Evaluation Warning: The document was created with Spire.Doc for Python.

**大金牙麻将（ 2.3.5版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 大金牙麻将 |
| 版本 | 2.3.5 |
| 包名 | com.leyou.ruianmahjong |
| 域名线索 | 36条 |
| URL线索 | 30条 |
| APP图标 |  |
| 分析日期 | 2025年8月7日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | o\_1i9o4aaht1a6ttuu10ok10iaosa.apk |
| 文件大小 | 124.3MB |
| MD5值 | ef9d81990eae0af2f0955f0379289dc9 |
| SHA1值 | 941657aebe727598eaf481d250534f3ad925c098 |
| SHA256值 | 77a32b529c277f1b6b967e4f0854f4837ec695581ff601bd70a6c1b59d297c81 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| www.opensource.org | IP: 104.21.84.214  所属国家: United States of America  地区: California  城市: San Francisco |
| restapi.amap.com | IP: 203.119.169.174  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pingma.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| m.alipay.com | IP: 203.209.245.74  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| dualstack-arestapi.amap.com | IP: 39.98.22.142  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| mclient.alipay.com | IP: 1.190.42.122  所属国家: China  地区: Heilongjiang  城市: Harbin |
| example.com | IP: 93.184.215.14  所属国家: United States of America  地区: California  城市: Los Angeles |
| lbs.amap.com | IP: 110.253.188.148  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| mta.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| wappaygw.alipay.com | IP: 61.182.131.214  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| bugzilla.mozilla.org | IP: 34.110.178.183  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.browserleaks.com | IP: 104.236.69.55  所属国家: United States of America  地区: New Jersey  城市: Clifton |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| valve.github.io | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| open.weixin.qq.com | IP: 220.196.154.28  所属国家: China  地区: Jiangsu  城市: Wuxi |
| apilocate.amap.com | IP: 59.82.31.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| stats.magicwindow.cn | IP: 118.31.214.104  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| android.bugly.qq.com | IP: 124.95.225.169  所属国家: China  地区: Liaoning  城市: Shenyang |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| rqd.uu.qq.com | IP: 60.29.240.104  所属国家: China  地区: Tianjin  城市: Tianjin |
| sites.google.com | IP: 31.13.73.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| mcgw.alipay.com | IP: 61.182.131.214  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| cgicol.amap.com | IP: 110.253.188.148  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| abroad.apilocate.amap.com | IP: 59.82.44.11  所属国家: China  地区: Shanghai  城市: Shanghai |
| mobilegw.alipay.com | IP: 203.209.250.2  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| dualstack-a.apilocate.amap.com | IP: 106.11.40.50  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| restsdk.amap.com | IP: 59.82.132.217  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| paygate-yf.meituan.com | IP: 101.236.69.63  所属国家: China  地区: Beijing  城市: Beijing |
| adiu.amap.com | IP: 110.253.189.147  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| h5.m.taobao.com | IP: 125.38.11.131  所属国家: China  地区: Tianjin  城市: Tianjin |
| mta.oa.com | IP: 141.144.196.217  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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://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://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/amap/api/location/AMapLocation.java |
| https://adiu.amap.com/ws/device/adius | com/loc/bo.java |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74& | com/loc/df.java |
| http://apilocate.amap.com/mobile/binary | com/loc/fv.java |
| http://dualstack-a.apilocate.amap.com/mobile/binary | com/loc/fv.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fv.java |
| https://restsdk.amap.com/sdk/compliance/params | com/loc/ay.java |
| http://restsdk.amap.com/sdk/compliance/params | com/loc/ay.java |
| http://restsdk.amap.com | com/loc/w.java |
| https://restapi.amap.com/rest/aaid/get | com/loc/ag.java |
| http://restapi.amap.com/rest/aaid/get | com/loc/ag.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/gb.java |
| https://restsdk.amap.com/v3/iasdkauth | com/loc/n.java |
| https://dualstack-arestapi.amap.com/v3/iasdkauth | com/loc/n.java |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo | com/loc/fq.java |
| http://restsdk.amap.com/v3/geocode/regeo | com/loc/fq.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fo.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://android.bugly.qq.com/rqd/async | com/tencent/bugly/beta/upgrade/BetaUploadStrategy.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 |
| 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&timestamp=%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.browserleaks.com/canvas | 摸瓜V2引擎 |
| http://valve.github.io'; | 摸瓜V2引擎 |

### **4.3 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 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14222222222 | com/loc/n.java |

## **5. 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**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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的电话号码和序列号,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.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。 |

## **10. 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**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**