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

**desire（ 1.0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 | desire |
| 版本 | 1.0 |
| 包名 |  |
| 域名线索 | 102条 |
| URL线索 | 90条 |
| APP图标 |  |
| 分析日期 | 2025年7月18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 | mUUAQGjl.apk |
| 文件大小 | 34.85MB |
| MD5值 | a8fdb232309ed786b2053d1366d7d6d5 |
| SHA1值 | 0e80a227bbc307f595eebfb4d3b86dee2e4a7a83 |
| SHA256值 | e58a9b27c30b0d1a4c6910d30a6cd765ef1f10a2c944f5e30b77dcad3c7aeee7 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | desire |
| 包名 |  |
| 主活动Activity | [] |
| 安卓版本名称 | 1.0 |
| 安卓版本 | [] |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| plbslog.umeng.com | IP: 36.156.202.73 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| restsdk.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| long.open.weixin.qq.com | IP: 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umengcloud.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| api-push.meizu.com | IP: 125.94.213.129 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| store.hispace.hicloud.com | IP: 121.36.117.66 所属国家: China 地区: Beijing 城市: Beijing  |
| cn.register.xmpush.xiaomi.com | IP: 118.26.252.220 所属国家: China 地区: Beijing 城市: Beijing  |
| 124.71.10.22 | IP: 124.71.10.22 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| resolver.msg.global.xiaomi.net | IP: 47.241.174.254 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| cgicol.amap.com | IP: 59.82.31.67 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| t2.xiaohongshu.com | IP: 54.223.156.52 所属国家: China 地区: Beijing 城市: Beijing  |
| alogus.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| android.bugly.qq.com | IP: 109.244.244.137 所属国家: China 地区: Beijing 城市: Beijing  |
| log.tbs.qq.com | IP: 109.244.244.37 所属国家: China 地区: Beijing 城市: Beijing  |
| tsis.jpush.cn | IP: 139.159.155.189 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| httpdns.bcelive.com | IP: 110.242.68.62 所属国家: China 地区: Hebei 城市: Baoding  |
| resolver.msg.xiaomi.net | IP: 120.92.96.13 所属国家: China 地区: Beijing 城市: Beijing  |
| pms.mb.qq.com | IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing  |
| fr.register.xmpush.global.xiaomi.com | IP: 52.28.40.92 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| idmb.register.xmpush.global.xiaomi.com | IP: 13.126.73.115 所属国家: India 地区: Maharashtra 城市: Mumbai  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| m5.amap.com | IP: 59.82.113.187 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.weixin.qq.com | IP: 109.244.145.152 所属国家: China 地区: Beijing 城市: Beijing  |
| debugx5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| apidns.kwd.inkuai.com | IP: 103.107.219.31 所属国家: China 地区: Beijing 城市: Beijing  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| cfg.imtt.qq.com | IP: 109.244.173.227 所属国家: China 地区: Beijing 城市: Beijing  |
| cgi.qplus.com | 没有服务器地理信息.  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| schemas.microsoft.com | IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| api.xmpush.xiaomi.com | IP: 220.181.52.239 所属国家: China 地区: Beijing 城市: Beijing  |
| aaid.umeng.com | IP: 218.91.197.68 所属国家: China 地区: Jiangsu 城市: Nantong  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| pslog.umeng.com | IP: 59.82.31.92 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| adiu.amap.com | IP: 59.82.31.202 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.xiaohongshu.com | IP: 212.64.115.100 所属国家: China 地区: Beijing 城市: Beijing  |
| 183.232.58.240 | IP: 183.232.58.240 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.asia | 没有服务器地理信息.  |
| 183.134.98.111 | IP: 183.134.98.111 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| p2.a.yximgs.com | IP: 220.181.135.139 所属国家: China 地区: Beijing 城市: Beijing  |
| material.io | IP: 216.239.36.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| soft.tbs.imtt.qq.com | IP: 121.51.175.105 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| api2.e.kuaishou.com | IP: 103.102.202.74 所属国家: China 地区: Beijing 城市: Beijing  |
| sdk-open-phone.getui.com | IP: 115.227.15.229 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| debugtbs.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| alogsus.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| wap.amap.com | IP: 42.81.22.183 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 120.46.157.112 | IP: 120.46.157.112 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| static.yximgs.com | IP: 211.93.242.56 所属国家: China 地区: Beijing 城市: Beijing  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| lbs.amap.com | IP: 59.82.31.137 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mdc.html5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| edith.xiaohongshu.com | IP: 119.45.249.52 所属国家: China 地区: Beijing 城市: Beijing  |
| openmobile.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |
| open.weixin.qq.com | IP: 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| grs.dbankcloud.com | IP: 42.81.226.18 所属国家: China 地区: Tianjin 城市: Tianjin  |
| yoda.kwd.inkuai.com | IP: 103.102.202.153 所属国家: China 地区: Beijing 城市: Beijing  |
| 183.134.98.75 | IP: 183.134.98.75 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 183.134.98.34 | IP: 183.134.98.34 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| 43.129.255.160 | IP: 43.129.255.160 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 49.233.102.113 | IP: 49.233.102.113 所属国家: China 地区: Beijing 城市: Beijing  |
| 118.26.252.225 | IP: 118.26.252.225 所属国家: China 地区: Beijing 城市: Beijing  |
| cgi.connect.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |
| p5.a.yximgs.com | IP: 119.176.24.41 所属国家: China 地区: Shandong 城市: Weifang  |
| developer.umeng.com | IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| adash.man.aliyuncs.com | IP: 59.82.40.77 所属国家: China 地区: Shanghai 城市: Shanghai  |
| dualstack-a.apilocate.amap.com | IP: 106.11.40.50 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wb.amap.com | IP: 59.82.60.46 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| login.sina.com.cn | IP: 49.7.36.224 所属国家: China 地区: Beijing 城市: Beijing  |
| graph.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |
| 103.102.200.38 | IP: 103.102.200.38 所属国家: China 地区: Beijing 城市: Beijing  |
| 43.226.164.41 | IP: 43.226.164.41 所属国家: China 地区: Jiangsu 城市: Suqian  |
| rqd.uu.qq.com | IP: 175.27.12.121 所属国家: China 地区: Beijing 城市: Beijing  |
| dualstack-arestapi.amap.com | IP: 39.98.22.142 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mpsapi.amap.com | IP: 106.11.43.68 所属国家: China 地区: Beijing 城市: Beijing  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| playready.directtaps.net | IP: 104.45.231.79 所属国家: United States of America 地区: California 城市: San Francisco  |
| ulogs.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| wup.imtt.qq.com | IP: 42.187.184.40 所属国家: China 地区: Beijing 城市: Beijing  |
| cc.map.qq.com | IP: 175.27.9.125 所属国家: China 地区: Beijing 城市: Beijing  |
| ali-stats.jpush.cn | IP: 120.233.50.82 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| norma-external-collect.meizu.com | IP: 113.106.27.98 所属国家: China 地区: Guangdong 城市: Zhongshan  |
| ouplog.umeng.com | IP: 47.246.110.94 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| appsupport.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |
| mst01.is.autonavi.com | IP: 59.82.31.67 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| huatuocode.huatuo.qq.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  |
| login.imgcache.qq.com | IP: 182.254.59.182 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| 175.24.251.189 | IP: 175.24.251.189 所属国家: China 地区: Beijing 城市: Beijing  |
| aexception.bugly.qq.com | IP: 101.226.233.161 所属国家: China 地区: Shanghai 城市: Shanghai  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing  |
| 49.51.177.180 | IP: 49.51.177.180 所属国家: United States of America 地区: California 城市: Los Angeles  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| http://restsdk.amap.com/v3  | com/amap/api/col/s/h.java  |
| https://restsdk.amap.com/v3  | com/amap/api/col/s/h.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/s/h.java  |
| https://restsdk.amap.com/v4  | com/amap/api/col/s/h.java  |
| http://yuntuapi.amap.com  | com/amap/api/col/s/h.java  |
| https://yuntuapi.amap.com  | com/amap/api/col/s/h.java  |
| http://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/s/h.java  |
| https://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/s/h.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/s/h.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/s/h.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/s/bj.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/s/bj.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/col/s/bk.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/s/cr.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/bf.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bf.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/s/bf.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bf.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://restsdk.amap.com  | com/amap/api/mapcore/util/fe.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/mapcore/util/ew.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/mapcore/util/ew.java  |
| http://apilocate.amap.com/mobile/binary  | com/amap/api/mapcore/util/io.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/amap/api/mapcore/util/io.java  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/amap/api/mapcore/util/eq.java  |
| http://restsdk.amap.com/v4  | com/amap/api/mapcore/util/i.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/mapcore/util/gv.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/mapcore/util/ex.java  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\  | com/amap/api/mapcore/util/b.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/amap/api/mapcore/util/cs.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/mapcore/util/cs.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/mapcore/util/ct.java  |
| http://restsdk.amap.com/v4  | com/amap/api/mapcore/util/cf.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.java  |
| https://material.io/design/components/dialogs.html  | com/afollestad/materialdialogs/MaterialDialog.java  |
| http://xml.apache.org/xslt  | com/wind/imlib/utils/KitReleaseLogUtils.java  |
| https://t2.xiaohongshu.com/api/collect  | com/fakerandroid/boot/CheckUntil.java  |
| https://edith.xiaohongshu.com/api/sns/v1/system\_service/config?launchtimes=9  | com/fakerandroid/boot/CheckUntil.java  |
| https://edith.xiaohongshu.com/api/sns/v1/search/placeholder?is\_new\_user=true  | com/fakerandroid/boot/CheckUntil.java  |
| https://www.xiaohongshu.com/api/im/users/following/all  | com/fakerandroid/boot/CheckUntil.java  |
| https://cc.map.qq.com/?desc\_c  | com/fakerandroid/boot/CheckUntil.java  |
| https://43.129.255.160:8081  | com/fakerandroid/boot/CheckUntil.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/fakerandroid/boot/CheckUntil.java  |
| https://183.232.58.240:21004  | com/fakerandroid/boot/CheckUntil.java  |
| https://118.26.252.225:5222  | com/fakerandroid/boot/CheckUntil.java  |
| https://120.46.157.112:7002  | com/fakerandroid/boot/CheckUntil.java  |
| https://49.51.177.180:5333  | com/fakerandroid/boot/CheckUntil.java  |
| https://183.134.98.111:5224  | com/fakerandroid/boot/CheckUntil.java  |
| https://183.134.98.34:5224  | com/fakerandroid/boot/CheckUntil.java  |
| https://183.134.98.75:5224  | com/fakerandroid/boot/CheckUntil.java  |
| https://login.sina.com.cn/visitor/signin  | com/fakerandroid/boot/CheckUntil.java  |
| https://sdk-open-phone.getui.com/api.php?format=json&t=1  | com/fakerandroid/boot/CheckUntil.java  |
| https://tsis.jpush.cn/  | com/fakerandroid/boot/CheckUntil.java  |
| https://ali-stats.jpush.cn  | com/fakerandroid/boot/CheckUntil.java  |
| https://49.233.102.113:5333  | com/fakerandroid/boot/CheckUntil.java  |
| https://124.71.10.22:7002  | com/fakerandroid/boot/CheckUntil.java  |
| https://175.24.251.189:5333  | com/fakerandroid/boot/CheckUntil.java  |
| https://103.102.200.38:80  | com/fakerandroid/boot/CheckUntil.java  |
| http://p5.a.yximgs.com/uhead/AB/2022/05/22/01/BMjAyMjA1MjIwMTUzMjdfMjI5NzUxOTU2OV8xX2hkNDc0XzE0OQ==\_s.jpg  | com/fakerandroid/boot/CheckUntil.java  |
| https://api2.e.kuaishou.com/rest/e/load/styleTemplate  | com/fakerandroid/boot/CheckUntil.java  |
| https://apidns.kwd.inkuai.com/label\_resolve?label=kwai-api&biz=aegon-android  | com/fakerandroid/boot/CheckUntil.java  |
| https://yoda.kwd.inkuai.com  | com/fakerandroid/boot/CheckUntil.java  |
| http://httpdns.bcelive.com/?dns=bd-origin.pull.yximgs.com,bd-adaptive-pull.live-voip.com,bd-adaptive-pull.video-voip.com,bd-adaptive.pull.yximgs.com,bd-origin-pull.live-voip.com,bd-origin-pull.video-voip.com,bd-p2p-pull.live-voip.com,bd-p2p-pull.video-voip.com,bd-p2p.pull.yximgs.com,bd-proxy.pull.yximgs.com,bd-pull.live-voip.com,bd-pull.video-voip.com,bd.pull.yximgs.com,bd.push.yximgs.com,d5-ks.a.kwimgs.com,p5-live.a.yximgs.com,p5.a.yximgs.com,v5-skvod.kwaicdn.com,v5.kwaicdn.com&type=a  | com/fakerandroid/boot/CheckUntil.java  |
| https://static.yximgs.com/bs2/adminBlock/treasure-1675409076903-xYWwjlqm.png  | com/fakerandroid/boot/CheckUntil.java  |
| https://43.226.164.41  | com/fakerandroid/boot/CheckUntil.java  |
| http://p2.a.yximgs.com/uhead/AB/2021/08/16/17/  | com/fakerandroid/boot/CheckUntil.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | com/xiaomi/push/gn.java  |
| https://%1$s/gslb/?ver=4.0  | com/xiaomi/push/cw.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gv.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gu.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gc.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fq.java  |
| https://api.xmpush.xiaomi.com/v1/trace/report/sdk  | com/xiaomi/push/df.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://fr.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://ru.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://idmb.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://resolver.msg.global.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bp.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bp.java  |
| https://adiu.amap.com/ws/device/adius  | com/loc/bb.java  |
| http://restsdk.amap.com  | com/loc/s.java  |
| http://restsdk.amap.com/v3/place/text?  | com/loc/a.java  |
| http://restsdk.amap.com/v3/config/district?  | com/loc/a.java  |
| http://restsdk.amap.com/v3/place/around?  | com/loc/a.java  |
| http://apilocate.amap.com/mobile/binary  | com/loc/ff.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/loc/ff.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/ff.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/loc/l.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/loc/l.java  |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo  | com/loc/fa.java  |
| http://restsdk.amap.com/v3/geocode/regeo  | com/loc/fa.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/loc/cr.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/ey.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/fk.java  |
| https://adash.man.aliyuncs.com/man/api?ak=23356390&s=  | com/alibaba/sdk/android/utils/AMSDevReporter.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  |
| http://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| http://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/autonavi/amap/mapcore/Inner\_3dMap\_location.java  |
| http://m5.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://restsdk.amap.com/rest/lbs/dem/dataservice?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  |
| https://graph.qq.com/  | com/imacapp/wind/api/LoginService.java  |
| https://api.weixin.qq.com/  | com/imacapp/wind/api/LoginService.java  |
| https://aaid.umeng.com/api/updateZdata/v3  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/postZdata/v3  | com/umeng/umzid/ZIDManager.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.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  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| http://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/crashreport/CrashReport.java  |
| http://rqd.uu.qq.com/rqd/sync  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/a.java  |
| http://aexception.bugly.qq.com:8012/rqd/async  | com/tencent/bugly/crashreport/common/strategy/a.java  |
| http://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/n.java  |
| http://wup.imtt.qq.com:8080  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/n.java  |
| http://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/n.java  |
| http://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/n.java  |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| http://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/j.java  |
| http://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| http://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| http://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| http://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/a/c.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/b/a/a.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/b/a/a.java  |
| https://openmobile.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.java  |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | com/tencent/connect/common/BaseApi.java  |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/common/BaseApi.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | 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://login.imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/auth/a.java  |
| https://login.imgcache.qq.com/open/mobile/request/sdk\_request.html?  | com/tencent/open/SocialApiIml.java  |
| https://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| https://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| https://login.imgcache.qq.com  | com/tencent/open/SocialApiIml.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind  | com/tencent/open/SocialOperation.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group  | com/tencent/open/SocialOperation.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/g.java  |
| https://cgi.qplus.com/report/report  | com/tencent/open/utils/l.java  |
| https://huatuocode.huatuo.qq.com  | com/tencent/open/a/d.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://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| https://play.google.com/store  | Mogua Engine V1  |
| https://appgallery.cloud.huawei.com/app/  | Mogua Engine V1  |
| https://play.google.com/store/apps/details?id=  | Mogua Engine V1  |
| https://appgallery.cloud.huawei.com  | Mogua Engine V1  |
| https://store.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V1  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/videocache/HttpUrlSource.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=CN, ST=zbQhlrsV, L=vQzkBwsp, O=TnELIPqb, OU=lGztcaCR, CN=LTOFcUNG 签名算法: rsassa\_pkcs1v15 有效期自: 2023-06-25 07:15:53+00:00 有效期至: 2050-11-10 07:15:53+00:00 发行人: C=CN, ST=zbQhlrsV, L=vQzkBwsp, O=TnELIPqb, OU=lGztcaCR, CN=LTOFcUNG 序列号: 0x2430af6c 哈希算法: sha256 md5值: 048f3ee661d09c92c6e965867b961da7 sha1值: 4c55587e6c30ce416e0b1ae7ccc1a580fba334b9 sha256值: 3674f637e00ff31bab2aee1043051a6e173b927f881a3b5a0f6e21e1603b2285 sha512值: 414c57a214f75a1d26c87e049836c61f2e7ada9befbd2707feb1eba6e67d92a3daa9ca6f25034e30364e1dda4e6f1566eb29e35128d971d8ba5097d3b7f6cb9a 公钥算法: rsa 密钥长度: 2048 指纹: 89d2de8e3bab04513d02f0fef67562076fdb435a9d121f0fd23619a11275c182**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "wx\_appsecret" : ""  |

## **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**

## **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。**