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

**吾圈pro（ \ 2025052014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 | 吾圈pro |
| 版本 | \ 2025052014 |
| 包名 | com.kingim.fivequan |
| 域名线索 | 64条 |
| URL线索 | 74条 |
| APP图标 |  |
| 分析日期 | 2025年6月9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 | wuquan.apk |
| 文件大小 | 36.73MB |
| MD5值 | 519cf9d17811d2162795aa4121d47fab |
| SHA1值 | df9f44a6bf765387b4c7ce8a35b60ab44fcae270 |
| SHA256值 | 6f8ca2cf69ef7a3ad6e85eb2aa28070fad4aa7393881a4bb296e3e3e14ebf9ff |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 吾圈pro |
| 包名 | com.kingim.fivequan |
| 主活动Activity | com.suxun.im.SplashActivity |
| 安卓版本名称 | \ 2025052014 |
| 安卓版本 | 2025052014 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.iwuquan.com | IP: 23.224.194.30 所属国家: United States of America 地区: California 城市: Los Angeles  |
| android.bugly.qq.com | IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang  |
| im.sdk.qcloud.com | IP: 116.196.150.241 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| privacy.qq.com | IP: 221.204.18.229 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| web.sdk.qcloud.com | IP: 221.204.14.66 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| astat.bugly.cros.wr.pvp.net | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| api-e189.21cn.com | IP: 222.93.106.185 所属国家: China 地区: Jiangsu 城市: Suzhou  |
| opencloud.wostore.cn | IP: 116.128.209.136 所属国家: China 地区: Beijing 城市: Beijing  |
| rap2api.taobao.org | IP: 47.105.93.229 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.ahctop.com | 没有服务器地理信息.  |
| datatracker.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| uq888.oss-cn-beijing.aliyuncs.com | IP: 61.135.144.151 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| cstaticdun.126.net | IP: 125.39.135.219 所属国家: China 地区: Tianjin 城市: Tianjin  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| tools.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| msv6.wosms.cn | IP: 124.64.196.27 所属国家: China 地区: Beijing 城市: Beijing  |
| open.weixin.qq.com | IP: 116.128.169.212 所属国家: China 地区: Shanghai 城市: Shanghai  |
| 23.224.194.30 | IP: 23.224.194.30 所属国家: United States of America 地区: California 城市: Los Angeles  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.cn | IP: 49.4.45.231 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| api.5quan.org | IP: 34.80.217.216 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei  |
| ye.dun.163yun.com | IP: 59.111.248.82 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.baidu.com | IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding  |
| cloud.tencent.com | IP: 101.72.227.133 所属国家: China 地区: Hebei 城市: Langfang  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| open.e.189.cn | IP: 42.123.76.75 所属国家: China 地区: Beijing 城市: Beijing  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| 162.14.19.114 | IP: 162.14.19.114 所属国家: China 地区: Beijing 城市: Beijing  |
| intl.cloud.tencent.com | IP: 60.28.220.193 所属国家: China 地区: Tianjin 城市: Tianjin  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| phosphoricons.com | IP: 67.205.31.19 所属国家: United States of America 地区: California 城市: Brea  |
| 162.14.3.250 | IP: 162.14.3.250 所属国家: China 地区: Beijing 城市: Beijing  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| 119.29.29.98 | IP: 119.29.29.98 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.tencentcloud.com | IP: 43.175.93.11 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| norma-external-collect.meizu.com | 没有服务器地理信息.  |
| cn.register.xmpush.xiaomi.com | IP: 123.125.102.39 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  |
| demos.trtc.tencent-cloud.com | IP: 124.163.195.89 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| da.dun.163.com | IP: 59.111.248.82 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| apifoxmock.com | IP: 47.99.105.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| crash.163.com | IP: 45.254.50.146 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| mikepenz.com | IP: 172.67.141.197 所属国家: United States of America 地区: California 城市: San Francisco  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| wap.cmpassport.com | IP: 120.232.169.168 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| 27.150.128.90 | IP: 27.150.128.90 所属国家: China 地区: Fujian 城市: Xiamen  |
| dnsrepo-pub.alibaba.com | IP: 106.11.43.250 所属国家: China 地区: Beijing 城市: Beijing  |
| e.189.cn | IP: 42.123.76.65 所属国家: China 地区: Beijing 城市: Beijing  |
| 23.225.71.125 | IP: 23.225.71.125 所属国家: United States of America 地区: California 城市: Los Angeles  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **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/d/g.java  |
| https://api-e189.21cn.com/gw/client/accountMsg.do  | cn/com/chinatelecom/account/api/d/g.java  |
| https://dnsrepo-pub.alibaba.com/api/internet/putTermData  | com/alibaba/pdns/h.java  |
| https://dnsrepo-pub.alibaba.com/api/internet/putTermStatusData  | com/alibaba/pdns/h.java  |
| https://api.ahctop.com  | com/chen/apilibrary/config/preference/ServerUrlPreferences.java  |
| https://api.iwuquan.com  | com/chen/apilibrary/config/preference/ServerUrlPreferences.java  |
| https://api.5quan.org  | com/chen/apilibrary/config/preference/ServerUrlPreferences.java  |
| http://23.225.71.125:8802  | com/chen/apilibrary/config/preference/ServerUrlPreferences.java  |
| http://23.224.194.30:8802  | com/chen/apilibrary/config/preference/ServerUrlPreferences.java  |
| http://27.150.128.90:8843  | com/chen/apilibrary/config/preference/ServerUrlPreferences.java  |
| https://apifoxmock.com/m1/5850090-5535971-default/api  | com/chen/apilibrary/contact/URLConstant.java  |
| http://rap2api.taobao.org/app/mock/data/2504819?scope=response  | com/chen/apilibrary/contact/URLConstant.java  |
| https://uq888.oss-cn-beijing.aliyuncs.com/apis.json  | com/chen/apilibrary/contact/URLConstant.java  |
| https://wap.cmpassport.com/resources/html/contract.html  | com/cmic/gen/sdk/view/GenLoginAuthActivity.java  |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true  | com/cmic/gen/sdk/view/GenLoginAuthActivity.java  |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true  | com/cmic/gen/sdk/view/GenLoginAuthActivity.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/namespace-prefixes  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-general-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/string-interning  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xmlpull.org/v1/doc/features.html  | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java  |
| https://api-push.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.in.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://ye.dun.163yun.com/v1/oneclick/preCheck  | com/netease/nis/quicklogin/b.java  |
| https://ye.dun.163yun.com/v1/preCheck  | com/netease/nis/quicklogin/b.java  |
| https://wap.cmpassport.com/resources/html/contract.html  | com/netease/nis/quicklogin/utils/e.java  |
| https://msv6.wosms.cn/html/oauth/protocol2.html  | com/netease/nis/quicklogin/utils/e.java  |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true  | com/netease/nis/quicklogin/utils/e.java  |
| https://da.dun.163.com/sn.gif?d=  | com/netease/nis/quicklogin/utils/g.java  |
| https://crash.163.com/uploadCrashLogInfo.do  | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java  |
| https://crash.163.com/client/api/uploadStartUpInfo.do  | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java  |
| https://da.dun.163.com/sn.gif?d=  | com/netease/nis/captcha/g.java  |
| https://cstaticdun.126.net/api/v2/mobile.v2.13.5.html  | com/netease/nis/captcha/a.java  |
| https://github.com/phosphor-icons/phosphor-home/blob/master/LICENSE  | com/mikepenz/iconics/typeface/library/phosphor/Phosphor.java  |
| https://phosphoricons.com/s  | com/mikepenz/iconics/typeface/library/phosphor/Phosphor.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/avatar/avatar\_%s.png  | com/suxun/im/utils/Constants.java  |
| https://cloud.tencent.com/product/im  | com/suxun/im/utils/Constants.java  |
| https://privacy.qq.com/document/preview/c63a48325d0e4a35b93f675205a65a77  | com/suxun/im/utils/Constants.java  |
| https://privacy.qq.com/document/preview/1cfe904fb7004b8ab1193a55857f7272  | com/suxun/im/utils/Constants.java  |
| https://privacy.qq.com/document/preview/45ba982a1ce6493597a00f8c86b52a1e  | com/suxun/im/utils/Constants.java  |
| https://privacy.qq.com/document/preview/dea84ac4bb88454794928b77126e9246  | com/suxun/im/utils/Constants.java  |
| https://web.sdk.qcloud.com/document/Tencent-IM-User-Agreement.html  | com/suxun/im/utils/Constants.java  |
| https://cloud.tencent.com/product/im  | com/suxun/im/profile/AboutIMMinamalistActivity.java  |
| https://cloud.tencent.com/product/im  | com/suxun/im/profile/AboutIMActivity.java  |
| https://www.baidu.com  | com/suxun/im/login/onepassconfig/UiConfigs.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.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://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.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/b.java  |
| https://cloud.tencent.com/document/product/269/32458  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg=  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://cloud.tencent.com/document/product/269/11673?from=17219  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://www.tencentcloud.com/document/product/1047/34349  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s\_full.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://demos.trtc.tencent-cloud.com/prod/base/v1/events/stat  | com/tencent/qcloud/tuicore/TUIConfig.java  |
| https://cloud.tencent.com/document/product/269/32458  | com/tencent/qcloud/tuikit/tuichat/TUIChatConstants.java  |
| https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg=  | com/tencent/qcloud/tuikit/tuichat/TUIChatConstants.java  |
| https://cloud.tencent.com/document/product/269/3794  | com/tencent/qcloud/tuikit/tuichat/bean/CustomHelloMessage.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/ui/page/CreateCommunityActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/ui/page/CommunitySettingsActivity.java  |
| https://cloud.tencent.com/document/product/269/75979  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/community-cover/community\_cover\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/community-cover/community\_cover\_default.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_default.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://cloud.tencent.com/document/product/269/36852  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://cloud.tencent.com/act/pro/imnew?from=17971  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/TUIContactConstants.java  |
| https://www.tencentcloud.com/products/im?lang=en&pg=  | com/tencent/qcloud/tuikit/tuicontact/TUIContactConstants.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/GroupTypeSelectMinimalistActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/CreateGroupMinimalistActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/CreateGroupMinimalistActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/GroupTypeSelectActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/CreateGroupActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/CreateGroupActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/TUIGroupConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/minimalistui/page/GroupInfoMinimalistFragment.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/classicui/page/GroupInfoFragment.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fg.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fy.java  |
| https://%1$s/gslb/?ver=5.0  | com/xiaomi/push/bw.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fz.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/et.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/az.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/cq.java  |
| https://tools.ietf.org/html/rfc7518  | io/jsonwebtoken/SignatureAlgorithm.java  |
| https://github.com/jwtk/jjwt  | io/jsonwebtoken/impl/DefaultClaims.java  |
| https://datatracker.ietf.org/doc/html/rfc7518  | io/jsonwebtoken/impl/crypto/EllipticCurveProvider.java  |
| https://datatracker.ietf.org/doc/html/rfc7518  | io/jsonwebtoken/impl/crypto/EllipticCurveSignatureValidator.java  |
| https://tools.ietf.org/html/rfc7518  | io/jsonwebtoken/security/Keys.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/rxjava3/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://www.tencentcloud.com/document/product/1047/34286  | 摸瓜V1引擎  |
| http://mikepenz.com/  | 摸瓜V1引擎  |
| https://github.com/mikepenz/Android-Iconics  | 摸瓜V1引擎  |
| https://phosphoricons.com/  | 摸瓜V1引擎  |
| https://github.com/phosphor-icons/phosphor-home  | 摸瓜V1引擎  |
| https://cloud.tencent.com/document/product/269/37059  | 摸瓜V1引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libconceal.so  |
| http://162.14.3.250/v4/ConfigGetSvc/GetOpenSSOIPList  | lib/armeabi-v7a/libImSDK.so  |
| http://119.29.29.98/d?id=39662  | lib/armeabi-v7a/libImSDK.so  |
| http://162.14.19.114/  | lib/armeabi-v7a/libImSDK.so  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=fivequan, O=fivequan 签名算法: rsassa\_pkcs1v15 有效期自: 2025-03-04 03:21:07+00:00 有效期至: 2075-02-20 03:21:07+00:00 发行人: CN=fivequan, O=fivequan 序列号: 0x1 哈希算法: sha256 md5值: b98a377e402b8e7327c3ce31ddf6f1f0 sha1值: e111b272d2c935ddc677e1b2b81039763316061b sha256值: 2371ef5e70125b6fdbd1085dddaba4788d39a5d705a3230723839aaaaa2d01bb sha512值: c90c8439314f43426cd8a23beb086b9c641b3c3d23f88c44efdb885b18c79b107c52802f776d3cd2fabe02e3a26c8bc659ada2524fe1e166bd8b30ae65ad86ab 公钥算法: rsa 密钥长度: 2048 指纹: 2964cca14f96cea0f42226874d0b2820442a25bcbbbada204e120fe9f772d508**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "contact\_no\_such\_user" : "This user does not exist."  |
| "firebase\_database\_url" : "\*\*\*\*\*\*"  |
| "google\_api\_key" : "\*\*\*\*\*\*"  |
| "google\_crash\_reporting\_api\_key" : "\*\*\*\*\*\*"  |
| "input\_password" : "请输入密码，6~20位字母或者数字"  |
| "library\_AndroidIconics\_author" : "Mike Penz"  |
| "library\_AndroidIconics\_authorWebsite" : "http://mikepenz.com/"  |
| "library\_Octicons\_author" : "Helena Zhang, Toby Fried"  |
| "library\_Octicons\_authorWebsite" : "https://phosphoricons.com/"  |
| "password" : "Password"  |
| "private\_group" : "Discussion Group"  |
| "umcsdk\_oauth\_version\_name" : "v1.4.1"  |
| "contact\_no\_such\_user" : "该用户不存在"  |
| "input\_password" : "请输入密码，8~20位字母+数字"  |
| "password" : "密码"  |
| "private\_group" : "讨论组"  |

## **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.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\_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.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.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 |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.kingim.fivequan.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.kingim.fivequan.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.kingim.fivequan.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| android.permission.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| 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.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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.kingim.fivequan.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| com.kingim.fivequan.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.kingim.fivequan.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.suxun.im.main.MainActivity | **Schemes**: pushscheme://, **Hosts:** com.tencent.qcloud, **Paths:** /detail,  |
| com.suxun.im.main.MainMinimalistActivity | **Schemes**: pushscheme://, **Hosts:** com.tencent.qcloud, **Paths:** /detail,  |
| com.tencent.qcloud.tim.tuiofflinepush.OpenActivity | **Schemes**: pushscheme://, **Hosts:** com.tencent.qcloud.uniapp, **Paths:** /detail,  |

**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。**