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

**育托帮管理（ 1.1.4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 | 育托帮管理 |
| 版本 | 1.1.4 |
| 包名 | net.yutuobang.admin |
| 域名线索 | 86条 |
| URL线索 | 91条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | net.yutuobang.admin.apk |
| 文件大小 | 33.96MB |
| MD5值 | ac802a31dbddcd37c99b7078eba82a43 |
| SHA1值 | e28f185f62600791cdf6bd13d02f627a5f96ef97 |
| SHA256值 | 392530a6afc64613cdf5de2ba759d94625d74dc17f9600856be3f822407177f0 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 育托帮管理 |
| 包名 | net.yutuobang.admin |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.1.4 |
| 安卓版本 | 114 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.google.com | IP: 199.16.158.9 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  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.cn | IP: 49.4.45.231 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| cgicol.amap.com | IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| wap.amap.com | IP: 175.22.51.222 所属国家: China 地区: Jilin 城市: Changchun  |
| d-gt.getui.com | 没有服务器地理信息.  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| cdn.yutuobang.net | IP: 101.28.133.74 所属国家: China 地区: Hebei 城市: Handan  |
| lame.sf.net | IP: 104.18.20.237 所属国家: United States of America 地区: California 城市: San Francisco  |
| sdk-open-phone.getui.com | IP: 101.68.218.174 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| lbs.amap.com | IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| er.dcloud.io | 没有服务器地理信息.  |
| b-gtc.getui.nethttps | 没有服务器地理信息.  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api.weixin.qq.com | IP: 116.128.184.169 所属国家: China 地区: Shanghai 城市: Shanghai  |
| utils.yutuobang.net | IP: 121.40.163.230 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| xmlpull.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mps.amap.com | IP: 203.119.169.143 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mp.weixin.qq.com | IP: 140.207.191.167 所属国家: China 地区: Shanghai 城市: Shanghai  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| stream.mobihtml5.com | 没有服务器地理信息.  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| gtc.getui.nethttps | 没有服务器地理信息.  |
| maps.testing.amap.com | IP: 59.82.57.204 所属国家: China 地区: Beijing 城市: Beijing  |
| wb.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| mdc.html5.qq.com | IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing  |
| tbsrecovery.imtt.qq.com | IP: 61.181.204.91 所属国家: China 地区: Tianjin 城市: Tianjin  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| service.dcloud.net.cn | IP: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing  |
| open.weixin.qq.com | IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai  |
| quilljs.com | IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| mpsapi.amap.com | IP: 203.119.169.143 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  |
| data.yutuobang.net | IP: 101.67.62.25 所属国家: China 地区: Zhejiang 城市: Huzhou  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| apiinit.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m3w.cn | IP: 221.204.14.200 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| apis.map.qq.com | IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| er.dcloud.net.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| stream.dcloud.net.cn | IP: 43.142.166.20 所属国家: China 地区: Beijing 城市: Beijing  |
| ask.dcloud.net.cn | IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing  |
| dualstack-a.apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| upload.yutuobang.net | IP: 101.67.62.33 所属国家: China 地区: Zhejiang 城市: Huzhou  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| m5.amap.com | IP: 106.11.43.74 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| shop.yutuobang.net | IP: 116.142.237.86 所属国家: China 地区: Beijing 城市: Beijing  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| api.yutuobang.net | IP: 121.41.83.136 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| c-gtc.getui.nethttps | 没有服务器地理信息.  |
| c-hzgt2.getui.com | IP: 124.160.155.59 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| tbs.imtt.qq.com | IP: 61.161.0.179 所属国家: China 地区: Jilin 城市: Siping  |
| norma-external-collect.meizu.com | 没有服务器地理信息.  |
| at.alicdn.com | IP: 221.195.63.238 所属国家: China 地区: Hebei 城市: Cangzhou  |
| ns.adobe.com | 没有服务器地理信息.  |
| page.yutuobang.net | IP: 101.28.133.122 所属国家: China 地区: Hebei 城市: Handan  |
| adiu.amap.com | IP: 110.253.189.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| admin.yutuobang.net | IP: 47.97.97.182 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dualstack-arestapi.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mst01.is.autonavi.com | IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://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/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  | com/amap/api/col/p0003l/fq.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://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  |
| 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://m5.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.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  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/namespace-prefixes  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-general-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/string-interning  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xmlpull.org/v1/doc/features.html  | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java  |
| https://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  |
| http://bi.  | com/igexin/push/config/b.java  |
| http://config.  | com/igexin/push/config/b.java  |
| http://bi.  | com/igexin/push/config/g.java  |
| http://config.  | com/igexin/push/config/g.java  |
| https://api-push.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.in.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://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://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/l.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/o.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/o.java  |
| https://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/o.java  |
| https://tbsrecovery.imtt.qq.com/getconfig  | com/tencent/smtt/utils/o.java  |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs  | com/tencent/smtt/utils/d.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://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| http://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://stream.mobihtml5.com/  | io/dcloud/common/constant/StringConst.java  |
| https://stream.dcloud.net.cn/  | io/dcloud/common/constant/StringConst.java  |
| http://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://api.weixin.qq.com/sns/auth?access\_token=%s&openid=%s  | io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java  |
| https://api.weixin.qq.com/sns/oauth2/access\_token?appid=%s&secret=%s&code=%s&grant\_type=authorization\_code  | io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java  |
| https://api.weixin.qq.com/sns/userinfo?access\_token=%s&openid=%s&lang=zh\_CN  | io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java  |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token?appid=%s&grant\_type=refresh\_token&refresh\_token=%s  | io/dcloud/feature/oauth/weixin/WeiXinOAuthService.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/35627  | io/dcloud/e/b/a.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/e/b/a.java  |
| https://er.dcloud.io/rv  | io/dcloud/e/c/h/b.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/e/c/h/b.java  |
| http://lbs.amap.com/api/android-sdk/guide/error/  | io/dcloud/js/map/amap/adapter/AMapLink.java  |
| http://ask.dcloud.net.cn/article/283  | io/dcloud/g/b.java  |
| https://ask.dcloud.net.cn/article/287  | io/dcloud/share/IFShareApi.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/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://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://metrics5.dt.dbankcloud.ru:6447  | 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://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://page.yutuobang.net/defaults/user-usage-protocol.html\  | 摸瓜V2引擎  |
| https://page.yutuobang.net/defaults/user-privacy-protocol.html\  | 摸瓜V2引擎  |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=  | 摸瓜V2引擎  |
| https://www.google.com/maps/?daddr=  | 摸瓜V2引擎  |
| https://www.google.com/maps/  | 摸瓜V2引擎  |
| https://cdn.yutuobang.net/defaults/wx-mp-empty.html  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://page.yutuobang.net/defaults/user-  | 摸瓜V2引擎  |
| https://feross.org/opensource>  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| https://data.yutuobang.net  | 摸瓜V2引擎  |
| https://cdn.yutuobang.net  | 摸瓜V2引擎  |
| https://admin.yutuobang.net  | 摸瓜V2引擎  |
| https://shop.yutuobang.net  | 摸瓜V2引擎  |
| https://api.yutuobang.net  | 摸瓜V2引擎  |
| https://upload.yutuobang.net  | 摸瓜V2引擎  |
| https://utils.yutuobang.net  | 摸瓜V2引擎  |
| https://page.yutuobang.net/prod  | 摸瓜V2引擎  |
| https://cdn.yutuobang.net/defaults/jz\_insurance.jpg\_thumb200  | 摸瓜V2引擎  |
| https://cdn.yutuobang.net/defaults/jz\_health.jpg\_thumb200  | 摸瓜V2引擎  |
| https://mp.weixin.qq.com/s?\_\_biz=MzUzMTAwODA2MA==&mid=2247484243&idx=1&sn=dbfa4ac89949a84d94511798f6d6f8fb  | 摸瓜V2引擎  |
| https://page.yutuobang.net/defaults/user-usage-protocol.html?v  | 摸瓜V2引擎  |
| https://page.yutuobang.net/defaults/user-privacy-protocol.html?v  | 摸瓜V2引擎  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf)  | 摸瓜V2引擎  |
| https://cdn.yutuobang.net/defaults/admin-menus-fonts/iconfont.ttf)  | 摸瓜V2引擎  |
| https://quilljs.com/  | 摸瓜V2引擎  |
| https://quilljs.com  | 摸瓜V2引擎  |
| https://cdn.yutuobang.net/defaults/wx-mp-empty.html  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://crbug.com/v8/8520  | lib/armeabi-v7a/libweexjss.so  |
| http://lame.sf.net  | lib/armeabi-v7a/liblamemp3.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libnative-imagetranscoder.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libstatic-webp.so  |
| http://mpsapi.amap.com/ws/mps/vmap/  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://mpsapi.amap.com/ws/mps/rtt/  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://mpsapi.amap.com/ws/mps/smap  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://mpsapi.amap.com/  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://m5.amap.com  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/rtt  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/vmap  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://maps.testing.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/smap  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/spot  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/hot  | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libweexjss.so  |
| http://lame.sf.net  | lib/arm64-v8a/liblamemp3.so  |
| http://mpsapi.amap.com/ws/mps/vmap/  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://mpsapi.amap.com/ws/mps/rtt/  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://mpsapi.amap.com/ws/mps/smap  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://mpsapi.amap.com/  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| http://m5.amap.com  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/rtt  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/vmap  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://maps.testing.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/smap  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/spot  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |
| https://mps.amap.com/ws/mps/hot  | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_5\_0.so  |

### **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  |
| 18222222222  | com/tencent/smtt/sdk/o.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=, L=, O=Android, OU=Android, CN=%2FL0tnIZk5JqH%2BbXNPh3PHFcUN5QJqpXFskw4deE6E5FoqRAmqPZ12%2B4HeWfKD6%2FUfPVzrn%2FuHKPlbLdhAIG3Hg%3D%3D 签名算法: rsassa\_pkcs1v15 有效期自: 2023-03-21 08:42:06+00:00 有效期至: 2123-02-25 08:42:06+00:00 发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=%2FL0tnIZk5JqH%2BbXNPh3PHFcUN5QJqpXFskw4deE6E5FoqRAmqPZ12%2B4HeWfKD6%2FUfPVzrn%2FuHKPlbLdhAIG3Hg%3D%3D 序列号: 0x3226940 哈希算法: sha256 md5值: 06e707564905e3c66092091bfdf58704 sha1值: 9182604d36b8ff3247df851cc22a28d2c938d9c5 sha256值: 36467198ad30c05e33b38ce6be1c4bb1a7189a973f2a48a530646d454aea02a2 sha512值: 7864e46ab0d0e7e4a6b494840c8a54e694328e80c5f6178dc8ff352c5fe2c46eefeb9bb35afa53e2122248d6287d2b0a50b8dac9453b803db949d06bd0d9f729 公钥算法: rsa 密钥长度: 2048 指纹: cf2f0098b92b44e4ca2a2e2be2ff1fdd0b49024b9be329429347927111c25b33**

## **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\_feature\_oauth\_weixin\_plugin\_description" : "wechat"  |
| "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"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_feature\_oauth\_weixin\_plugin\_description" : "微信"  |
| "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.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.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.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。 |
| 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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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\_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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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\_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.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.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.BROADCAST\_PACKAGE\_ADDED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_CHANGED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_INSTALL | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_REPLACED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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 |
| net.yutuobang.admin.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| net.yutuobang.admin.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| getui.permission.GetuiService.net.yutuobang.admin | 未知 | Unknown permission | Unknown permission from android reference |
| net.yutuobang.admin.permission.MIPUSH\_RECEIVE | 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 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 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 |
| net.yutuobang.admin.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| net.yutuobang.admin.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: unipush://, ytbadmin://, **Hosts:** io.dcloud.unipush, **Paths:** /,  |

**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。**