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

**光大证券（ 25.02.11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 | 光大证券 |
| 版本 | 25.02.11 |
| 包名 | com.g2501.app |
| 域名线索 | 56条 |
| URL线索 | 82条 |
| APP图标 |  |
| 分析日期 | 2025年4月3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 | 光大证券.apk |
| 文件大小 | 59.16MB |
| MD5值 | b8c472ea53024da13d464715279f6923 |
| SHA1值 | c587361ababe599731a300ff5722f5f39e0399ca |
| SHA256值 | c06ccfe244be8c14df1d70dad5b53d3845cded420a0e7347ff792d8fb76d562c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 光大证券 |
| 包名 | com.g2501.app |
| 主活动Activity | io.dcloud.NewPandoraEntry |
| 安卓版本名称 | 25.02.11 |
| 安卓版本 | 250211 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| m5.amap.com | IP: 59.82.113.187 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.weixin.qq.com | IP: 140.207.191.167 所属国家: China 地区: Shanghai 城市: Shanghai  |
| loggw-exsdk.alipay.com | IP: 119.42.231.4 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| c-gtc.getui.nethttps | 没有服务器地理信息.  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| alogsus.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| m3w.cn | IP: 123.6.37.172 所属国家: China 地区: Henan 城市: Zhengzhou  |
| mcgw.alipay.com | IP: 123.125.216.192 所属国家: China 地区: Beijing 城市: Beijing  |
| d-gt.getui.com | 没有服务器地理信息.  |
| developer.umeng.com | IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| c-hzgt2.getui.com | IP: 124.160.155.55 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| zxid-m.mobileservice.cn | IP: 101.69.207.69 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| restsdk.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| adiu.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| gtc.getui.nethttps | 没有服务器地理信息.  |
| mobilegwpre.alipay.com | IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| aspect-upush.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| aid.mobileservice.cn | IP: 101.69.207.68 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| b-gtc.getui.nethttps | 没有服务器地理信息.  |
| mobilegw.alipay.com | IP: 203.209.245.129 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ulogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| mclient.alipay.com | IP: 123.6.22.250 所属国家: China 地区: Henan 城市: Zhengzhou  |
| wap.amap.com | IP: 116.142.235.229 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umengcloud.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| wappaygw.alipay.com | IP: 123.125.216.191 所属国家: China 地区: Beijing 城市: Beijing  |
| errnewlogos.umeng.com | IP: 47.246.110.96 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ucc.umeng.com | IP: 203.119.169.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cgicol.amap.com | IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| render.alipay.com | IP: 27.221.79.105 所属国家: China 地区: Shandong 城市: Qingdao  |
| utoken.umeng.com | IP: 223.109.148.171 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  |
| ns.adobe.com | 没有服务器地理信息.  |
| dualstack-arestapi.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| errlogos.umeng.com | IP: 47.246.110.96 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| errlog.umeng.com | IP: 223.109.148.142 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| lbs.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| mpsapi.amap.com | IP: 203.119.169.143 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wb.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| nisportal.10010.com | IP: 124.64.196.20 所属国家: China 地区: Beijing 城市: Beijing  |
| er.dcloud.net.cn | IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| h5.m.taobao.com | IP: 125.38.11.131 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mst01.is.autonavi.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| errnewlog.umeng.com | IP: 223.109.148.129 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| apiinit.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| er.dcloud.io | 没有服务器地理信息.  |
| sdk-open-phone.getui.com | IP: 101.68.218.163 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| dualstack-a.apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| ask.dcloud.net.cn | IP: 115.56.90.192 所属国家: China 地区: Henan 城市: Jiaozuo  |
| plbslog.umeng.com | IP: 36.156.202.68 所属国家: China 地区: Jiangsu 城市: Yangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/sdk/m/l/a.java  |
| https://mobilegw.alipaydev.com/mgw.htm  | com/alipay/sdk/m/l/a.java  |
| https://mcgw.alipay.com/sdklog.do  | com/alipay/sdk/m/l/a.java  |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do  | com/alipay/sdk/m/l/a.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/m/l/a.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/m/l/a.java  |
| https://h5.m.taobao.com/mlapp/olist.html  | com/alipay/sdk/m/m/a.java  |
| https://render.alipay.com/p/s/i?scheme=%s  | com/alipay/sdk/app/OpenAuthTask.java  |
| https://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mobilegwpre.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/p0003l/hk.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/amap/api/col/p0003l/je.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/p0003l/fh.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/p0003l/fh.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003l/gu.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003l/gu.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003l/fq.java  |
| http://restsdk.amap.com/v3/place/text?  | com/amap/api/col/p0003l/a.java  |
| http://restsdk.amap.com/v3/place/around?  | com/amap/api/col/p0003l/a.java  |
| http://restsdk.amap.com/v3/config/district?  | com/amap/api/col/p0003l/a.java  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/amap/api/col/p0003l/fb.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003l/df.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003l/s.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/amap/api/col/p0003l/de.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003l/de.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003l/cr.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003l/v.java  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\  | com/amap/api/col/p0003l/l.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/s/df.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/col/s/bt.java  |
| http://restsdk.amap.com/v3  | com/amap/api/col/s/i.java  |
| https://restsdk.amap.com/v3  | com/amap/api/col/s/i.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/s/i.java  |
| https://restsdk.amap.com/v4  | com/amap/api/col/s/i.java  |
| http://restsdk.amap.com/v5  | com/amap/api/col/s/i.java  |
| https://restsdk.amap.com/v5  | com/amap/api/col/s/i.java  |
| http://yuntuapi.amap.com  | com/amap/api/col/s/i.java  |
| https://yuntuapi.amap.com  | com/amap/api/col/s/i.java  |
| http://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/s/i.java  |
| https://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/s/i.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/s/i.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/s/i.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/s/cu.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/s/cu.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/s/bs.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/s/bs.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/s/bo.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bo.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/s/bo.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bo.java  |
| http://wap.amap.com/  | com/amap/api/maps/AMapUtils.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://m5.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.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://apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/g.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/trans/a.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  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/f/c.java  |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| 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.getui.com/  | com/getui/gtc/i/d/b.java  |
| https://sdk-open-phone.getui.com/api.php  | com/igexin/push/a.java  |
| https://c-hzgt2.getui.com/api.php  | com/igexin/push/a.java  |
| https://d-gt.getui.com/api.htm  | com/igexin/push/a.java  |
| https://bi.  | com/igexin/push/config/b.java  |
| https://config.  | com/igexin/push/config/b.java  |
| https://bi.  | com/igexin/push/config/h.java  |
| https://config.  | com/igexin/push/config/h.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | com/umeng/analytics/pro/am.java  |
| https://ucc.umeng.com/v2/inn/fetch  | com/umeng/analytics/pro/an.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/c/b.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/c/b.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://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://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://errnewlog.umeng.com  | com/umeng/umcrash/UMCrashContent.java  |
| https://errnewlogos.umeng.com  | com/umeng/umcrash/UMCrashContent.java  |
| https://errnewlogos.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlogos.umeng.com  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlog.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlog.umeng.com  | com/umeng/umcrash/UMCrash.java  |
| https://utoken.umeng.com  | com/umeng/umzid/ZIDManager.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://aid.mobileservice.cn/  | com/zx/a/I8b7/j3.java  |
| https://zxid-m.mobileservice.cn/sdk/config/v2/init  | com/zx/a/I8b7/n.java  |
| https://nisportal.10010.com:9001  | com/zx/a/I8b7/f1.java  |
| https://zxid-m.mobileservice.cn/sdk/config/init  | com/zx/a/I8b7/l.java  |
| https://zxid-m.mobileservice.cn/sdk/app/depAnalysis  | com/zx/a/I8b7/d1.java  |
| https://zxid-m.mobileservice.cn/sdk/module/getCoreModule  | com/zx/a/I8b7/f0.java  |
| https://zxid-m.mobileservice.cn/sdk/uaid/reportAuthToken  | com/zx/a/I8b7/v1.java  |
| https://zxid-m.mobileservice.cn/sdk/uaid/get  | com/zx/a/I8b7/w1.java  |
| https://zxid-m.mobileservice.cn/sdk/extend/tag  | com/zx/a/I8b7/b2.java  |
| https://zxid-m.mobileservice.cn/sdk/ext/pconfig  | com/zx/a/I8b7/f.java  |
| https://zxid-m.mobileservice.cn/sdk/channel/report  | com/zx/a/I8b7/p1.java  |
| https://ask.dcloud.net.cn/article/35627  | b/a.java  |
| https://ask.dcloud.net.cn/article/35877  | b/a.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| https://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| https://er.dcloud.io/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://er.dcloud.net.cn/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://ask.dcloud.net.cn/article/287  | io/dcloud/share/IFShareApi.java  |
| https://er.dcloud.io/rv  | d/c.java  |
| https://er.dcloud.net.cn/rv  | d/c.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifViewUtils.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/283  | j/b.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14222222222  | com/amap/api/col/s/bs.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=CN, ST=lfUKDaorpQzJCMkH, L=lfUKDaorpQzJCMkH, O=lfUKDaorpQzJCMkH, OU=lfUKDaorpQzJCMkH, CN=lfUKDaorpQzJCMkH 签名算法: rsassa\_pkcs1v15 有效期自: 2025-03-04 05:42:28+00:00 有效期至: 2079-12-06 05:42:28+00:00 发行人: C=CN, ST=lfUKDaorpQzJCMkH, L=lfUKDaorpQzJCMkH, O=lfUKDaorpQzJCMkH, OU=lfUKDaorpQzJCMkH, CN=lfUKDaorpQzJCMkH 序列号: 0xe3773d81306fc60e 哈希算法: sha256 md5值: 82136cc30b83ed2fb0afb5c6e8f3a4ee sha1值: d69e356d32298aa8bf5960f7babddc140b8cd68e sha256值: 9759b59f450ecd31ec785cdc2c7d57d484eca1bd7ce3133765fef400fd9bc86e sha512值: 1913b5cdfd10b79da8efbb57a32ad5ab70539ea207bf860291a04c7dd2c38b5970a197add7f7d69665c059a99b79f5de8daae9b1b83621155ab2103a7e5b3e6a 公钥算法: rsa 密钥长度: 2048 指纹: 952c612fc4a6a4d97cf408aa3c890376c4382d244c42de5988c4a483ba4f4516**

## **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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |
| 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\_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.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| 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\_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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.ACCESS\_MOCK\_LOCATION | 危险 | 用于测试的模拟位置源 | 创建模拟位置源进行测试。恶意应用程序可以使用它来覆盖由真实位置源（如 GPS 或网络提供商）返回的位置和/或状态 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| com.xiaomi.permission.AUTH\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 | 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.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.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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.SEND\_SMS | 危险 | 发送短信 | 允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价 |
| android.permission.WRITE\_SMS | 危险 | 编辑短信或彩信 | 允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息 |
| android.permission.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| 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\_VISUAL\_USER\_SELECTED | 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.vivo.notification.permission.BADGE\_ICON | 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 |
| 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.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。 |
| com.g2501.app.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 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| getui.permission.GetuiService.com.g2501.app | 未知 | Unknown permission | Unknown permission from android reference |
| 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.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntryActivity | **Schemes**: ://,  |

**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。**