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

**爱爱网（ 3.5.1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 | 爱爱网 |
| 版本 | 3.5.1 |
| 包名 | cn.qrqr.www |
| 域名线索 | 94条 |
| URL线索 | 57条 |
| APP图标 |  |
| 分析日期 | 2025年9月27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 | app-release-08-29.apk |
| 文件大小 | 200.81MB |
| MD5值 | 0f7230e9872478837040b4c4d8b514d4 |
| SHA1值 | 2ad7a8998da75327b74619ff765cd9cc6a2b0008 |
| SHA256值 | ebde9a0a457b4bf4a698867f6204e2272204f3b34a88ad83168e4e1c9d6cd78d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 爱爱网 |
| 包名 | cn.qrqr.www |
| 主活动Activity | cn.qrqr.www.MainActivity |
| 安卓版本名称 | 3.5.1 |
| 安卓版本 | 2 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| aa5.com | IP: 172.247.18.202 所属国家: United States of America 地区: California 城市: Los Angeles  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.example.com | IP: 23.217.139.135 所属国家: Australia 地区: New South Wales 城市: Sydney  |
| norma-external-collect.meizu.com | IP: 183.60.176.112 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| osmand.net | IP: 66.220.146.94 所属国家: United States of America 地区: California 城市: Menlo Park  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| aaw-2024-04-12.oss-cn-shanghai.aliyuncs.com | IP: 139.227.228.227 所属国家: China 地区: Shanghai 城市: Shanghai  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| store2.hispace.hicloud.com | IP: 3.166.228.94 所属国家: United States of America 地区: Washington 城市: Seattle  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| lqstorage-1318180133.cos.ap-shanghai.myqcloud.com | IP: 61.241.129.102 所属国家: China 地区: Anhui 城市: Hefei  |
| ins-9fciednc.ias.tencent-cloud.net | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| gtc.getui.nethttps | 没有服务器地理信息.  |
| gtc.getui.net | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| aspect-upush.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| default.url | 没有服务器地理信息.  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ucc.umeng.com | IP: 203.119.145.45 所属国家: China 地区: Beijing 城市: Beijing  |
| xmlpull.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| store3.hispace.hicloud.com | IP: 23.217.205.207 所属国家: United States of America 地区: Colorado 城市: Denver  |
| aomediacodec.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| ulogs.umengcloud.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| b-gtc.getui.net | IP: 101.68.218.163 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| c-hzgt2.getui.com | IP: 124.160.155.55 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| sc-2wln.cn-shanghai.oss-adns.aliyuncs.com | IP: 139.227.228.227 所属国家: China 地区: Shanghai 城市: Shanghai  |
| b-gtc.gepush.com | IP: 101.68.218.161 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| resource02.ulifestyle.com.hk | IP: 162.125.83.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| utoken.umeng.com | IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| grs.dbankcloud.cn | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| c-gtc.gepush.com | IP: 124.160.155.57 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| resolver.msg.xiaomi.net | IP: 111.206.174.194 所属国家: China 地区: Beijing 城市: Beijing  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.brynosaurus.com | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| sdk.open.phone.igexin.com | IP: 101.68.218.161 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| youtrack.jetbrains.com | IP: 63.35.30.167 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| store-at-dre.hispace.dbankcloud.com | 没有服务器地理信息.  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| store-drru.hispace.hicloud.com | IP: 159.138.201.153 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| appgallery.cloud.huawei.com | IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| aawapi-v3.trh999.com.w.cdngslb.com | IP: 61.48.83.230 所属国家: China 地区: Beijing 城市: Beijing  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| aawapi-v3.lvshi68.com | IP: 163.181.78.184 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| developer.umeng.com | IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.dbankcloud.asia | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| android.googlesource.com | IP: 142.250.99.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| journeyapps.com | IP: 3.165.75.51 所属国家: United States of America 地区: Washington 城市: Seattle  |
| c-gtc.getui.net | IP: 124.160.155.57 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ask.dcloud.net.cn | IP: 116.131.57.100 所属国家: China 地区: Beijing 城市: Beijing  |
| b-gtc.getui.nethttps | 没有服务器地理信息.  |
| crl.securetrust.com | IP: 23.200.86.82 所属国家: France 地区: Ile-de-France 城市: Paris  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| gcc.gnu.org | IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| developer.android.com | IP: 142.250.69.206 所属国家: United States of America 地区: California 城市: Mountain View  |
| webrd01.is.autonavi.com | IP: 60.222.200.221 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| cos-v3.024kh.com | IP: 43.248.103.26 所属国家: China 地区: Jiangsu 城市: Zhenjiang  |
| store.hispace.hicloud.com | IP: 49.4.47.241 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| 10.2.31.245 | IP: 10.2.31.245 所属国家: - 地区: - 城市: -  |
| aawapi-v3.lvshi68.com.w.cdngslb.com | IP: 155.102.4.6 所属国家: United States of America 地区: California 城市: San Mateo  |
| sc-2wln.cn-shanghai.oss-adns.aliyuncs.com.gds.alibabadns.com | IP: 139.227.228.227 所属国家: China 地区: Shanghai 城市: Shanghai  |
| sh.file.myqcloud.com | IP: 61.241.129.104 所属国家: China 地区: Anhui 城市: Hefei  |
| schemas.android.com | 没有服务器地理信息.  |
| gtc.gepush.com | IP: 43.231.145.97 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| alogsus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| aawapi-v3.trh999.com | IP: 61.48.83.230 所属国家: China 地区: Beijing 城市: Beijing  |
| 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  |
| fontawesome.comversion | 没有服务器地理信息.  |
| developers.google.com | IP: 172.217.14.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| aomedia.org | IP: 208.101.21.43 所属国家: United States of America 地区: Texas 城市: Dallas  |
| aaw-2024-04-12-1318180133.cos.ap-shanghai.myqcloud.com | IP: 61.241.129.103 所属国家: China 地区: Anhui 城市: Hefei  |
| ulogs.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| ns.adobe.com | 没有服务器地理信息.  |
| share.here.com | IP: 108.156.144.114 所属国家: United States of America 地区: Washington 城市: Seattle  |
| store1.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| g.co | IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| c-gtc.getui.nethttps | 没有服务器地理信息.  |
| plbslog.umeng.com | IP: 36.156.202.75 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| d-gt.getui.com | 没有服务器地理信息.  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://c-gtc.getui.net,https://c-gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://gtc.getui.net,https://gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://b-gtc.getui.net,https://b-gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://sdk.open.phone.igexin.com/api.php  | com/igexin/push/a.java  |
| http://c-hzgt2.getui.com/api.php  | com/igexin/push/a.java  |
| https://d-gt.getui.com/api.htm  | com/igexin/push/a.java  |
| http://bi.  | com/igexin/push/config/g.java  |
| http://config.  | com/igexin/push/config/g.java  |
| http://bi.  | com/igexin/push/config/b.java  |
| http://config.  | com/igexin/push/config/b.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  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/c.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/crashreport/common/strategy/c.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/l.java  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | com/umeng/analytics/pro/ap.java  |
| https://ucc.umeng.com/v2/inn/fetch  | com/umeng/analytics/pro/aq.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://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://developer.umeng.com/docs/119267/detail/118637  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.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://utoken.umeng.com  | com/umeng/umzid/ZIDManager.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fa.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fs.java  |
| https://%1$s/gslb/?ver=5.0  | com/xiaomi/push/bt.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/ft.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/en.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/cp.java  |
| http://schemas.android.com/apk/res/android  | defpackage/yg4.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | defpackage/r41.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | defpackage/s41.java  |
| https://developers.google.com/tink/design/access\_control  | defpackage/l5.java  |
| https://developers.google.com/tink/design/access\_control  | defpackage/b15.java  |
| https://developers.google.com/tink/design/access\_control  | defpackage/rs1.java  |
| https://developers.google.com/tink/design/access\_control  | defpackage/d6.java  |
| https://developers.google.com/tink/design/access\_control  | defpackage/iy.java  |
| https://developers.google.com/tink/design/access\_control  | defpackage/q6.java  |
| https://developers.google.com/tink/design/access\_control  | defpackage/y6.java  |
| http://ns.adobe.com/xap/1.0/  | defpackage/t82.java  |
| http://ns.adobe.com/xap/1.0/  | defpackage/r82.java  |
| http://dashif.org/guidelines/last-segment-number  | defpackage/td0.java  |
| http://dashif.org/guidelines/trickmode  | defpackage/td0.java  |
| http://dashif.org/thumbnail\_tile  | defpackage/td0.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | defpackage/td0.java  |
| http://dashif.org/guidelines/last-segment-number  | defpackage/sd0.java  |
| http://dashif.org/guidelines/trickmode  | defpackage/sd0.java  |
| http://dashif.org/thumbnail\_tile  | defpackage/sd0.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | defpackage/sd0.java  |
| https://ask.dcloud.net.cn/article/35627  | defpackage/s25.java  |
| https://ask.dcloud.net.cn/article/35877  | defpackage/s25.java  |
| https://ask.dcloud.net.cn/article/283  | defpackage/s45.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | defpackage/l71.java  |
| https://docs.flutter.dev/deployment/android  | io/flutter/embedding/engine/loader/FlutterLoader.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/b.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| https://ask.dcloud.net.cn/article/36199  | 摸瓜V1引擎  |
| https://play.google.com/store/apps/details?id=  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com  | 摸瓜V1引擎  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| https://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V1引擎  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | 摸瓜V2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.data.hicloud.com:6447  | 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://store1.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | 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.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |
| http://crl.securetrust.com/STCA.crl0  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| https://developer.umeng.com/docs/119267/detail/182050  | 摸瓜V3引擎  |
| https://developer.android.com/guide/topics/permissions/overview  | 摸瓜V3引擎  |
| https://fontawesome.comVersion  | 摸瓜V3引擎  |
| https://api-push.in.meizu.com/garcia/api/client/  | 摸瓜V3引擎  |
| aaw-2024-04-12.oss-cn-shanghai.aliyuncs.com  | 摸瓜V3引擎  |
| https://aomediacodec.github.io/av1-rtp-spec/#dependency-descriptor-rtp-header-extension  | 摸瓜V3引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V3引擎  |
| http://www.brynosaurus.com/cachedir/  | 摸瓜V3引擎  |
| https://aomedia.org/emsg/ID3  | 摸瓜V3引擎  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | 摸瓜V3引擎  |
| https://aawapi-v3.trh999.com/msg\_api  | 摸瓜V3引擎  |
| ins-9fciednc.ias.tencent-cloud.net  | 摸瓜V3引擎  |
| https://webrd01.is.autonavi.com/appmaptile?lang=zh\_cn&size=1&scale=1&style=8&x=  | 摸瓜V3引擎  |
| ucc.umeng.com  | 摸瓜V3引擎  |
| https://aaw-2024-04-12-1318180133.cos.ap-shanghai.myqcloud.com/api.json  | 摸瓜V3引擎  |
| play.googleapis.com  | 摸瓜V3引擎  |
| https://b-gtc.gepush.com  | 摸瓜V3引擎  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | 摸瓜V3引擎  |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html  | 摸瓜V3引擎  |
| https://%1$s/gslb/?ver=5.0  | 摸瓜V3引擎  |
| https://d-gt.getui.com/api.htm  | 摸瓜V3引擎  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | 摸瓜V3引擎  |
| https://docs.flutter.dev/deployment/android#what-are-the-supported-target-architectures  | 摸瓜V3引擎  |
| http://aa5.com/?invite=  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| sc-2wln.cn-shanghai.oss-adns.aliyuncs.com  | 摸瓜V3引擎  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | 摸瓜V3引擎  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | 摸瓜V3引擎  |
| https://share.here.com/l/  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/  | 摸瓜V3引擎  |
| utoken.umeng.com  | 摸瓜V3引擎  |
| https://ucc.umeng.com/v2/inn/fetch  | 摸瓜V3引擎  |
| http://10.2.31.245:9033/uploads/d280c171-2e50-4a91-bfd2-a52c43708f9d.wgt  | 摸瓜V3引擎  |
| http://aawapi-v3.lvshi68.com:100082  | 摸瓜V3引擎  |
| https://aaw-2024-04-12.oss-cn-shanghai.aliyuncs.com/api.json2  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.2  | 摸瓜V3引擎  |
| http://developer.umeng.com/docs/66650/cate/66650  | 摸瓜V3引擎  |
| https://gtc.gepush.com  | 摸瓜V3引擎  |
| http://aawapi-v3.lvshi68.com:100022  | 摸瓜V3引擎  |
| https://lqstorage-1318180133.cos.ap-shanghai.myqcloud.com/app/learn.mp42  | 摸瓜V3引擎  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | 摸瓜V3引擎  |
| https://gtc.getui.net  | 摸瓜V3引擎  |
| https://aawapi-v3.lvshi68.com/msg\_demo  | 摸瓜V3引擎  |
| aawapi-v3.trh999.com.w.cdngslb.com  | 摸瓜V3引擎  |
| https://lqstorage-1318180133.cos.ap-shanghai.myqcloud.com/app/learn.mp4  | 摸瓜V3引擎  |
| aawapi-v3.lvshi68.com  | 摸瓜V3引擎  |
| https://c-gtc.getui.net  | 摸瓜V3引擎  |
| https://aawapi-v3.lvshi68.com/msg\_api  | 摸瓜V3引擎  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html2  | 摸瓜V3引擎  |
| https://resource02.ulifestyle.com.hk/ulcms/content/article/thumbnail/1280x720/ub/20190909190445\_\_8ac  | 摸瓜V3引擎  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | 摸瓜V3引擎  |
| https://developer.umeng.com/docs/119267/detail/118637#3091c7c11fx3q  | 摸瓜V3引擎  |
| https://youtrack.jetbrains.com/issue/KT-55980  | 摸瓜V3引擎  |
| https://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V3引擎  |
| http://osmand.net/go2  | 摸瓜V3引擎  |
| http://g.co/dev/packagevisibility.  | 摸瓜V3引擎  |
| https://developer.umeng.com/docs/66632/detail/  | 摸瓜V3引擎  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | 摸瓜V3引擎  |
| https://journeyapps.com/  | 摸瓜V3引擎  |
| http://aa5.com/?invite=2  | 摸瓜V3引擎  |
| https://aaw-2024-04-12-1318180133.cos.ap-shanghai.myqcloud.com/api.json2  | 摸瓜V3引擎  |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status  | 摸瓜V3引擎  |
| cos-v3.024kh.com  | 摸瓜V3引擎  |
| https://api-push.meizu.com/garcia/api/client/  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| aawapi-v3.lvshi68.com.w.cdngslb.com  | 摸瓜V3引擎  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | 摸瓜V3引擎  |
| sc-2wln.cn-shanghai.oss-adns.aliyuncs.com.gds.alibabadns.com  | 摸瓜V3引擎  |
| https://aomediacodec.github.io/av1-rtp-spec/#dependency-descriptor-rtp-header-extension2  | 摸瓜V3引擎  |
| sh.file.myqcloud.com  | 摸瓜V3引擎  |
| http://10.2.31.245:9033/uploads/5ebca27b-10db-4a9f-b1cc-22e089903192.wgt  | 摸瓜V3引擎  |
| http://aawapi-v3.lvshi68.com:10008  | 摸瓜V3引擎  |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status2  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/trickmode  | 摸瓜V3引擎  |
| aawapi-v3.trh999.com  | 摸瓜V3引擎  |
| https://sdk.open.phone.igexin.com/api.php  | 摸瓜V3引擎  |
| https://cn.register.xmpush.xiaomi.com  | 摸瓜V3引擎  |
| https://b-gtc.getui.net  | 摸瓜V3引擎  |
| https://github.com/dart-lang/language/issues/3488  | 摸瓜V3引擎  |
| https://default.url  | 摸瓜V3引擎  |
| http://aawapi-v3.lvshi68.com:10002  | 摸瓜V3引擎  |
| aaw-2024-04-12-1318180133.cos.ap-shanghai.myqcloud.com  | 摸瓜V3引擎  |
| https://c-gtc.gepush.com  | 摸瓜V3引擎  |
| ulogs.umeng.com  | 摸瓜V3引擎  |
| http://c-hzgt2.getui.com/api.php  | 摸瓜V3引擎  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | 摸瓜V3引擎  |
| http://xmlpull.org/v1/doc/features.html#process-namespaces  | 摸瓜V3引擎  |
| http://10.2.31.245:9033/uploads/d280c171-2e50-4a91-bfd2-a52c43708f9d.wgt2  | 摸瓜V3引擎  |
| http://10.2.31.245:9033/uploads/5ebca27b-10db-4a9f-b1cc-22e089903192.wgt2  | 摸瓜V3引擎  |
| https://aawapi-v3.lvshi68.com/msg\_api2  | 摸瓜V3引擎  |
| http://gcc.gnu.org/bugs.html):  | 摸瓜V3引擎  |
| https://aawapi-v3.lvshi68.com/msg\_demo2  | 摸瓜V3引擎  |
| android.bugly.qq.com  | 摸瓜V3引擎  |
| https://share.here.com/l/2  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | defpackage/og5.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15724800000  | cn/jiguang/am/a.java  |
| 17512775099  | defpackage/kn.java  |

## **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: C=000000, ST=openim, L=openim, O=openim, OU=openim, CN=openim 签名算法: rsassa\_pkcs1v15 有效期自: 2021-10-26 08:47:56+00:00 有效期至: 2046-10-20 08:47:56+00:00 发行人: C=000000, ST=openim, L=openim, O=openim, OU=openim, CN=openim 序列号: 0x19e05291 哈希算法: sha256 md5值: 05d03bd8459d4a87134eb128e3dab5fd sha1值: 57ce8b8feb004052692f721f7ffa52be51def128 sha256值: 1f38a82fb3c33be7951fb5d964ef5bd9c6c9bfc084ae1e2a8a40a0d1f44ae1fe sha512值: 797e3ccaf31be41cfce915486e9027118413d22103ba02737cf0ae37904874a7791ab675fb4508cf7b9edfa6044393cb1e282f99eb133f515fe1afdc2447cc0d 公钥算法: rsa 密钥长度: 2048 指纹: 0b749ba3321060732b29f063fbabeb507e14e7e949653bdabdbd3bd3139c14e2**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API"  |
| "dcloud\_io\_without\_authorization" : "not authorized"  |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service"  |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed"  |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained"  |
| "dcloud\_oauth\_token\_failed" : "failed to get token"  |
| "dcloud\_permissions\_reauthorization" : "reauthorize"  |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_io\_without\_authorization" : "没有获得授权"  |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权"  |
| "dcloud\_oauth\_token\_failed" : "获取token失败"  |
| "dcloud\_permissions\_reauthorization" : "重新授权"  |

## **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.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.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\_INTERNAL\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| 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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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.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.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.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.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.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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| 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.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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。 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 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 |
| android.permission.POST\_NOTIFICATIONS | 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。 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| cn.qrqr.www.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| cn.qrqr.www.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| cn.qrqr.www.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| cn.qrqr.www.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| cn.qrqr.www.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| cn.qrqr.www.permission.MIPUSH\_RECEIVE | 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 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 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.huawei.android.launcher.permission.WRITE\_SETTINGS | 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 |
| android.permission.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |
| cn.qrqr.www.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| getui.permission.GetuiService.cn.qrqr.www | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**