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

**してる（ 4.7.9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 | してる |
| 版本 | 4.7.9 |
| 包名 | fhomkll.nohdul.ohmfd |
| 域名线索 | 115条 |
| URL线索 | 42条 |
| APP图标 |  |
| 分析日期 | 2025年8月2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 | jimeng-new.apk |
| 文件大小 | 25.52MB |
| MD5值 | e2196467aea75abbfd27557617266d81 |
| SHA1值 | 4c564e590d76725c936ee6be0e6326109f21549d |
| SHA256值 | 47616ca7e222ebb8e882162a9fe97ab89f3ff682f0ea8c37b6102ef0a87ff2ed |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | してる |
| 包名 | fhomkll.nohdul.ohmfd |
| 主活动Activity | com.wind.im.MainActivity |
| 安卓版本名称 | 4.7.9 |
| 安卓版本 | 20240828 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 103.102.200.38 | IP: 103.102.200.38 所属国家: China 地区: Beijing 城市: Beijing  |
| ali-stats.jpush.cn | IP: 120.233.114.191 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| 10.38.162.35 | IP: 10.38.162.35 所属国家: - 地区: - 城市: -  |
| zhihu-web-analytics.zhihu.com | IP: 120.92.107.7 所属国家: China 地区: Beijing 城市: Beijing  |
| cloud.xdrig.com | IP: 116.198.14.26 所属国家: China 地区: Beijing 城市: Beijing  |
| i.gtimg.cn | IP: 123.6.25.115 所属国家: China 地区: Henan 城市: Zhengzhou  |
| playready.directtaps.net | IP: 104.45.231.79 所属国家: United States of America 地区: California 城市: San Francisco  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| httpdns.bcelive.com | IP: 110.242.68.62 所属国家: China 地区: Hebei 城市: Baoding  |
| data.video.iqiyi.com | IP: 110.242.72.8 所属国家: China 地区: Hebei 城市: Baoding  |
| sf3-fe-tos.pglstatp-toutiao.com | IP: 221.194.161.230 所属国家: China 地区: Hebei 城市: Langfang  |
| m.douban.com | IP: 81.70.124.99 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| lf1-cdn-tos.bytegoofy.com | IP: 221.194.161.232 所属国家: China 地区: Hebei 城市: Langfang  |
| tsis.jpush.cn | IP: 1.94.113.76 所属国家: China 地区: Beijing 城市: Beijing  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| grs.dbankcloud.cn | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| 1.12.12.12 | IP: 1.12.12.12 所属国家: China 地区: Beijing 城市: Beijing  |
| 43.129.255.160 | IP: 43.129.255.160 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| doh.pub | IP: 1.12.12.12 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  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| kepler.jd.com | IP: 36.110.181.182 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| openmobile.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| static.yximgs.com | IP: 101.73.101.235 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| developer.umeng.com | IP: 59.82.29.248 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| res.openinstall.com | IP: 60.222.200.219 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| sf6-fe-tos.pglstatp-toutiao.com | IP: 111.161.117.180 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 43.226.164.41 | IP: 43.226.164.41 所属国家: China 地区: Jiangsu 城市: Suqian  |
| zconfig.alibabausercontent.com | IP: 123.125.216.218 所属国家: China 地区: Beijing 城市: Beijing  |
| s3.pstatp.com | IP: 124.95.172.93 所属国家: China 地区: Liaoning 城市: Shenyang  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| store.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| ac.dun.163.com | IP: 45.254.50.146 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| graph.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| lf-cdn-tos.bytescm.com | IP: 120.52.152.210 所属国家: China 地区: Hebei 城市: Langfang  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| amonsul.douban.com | IP: 120.53.130.158 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| cgi.connect.qq.com | IP: 60.28.215.27 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  |
| login.sina.com.cn | IP: 202.108.0.130 所属国家: China 地区: Beijing 城市: Beijing  |
| dns.alidns.com | IP: 223.5.5.5 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 183.134.98.111 | IP: 183.134.98.111 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| yoda.kwd.inkuai.com | IP: 103.102.202.50 所属国家: China 地区: Beijing 城市: Beijing  |
| baichuan-sdk.alicdn.com | IP: 101.72.202.239 所属国家: China 地区: Hebei 城市: Langfang  |
| edith.xiaohongshu.com | IP: 47.97.66.48 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.xiaohongshu.com | IP: 81.69.116.86 所属国家: China 地区: Beijing 城市: Beijing  |
| iface2.iqiyi.com | IP: 123.126.131.95 所属国家: China 地区: Beijing 城市: Beijing  |
| mapi.m.jd.com | IP: 36.110.181.150 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tbsrecovery.imtt.qq.com | IP: 61.181.204.91 所属国家: China 地区: Tianjin 城市: Tianjin  |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| ranks.hao.360.com | IP: 112.65.69.124 所属国家: China 地区: Shanghai 城市: Shanghai  |
| photo.home.163.com | IP: 220.197.30.51 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| 49.233.102.113 | IP: 49.233.102.113 所属国家: China 地区: Beijing 城市: Beijing  |
| appgallery.cloud.huawei.com | IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| wspeed.qq.com | 没有服务器地理信息.  |
| 183.232.58.240 | IP: 183.232.58.240 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| ip.taobao.com | IP: 59.82.121.163 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  |
| qzs.gdtimg.com | IP: 119.188.44.177 所属国家: China 地区: Shandong 城市: Jinan  |
| userlink.alicdn.com | IP: 1.190.42.102 所属国家: China 地区: Heilongjiang 城市: Harbin  |
| 175.24.251.189 | IP: 175.24.251.189 所属国家: China 地区: Beijing 城市: Beijing  |
| appsupport.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api.weibo.cn | IP: 123.125.107.17 所属国家: China 地区: Beijing 城市: Beijing  |
| dp.im.weibo.cn | IP: 202.108.0.98 所属国家: China 地区: Beijing 城市: Beijing  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |
| cosmos-open.immomo.com | IP: 47.93.181.248 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 118.26.252.225 | IP: 118.26.252.225 所属国家: China 地区: Beijing 城市: Beijing  |
| cosmos-compass-api.immomo.com | IP: 43.231.168.216 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| 49.51.177.180 | IP: 49.51.177.180 所属国家: United States of America 地区: California 城市: Los Angeles  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| vd6.l.qq.com | IP: 60.29.238.103 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api.bilibili.com | IP: 221.204.56.95 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| acs.m.taobao.com | IP: 203.119.169.100 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| exoplayer.dev | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| gw.m.163.com | IP: 125.39.135.186 所属国家: China 地区: Tianjin 城市: Tianjin  |
| p5.a.yximgs.com | IP: 123.117.133.41 所属国家: China 地区: Beijing 城市: Beijing  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| cosmos-lua.immomo.com | IP: 39.107.125.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| norma-external-collect.meizu.com | IP: 183.60.176.112 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| new-service.biliapi.net | IP: 221.204.14.54 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| api.zhihu.com | IP: 119.188.180.230 所属国家: China 地区: Shandong 城市: Jinan  |
| p2.a.yximgs.com | IP: 120.52.78.215 所属国家: China 地区: Hebei 城市: Langfang  |
| www.sina.com.cn | IP: 123.126.45.205 所属国家: China 地区: Beijing 城市: Beijing  |
| 183.134.98.34 | IP: 183.134.98.34 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 124.71.10.22 | IP: 124.71.10.22 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| doh.360.cn | IP: 101.199.254.118 所属国家: China 地区: Beijing 城市: Beijing  |
| pslog.umeng.com | IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| t2.xiaohongshu.com | IP: 43.142.215.97 所属国家: China 地区: Beijing 城市: Beijing  |
| m-cloud.zhihu.com | IP: 221.204.43.106 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| sdkapp.uve.weibo.com | IP: 123.126.45.190 所属国家: China 地区: Beijing 城市: Beijing  |
| cc.map.qq.com | IP: 125.36.181.145 所属国家: China 地区: Tianjin 城市: Tianjin  |
| sdk-open-phone.getui.com | IP: 124.160.155.44 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| 223.5.5.5 | IP: 223.5.5.5 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| frodo.douban.com | IP: 140.143.177.206 所属国家: China 地区: Beijing 城市: Beijing  |
| sealine.youku.com | IP: 106.11.43.107 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| imgcache.qq.com | IP: 123.6.40.249 所属国家: China 地区: Henan 城市: Zhengzhou  |
| apidns.kwd.inkuai.com | IP: 103.107.218.240 所属国家: China 地区: Beijing 城市: Beijing  |
| mdc.html5.qq.com | IP: 125.39.196.199 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  |
| dashif.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.zhihu.com | IP: 119.188.180.230 所属国家: China 地区: Shandong 城市: Jinan  |
| open.weixin.qq.com | IP: 220.196.139.154 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| m.immomo.com | IP: 43.231.168.211 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.hao123.com | IP: 110.242.68.247 所属国家: China 地区: Hebei 城市: Baoding  |
| api.iqiyi.com | IP: 110.242.72.1 所属国家: China 地区: Hebei 城市: Baoding  |
| api2.e.kuaishou.com | IP: 103.102.202.151 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  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://openmobile.qq.com/  | ae/b.java  |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | ae/a.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | ae/h.java  |
| https://doh.pub/dns-query  | a0/c.java  |
| https://1.12.12.12/dns-query  | a0/c.java  |
| https://dns.alidns.com/dns-query  | a0/c.java  |
| https://223.5.5.5/dns-query  | a0/c.java  |
| https://doh.360.cn/dns-query  | a0/c.java  |
| https://ulogs.umeng.com  | a7/b.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://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/WebView.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://m.immomo.com/inc/android/agreement.html?v=5968  | com/wind/im/MainActivity.java  |
| https://cosmos-lua.immomo.com/v1/api/index/patch  | com/wind/im/MainActivity.java  |
| https://cosmos-lua.immomo.com/v1/api/index/limit  | com/wind/im/MainActivity.java  |
| https://cosmos-open.immomo.com/login/index/logs  | com/wind/im/MainActivity.java  |
| https://cosmos-compass-api.immomo.com/uploadCodeStart  | com/wind/im/MainActivity.java  |
| https://s3.pstatp.com/bytecom/resource/tetris/pi.ad6e3a13.js  | com/wind/im/MainActivity.java  |
| https://ip.taobao.com/service/getIpInfo.php?ip=myip  | com/wind/im/MainActivity.java  |
| https://api.weibo.cn/2/hot/hours\_spotlight?wm=3333\_2001  | com/wind/im/MainActivity.java  |
| https://api.weibo.cn/2/guest/login?wm=3333\_2001  | com/wind/im/MainActivity.java  |
| https://api.weibo.cn/2/client/get\_grayfeature  | com/wind/im/MainActivity.java  |
| https://baichuan-sdk.alicdn.com/4.0.1.10/23208668/1.0.0/ios/rule.htm  | com/wind/im/MainActivity.java  |
| https://sdkapp.uve.weibo.com/interface/sdk/sdkconfig.php?platform=ipad&version=7  | com/wind/im/MainActivity.java  |
| https://userlink.alicdn.com/smart\_link/ios/alsl\_switch\_config.json  | com/wind/im/MainActivity.java  |
| https://userlink.alicdn.com/matrix\_app/ios/matrix\_app\_config.json  | com/wind/im/MainActivity.java  |
| https://dp.im.weibo.cn/entrance  | com/wind/im/MainActivity.java  |
| https://sdkapp.uve.weibo.com/interface/sdk/sdkconfig.php?platform=ipad&version=11  | com/wind/im/MainActivity.java  |
| https://new-service.biliapi.net/chat-sdk/sdk/user/v1/config.action?appId=3cf3af32ac5049369af06fabb87a36d1&from=3&version=2.8.2  | com/wind/im/MainActivity.java  |
| https://amonsul.douban.com/check2?app\_name=Frodo\_iPhone&apikey=0ab215a8b1977939201640fa14c66bab&sdkVersion=1.9.0  | com/wind/im/MainActivity.java  |
| https://frodo.douban.com/frodo\_rexxar/api/routes?device\_id=  | com/wind/im/MainActivity.java  |
| https://m.douban.com/  | com/wind/im/MainActivity.java  |
| https://i.gtimg.cn/ams-web/page-performance/page-performance.min.js?v=1  | com/wind/im/MainActivity.java  |
| https://kepler.jd.com/console/admin/getConfigNew  | com/wind/im/MainActivity.java  |
| https://mapi.m.jd.com/ksdk/updlist.json  | com/wind/im/MainActivity.java  |
| https://api.zhihu.com/zst/events/p  | com/wind/im/MainActivity.java  |
| https://zhihu-web-analytics.zhihu.com/api/v1/server\_tsp  | com/wind/im/MainActivity.java  |
| https://m-cloud.zhihu.com/api/apm/sampling/get?appKey=XoO7so  | com/wind/im/MainActivity.java  |
| https://api.zhihu.com/market/popovers\_v2  | com/wind/im/MainActivity.java  |
| https://api.zhihu.com/api/v4/ecom\_data/config  | com/wind/im/MainActivity.java  |
| https://api.zhihu.com/account/toggle  | com/wind/im/MainActivity.java  |
| https://api.zhihu.com/moments/tab\_v2?feed\_type=recommend  | com/wind/im/MainActivity.java  |
| https://m-cloud.zhihu.com/api/app/monitor/sampling/sync?appKey=XoO7so  | com/wind/im/MainActivity.java  |
| https://qzs.gdtimg.com/union/res/union\_temp\_v2/page/ANTempMob/tempMob.1659340444417.package.json  | com/wind/im/MainActivity.java  |
| https://iface2.iqiyi.com/fusion/3.0/switch/ext?content=dfp\_config&platform\_id=12  | com/wind/im/MainActivity.java  |
| https://api.iqiyi.com/3f4/emoticon-sns.iqiyi.com/jaguar-core/query\_config?bussiness=feedStatic&agenttype=268&version=3.8.10  | com/wind/im/MainActivity.java  |
| https://sf6-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/renderer/6259e2/package.json?aid=5000546&version\_code=5.4.0.5&device\_platform=ipad  | com/wind/im/MainActivity.java  |
| https://data.video.iqiyi.com/t  | com/wind/im/MainActivity.java  |
| https://lf-cdn-tos.bytescm.com/obj/static/ad/play-comp/playable-component-sdk/package.ugen.json?aid=5000546&version\_code=5.4.0.5&device\_platform=ipad  | com/wind/im/MainActivity.java  |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/renderer/6259e2/fallback.js  | com/wind/im/MainActivity.java  |
| https://lf1-cdn-tos.bytegoofy.com/goofy/fe/ies/bridge/bytedance/jsbridge-2.2.10.umd.js  | com/wind/im/MainActivity.java  |
| https://api.iqiyi.com/keepalive  | com/wind/im/MainActivity.java  |
| https://acs.m.taobao.com/gw/mtop.common.getTimestamp/\*  | com/wind/im/MainActivity.java  |
| https://zconfig.alibabausercontent.com/zconfig/23569910/11.0.50/0  | com/wind/im/MainActivity.java  |
| https://sealine.youku.com/sdkconfig\_60.xml  | com/wind/im/MainActivity.java  |
| https://gw.m.163.com/nc/api/v1/search/hot-word  | com/wind/im/MainActivity.java  |
| https://gw.m.163.com/nc-notify/api/v5/notify/homeunreadnum  | com/wind/im/MainActivity.java  |
| https://gw.m.163.com/commons-user-incentive/api/v1/commons/incentive/taskConfig  | com/wind/im/MainActivity.java  |
| https://gw.m.163.com/nc/api/v1/local/city.html  | com/wind/im/MainActivity.java  |
| https://gw.m.163.com/nc-gateway/api/v1/topicset/ios/topicsetList  | com/wind/im/MainActivity.java  |
| https://gw.m.163.com/commons-user-main/api/v1/commons/main/anonymous/allFollowList  | com/wind/im/MainActivity.java  |
| https://cloud.xdrig.com/configcloud/rest/sdk/gdprCheck  | com/wind/im/MainActivity.java  |
| https://t2.xiaohongshu.com/api/collect  | com/wind/im/MainActivity.java  |
| https://edith.xiaohongshu.com/api/sns/v1/system\_service/config?launchtimes=9  | com/wind/im/MainActivity.java  |
| https://edith.xiaohongshu.com/api/sns/v1/search/placeholder?is\_new\_user=true  | com/wind/im/MainActivity.java  |
| https://www.xiaohongshu.com/api/im/users/following/all  | com/wind/im/MainActivity.java  |
| https://cc.map.qq.com/?desc\_c  | com/wind/im/MainActivity.java  |
| https://43.129.255.160:8081  | com/wind/im/MainActivity.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/wind/im/MainActivity.java  |
| https://183.232.58.240:21004  | com/wind/im/MainActivity.java  |
| https://118.26.252.225:5222  | com/wind/im/MainActivity.java  |
| https://120.46.157.112:7002  | com/wind/im/MainActivity.java  |
| https://49.51.177.180:5333  | com/wind/im/MainActivity.java  |
| https://183.134.98.111:5224  | com/wind/im/MainActivity.java  |
| https://183.134.98.34:5224  | com/wind/im/MainActivity.java  |
| https://183.134.98.75:5224  | com/wind/im/MainActivity.java  |
| https://login.sina.com.cn/visitor/signin  | com/wind/im/MainActivity.java  |
| https://sdk-open-phone.getui.com/api.php?format=json&t=1  | com/wind/im/MainActivity.java  |
| https://tsis.jpush.cn/  | com/wind/im/MainActivity.java  |
| https://ali-stats.jpush.cn  | com/wind/im/MainActivity.java  |
| https://49.233.102.113:5333  | com/wind/im/MainActivity.java  |
| https://124.71.10.22:7002  | com/wind/im/MainActivity.java  |
| https://175.24.251.189:5333  | com/wind/im/MainActivity.java  |
| https://103.102.200.38:80  | com/wind/im/MainActivity.java  |
| http://p5.a.yximgs.com/uhead/AB/2022/05/22/01/BMjAyMjA1MjIwMTUzMjdfMjI5NzUxOTU2OV8xX2hkNDc0XzE0OQ==\_s.jpg  | com/wind/im/MainActivity.java  |
| https://api2.e.kuaishou.com/rest/e/load/styleTemplate  | com/wind/im/MainActivity.java  |
| https://apidns.kwd.inkuai.com/label\_resolve?label=kwai-api&biz=aegon-android  | com/wind/im/MainActivity.java  |
| https://yoda.kwd.inkuai.com  | com/wind/im/MainActivity.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/wind/im/MainActivity.java  |
| https://static.yximgs.com/bs2/adminBlock/treasure-1675409076903-xYWwjlqm.png  | com/wind/im/MainActivity.java  |
| https://43.226.164.41  | com/wind/im/MainActivity.java  |
| http://p2.a.yximgs.com/uhead/AB/2021/08/16/17/  | com/wind/im/MainActivity.java  |
| https://www.hao123.com/api/gethitthecity  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://www.hao123.com/api/citymenu  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://www.hao123.com/api/getgoodthing  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://www.hao123.com/api/tnwhilte  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://www.hao123.com/api/sample  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://www.hao123.com/api/getgamedata  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://www.hao123.com/api/getgameboxindexdata  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://vd6.l.qq.com/proxyhttp  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://www.sina.com.cn/api/hotword.json  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://gw.m.163.com/search/api/v1/pc-wap/rolling-word  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://photo.home.163.com/api/designer/pc/home/index/word  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://ac.dun.163.com/v3/d  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://www.zhihu.com/api/v4/search/top\_search  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://ranks.hao.360.com/shortvideo-api/hotnews  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| https://api.bilibili.com/x/web-interface/nav  | com/imacapp/message/vm/ChatRoomViewModel.java  |
| http://10.38.162.35:9085  | com/xiaomi/push/service/w1.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/w1.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/b.java  |
| https://pslog.umeng.com  | cf/a.java  |
| https://ulogs.umeng.com  | cf/a.java  |
| https://res.openinstall.com/%s.dnc  | io/openinstall/sdk/j.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | j0/j0.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | je/t.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | je/t.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | je/t.java  |
| https://tbsrecovery.imtt.qq.com/getconfig  | je/t.java  |
| http://dashif.org/guidelines/last-segment-number  | l1/c.java  |
| http://xmlpull.org/v1/doc/features.html  | nh/d4.java  |
| http://xmlpull.org/v1/doc/features.html  | nh/t4.java  |
| https://%1$s/gslb/?ver=5.0  | nh/o0.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | nh/s0.java  |
| http://xmlpull.org/v1/doc/features.html  | nh/u4.java  |
| http://xmlpull.org/v1/doc/features.html  | nh/u3.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | sd/k.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | sd/e.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | qi/d.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://github.com/danikula/AndroidVideoCache/issues/88.  | w/k.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | w/k.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | w/k.java  |
| http://%s:%d/%s  | w/n.java  |
| http://%s:%d/%s  | w/f.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | w/f.java  |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | td/a.java  |
| https://h.trace.qq.com/kv  | yd/c.java  |
| https://wspeed.qq.com/w.cgi  | yd/j.java  |
| https://huatuocode.huatuo.qq.com?domain=mobile.opensdk.com&cgi=opensdk&type=  | yd/f.java  |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report  | yd/k.java  |
| https://graph.qq.com/  | y9/k.java  |
| https://api.weixin.qq.com/  | y9/k.java  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | ob/b.java  |
| https://ulogs.umeng.com  | a5/a.java  |
| https://ulogs.umengcloud.com  | a5/a.java  |
| https://developer.umeng.com/docs/66632/detail/  | a5/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/registerPush  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/unRegisterPush  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/getRegisterSwitch  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/changeRegisterSwitch  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/changeAllSwitch  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/subscribeTags  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/unSubscribeTags  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/unSubAllTags  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/getSubTags  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/subscribeAlias  | sc/a.java  |
| https://api-push.meizu.com/garcia/api/client/message/unSubscribeAlias  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/registerPush  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/unRegisterPush  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/getRegisterSwitch  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/changeRegisterSwitch  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/changeAllSwitch  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/subscribeTags  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/unSubscribeTags  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/unSubAllTags  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/getSubTags  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/subscribeAlias  | sc/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/message/unSubscribeAlias  | sc/a.java  |
| https://play.google.com/store  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com/app/  | 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://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V1引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | w/k.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: False 找到 1 个唯一证书 主题: C=bqfbwrmxcwurv, ST=fgssrkkyelkvg, L=pgncmbyqzrjrd, O=cah1733039451921, OU=njk1733039451921, CN=TG@apkfangdujiagu 签名算法: rsassa\_pkcs1v15 有效期自: 2024-12-01 07:50:51+00:00 有效期至: 2074-11-19 07:50:51+00:00 发行人: C=bqfbwrmxcwurv, ST=fgssrkkyelkvg, L=pgncmbyqzrjrd, O=cah1733039451921, OU=njk1733039451921, CN=TG@apkfangdujiagu 序列号: 0x501934eb 哈希算法: sha1 md5值: a7ef82ece4e3369b2fa97fe62a0c853b sha1值: f397cbf3bb6a0a983b704edb0a5e837b8fd4694e sha256值: 7dc10bff81e6ad926b40e15d98c6f8c8d46b0986b409b5e260d7c0a98a7731cd sha512值: fbd68ea5a9c39d6d2dfdae4a128822428cb1e45ff1b1edef9663b6a890f5625b3f5604738cc78a864d9c314b2457bff53e007489404ebf372c790383ce8e615e 公钥算法: rsa 密钥长度: 1024 指纹: 900a50ed70c33c5d539ddeba793987353016ae91dc2b067a5b11950caea91633**

## **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**

| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.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.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.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 |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| fhomkll.nohdul.ohmfd\_com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd\_com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd\_com.huawei.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| fhomkll.nohdul.ohmfd.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd\_com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd\_com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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 |
| fhomkll.nohdul.ohmfd.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| fhomkll.nohdul.ohmfd\_com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd\_com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| fhomkll.nohdul.ohmfd\_com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| fhomkll.nohdul.ohmfd\_freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.wind.im.MainActivity | **Schemes**: jdz5pr://,  |
| com.imacapp.common.WindCommTransitActivity | **Schemes**: xqchat://,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent111111://,  |

**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。**