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

**赤金沉默（ 4.6.2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 | 赤金沉默 |
| 版本 | 4.6.2 |
| 包名 | com.fgcq.a115286 |
| 域名线索 | 116条 |
| URL线索 | 67条 |
| APP图标 |  |
| 分析日期 | 2025年6月21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\_1isqntmq512kp1tfu17cfpnoi669.apk |
| 文件大小 | 141.54MB |
| MD5值 | 39a739efc63a8f4558b0b0866d4ef79a |
| SHA1值 | ebef00cb59b5c81caf7d10174481253d0bb54e30 |
| SHA256值 | 90559ff2b7b4cb132ceb9f2b0ded0711921e8e860acc6a2528c6fcc90670bd7c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 赤金沉默 |
| 包名 | com.fgcq.a115286 |
| 主活动Activity | org.cocos2dx.cpp.AppActivity |
| 安卓版本名称 | 4.6.2 |
| 安卓版本 | 400000068 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| fortest.suqi.tech | IP: 122.9.98.227  所属国家: China  地区: Guangdong  城市: Guangzhou |
| pslog.umeng.com | IP: 59.82.31.160  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ye.dun.163yun.com | IP: 59.111.248.82  所属国家: China  地区: Guangdong  城市: Guangzhou |
| da.dun.163.com | IP: 59.111.248.82  所属国家: China  地区: Guangdong  城市: Guangzhou |
| ad.partner.gifshow.com | IP: 103.102.202.39  所属国家: China  地区: Beijing  城市: Beijing |
| ad-test.tj.996sdk.com | IP: 125.39.43.214  所属国家: China  地区: Tianjin  城市: Tianjin |
| utoken.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |
| open.e.189.cn | IP: 42.123.76.75  所属国家: China  地区: Beijing  城市: Beijing |
| fzb.tj.db996.cn | IP: 111.161.126.181  所属国家: China  地区: Tianjin  城市: Tianjin |
| api-pre.tj.996sdk.com | IP: 111.202.5.202  所属国家: China  地区: Beijing  城市: Beijing |
| cn-hangzhou.log.aliyuncs.com | IP: 121.43.10.93  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pay-sdkv2.ppp996.vkcgd.cn | IP: 111.161.126.184  所属国家: China  地区: Tianjin  城市: Tianjin |
| pay-sdkv2-test1.ppp996.vkcgd.cn | 没有服务器地理信息. |
| push-test.tj.996sdk.com | IP: 218.11.15.214  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| hhc.huohucloud.com | IP: 121.40.49.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| user-sdkv2.tj.db996.cn | IP: 111.202.5.195  所属国家: China  地区: Beijing  城市: Beijing |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| voice-test.tj.996sdk.com | IP: 111.202.5.198  所属国家: China  地区: Beijing  城市: Beijing |
| opencloud.wostore.cn | IP: 116.128.209.136  所属国家: China  地区: Beijing  城市: Beijing |
| sqc.pkfun.com | IP: 122.9.119.77  所属国家: China  地区: Guangdong  城市: Guangzhou |
| ad.tj.996sdk.com | IP: 218.11.15.214  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| mcgw.alipay.com | IP: 111.202.5.209  所属国家: China  地区: Beijing  城市: Beijing |
| privacy.data.znltc.net | IP: 124.95.150.70  所属国家: China  地区: Liaoning  城市: Shenyang |
| voice-test1.tj.996sdk.com | 没有服务器地理信息. |
| user-sdkv2.dhsf.996db.cn | IP: 111.202.5.195  所属国家: China  地区: Beijing  城市: Beijing |
| pay.ipaynow.cn | IP: 203.107.44.71  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| example.com | IP: 23.192.228.80  所属国家: United States of America  地区: California  城市: Santa Clara |
| api.e.kuaishou.com | IP: 116.136.202.194  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.slf4j.org | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| mobilegwpre.alipay.com | IP: 110.75.138.35  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| abtest.volceapplog.com | IP: 101.72.221.220  所属国家: China  地区: Hebei  城市: Langfang |
| api.api.znltc.cn | IP: 125.39.43.219  所属国家: China  地区: Tianjin  城市: Tianjin |
| api-e189.21cn.com | IP: 222.93.106.185  所属国家: China  地区: Jiangsu  城市: Suzhou |
| log.trackingio.com | IP: 52.80.89.130  所属国家: China  地区: Beijing  城市: Beijing |
| track-test.tj.996sdk.com | IP: 47.111.78.110  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| toblog.volceapplog.com | IP: 219.154.251.58  所属国家: China  地区: Henan  城市: Zhumadian |
| link.trackingio.com | IP: 54.223.80.43  所属国家: China  地区: Beijing  城市: Beijing |
| crash.163.com | IP: 45.254.50.146  所属国家: China  地区: Guangdong  城市: Guangzhou |
| tobapplog.volceapplog.com | IP: 125.39.61.78  所属国家: China  地区: Tianjin  城市: Tianjin |
| user-sdkv2.api.znltc.cn | IP: 125.39.61.78  所属国家: China  地区: Tianjin  城市: Tianjin |
| res.kf.996sdk.net | IP: 116.142.235.229  所属国家: China  地区: Beijing  城市: Beijing |
| pay-sdkv2-test.ppp996.vkcgd.cn | IP: 218.11.15.211  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| api-test1.tj.996sdk.com | 没有服务器地理信息. |
| user-sdkv2-test1.ppp996.hqyxkj.cn | 没有服务器地理信息. |
| pay-sdkv2.api.znltc.cn | IP: 111.161.126.183  所属国家: China  地区: Tianjin  城市: Tianjin |
| log-pre.tj.996sdk.com | IP: 125.39.61.80  所属国家: China  地区: Tianjin  城市: Tianjin |
| uri6.com | IP: 54.223.51.14  所属国家: China  地区: Beijing  城市: Beijing |
| openapi.dhsf.xqhuyu.com | IP: 111.161.126.180  所属国家: China  地区: Tianjin  城市: Tianjin |
| tdid.m.qq.com | IP: 60.29.239.156  所属国家: China  地区: Tianjin  城市: Tianjin |
| developer.umeng.com | IP: 59.82.31.210  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.ipify.org | IP: 104.26.12.205  所属国家: United States of America  地区: California  城市: San Francisco |
| alogsus.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pay-sdkv2.tj.db996.cn | IP: 111.202.5.202  所属国家: China  地区: Beijing  城市: Beijing |
| id6.me | IP: 42.123.77.138  所属国家: China  地区: Beijing  城市: Beijing |
| a.gdt.qq.com | IP: 220.194.116.30  所属国家: China  地区: Tianjin  城市: Tianjin |
| d.alipay.com | IP: 111.202.5.209  所属国家: China  地区: Beijing  城市: Beijing |
| hhc-server1.huohucloud.com | IP: 115.29.201.15  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mclient.alipay.com | IP: 116.142.235.203  所属国家: China  地区: Beijing  城市: Beijing |
| wap.cmpassport.com | IP: 120.232.169.168  所属国家: China  地区: Guangdong  城市: Guangzhou |
| user-sdkv2-test.ppp996.hqyxkj.cn | IP: 125.39.135.185  所属国家: China  地区: Tianjin  城市: Tianjin |
| ap-southeast-1.log.aliyuncs.com | IP: 161.117.125.94  所属国家: Singapore  地区: Singapore  城市: Singapore |
| pay-sdkv2.dhsf.996db.cn | IP: 111.161.126.179  所属国家: China  地区: Tianjin  城市: Tianjin |
| log.api.znltc.cn | IP: 47.97.49.18  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| event.gdt.qq.com | IP: 157.255.221.54  所属国家: China  地区: Guangdong  城市: Shenzhen |
| ulogs.umengcloud.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pay-sdkv2-test.ppp996.hqyxkj.cn | IP: 125.39.61.80  所属国家: China  地区: Tianjin  城市: Tianjin |
| test.huohucloud.com | IP: 47.97.40.93  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| user-sdkv2.api.znltc.net | IP: 111.161.126.180  所属国家: China  地区: Tianjin  城市: Tianjin |
| schemas.android.com | 没有服务器地理信息. |
| user-sdkv2-pre.dhsf.996db.cn | IP: 111.161.126.181  所属国家: China  地区: Tianjin  城市: Tianjin |
| klink.volceapplog.com | IP: 221.194.162.230  所属国家: China  地区: Hebei  城市: Langfang |
| api-test.tj.996sdk.com | IP: 111.202.5.201  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.alipay.com | IP: 203.209.243.27  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogus.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| api.tj.db996.cn | IP: 218.11.15.214  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| api.huohucloud.com | IP: 111.202.5.198  所属国家: China  地区: Beijing  城市: Beijing |
| api-pre.huohucloud.com | IP: 218.11.15.212  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| nisportal.10010.com | IP: 124.64.196.20  所属国家: China  地区: Beijing  城市: Beijing |
| pay-sdkv2-test1.ppp996.hqyxkj.cn | 没有服务器地理信息. |
| newtest.pkfun.com | IP: 47.107.105.60  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| servetf221.suqi.tech | IP: 122.9.48.225  所属国家: China  地区: Guangdong  城市: Guangzhou |
| ms.zzx9.cn | IP: 124.64.196.28  所属国家: China  地区: Beijing  城市: Beijing |
| privacy.tj.996sdk.com | IP: 218.11.15.215  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| m.alipay.com | IP: 203.209.245.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| plbslog.umeng.com | IP: 36.156.202.75  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| www.trackingio.com | IP: 52.80.176.105  所属国家: China  地区: Beijing  城市: Beijing |
| api.tj.996sdk.com | IP: 111.202.5.200  所属国家: China  地区: Beijing  城市: Beijing |
| voice.tj.db996.cn | IP: 221.194.162.224  所属国家: China  地区: Hebei  城市: Langfang |
| ad-pre.tj.996sdk.com | IP: 125.39.43.215  所属国家: China  地区: Tianjin  城市: Tianjin |
| analytics.oceanengine.com | IP: 219.154.251.56  所属国家: China  地区: Henan  城市: Zhumadian |
| alink.volceapplog.com | IP: 123.6.144.210  所属国家: China  地区: Henan  城市: Zhengzhou |
| pay-sdkv2-pre.dhsf.996db.cn | IP: 111.161.126.181  所属国家: China  地区: Tianjin  城市: Tianjin |
| h5pay.huohucloud.com | IP: 47.97.40.93  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.api.znltc.net | IP: 125.39.61.80  所属国家: China  地区: Tianjin  城市: Tianjin |
| voice.tj.996sdk.com | IP: 125.39.43.217  所属国家: China  地区: Tianjin  城市: Tianjin |
| log.reyun.com | IP: 54.223.72.156  所属国家: China  地区: Beijing  城市: Beijing |
| wappaygw.alipay.com | IP: 111.202.5.210  所属国家: China  地区: Beijing  城市: Beijing |
| h.trace.qq.com | IP: 113.56.189.246  所属国家: China  地区: Hubei  城市: Huangshi |
| yyx.pkfun.com | IP: 121.37.241.11  所属国家: China  地区: Guangdong  城市: Guangzhou |
| forsqc.suqi.tech | 没有服务器地理信息. |
| h5.m.taobao.com | IP: 101.72.202.199  所属国家: China  地区: Hebei  城市: Langfang |
| push-pre.tj.996sdk.com | IP: 125.39.61.76  所属国家: China  地区: Tianjin  城市: Tianjin |
| cptest.yaltc.cn | IP: 101.37.38.172  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| push.tj.996sdk.com | IP: 125.39.61.77  所属国家: China  地区: Tianjin  城市: Tianjin |
| msg.cmpassport.com | IP: 112.33.111.188  所属国家: China  地区: Anhui  城市: Hefei |
| log.tj.996sdk.com | IP: 47.111.88.34  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| databyterangers.com.cn | 没有服务器地理信息. |
| fzb.dhsf.996db.cn | IP: 111.202.5.196  所属国家: China  地区: Beijing  城市: Beijing |
| android.bugly.qq.com | IP: 124.95.225.146  所属国家: China  地区: Liaoning  城市: Shenyang |
| loggw-exsdk.alipay.com | IP: 110.76.6.75  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.95516.com | IP: 123.126.74.16  所属国家: China  地区: Beijing  城市: Beijing |
| ulogs.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pay-sdkv2.api.znltc.net | IP: 111.161.126.183  所属国家: China  地区: Tianjin  城市: Tianjin |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26  所属国家: United States of America  地区: California  城市: San Francisco |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://open.e.189.cn/openapi/special/getTimeStamp.do | cn/com/chinatelecom/account/api/e/h.java |
| https://api-e189.21cn.com/gw/client/accountMsg.do | cn/com/chinatelecom/account/api/e/h.java |
| https://cn-hangzhou.log.aliyuncs.com | com/alibaba/netspeed/network/Log.java |
| https://ap-southeast-1.log.aliyuncs.com | com/alibaba/netspeed/network/Log.java |
| http://m.alipay.com/?action=h5quit | com/alipay/sdk/m/x/e.java |
| https://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/app/PayTask.java |
| https://newtest.pkfun.com/cpc\_pro | com/cloudapp/client/request/cpc/HttpConfig.java |
| https://yyx.pkfun.com/cpc\_pro | com/cloudapp/client/request/cpc/HttpConfig.java |
| https://sqc.pkfun.com/cpc\_pro | com/cloudapp/client/request/cpc/HttpConfig.java |
| https://hhc-server1.huohucloud.com/ | com/cloudapp/client/trace/StreamSdkE.java |
| https://servetf221.suqi.tech/ | com/cloudapp/client/trace/StreamSdkE.java |
| https://cn-hangzhou.log.aliyuncs.com | com/cloudapp/client/trace/ali/StreamSdkQ.java |
| https://api.ipify.org | com/cloudapp/client/utils/Utils.java |
| http://wap.cmpassport.com/resources/html/contract.html | com/cmic/sso/sdk/view/LoginAuthActivity.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | com/cmic/sso/sdk/view/LoginAuthActivity.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/cmic/sso/sdk/view/LoginAuthActivity.java |
| https://pay.ipaynow.cn | com/ipaynow/plugin/inner\_plugin/wechatwp/activity/WeChatNotifyActivity.java |
| https://crash.163.com/uploadCrashLogInfo.do | com/netease/htprotect/necrash/nis/crashreport/O8oO888.java |
| https://crash.163.com/uploadCrashLogInfo.do | com/netease/htprotect/necrash/nis/p001O8oO888/p002O8oO888/O8oO888.java |
| https://da.dun.163.com/sn.gif?d= | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java |
| https://ye.dun.163yun.com/v1/preCheck | com/netease/nis/quicklogin/QuickLogin.java |
| https://ye.dun.163yun.com/v1/oneclick/preCheck | com/netease/nis/quicklogin/QuickLogin.java |
| https://a.gdt.qq.com/getSdkConf | com/qq/gdt/action/i/b.java |
| http://a.gdt.qq.com/getSdkConf | com/qq/gdt/action/i/b.java |
| https://a.gdt.qq.com/sdk | com/qq/gdt/action/i/c.java |
| http://a.gdt.qq.com/sdk | com/qq/gdt/action/i/c.java |
| http://event.gdt.qq.com/report | com/qq/gdt/action/i/a.java |
| https://event.gdt.qq.com/report | com/qq/gdt/action/i/a.java |
| https://log.reyun.com/receive/pkginfo | com/reyun/tracking/utils/c.java |
| https://log.trackingio.com/ | com/reyun/tracking/utils/c.java |
| https://link.trackingio.com/dpquery | com/reyun/tracking/utils/r.java |
| https://uri6.com/tkio/attributionquery?os=android&appkey= | com/reyun/tracking/utils/t.java |
| https://www.trackingio.com/authorization/close\_data\_share | com/reyun/tracking/sdk/g.java |
| http://schemas.android.com/android/skin | com/sq/libhotfix/skin/SUnionSdkWW.java |
| https://cptest.yaltc.cn\ | com/sq/sdk/cloudgame/CloudSdk.java |
| https://hhc-server1.huohucloud.com\ | com/sq/sdk/cloudgame/CloudSdk.java |
| https://hhc.huohucloud.com\ | com/sq/sdk/cloudgame/CloudSdk.java |
| https://yyx.pkfun.com/fastcloud\_h5/game.html?sqcloudsample://open/params? | com/sq/sdk/cloudgame/ui/CloudJoinLivePlayActivity.java |
| https://yyx.pkfun.com/fastcloud\_h5/game.html?sqcloudsample://open/params? | com/sq/sdk/cloudgame/ui/CloudPlayerActivity.java |
| https://sqc.pkfun.com/fastcloud\_h5/game.html?sqcloudsample://open/params? | com/sq/sdk/cloudgame/ui/ctrl/TphdControlBar.java |
| https://yyx.pkfun.com/fastcloud\_h5/game.html?sqcloudsample://open/params? | com/sq/sdk/cloudgame/ui/ctrl/TphdControlBar.java |
| https://newtest.pkfun.com/fastcloud\_h5/game.html?sqcloudsample://open/params? | com/sq/sdk/cloudgame/ui/ctrl/TphdControlBar.java |
| https://tdid.m.qq.com?mc=2 | com/tencent/turingfd/sdk/ams/ad/Core.java |
| https://h.trace.qq.com/kv | com/tencent/bugly/proguard/ad.java |
| https://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/proguard/ac.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/proguard/ac.java |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://utoken.umeng.com/api/postZdata/v4 | com/umeng/umzid/ZIDManager.java |
| https://utoken.umeng.com/api/updateZdata/v4 | com/umeng/umzid/ZIDManager.java |
| https://res.kf.996sdk.net/im/customer/ | com/xqhy/customerservice/view/CustomerServiceWebView.java |
| https://fzb.dhsf.996db.cn | com/xqhy/lib/network/net/HttpConstant.java |
| https://privacy.tj.996sdk.com/children.html?game\_id=2 | com/xqhy/lib/network/net/HttpConstant.java |
| https://privacy.tj.996sdk.com/tripartite.html?game\_id=2 | com/xqhy/lib/network/net/HttpConstant.java |
| https://privacy.tj.996sdk.com/Privacy.html?game\_id=2 | com/xqhy/lib/network/net/HttpConstant.java |
| https://privacy.tj.996sdk.com/register.html?game\_id=2 | com/xqhy/lib/network/net/HttpConstant.java |
| https://user-sdkv2.tj.db996.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2.tj.db996.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://api.tj.db996.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://voice.tj.db996.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://fzb.tj.db996.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://track-test.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://api-test.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://user-sdkv2-test.ppp996.hqyxkj.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2-test.ppp996.hqyxkj.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2-test.ppp996.vkcgd.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://voice-test.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://push-test.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://ad-test.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://log-pre.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://api-pre.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://user-sdkv2-pre.dhsf.996db.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2-pre.dhsf.996db.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://push-pre.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://ad-pre.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://log.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://api.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://user-sdkv2.dhsf.996db.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2.dhsf.996db.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2.ppp996.vkcgd.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://voice.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://push.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://ad.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://privacy.data.znltc.net/Privacy.html?game\_id=12 | com/xqhy/lib/network/net/DomainUtil.java |
| https://privacy.data.znltc.net/register.html?game\_id=12 | com/xqhy/lib/network/net/DomainUtil.java |
| https://privacy.data.znltc.net/children.html?game\_id=12 | com/xqhy/lib/network/net/DomainUtil.java |
| https://privacy.data.znltc.net/tripartite.html?game\_id=12 | com/xqhy/lib/network/net/DomainUtil.java |
| https://user-sdkv2.api.znltc.net | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2.api.znltc.net | com/xqhy/lib/network/net/DomainUtil.java |
| https://api.api.znltc.net | com/xqhy/lib/network/net/DomainUtil.java |
| https://log.api.znltc.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://api-test1.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://user-sdkv2-test1.ppp996.hqyxkj.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2-test1.ppp996.hqyxkj.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2-test1.ppp996.vkcgd.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://voice-test1.tj.996sdk.com | com/xqhy/lib/network/net/DomainUtil.java |
| https://api.api.znltc.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://user-sdkv2.api.znltc.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://pay-sdkv2.api.znltc.cn | com/xqhy/lib/network/net/DomainUtil.java |
| https://api-pre.huohucloud.com | com/xqhy/cloudphone/util/CloudPhoneUrlConstant$CP\_BASE\_URL$2.java |
| https://api.huohucloud.com | com/xqhy/cloudphone/util/CloudPhoneUrlConstant$CP\_BASE\_URL$2.java |
| https://test.huohucloud.com | com/xqhy/cloudphone/util/CloudPhoneUrlConstant$CP\_WX\_PAY\_REFERER$2.java |
| https://h5pay.huohucloud.com | com/xqhy/cloudphone/util/CloudPhoneUrlConstant$CP\_WX\_PAY\_REFERER$2.java |
| https://h5pay.huohucloud.com/chat | com/xqhy/cloudphone/util/CloudPhoneUrlConstant$USER\_CUSTOMER\_URL$2.java |
| http://mclient.alipay.com | com/xqhy/pay/wechat/WechatPayWebActivity.java |
| https://mclient.alipay.com | com/xqhy/pay/wechat/WechatPayWebActivity.java |
| https://api.e.kuaishou.com/rest/config/client/v1/open/sdkGatherConfig | com/xqhy/tripartite/TripartiteSdkManager.java |
| http://example.com/ | cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java |
| https://d.alipay.com | org/cocos2dx/lib/Cocos2dxWebView.java |
| http://openapi.dhsf.xqhuyu.com/api/UserInfo/getUserBaseInfo? | org/cocos2dx/cpp/SDKUtil.java |
| http://www.slf4j.org/codes.html | org/slf4j/MDC.java |
| http://www.slf4j.org/codes.html | org/slf4j/LoggerFactory.java |
| https://h5.m.taobao.com/mlapp/olist.html | xqj/xqj/hyj/xqk/n/xqj.java |
| https://mcgw.alipay.com/sdklog.do | xqj/xqj/hyj/xqk/u/xqk.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | xqj/xqj/hyj/xqk/u/xql.java |
| https://mobilegw.alipaydev.com/mgw.htm | xqj/xqj/xqj/xqj/xqj/xqj/r.java |
| https://mobilegw.alipay.com/mgw.htm | xqj/xqj/xqj/xqj/xqj/xqj/r.java |
| https://mobilegwpre.alipay.com/mgw.htm | xqj/xqj/xqk/xqk/xqj.java |
| https://mobilegw.alipay.com/mgw.htm | xqj/xqj/xqk/xqk/xqj.java |
| https://pay.ipaynow.cn/sdk/syncException | xqj/xql/xqj/xqk/xql.java |
| https://ye.dun.163yun.com/v2/collect | xqg/xqg/xqg/xqg/hyg/hyh.java |
| https://ms.zzx9.cn/html/oauth/protocol2.html | xqg/xqg/xqg/xqg/hyg/xqh.java |
| https://wap.cmpassport.com/resources/html/contract.html | xqg/xqg/xqg/xqg/hyg/xqh.java |
| https://e.189.cn/sdk/agreement/content.do?type=main&appKey=&hidetop=true | xqg/xqg/xqg/xqg/hyg/xqh.java |
| https://api.e.kuaishou.com/rest/config/client/v1/open/globalId | xqu/xqu/xqu/xqv/hyv.java |
| https://ad.partner.gifshow.com/api/v2/sdk/log?token=dee6172daef74f0895c7d185956ac0a7 | xqu/xqu/xqu/xqv/hyv.java |
| https://api.e.kuaishou.com/rest/config/client/v1/open/sdkGatherConfig | xqu/xqu/xqu/hyv/xqv.java |
| https://databyterangers.com.cn | xqv/xqu/hyu/q2.java |
| https://nisportal.10010.com:9001/api?appid=1554778161154 | xqv/xqu/xqu/xqu/xqu/xqu/hyu.java |
| https://msg.cmpassport.com/h5/getMobile | xqv/xqu/xqu/xqu/xqu/xqu/xqv.java |
| https://id6.me/gw/preuniq.do | xqv/xqu/xqu/xqu/xqu/xqu/xqw.java |
| https://analytics.oceanengine.com/sdk/app/ | xqv/xqu/xqv/xqu/a/c.java |
| https://klink.volceapplog.com/service/2/device\_register/ | xqv/xqu/xqw/q/hyv.java |
| https://klink.volceapplog.com/service/2/device\_update | xqv/xqu/xqw/q/hyv.java |
| https://klink.volceapplog.com/service/2/app\_alert\_check/ | xqv/xqu/xqw/q/hyv.java |
| https://toblog.volceapplog.com/service/2/app\_log/ | xqv/xqu/xqw/q/hyv.java |
| https://tobapplog.volceapplog.com/service/2/app\_log/ | xqv/xqu/xqw/q/hyv.java |
| https://toblog.volceapplog.com/service/2/profile/ | xqv/xqu/xqw/q/hyv.java |
| https://toblog.volceapplog.com/service/2/log\_settings/ | xqv/xqu/xqw/q/hyv.java |
| https://abtest.volceapplog.com/service/2/abtest\_config/ | xqv/xqu/xqw/q/hyv.java |
| https://alink.volceapplog.com/service/2/attribution\_data | xqv/xqu/xqw/q/hyv.java |
| https://alink.volceapplog.com/service/2/alink\_data | xqv/xqu/xqw/q/hyv.java |
| https://newtest.pkfun.com/ | 摸瓜V1引擎 |
| https://yyx.pkfun.com/ | 摸瓜V1引擎 |
| https://sqc.pkfun.com/ | 摸瓜V1引擎 |
| https://forsqc.suqi.tech/ | 摸瓜V1引擎 |
| https://fortest.suqi.tech/ | 摸瓜V1引擎 |
| https://www.95516.com/portal/open/init.do?entry=open | 摸瓜V1引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| .apk@classes.dex | com/tencent/turingfd/sdk/ams/ad/Cstatic.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13200000256 | com/sq/sdk/cloudgame/Constants.java |
| 13300000121 | com/sq/sdk/cloudgame/Constants.java |
| 15251596565 | com/sq/sdk/cloudgame/Constants.java |
| 15251580731 | com/sq/sdk/cloudgame/Constants.java |
| 13300000091 | com/sq/sdk/cloudgame/CloudSdk.java |
| 13200000126 | com/sq/sdk/cloudgame/CloudSdk.java |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=CN, ST=hangzhou, L=hangzhou, O=xianqu, OU=xianqu, CN=shengfeiyue 签名算法: rsassa\_pkcs1v15 有效期自: 2020-12-23 03:32:48+00:00 有效期至: 2048-05-10 03:32:48+00:00 发行人: C=CN, ST=hangzhou, L=hangzhou, O=xianqu, OU=xianqu, CN=shengfeiyue 序列号: 0x77862009 哈希算法: sha256 md5值: a00e20e1bde5d12b30843c7eb2263ab3 sha1值: 2bf8b0f7ec08d9f5cba9811766582d75aa39a983 sha256值: 7eb19077fb5e0a0a37d89575c6750421748f6009ef571b9f7255e212f269f250 sha512值: 4dd6c6d7ad85bb8473cd08cf9155c102ec3c00395e6eb13b070a00c6c8b91f279b251b6e097bbebd6b52d5905ff2b5bb886d6ade6cc9d6386a7863d5c51aaa07 公钥算法: rsa 密钥长度: 2048 指纹: 64b9d57b96a1a4edc28497c544899a348ec4ab54725f8f17497d1fb18bd91a66**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "again\_input\_password" : "再次输入密码" |
| "api\_auth\_token" : "yun/temp/auth.json" |
| "api\_check\_token\_reconnect" : "room/yun/check/box/device/check/reconnect" |
| "api\_client\_kick\_user" : "yun/client/room/visitor/exit" |
| "api\_client\_token\_batchStorage" : "yun/client/inner/yun/batchStorage" |
| "api\_client\_token\_device\_check\_support\_dec\_optimization" : "yun/client/inner/check/supportDecOptimization" |
| "api\_client\_token\_device\_get\_asyn\_autostream" : "yun/client/inner/device/open/autostreamingjobresult" |
| "api\_client\_token\_device\_set\_afk\_time" : "yun/client/inner/hang/up/time" |
| "api\_client\_token\_download\_backup\_files" : "yun/client/inner/get/temporary/url" |
| "api\_client\_token\_get\_osb\_tmp\_url" : "yun/client/device/get/app/upload/url" |
| "api\_client\_token\_get\_profile" : "yun/client/inner/get/proFile" |
| "api\_client\_token\_get\_token" : "yun/temp/token/client/auth" |
| "api\_client\_token\_install\_apk" : "yun/client/device/notice/upload/and/install/app" |
| "api\_client\_token\_join" : "yun/client/inner/room/get" |
| "api\_client\_token\_last\_profile\_codec" : "yun/client/inner/get/category/coding" |
| "api\_client\_token\_open\_streaming" : "yun/client/inner/device/open/streaming" |
| "api\_client\_token\_reboot" : "yun/client/device/reboot" |
| "api\_client\_token\_record\_codec" : "yun/client/inner/record/category/coding" |
| "api\_client\_token\_restart" : "/yun/client/device/user/restart" |
| "api\_client\_token\_root" : "/yun/client/device/toggle/root" |
| "api\_client\_token\_rtsa\_batchStorage" : "yun/client/inner/rtsa/v2/yun/batchStorage" |
| "api\_client\_token\_rtsa\_device\_check\_support\_dec\_optimization" : "yun/client/inner/rtsa/v2/check/supportDecOptimization" |
| "api\_client\_token\_rtsa\_device\_get\_asyn\_autostream" : "yun/client/inner/rtsa/v2/open/autostreamingjobresult" |
| "api\_client\_token\_rtsa\_device\_set\_afk\_time" : "yun/client/inner/rtsa/v2/hang/up/time" |
| "api\_client\_token\_rtsa\_download\_backup\_files" : "yun/client/inner/rtsa/v2/get/temporary/url" |
| "api\_client\_token\_rtsa\_get\_osb\_tmp\_url" : "yun/client/device/get/app/upload/url" |
| "api\_client\_token\_rtsa\_get\_profile" : "yun/client/inner/rtsa/v2/get/proFile" |
| "api\_client\_token\_rtsa\_install\_apk" : "yun/client/device/notice/upload/and/install/app" |
| "api\_client\_token\_rtsa\_join" : "yun/client/inner/rtsa/v2/room/get" |
| "api\_client\_token\_rtsa\_last\_profile\_codec" : "yun/client/inner/rtsa/v2/get/category/coding" |
| "api\_client\_token\_rtsa\_open\_streaming" : "yun/client/inner/rtsa/v2/open/streaming" |
| "api\_client\_token\_rtsa\_reboot" : "yun/client/device/reboot" |
| "api\_client\_token\_rtsa\_record\_codec" : "yun/client/inner/rtsa/v2/record/category/coding" |
| "api\_client\_token\_rtsa\_screenshot" : "yun/client/inner/rtsa/v2/get/param/screenshot" |
| "api\_client\_token\_rtsa\_start" : "yun/client/inner/rtsa/v2/open/autostreaming" |
| "api\_client\_token\_rtsa\_state\_query" : "yun/client/inner/rtsa/v2/get/isOk" |
| "api\_client\_token\_screenshot" : "yun/client/inner/get/param/screenshot" |
| "api\_client\_token\_start" : "yun/client/inner/device/open/autostreaming" |
| "api\_client\_token\_state\_query" : "yun/client/inner/get/isOk" |
| "api\_get\_token" : "yun/user/token/auth" |
| "api\_kick\_user" : "yun/mix/inner/room/visitor/exit" |
| "api\_queue\_token\_check" : "yun/inner/queue/token/valid" |
| "api\_rtsa\_check\_token\_reconnect" : "room/yun/check/Rtsa/device/check/reconnect" |
| "app\_key" : "4ce7a679d57aa7d682eac30493c79f8e" |
| "err\_auth\_dented" : "认证被否决" |
| "forget\_password" : "忘记密码" |
| "forget\_pwd" : "忘记密码" |
| "input\_password" : "请输入密码" |
| "input\_username" : "请输入您的用户名" |
| "login\_forget\_password" : "忘记密码？" |
| "password" : "密码" |
| "please\_input\_enter\_password" : "请输入正确的密码" |
| "please\_input\_password" : "请输入密码" |
| "pos\_pwd\_display\_yiqianbao" : "请输入壹钱包支付密码:" |
| "ppplugin\_dialog\_purse\_not\_get\_pwdinfo\_yiqianbao" : "壹钱包密码键盘无密文信息返回" |
| "ppplugin\_forgetpwd\_prompt" : "忘记密码" |
| "ppplugin\_input\_cardinfo\_cardpwd\_prompt" : "确认密码" |
| "ppplugin\_inputpaypwd\_pos\_prompt" : "请输入6位全民付移动支付密码" |
| "ppplugin\_inputpaypwd\_prompt" : "请输入6位支付密码" |
| "ppplugin\_inputpwddialog\_accbalance\_prompt" : "账户余额" |
| "ppplugin\_inputpwddialog\_coupon\_prompt" : "优惠券" |
| "ppplugin\_microfreepwd\_amount\_prompt" : "免密金额" |
| "ppplugin\_microfreepwd\_pay\_prompt" : "小额免密支付" |
| "ppplugin\_microfreepwd\_prompt" : "小额免密" |
| "ppplugin\_microfreepwd\_switchoff" : "关闭" |
| "ppplugin\_microfreepwd\_switchon" : "已开启" |
| "ppplugin\_microfreepwd\_use\_prompt" : "超过免密额度时，需要验证支付密码，并且系统会移除可疑交易。" |
| "ppplugin\_modifypaypwd\_ok" : "支付密码修改成功" |
| "ppplugin\_modifypwd\_prompt" : "修改支付密码" |
| "ppplugin\_resetpaypwd\_ok" : "支付密码重置成功" |
| "ppplugin\_session\_timeout\_prompt" : "由于您长时间未操作，请重新登录" |
| "ppplugin\_set\_pwd\_prompt" : "设置密码" |
| "session\_timeout" : "会话超时,请重新登录" |
| "streamsdk\_auth\_label" : "<font color=#F4F5F6>确定授权给您的好友</font><font color=#008577>%1$s</font><font color=#F4F5F6>吗，授权后他将有权限操控您当前应用的屏幕，可以与您和其他观众进行同屏互动!</font>" |
| "streamsdk\_dialog\_auth" : "授权" |
| "streamsdk\_dialog\_un\_auth" : "授权收回" |
| "streamsdk\_dialog\_un\_auth\_label" : "<font color=#F4F5F6>确定收回您的好友</font><font color=#008577>%1$s</font><font color=#F4F5F6>的操控权限吗，收回后他将只能观看您当前应用的屏幕，您可再次授权给他进行同屏互动</font>" |
| "streamsdk\_ui\_auth\_user" : "授权接力" |
| "streamsdk\_ui\_dialog\_duplicated\_user" : "当前云机已在其它设备登录，请退出重试或联系客服!" |
| "streamsdk\_ui\_terminate\_session" : "云机服务已结束" |
| "streamsdk\_ui\_unauth\_user" : "取消授权" |
| "tips\_amount\_free\_pwd" : "已为您开启200元额度小额免密，可在右上角设置" |
| "tips\_input\_password" : "为了您的账号安全请输入支付密码" |
| "umcsdk\_oauth\_version\_name" : "v1.4.1" |
| "umeng\_appkey" : "615ec92814e22b6a4f1503fd" |
| "unisdk\_dialog\_auth" : "授权" |
| "unisdk\_dialog\_auth\_user" : "是否授予控制权限给您已分享出去的用户 %s, 授权后他将有权限操控您当前应用的屏幕，可以与您和其他观众进行同屏互动!" |
| "unisdk\_dialog\_un\_auth" : "授权收回" |
| "unisdk\_dialog\_un\_auth\_user" : "确定收回您的好友 %s 的操控权限吗? 收回后他将只能观看您当前应用的屏幕，您可再次授权给他进行同屏互动" |
| "unisdk\_ui\_auth\_user" : "授权接力" |
| "unisdk\_ui\_unauth\_user" : "取消授权" |
| "xqhy\_cs\_stopSessionDesc" : "当前正在会话中，确定结束会话？" |
| "streamsdk\_auth\_label" : "<font color=#F4F5F6>Authorize your friend?</font><font color=#008577>%1$s</font><font color=#F4F5F6>This will give him the ability to control the screen of your current application and interact with you and other viewers on the room!</font>" |
| "streamsdk\_dialog\_auth" : "Authorization" |
| "streamsdk\_dialog\_un\_auth" : "Revoke authorization" |
| "streamsdk\_dialog\_un\_auth\_label" : "<font color=#F4F5F6>Are you sure to revoke your friend's control rights</font><font color=#008577>%1$s</font><font color=#F4F5F6>If you revoke your friend's control rights, he will only be able to view the screen of your current application, and you can authorize him to interact with the screen again</font>" |
| "streamsdk\_ui\_auth\_user" : "Authorized Relay" |
| "streamsdk\_ui\_dialog\_duplicated\_user" : "Has been logged in on another device, please exit and try again or contact us!" |
| "streamsdk\_ui\_terminate\_session" : "Streaming session terminated" |
| "streamsdk\_ui\_unauth\_user" : "Cancel Authorization" |
| "unisdk\_dialog\_auth" : "Authorization" |
| "unisdk\_dialog\_auth\_user" : "Whether to grant control rights to your shared user %s, after authorization, he will have the right to control the screen of your current application, can interact with you and other viewers on the same screen!" |
| "unisdk\_dialog\_un\_auth" : "Revoke authorization" |
| "unisdk\_dialog\_un\_auth\_user" : "Are you sure to take back control of your friend %s? After it is taken back, he will only be able to view the screen of your current app, and you can authorize him to interact with the same screen again" |
| "unisdk\_ui\_auth\_user" : "Authorized Relay" |
| "unisdk\_ui\_unauth\_user" : "Cancel Authorization" |
| "streamsdk\_auth\_label" : "<font color=#F4F5F6>確定授權給您的好友</font><font color=#008577>%1$s</font><font color=#F4F5F6>嗎，授權後他將有權限操控您當前應用的屏幕，可以與您和其他觀眾進行同屏互動!</font>" |
| "streamsdk\_dialog\_auth" : "授權" |
| "streamsdk\_dialog\_un\_auth" : "授權收回" |
| "streamsdk\_dialog\_un\_auth\_label" : "<font color=#F4F5F6>確定收回您的好友</font><font color=#008577>%1$s</font><font color=#F4F5F6>的操控權限嗎，收回後他將只能觀看您當前應用的屏幕，您可再次授權給他進行同屏互動</font>" |
| "streamsdk\_ui\_auth\_user" : "授權接力" |
| "streamsdk\_ui\_dialog\_duplicated\_user" : "當前雲機已在其它設備登錄，請退出重試或聯繫客服!" |
| "streamsdk\_ui\_terminate\_session" : "串流會話終止" |
| "streamsdk\_ui\_unauth\_user" : "取消授權" |

## **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.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\_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.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.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.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。 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.DEVICE\_POWER | 合法 | 打开或关闭手机 | 允许应用程序打开或关闭手机 |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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 |
| com.asus.permission.READ\_SDID\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| com.fgcq.a115286.gdt.qq.SEND\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.fgcq.a115286.gdt.qq.RECEIVE\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| org.cocos2dx.cpp.AppActivity | **Schemes**: 615ec92814e22b6a4f1503fd://, |
| com.xqhy.pay.PayActivity | **Schemes**: xqhy115286://, |

**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。**