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

**国能在线G（ 9.0.26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 | 国能在线G |
| 版本 | 9.0.26 |
| 包名 | com.tiocloud.fchatssgnzxgx |
| 域名线索 | 50条 |
| URL线索 | 59条 |
| APP图标 |  |
| 分析日期 | 2025年5月12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(1).apk |
| 文件大小 | 91.76MB |
| MD5值 | c09d40f611c084dab5c4b0657c992b60 |
| SHA1值 | c3d1dff13044310c502e8a7ce37975f3a2820170 |
| SHA256值 | 0ffc5be5f91daea58898caf01c3b744ed5f589f140c1fa84e1858ea2e4162989 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 国能在线G |
| 包名 | com.tiocloud.fchatssgnzxgx |
| 主活动Activity | com.tiocloud.fchat.MainActivity |
| 安卓版本名称 | 9.0.26 |
| 安卓版本 | 226 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| vectormap0.bdimg.com | IP: 119.249.50.38 所属国家: China 地区: Hebei 城市: Baoding  |
| openmobile.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mp.weixin.qq.com | IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai  |
| developer.apple.com | IP: 17.253.87.206 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| parking.baidu.com | IP: 111.206.209.179 所属国家: China 地区: Beijing 城市: Beijing  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| aomedia.org | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| indoorsearch.map.baidu.com | IP: 111.206.209.201 所属国家: China 地区: Beijing 城市: Beijing  |
| loc.map.baidu.com | IP: 111.206.209.174 所属国家: China 地区: Beijing 城市: Beijing  |
| journeyapps.com | IP: 18.155.68.69 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ns.adobe.com | 没有服务器地理信息.  |
| appsupport.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| newclient.map.baidu.com | IP: 111.206.209.17 所属国家: China 地区: Beijing 城市: Beijing  |
| client.map.baidu.com | IP: 111.206.209.120 所属国家: China 地区: Beijing 城市: Beijing  |
| daohang.map.baidu.com | IP: 111.206.209.190 所属国家: China 地区: Beijing 城市: Beijing  |
| mapoffdownload.bdstatic.com | IP: 101.72.203.36 所属国家: China 地区: Hebei 城市: Langfang  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| daup.map.baidu.com | IP: 110.242.69.98 所属国家: China 地区: Hebei 城市: Baoding  |
| imgcache.qq.com | IP: 119.36.224.11 所属国家: China 地区: Hubei 城市: Xiangyang  |
| default.url | 没有服务器地理信息.  |
| v.map.baidu.com | IP: 111.206.209.185 所属国家: China 地区: Beijing 城市: Beijing  |
| sv.map.baidu.com | IP: 111.206.209.186 所属国家: China 地区: Beijing 城市: Beijing  |
| offmap2.baidu.com | IP: 221.204.49.38 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| wapmap.baidu.com | IP: 111.206.209.212 所属国家: China 地区: Beijing 城市: Beijing  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| ofloc.map.baidu.com | IP: 110.242.70.118 所属国家: China 地区: Hebei 城市: Baoding  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| cgi.qplus.com | 没有服务器地理信息.  |
| map.baidu.com | IP: 111.206.208.32 所属国家: China 地区: Beijing 城市: Beijing  |
| app.navi.baidu.com | IP: 111.206.209.213 所属国家: China 地区: Beijing 城市: Beijing  |
| h.trace.qq.com | IP: 113.56.189.162 所属国家: China 地区: Hubei 城市: Huangshi  |
| j.map.baidu.com | IP: 111.206.209.187 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| xmlpull.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| newvector.map.baidu.com | IP: 111.206.209.171 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.android.com | IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto  |
| open.weixin.qq.com | IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai  |
| cgi.connect.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| ce3e75d5.jpush.cn | IP: 120.233.33.204 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| itsmap3.baidu.com | IP: 153.3.237.86 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | L1/z.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | P0/C0411b0.java  |
| https://x</LA\_URL>  | T0/M.java  |
| https://default.url  | T0/M.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | T0/N.java  |
| https://ce3e75d5.jpush.cn/wi/cjc4sa  | cn/jiguang/aw/c.java  |
| https://ce3e75d5.jpush.cn/wi/d8n3hj  | cn/jiguang/aw/c.java  |
| https://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/h/d.java  |
| https://loc.map.baidu.com/tcu.php  | com/baidu/location/h/d.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/h/d.java  |
| https://loc.map.baidu.com/cfgs/loc/commcfgs  | com/baidu/location/h/d.java  |
| https://client.map.baidu.com/phpui2/?  | com/baidu/location/h/d.java  |
| https://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet  | com/baidu/location/h/d.java  |
| https://loc.map.baidu.com/check\_indoor\_data\_update  | com/baidu/location/h/d.java  |
| https://parking.baidu.com/parking/api/parkingdata/getcarportlistforlocation?  | com/baidu/location/h/d.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/h/d.java  |
| https://ofloc.map.baidu.com/LocBrokerService/do\_loc\_map\_match  | com/baidu/location/h/d.java  |
| https://ofloc.map.baidu.com/PlanarStartService/detect\_parking\_exits  | com/baidu/location/h/d.java  |
| https://loc.map.baidu.com/indoorlocbuildinginfo.php  | com/baidu/location/indoor/a.java  |
| https://ofloc.map.baidu.com/locnu  | com/baidu/location/b/x.java  |
| https://loc.map.baidu.com/cc.php  | com/baidu/location/b/i.java  |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/b/i.java  |
| https://loc.map.baidu.com/gpsz  | com/baidu/location/c/a.java  |
| http://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/e/d.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/e/f.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/e/c.java  |
| http://%s/%s  | com/baidu/location/e/b.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/e/b.java  |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| https://app.navi.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| https://daohang.map.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| https://map.baidu.com/zt/client/index/?fr=sdk\_[  | com/baidu/mapapi/utils/OpenClientUtil.java  |
| https://api.map.baidu.com/place/detail?uid=  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| https://api.map.baidu.com/place/search?  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| https://api.map.baidu.com/direction?  | com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java  |
| https://api.map.baidu.com/lbs\_sdkcc/report  | com/baidu/mapsdkplatform/comapi/c/a/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_locsdk/geocoding/v3/  | com/baidu/geofence/a/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_locsdk/geocoding/v3/?  | com/baidu/geofence/a/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_locsdk/place/v2/search  | com/baidu/geofence/a/c.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_locsdk/place/v2/search?  | com/baidu/geofence/a/c.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/parking/search  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/polygon/v1/fuzzy\_search  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/weather\_abroad/v1/  | com/baidu/platform/domain/b.java  |
| https://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/weather/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/b.java  |
| https://j.map.baidu.com/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/reverse\_geocoding/v3  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail  | com/baidu/platform/domain/b.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/parking/search  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/polygon/v1/search  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/weather\_abroad/v1/  | com/baidu/platform/domain/a.java  |
| http://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/weather/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/a.java  |
| http://j.map.baidu.com/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/reverse\_geocoding/v3  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail  | com/baidu/platform/domain/a.java  |
| https://wapmap.baidu.com/s?tn=Detail&pid=  | com/baidu/platform/core/share/b.java  |
| https://map.baidu.com/?newmap=1&s=  | com/baidu/platform/core/share/d.java  |
| https://)([\\s\\S]+)  | com/huawei/hms/scankit/p/C0742bd.java  |
| https://imgcache.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com/open/mobile/request/sdk\_request.html?  | com/tencent/open/SocialApiIml.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group  | com/tencent/open/SocialOperation.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind  | com/tencent/open/SocialOperation.java  |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report  | com/tencent/open/b/h.java  |
| https://h.trace.qq.com/kv  | com/tencent/open/b/b.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/i.java  |
| https://openmobile.qq.com/  | com/tencent/open/utils/HttpUtils.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://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s  | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java  |
| https://openmobile.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.java  |
| https://cgi.qplus.com/report/report  | com/tencent/connect/avatar/ImageActivity.java  |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | com/tencent/connect/common/BaseApi.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/common/BaseApi.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/auth/a.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/v3/user/get\_info  | com/tencent/connect/auth/AuthAgent.java  |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | com/tencent/connect/auth/AuthAgent.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/ga.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gs.java  |
| https://%1$s/gslb/?ver=5.0  | com/xiaomi/push/ct.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gt.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fo.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bw.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/u.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| http://dashif.org/guidelines/last-segment-number  | v1/C1502d.java  |
| http://dashif.org/guidelines/trickmode  | v1/C1502d.java  |
| http://dashif.org/thumbnail\_tile  | v1/C1502d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | v1/C1502d.java  |
| http://ns.adobe.com/xap/1.0/  | Z0/a.java  |
| https://aomedia.org/emsg/ID3  | j1/C1223a.java  |
| https://developer.apple.com/streaming/emsg-id3  | j1/C1223a.java  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1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/nodeca/pica  | 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  |
| https://indoorsearch.map.baidu.com/is/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| http://map.baidu.com/zt/y2015/taohuayuan/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://sv.map.baidu.com/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://v.map.baidu.com/high/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://client.map.baidu.com/imap/sdk/tj?qt=vmap  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://client.map.baidu.com/heatmap/client?  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://newclient.map.baidu.com/client/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| http://map.baidu.com/zt/y2016/fudai/mobile/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://newclient.map.baidu.com/pic/newvector/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://newvector.map.baidu.com/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://vectormap0.bdimg.com/vecdata/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://api.map.baidu.com/api\_ulog/v1/up  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://client.map.baidu.com/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://sv.map.baidu.com  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://newclient.map.baidu.com/its/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://newvector.map.baidu.com/grid\_vc/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://v.map.baidu.com/low/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://v.map.baidu.com/indoorinside/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://api.map.baidu.com/api\_ulog/v1/control?  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://newvector.map.baidu.com/travel\_vc/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://newvector.map.baidu.com/starpic/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://offmap2.baidu.com/offline-search/?  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://newclient.map.baidu.com/pic/newvector/topic\_map/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://mapoffdownload.bdstatic.com/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://client.map.baidu.com/offline-search/?  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/statistics/v1/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://itsmap3.baidu.com/  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libBaiduMapSDK\_map\_v7\_5\_8.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | R1/a.java  |
| 18345352118  | com/baidu/mapsdkplatform/comapi/util/b.java  |
| 14222222222  | a1/C0594e.java  |
| 15222222222  | a1/C0594e.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=testkey 签名算法: rsassa\_pkcs1v15 有效期自: 2023-02-17 10:08:59+00:00 有效期至: 2048-02-11 10:08:59+00:00 发行人: CN=testkey 序列号: 0x1 哈希算法: sha256 md5值: 8bab51a4c3921100c8633b6138170a4a sha1值: 67a74d0575a23730358fc815be9fbcc7c0d10b4e sha256值: 94cafe8237991795a311a5cea99c9e84449854c96052569986837b353a19c0b1 sha512值: 7af4551d23ae2b27d64e7ccdae9b1c1b5d97688d1578ec2d3aa5977694d8bca4d8c3c5bceafc8cce757e0b6481621e842234128345e6cebdcd5afa2c71b64550 公钥算法: rsa 密钥长度: 2048 指纹: 924e45e7cb8f7dc8e4ad62a94c860cdb894dcbffa95e54bf703fb3061693cd1f**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |

## **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.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.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.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\_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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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 |
| com.android.launcher.permission.READ\_SETTINGS | 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 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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 |
| com.tiocloud.fchatssgnzxgx.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| com.tiocloud.fchatssgnzxgx.permission.MIPUSH\_RECEIVE | 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.tiocloud.fchatssgnzxgx.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent123456789://,  |

**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。**