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

**两步路（ 1.3.6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 | 两步路 |
| 版本 | 1.3.6 |
| 包名 | com.tbulu.watch |
| 域名线索 | 55条 |
| URL线索 | 53条 |
| APP图标 |  |
| 分析日期 | 2025年6月13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 | tubulu2.0.apk |
| 文件大小 | 33.79MB |
| MD5值 | 2726777f15e1e7b788bd47b85f5767b1 |
| SHA1值 | 7305a42c2170c67067b4bd38895f6efed5e0055a |
| SHA256值 | ce7636dbce0b9475943a8adf2ee485d0bbe099f323c09dc4e9090f411012722e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 两步路 |
| 包名 | com.tbulu.watch |
| 主活动Activity | com.tbulu.watch.ui.activity.WelcomeActivity |
| 安卓版本名称 | 1.3.6 |
| 安卓版本 | 83 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| alogsus.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| mpsapi.amap.com | IP: 59.82.113.71 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| dualstack-arestapi.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| maps.testing.amap.com | IP: 59.82.57.204 所属国家: China 地区: Beijing 城市: Beijing  |
| emei-helper.2bulu.com | IP: 122.9.101.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| resolve.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| lbs-3dtiles-service.amap.com | IP: 110.253.189.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| cgicol.amap.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| api.seniverse.com | IP: 116.62.81.138 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: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| astat.bugly.cros.wr.pvp.net | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| down-files.2bulu.com | IP: 218.12.124.152 所属国家: China 地区: Hebei 城市: Qinhuangdao  |
| emei.2bulu.com | IP: 122.9.101.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| restapi.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| restsdk.amap.com | IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing  |
| mps.amap.com | IP: 59.82.113.71 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| aspect-upush.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| render.amap.com | IP: 203.119.238.216 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dualstack-a.apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| img.alicdn.com | IP: 39.91.183.195 所属国家: China 地区: Shandong 城市: Linyi  |
| cnlogs.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| schemas.android.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| objectbox.io | IP: 85.13.163.69 所属国家: Germany 地区: Thuringen 城市: Friedersdorf  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| m5.amap.com | IP: 59.82.112.99 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| daily-orion.gaode.test | 没有服务器地理信息.  |
| lbs.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| docs.objectbox.io | IP: 172.64.147.209 所属国家: United States of America 地区: California 城市: San Francisco  |
| app.2bulu.com | IP: 218.245.100.222 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| ulogs.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ulogs.umengcloud.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| mst01.is.autonavi.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| adiu.amap.com | IP: 110.253.189.146 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| faas-image.amap.com | IP: 218.24.90.187 所属国家: China 地区: Liaoning 城市: Shenyang  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| apistore.amap.com | IP: 203.119.238.47 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| helper.2bulu.com | IP: 218.245.98.73 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| files.2bulu.com | IP: 218.245.100.222 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.google.com | IP: 31.13.73.169 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| wb.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| www.opengis.net | IP: 217.154.231.107 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Brighton  |
| developer.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.openweathermap.org | IP: 15.235.222.69 所属国家: Canada 地区: Quebec 城市: Montreal  |
| wap.amap.com | IP: 175.17.21.189 所属国家: China 地区: Jilin 城市: Changchun  |
| emei-file.2bulu.com | IP: 122.9.101.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| pslog.umeng.com | IP: 59.82.29.163 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| utoken.umeng.com | IP: 223.109.148.171 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.2bulu.com | IP: 218.245.100.222 所属国家: China 地区: Guangdong 城市: Guangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/p0003sl/o000O0O0.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/p0003sl/o000O00O.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/p0003sl/o000O00O.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003sl/Oooo0.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003sl/OooOOO.java  |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003sl/o000Oo0.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003sl/o000Oo0.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003sl/o000Oo0.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/p0003sl/o000Oo0.java  |
| https://restapi.amap.com/rest/lbs/geohub/3d/tiles?z=%d&x=%d&y=%d&id=  | com/amap/api/col/p0003sl/o00oOoo.java  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\  | com/amap/api/col/p0003sl/o00O00.java  |
| http://wap.amap.com/  | com/amap/api/maps/AMapUtils.java  |
| https://lbs-3dtiles-service.amap.com/basemap/tiles/staging?compose=building@1669011850923&compose=tree@1668678765481&z=%d&x=%d&y=%d  | com/amap/api/maps/model/amap3dmodeltile/AMap3DModelTileProvider.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://restsdk.amap.com/rest/lbs/dem/data?z=%d&x=%d&y=%d&type=2  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh\_cn&size=1&scale=1&style=6  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mpsapi.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://m5.amap.com  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://render.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://mpsapi.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://m5.amap.com  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://render.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://restsdk.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/c.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/c.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/c.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/i.java  |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo  | com/autonavi/aps/amapapi/trans/c.java  |
| http://restsdk.amap.com/v3/geocode/regeo  | com/autonavi/aps/amapapi/trans/c.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/trans/a.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/oplus/ocs/wearengine/core/ie3.java  |
| http://restsdk.amap.com/v3  | com/oplus/ocs/wearengine/core/w83.java  |
| https://restsdk.amap.com/v3  | com/oplus/ocs/wearengine/core/w83.java  |
| http://restsdk.amap.com/v4  | com/oplus/ocs/wearengine/core/w83.java  |
| https://restsdk.amap.com/v4  | com/oplus/ocs/wearengine/core/w83.java  |
| http://restsdk.amap.com/v5  | com/oplus/ocs/wearengine/core/w83.java  |
| https://restsdk.amap.com/v5  | com/oplus/ocs/wearengine/core/w83.java  |
| http://restsdk.amap.com/rest/me/cpoint  | com/oplus/ocs/wearengine/core/w83.java  |
| https://restsdk.amap.com/rest/me/cpoint  | com/oplus/ocs/wearengine/core/w83.java  |
| http://yuntuapi.amap.com  | com/oplus/ocs/wearengine/core/w83.java  |
| https://yuntuapi.amap.com  | com/oplus/ocs/wearengine/core/w83.java  |
| http://apistore.amap.com  | com/oplus/ocs/wearengine/core/w83.java  |
| https://apistore.amap.com  | com/oplus/ocs/wearengine/core/w83.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/oplus/ocs/wearengine/core/w83.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/oplus/ocs/wearengine/core/w83.java  |
| http://restsdk.amap.com  | com/oplus/ocs/wearengine/core/za3.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/oplus/ocs/wearengine/core/fc3.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/oplus/ocs/wearengine/core/fc3.java  |
| http://restsdk.amap.com/v3/place/text?  | com/oplus/ocs/wearengine/core/l33.java  |
| http://restsdk.amap.com/v3/config/district?  | com/oplus/ocs/wearengine/core/l33.java  |
| http://restsdk.amap.com/v3/place/around?  | com/oplus/ocs/wearengine/core/l33.java  |
| http://app.2bulu.com  | com/oplus/ocs/wearengine/core/mh2.java  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/oplus/ocs/wearengine/core/ma3.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/oplus/ocs/wearengine/core/u63.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/oplus/ocs/wearengine/core/u63.java  |
| http://restsdk.amap.com/v4  | com/oplus/ocs/wearengine/core/dg3.java  |
| http://restsdk.amap.com  | com/oplus/ocs/wearengine/core/eg3.java  |
| http://xmlpull.org/v1/doc/features.html  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://www.opengis.net/kml/2.2  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://www.google.com/kml/ext/2.2  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://files.2bulu.com/f/d1?downParams=BYohR0x5OLAr0OBxohfNOA%3D%3D%0A  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://files.2bulu.com/f/d1?downParams=n%2BVE0NaFmzwndk%2BZ75NU9A%3D%3D%0A  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://files.2bulu.com/f/d1?downParams=0Q3GJ5o%2FHpsr0OBxohfNOA%3D%3D%0A  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://files.2bulu.com/f/d1?downParams=vMzvc3dTBl0r0OBxohfNOA%3D%3D%0A  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://files.2bulu.com/f/d1?downParams=poL0RfxWHTIr0OBxohfNOA%3D%3D%0A  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://files.2bulu.com/f/d1?downParams=s2An6%2B3%2BIWUr0OBxohfNOA%3D%3D%0A  | com/oplus/ocs/wearengine/core/ye1.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| https://helper.2bulu.com/  | com/tbulu/watch/model/CommunicationEnvironment.java  |
| https://www.2bulu.com/  | com/tbulu/watch/model/CommunicationEnvironment.java  |
| https://files.2bulu.com/  | com/tbulu/watch/model/CommunicationEnvironment.java  |
| https://down-files.2bulu.com/  | com/tbulu/watch/model/CommunicationEnvironment.java  |
| https://emei-helper.2bulu.com/  | com/tbulu/watch/model/CommunicationEnvironment.java  |
| https://emei.2bulu.com/  | com/tbulu/watch/model/CommunicationEnvironment.java  |
| https://emei-file.2bulu.com/  | com/tbulu/watch/model/CommunicationEnvironment.java  |
| https://api.seniverse.com/v3/weather/now.json?key=  | com/tbulu/watch/logic/weather/XinzhiCurrentWeather.java  |
| https://api.openweathermap.org/data/2.5/weather?lat=  | com/tbulu/watch/logic/weather/OpenWeatherCurrentWeather.java  |
| https://www.2bulu.com/tilesServer/tiles/  | com/tbulu/watch/map/model/TileSources.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/l.java  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | com/umeng/analytics/pro/aq.java  |
| https://cnlogs.umeng.com/ext\_event  | com/umeng/analytics/pro/aq.java  |
| https://cnlogs.umeng.com/uapp\_ekverr\_logs  | com/umeng/analytics/pro/aq.java  |
| https://resolve.umeng.com/resolve  | com/umeng/analytics/pro/by.java  |
| https://ucc.umeng.com/v2/inn/fetch  | com/umeng/analytics/pro/ar.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://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://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/stateless/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://docs.objectbox.io/android/app-bundle-and-split-apk  | io/objectbox/internal/NativeLibraryLoader.java  |
| https://objectbox.io/sync/  | io/objectbox/sync/SyncBuilder.java  |
| https://objectbox.io/sync/  | io/objectbox/sync/server/SyncServerBuilder.java  |
| http://www.2bulu.com  | 摸瓜V1引擎  |
| http://restsdk.amap.com/rest/lbs/pos/log/upload  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://mps.amap.com/ws/mps/rtt  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://mps.amap.com/ws/mps/vmap  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://maps.testing.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://mps.amap.com/ws/mps/smap  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://mps.amap.com/ws/mps/spot  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://mps.amap.com/ws/mps/hot  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| http://maps.testing.amap.com/ws/mps/vmap  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| http://maps.testing.amap.com/ws/mps/rtt  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://faas-image.amap.com/acornCompressImageProd/%2523merge%2523%25402x-a2b2ad2c-50f4-46cc-9a68-9ef6a7c3d1be.png  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://img.alicdn.com/imgextra/i3/O1CN01BnLPsP1kjLlMfyzmX\_!!6000000004719-2-tps-64-64.png  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://m5.amap.com/  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| http://daily-orion.gaode.test  | lib/armeabi-v7a/libAMapSDK\_MAP\_v10\_0\_1000.so  |
| https://objectbox.io/sync/  | lib/armeabi-v7a/libobjectbox-jni.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| public@2bulu.com  | com/oplus/ocs/wearengine/core/jd.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18222222222  | com/amap/api/col/p0003sl/o000O00O.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=86, ST=guangdong, L=shenzhen, O=lolaage, OU=lolaage, CN=lolaage 签名算法: rsassa\_pkcs1v15 有效期自: 2013-02-03 08:54:50+00:00 有效期至: 3011-06-07 08:54:50+00:00 发行人: C=86, ST=guangdong, L=shenzhen, O=lolaage, OU=lolaage, CN=lolaage 序列号: 0x510e25da 哈希算法: sha1 md5值: 96864b1dd20f3aa32cc0c631bdcb0f18 sha1值: b1e568b6c144fbba1f709583877ac777563f771f sha256值: 6de9a1ff4644f48532bb63eff5b2108275ae1e367d1e6dc800e4e97ac97ea474 sha512值: 96b1998dbe9e2bfde1d1c758853ccd02ad5588991a71804863e932916d37405733bc8d819f57ec9cf2ac477bc04ce9f9f204ffd0a4fbe64dd61c6f7cbd009804 公钥算法: rsa 密钥长度: 1024 指纹: 0dbf7d44bab6cad49ad425264c264a2092f3185c9d58800daf2f7d1b1b290417**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

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

## **8. 第三方插件**

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

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.BODY\_SENSORS | 危险 |  | 允许应用程序访问来自传感器的数据,用户使用这些数据来测量他/她体内发生的事情,例如心率 |
| android.permission.BODY\_SENSORS\_BACKGROUND | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACTIVITY\_RECOGNITION | 危险 | 允许应用程序识别身体活动 | 允许应用程序识别身体活动 |
| 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.FOREGROUND\_SERVICE\_LOCATION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_DATA\_SYNC | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 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.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\_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\_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\_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.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 |
| heytap.wearable.permission.health.BIND\_EXERCISE\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.tbulu.watch.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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 |

## **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。**