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

**Feili（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 | Feili |
| 版本 |  |
| 包名 | agksdykxgdksg.dhkasgksgx.rpahskdhkxh |
| 域名线索 | 110条 |
| URL线索 | 40条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | 5lu11yzj.apk |
| 文件大小 | 29.4MB |
| MD5值 | 9aa98fe2589c8ca18726e24202053275 |
| SHA1值 | 473dd377e08ebf1ec98f9e2dec77c3dac6be4004 |
| SHA256值 | ddd30191528825a92a57504b7af0ae9dabe9fafad46a6773ba537054830ac68a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Feili |
| 包名 | agksdykxgdksg.dhkasgksgx.rpahskdhkxh |
| 主活动Activity |  |
| 安卓版本名称 |  |
| 安卓版本 |  |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| login.sina.com.cn | IP: 116.133.8.36  所属国家: China  地区: Beijing  城市: Beijing |
| tsis.jpush.cn | IP: 110.41.138.213  所属国家: China  地区: Guangdong  城市: Guangzhou |
| 120.46.157.112 | IP: 120.46.157.112  所属国家: China  地区: Guangdong  城市: Guangzhou |
| mdc.html5.qq.com | IP: 116.130.223.178  所属国家: China  地区: Beijing  城市: Beijing |
| resolver.msg.xiaomi.net | IP: 110.43.0.169  所属国家: China  地区: Beijing  城市: Beijing |
| www.hao123.com | IP: 110.242.68.247  所属国家: China  地区: Hebei  城市: Baoding |
| dns.alidns.com | IP: 223.5.5.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| data.video.iqiyi.com | IP: 123.126.131.136  所属国家: China  地区: Beijing  城市: Beijing |
| doh.pub | IP: 120.53.53.53  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 |
| api-push.in.meizu.com | IP: 206.161.233.191  所属国家: United States of America  地区: Virginia  城市: Herndon |
| cgi.connect.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| cosmos-open.immomo.com | IP: 82.157.134.81  所属国家: China  地区: Beijing  城市: Beijing |
| p5.a.yximgs.com | IP: 115.25.216.41  所属国家: China  地区: Beijing  城市: Beijing |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| log.tbs.qq.com | IP: 124.95.224.248  所属国家: China  地区: Liaoning  城市: Shenyang |
| api.iqiyi.com | IP: 110.242.72.1  所属国家: China  地区: Hebei  城市: Baoding |
| 183.134.98.111 | IP: 183.134.98.111  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 43.129.255.160 | IP: 43.129.255.160  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| doh.360.cn | IP: 101.199.254.118  所属国家: China  地区: Beijing  城市: Beijing |
| edith.xiaohongshu.com | IP: 114.55.236.88  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52  所属国家: China  地区: Hebei  城市: Langfang |
| cosmos-lua.immomo.com | IP: 39.107.125.82  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| kepler.jd.com | IP: 36.110.181.182  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 49.51.177.180 | IP: 49.51.177.180  所属国家: United States of America  地区: California  城市: Los Angeles |
| 49.233.102.113 | IP: 49.233.102.113  所属国家: China  地区: Beijing  城市: Beijing |
| 223.5.5.5 | IP: 223.5.5.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mapi.m.jd.com | IP: 36.110.181.150  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| i.gtimg.cn | IP: 42.236.6.230  所属国家: China  地区: Henan  城市: Zhengzhou |
| www.sina.com.cn | IP: 123.125.107.39  所属国家: China  地区: Beijing  城市: Beijing |
| www.zhihu.com | IP: 60.28.220.193  所属国家: China  地区: Tianjin  城市: Tianjin |
| httpdns.bcelive.com | IP: 163.177.18.242  所属国家: China  地区: Guangdong  城市: Guangzhou |
| sdkapp.uve.weibo.com | IP: 116.133.8.86  所属国家: China  地区: Beijing  城市: Beijing |
| qzs.gdtimg.com | IP: 119.188.209.130  所属国家: China  地区: Shandong  城市: Zaozhuang |
| iface2.iqiyi.com | IP: 111.202.15.23  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 |
| www.xiaohongshu.com | IP: 81.69.116.86  所属国家: China  地区: Beijing  城市: Beijing |
| lf1-cdn-tos.bytegoofy.com | IP: 221.195.209.95  所属国家: China  地区: Hebei  城市: Cangzhou |
| developer.umeng.com | IP: 59.82.29.249  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 103.102.200.38 | IP: 103.102.200.38  所属国家: China  地区: Beijing  城市: Beijing |
| 223.6.6.6 | IP: 223.6.6.6  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 120.53.53.53 | IP: 120.53.53.53  所属国家: China  地区: Beijing  城市: Beijing |
| gw.m.163.com | IP: 124.163.197.209  所属国家: China  地区: Shanxi  城市: Taiyuan |
| huatuocode.huatuo.qq.com | 没有服务器地理信息. |
| sf3-fe-tos.pglstatp-toutiao.com | IP: 125.38.11.59  所属国家: China  地区: Tianjin  城市: Tianjin |
| 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: 101.68.218.161  所属国家: China  地区: Zhejiang  城市: Jiaxing |
| 175.24.251.189 | IP: 175.24.251.189  所属国家: China  地区: Beijing  城市: Beijing |
| api.zhihu.com | IP: 101.72.227.133  所属国家: China  地区: Hebei  城市: Langfang |
| schemas.microsoft.com | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| 118.26.252.225 | IP: 118.26.252.225  所属国家: China  地区: Beijing  城市: Beijing |
| imgcache.qq.com | IP: 123.6.33.201  所属国家: China  地区: Henan  城市: Zhengzhou |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| amonsul.douban.com | IP: 140.143.177.206  所属国家: China  地区: Beijing  城市: Beijing |
| api-push.meizu.com | IP: 221.5.93.66  所属国家: China  地区: Guangdong  城市: Foshan |
| dashif.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| cloud.xdrig.com | IP: 116.198.14.56  所属国家: China  地区: Beijing  城市: Beijing |
| baichuan-sdk.alicdn.com | IP: 60.222.200.244  所属国家: China  地区: Shanxi  城市: Taiyuan |
| m.douban.com | IP: 81.70.124.99  所属国家: China  地区: Beijing  城市: Beijing |
| s3.pstatp.com | IP: 116.142.235.227  所属国家: China  地区: Beijing  城市: Beijing |
| m-cloud.zhihu.com | IP: 123.125.244.28  所属国家: China  地区: Beijing  城市: Beijing |
| userlink.alicdn.com | IP: 124.95.172.114  所属国家: China  地区: Liaoning  城市: Shenyang |
| ac.dun.163.com | IP: 220.197.32.185  所属国家: China  地区: Sichuan  城市: Mianyang |
| ranks.hao.360.com | IP: 112.65.69.124  所属国家: China  地区: Shanghai  城市: Shanghai |
| sf6-fe-tos.pglstatp-toutiao.com | IP: 121.18.236.110  所属国家: China  地区: Hebei  城市: Baoding |
| wspeed.qq.com | 没有服务器地理信息. |
| ali-stats.jpush.cn | IP: 119.147.121.149  所属国家: China  地区: Guangdong  城市: Dongguan |
| 183.134.98.34 | IP: 183.134.98.34  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulogs.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| norma-external-collect.meizu.com | 没有服务器地理信息. |
| frodo.douban.com | IP: 120.53.130.158  所属国家: China  地区: Beijing  城市: Beijing |
| m.immomo.com | IP: 82.157.134.81  所属国家: China  地区: Beijing  城市: Beijing |
| xmlpull.org | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| lf-cdn-tos.bytescm.com | IP: 222.141.5.44  所属国家: China  地区: Henan  城市: Luoyang |
| photo.home.163.com | IP: 220.197.30.51  所属国家: China  地区: Jiangsu  城市: Nanjing |
| graph.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| api.weibo.cn | IP: 114.250.52.125  所属国家: China  地区: Beijing  城市: Beijing |
| vd6.l.qq.com | IP: 60.29.238.103  所属国家: China  地区: Tianjin  城市: Tianjin |
| apidns.kwd.inkuai.com | IP: 103.102.202.124  所属国家: China  地区: Beijing  城市: Beijing |
| playready.directtaps.net | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| 183.134.98.75 | IP: 183.134.98.75  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| static.yximgs.com | IP: 61.240.144.170  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| 183.232.58.240 | IP: 183.232.58.240  所属国家: China  地区: Guangdong  城市: Guangzhou |
| acs.m.taobao.com | IP: 203.119.238.239  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulogs.umengcloud.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| appsupport.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| dp.im.weibo.cn | IP: 116.133.8.18  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 |
| api.bilibili.com | IP: 218.60.18.17  所属国家: China  地区: Liaoning  城市: Fuxin |
| p2.a.yximgs.com | IP: 124.165.124.207  所属国家: China  地区: Shanxi  城市: Taiyuan |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| yoda.kwd.inkuai.com | IP: 103.102.202.50  所属国家: China  地区: Beijing  城市: Beijing |
| h.trace.qq.com | IP: 113.56.189.162  所属国家: China  地区: Hubei  城市: Huangshi |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| openmobile.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| ip.taobao.com | IP: 59.82.121.179  所属国家: China  地区: Beijing  城市: Beijing |
| zconfig.alibabausercontent.com | IP: 116.196.141.49  所属国家: China  地区: Zhejiang  城市: Jinhua |
| cosmos-compass-api.immomo.com | IP: 82.157.134.81  所属国家: China  地区: Beijing  城市: Beijing |
| pslog.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| zhihu-web-analytics.zhihu.com | IP: 60.28.220.193  所属国家: China  地区: Tianjin  城市: Tianjin |
| api.weixin.qq.com | IP: 116.128.170.42  所属国家: China  地区: Shanghai  城市: Shanghai |
| res.openinstall.com | IP: 47.122.95.238  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| t2.xiaohongshu.com | IP: 153.99.244.110  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| 10.38.162.35 | IP: 10.38.162.35  所属国家: -  地区: -  城市: - |
| 124.71.10.22 | IP: 124.71.10.22  所属国家: China  地区: Guangdong  城市: Guangzhou |
| new-service.biliapi.net | IP: 221.204.15.89  所属国家: China  地区: Shanxi  城市: Taiyuan |
| sealine.youku.com | IP: 106.11.43.183  所属国家: China  地区: Beijing  城市: Beijing |
| tbsrecovery.imtt.qq.com | IP: 60.28.215.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| exoplayer.dev | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| open.weixin.qq.com | IP: 116.128.169.212  所属国家: China  地区: Shanghai  城市: Shanghai |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://developer.umeng.com/docs/66632/detail/ | a0/c.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 |
| 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://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 |
| http://10.38.162.35:9085 | com/xiaomi/push/service/w1.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/w1.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 |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/b.java |
| https://h.trace.qq.com/kv | ce/c.java |
| https://wspeed.qq.com/w.cgi | ce/j.java |
| https://huatuocode.huatuo.qq.com?domain=mobile.opensdk.com&cgi=opensdk&type= | ce/f.java |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report | ce/k.java |
| https://pslog.umeng.com | ff/a.java |
| https://ulogs.umeng.com | ff/a.java |
| https://openmobile.qq.com/ | ee/b.java |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | ee/a.java |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | ee/h.java |
| https://res.openinstall.com/%s.dnc | io/openinstall/sdk/j.java |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread | j0/k0.java |
| http://xmlpull.org/v1/doc/features.html | l1/k.java |
| http://dashif.org/guidelines/last-segment-number | l1/c.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | ne/t.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | ne/t.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | ne/t.java |
| https://tbsrecovery.imtt.qq.com/getconfig | ne/t.java |
| https://ulogs.umeng.com | ne/c.java |
| https://ulogs.umengcloud.com | ne/c.java |
| http://xmlpull.org/v1/doc/features.html | qh/c4.java |
| http://xmlpull.org/v1/doc/features.html | qh/s4.java |
| https://%1$s/gslb/?ver=5.0 | qh/o0.java |
| https://resolver.msg.xiaomi.net/psc/?t=a | qh/s0.java |
| http://xmlpull.org/v1/doc/features.html | qh/t4.java |
| https://ulogs.umeng.com | qh/v0.java |
| https://doh.pub/dns-query | qh/v0.java |
| https://1.12.12.12/dns-query | qh/v0.java |
| https://120.53.53.53/dns-query | qh/v0.java |
| https://dns.alidns.com/dns-query | qh/v0.java |
| https://223.5.5.5/dns-query | qh/v0.java |
| https://223.6.6.6/dns-query | qh/v0.java |
| https://doh.360.cn/dns-query | qh/v0.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/ReactiveX/RxJava/wiki/What's-different-in-2.0 | ti/d.java |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html? | vd/k.java |
| https://openmobile.qq.com/oauth2.0/m\_authorize? | vd/e.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? | xd/a.java |
| https://graph.qq.com/ | ba/k.java |
| https://api.weixin.qq.com/ | ba/k.java |
| https://api-push.meizu.com/garcia/api/client/log/upload | rb/b.java |
| https://api-push.meizu.com/garcia/api/client/message/registerPush | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/unRegisterPush | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/getRegisterSwitch | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/changeRegisterSwitch | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/changeAllSwitch | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/subscribeTags | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/unSubscribeTags | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/unSubAllTags | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/getSubTags | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/subscribeAlias | vc/a.java |
| https://api-push.meizu.com/garcia/api/client/message/unSubscribeAlias | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/registerPush | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/unRegisterPush | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/getRegisterSwitch | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/changeRegisterSwitch | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/changeAllSwitch | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/subscribeTags | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/unSubscribeTags | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/unSubAllTags | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/getSubTags | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/subscribeAlias | vc/a.java |
| https://api-push.in.meizu.com/garcia/api/client/message/unSubscribeAlias | vc/a.java |

### **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**

**无法读取代码签名证书.**

## **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 |
| --- | --- | --- | --- |
|  | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**