	IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
open.weixin.qq.com	IP: 140.207.121.14 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948

URL线索

URL信息	Url所在文件
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/c.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&	com/alipay/sdk/data/a.java

https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple\	com/alipay/test/a.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/ama/api/location/AMapLocation.java
https://adiu.amap.com/ws/device/adius	com/loc/bi.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/cy.java
http://apilocate.amap.com/mobile/binary	com/loc/fp.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/loc/fp.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fp.java
https://restsdk.amap.com/sdk/compliance/params	com/loc/as.java
http://restsdk.amap.com/sdk/compliance/params	com/loc/as.java
http://restsdk.amap.com	com/loc/w.java
https://restsdk.amap.com/v3/iasdkauth	com/loc/n.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/loc/n.java
http://restsdk.amap.com/v3/place/text?	com/loc/a.java
http://restsdk.amap.com/v3/config/district?	com/loc/a.java

http://restsdk.amap.com/v3/place/around?	com/loc/a.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fv.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/loc/fj.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/fj.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fh.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/b/a/a.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/b/a/e.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/beta/upgrade/BetaUploadStrategy.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://github.com/Tencent/tinker/issues	com/tencent/tinker/lib/reporter/DefaultPatchReporter.java
https://github.com/Tencent/tinker/issues	com/tencent/tinker/lib/reporter/DefaultLoadReporter.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java

http://stats.magicwindow.cn	com/zxinsight/analytics/a/a.java
http://example.com/	cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java
https://github.com/Valve/fingerprintjs	摸瓜V2引擎
http://www.opensource.org/licenses/mit-license.php)	摸瓜V2引擎
http://github.com/garycourt/murmurhash-js	摸瓜V2引擎
http://sites.google.com/site/murmurhash/	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=781447	摸瓜V2引擎
https://www.browerleaks.com/canvas	摸瓜V2引擎
http://valve.github.io/;	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
8223939@qq.com	org/cocos2dx/lua/LuaCallTest.java
valentin.vasilyev@outlook.com gary.court@gmail.com aappleby@gmail.com	摸瓜V2引擎

 手机线索

手机号	所在文件
14222222222	com/loc/n.java

🌟 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=kn, ST=jkj, L=kljlk, O=lkjklj, OU=lk, CN=kljl
签名算法: rsassa_pkcs1v15
有效期自: 2018-01-06 14:47:36+00:00
有效期至: 3016-05-09 14:47:36+00:00
发行人: C=kn, ST=jkj, L=kljlk, O=lkjklj, OU=lk, CN=kljl
序列号: 0x4574d055
哈希算法: sha256
md5值: 2ae1550456ee22301187008dd4de81b0
sha1值: b44297de3fe682fc308a4a388f4480a255e76a8f
sha256值: ec5432cfc34c178caea24555bae6cdd3e89b845447fe12e3a03832e66664ec43
sha512值: 98731da31342b8351f0baeda5c13963281d94b4f248ad4a70308982b6fb67d8732c51a4d45564605f34c1dd884a902432f4899835bb1ad4b833cf6eb1ad9b52d
公钥算法: rsa
密钥长度: 2048
指纹: 5779820baafc5b569022eea979faf6809a33a0d94e6b3d8cbbe77c106c9b7669

🔑 硬编码敏感信息

🌀 加壳分析

加壳类型	所属文件
☞ 未知 ☞	

第三方插件

名称	分类	URL链接
登录摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改

android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。

应用内通信

活动(ACTIVITY)	通信(INTENT)
org.cocos2dx.lua.AppActivity	Schemes: yylink://,

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。