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

**易大大（ null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 | 易大大 |
| 版本 | null |
| 包名 | sykbui.jljfdukb.jqgbv |
| 域名线索 | 70条 |
| URL线索 | 75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 | 1\_base.apk |
| 文件大小 | 106.71MB |
| MD5值 | bbefa09f5338f6b759cf1815de813b2c |
| SHA1值 | c0a22922dc296a41be3fc81faa4621467e727bcd |
| SHA256值 | aec14b8aceb3dd2dbbc7a04f5b293eb2901d7e2f4bf1781d16940fefe4eec097 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 易大大 |
| 包名 | sykbui.jljfdukb.jqgbv |
| 主活动Activity | im.rightkinghts.ui.LaunchActivity |
| 安卓版本名称 | null |
| 安卓版本 |  |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| vop.baidu.com | IP: 111.206.209.68 所属国家: China 地区: Beijing 城市: Beijing  |
| 106.13.253.35 | IP: 106.13.253.35 所属国家: China 地区: Beijing 城市: Beijing  |
| impyq.gz.bcebos.com | IP: 153.3.238.105 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  |
| game.bjz.com | 没有服务器地理信息.  |
| ip-api.com | IP: 208.95.112.1 所属国家: United States of America 地区: North Carolina 城市: Skyland  |
| wup.imtt.qq.com | IP: 125.39.196.183 所属国家: China 地区: Tianjin 城市: Tianjin  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 192.168.31.38 | IP: 192.168.31.38 所属国家: - 地区: - 城市: -  |
| openapi.baidu.com | IP: 110.242.69.36 所属国家: China 地区: Hebei 城市: Baoding  |
| game.imchat.im | 没有服务器地理信息.  |
| d.alipay.com | IP: 183.204.244.199 所属国家: China 地区: Henan 城市: Nanyang  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| 106.13.253.90 | IP: 106.13.253.90 所属国家: China 地区: Beijing 城市: Beijing  |
| static-maps.yandex.ru | IP: 213.180.204.41 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| www.ntsc.ac.cn | IP: 159.226.242.43 所属国家: China 地区: Beijing 城市: Beijing  |
| api.stripe.com | IP: 13.112.224.240 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| youtube.com | IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| usher.ttvnw.net | IP: 3.165.82.67 所属国家: United States of America 地区: Washington 城市: Seattle  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| app.navi.baidu.com | IP: 111.206.209.213 所属国家: China 地区: Beijing 城市: Beijing  |
| stripe.com | IP: 198.137.150.141 所属国家: United States of America 地区: New York 城市: New York City  |
| www.google.com | IP: 31.13.94.10 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| j.map.baidu.com | IP: 111.206.209.187 所属国家: China 地区: Beijing 城市: Beijing  |
| chatlink.mstatik.com | IP: 116.179.52.11 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| client.map.baidu.com | IP: 111.206.209.119 所属国家: China 地区: Beijing 城市: Beijing  |
| map.baidu.com | IP: 111.206.208.32 所属国家: China 地区: Beijing 城市: Beijing  |
| coub.com | IP: 95.213.253.85 所属国家: Russian Federation 地区: Sankt-Peterburg 城市: Saint Petersburg  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.youtube.com | IP: 31.13.88.169 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| www.smpte-ra.org | IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| m12345.cc | IP: 103.224.212.212 所属国家: Australia 地区: Victoria 城市: Beaumaris  |
| schemas.android.com | 没有服务器地理信息.  |
| m.bjz.com | 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  |
| ss3.4sqi.net | IP: 146.75.114.132 所属国家: Sweden 地区: Vastra Gotalands lan 城市: Goeteborg  |
| 192.200.1.242 | IP: 192.200.1.242 所属国家: United States of America 地区: New Jersey 城市: Jersey City  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| daohang.map.baidu.com | IP: 111.206.209.190 所属国家: China 地区: Beijing 城市: Beijing  |
| www.aparat.com | IP: 185.147.178.12 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran  |
| loc.map.baidu.com | IP: 111.206.209.175 所属国家: China 地区: Beijing 城市: Beijing  |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| youtube.googleapis.com | IP: 172.217.163.42 所属国家: United States of America 地区: California 城市: Mountain View  |
| maps.googleapis | 没有服务器地理信息.  |
| bbs.lbsyun.baidu.com | 没有服务器地理信息.  |
| 192.168.1.4 | IP: 192.168.1.4 所属国家: - 地区: - 城市: -  |
| instagram.com | IP: 192.133.77.191 所属国家: United States of America 地区: California 城市: San Francisco  |
| android.bugly.qq.com | IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang  |
| twitter.com | IP: 104.244.42.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.instagram.com | IP: 104.244.46.9 所属国家: United States of America 地区: California 城市: San Francisco  |
| daup.map.baidu.com | IP: 110.242.69.98 所属国家: China 地区: Hebei 城市: Baoding  |
| itsdata.map.baidu.com | IP: 111.206.209.180 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  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| mdc.html5.qq.com | IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing  |
| api.twitch.tv | IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| live.imchat.im | 没有服务器地理信息.  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| shibatch.sourceforge.net | IP: 104.18.13.149 所属国家: United States of America 地区: California 城市: San Francisco  |
| maps.google.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| wealthextend.huanhuit.com | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| wapmap.baidu.com | IP: 111.206.209.212 所属国家: China 地区: Beijing 城市: Beijing  |
| attheme.org | IP: 185.107.56.209 所属国家: Netherlands 地区: Noord-Brabant 城市: Roosendaal  |
| player.vimeo.com | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| www.shareinstall.com.cn | IP: 122.195.144.85 所属国家: China 地区: Jiangsu 城市: Suqian  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://map.baidu.com/zt/client/index/?fr=sdk\_[  | com/baidu/mapapi/utils/OpenClientUtil.java  |
| http://api.map.baidu.com/place/detail?uid=  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| http://api.map.baidu.com/place/search?  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| http://api.map.baidu.com/direction?  | com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java  |
| http://app.navi.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| http://daohang.map.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/custom/v2/getjsonstyle  | com/baidu/mapsdkplatform/comapi/map/h.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/custom/v2/getjsonstyle  | com/baidu/mapsdkplatform/comapi/map/h.java  |
| http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n=============================================\n  | com/baidu/mapsdkplatform/comapi/util/PermissionCheck.java  |
| https://api.map.baidu.com/lbs\_sdkcc/report  | com/baidu/mapsdkplatform/comapi/b/a/c.java  |
| http://loc.map.baidu.com/cc.php  | com/baidu/location/b/d.java  |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/b/f.java  |
| http://loc.map.baidu.com/sdk.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/user\_err.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/oqur.php  | com/baidu/location/g/k.java  |
| https://loc.map.baidu.com/tcu.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/rtbu.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/iofd.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/wloc  | com/baidu/location/g/k.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/g/k.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/indoorlocbuildinginfo.php  | com/baidu/location/indoor/a.java  |
| http://loc.map.baidu.com/check\_indoor\_data\_update  | com/baidu/location/indoor/mapversion/a/e.java  |
| https://loc.map.baidu.com/ios\_indoorloc  | com/baidu/location/indoor/mapversion/a/a.java  |
| http://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet  | com/baidu/location/indoor/mapversion/c/a.java  |
| https://loc.map.baidu.com/cfgs/loc/commcfgs  | com/baidu/location/c/e.java  |
| http://loc.map.baidu.com/gpsz  | com/baidu/location/c/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/a.java  |
| http://j.map.baidu.com/  | com/baidu/platform/domain/a.java  |
| http://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/a.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/b.java  |
| https://j.map.baidu.com/  | com/baidu/platform/domain/b.java  |
| https://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/b.java  |
| http://wapmap.baidu.com/s?tn=Detail&pid=  | com/baidu/platform/core/e/c.java  |
| http://map.baidu.com/?newmap=1&s=  | com/baidu/platform/core/e/e.java  |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| http://192.200.1.242:1999/  | com/bjz/comm/net/UrlConstant.java  |
| http://m.bjz.com/  | com/bjz/comm/net/UrlConstant.java  |
| https://106.13.253.35/  | com/bjz/comm/net/UrlConstant.java  |
| https://live.imchat.im/  | com/bjz/comm/net/UrlConstant.java  |
| http://game.bjz.com/  | com/bjz/comm/net/UrlConstant.java  |
| https://game.imchat.im  | com/bjz/comm/net/UrlConstant.java  |
| http://192.168.1.4:20000/  | com/bjz/comm/net/UrlConstant.java  |
| https://106.13.253.90/  | com/bjz/comm/net/UrlConstant.java  |
| https://impyq.gz.bcebos.com/  | com/bjz/comm/net/UrlConstant.java  |
| http://ip-api.com/json/  | com/bjz/comm/net/UrlConstant.java  |
| https://wealthextend.huanhuit.com/  | com/bjz/comm/net/UrlConstant.java  |
| https://impyq.gz.bcebos.com/  | com/bjz/comm/net/utils/HttpUtils.java  |
| https://vop.baidu.com/  | com/bjz/comm/net/factory/ApiTranslateAudioFactory.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/HttpUrlSource.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/134.  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.java  |
| http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt  | com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java  |
| http://schemas.android.com/apk/res/android  | com/tablayout/SlidingScaleTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/tablayout/SlidingTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/tablayout/SegmentTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/tablayout/CommonTabLayout.java  |
| http://xml.apache.org/xslt  | com/socks/library/klog/XmlLog.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/ad.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| http://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/ak.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/d.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/b/a/d.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/b/a/d.java  |
| http://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/v.java  |
| http://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/v.java  |
| http://wup.imtt.qq.com:8080  | com/tencent/smtt/utils/v.java  |
| http://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/v.java  |
| http://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/v.java  |
| http://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/v.java  |
| http://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/v.java  |
| http://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/v.java  |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/i.java  |
| https://stripe.com/docs/stripe.js.  | com/stripe/android/Stripe.java  |
| https://stripe.com/docs/stripe.js  | com/stripe/android/Stripe.java  |
| https://api.stripe.com  | com/stripe/android/net/StripeApiHandler.java  |
| https://stripe.com/api  | com/stripe/android/net/StripeApiHandler.java  |
| https://twitter.com/stripestatus,  | com/stripe/android/net/StripeApiHandler.java  |
| https://chatlink.mstatik.com/widget/standalone.html?eid=c4e431e16e2d152d1c9d7141c7cdf3de  | im/rightkinghts/messenger/BuildVars.java  |
| https://static-maps.yandex.ru/1.x/?ll=%.6f,%.6f&z=%d&size=%d,%d&l=map&scale=%d&pt=%.6f,%.6f,vkbkm&lang=%s  | im/rightkinghts/messenger/AndroidUtilities.java  |
| https://static-maps.yandex.ru/1.x/?ll=%.6f,%.6f&z=%d&size=%d,%d&l=map&scale=%d&lang=%s  | im/rightkinghts/messenger/AndroidUtilities.java  |
| http://api.map.baidu.com/staticimage/v2?ak=%s&mcode=%s&center=%.6f,%.6f&width=%d&height=%d&zoom=%d&scale=%d&coordtype=gcj02ll&copyright=1&dpiType=ph&markers=%.6f,%.6f&markerStyles=l,,red  | im/rightkinghts/messenger/AndroidUtilities.java  |
| http://api.map.baidu.com/staticimage/v2?ak=%s&mcode=%s&center=%.6f,%.6f&width=%d&height=%d&zoom=%d&scale=%d&coordtype=gcj02ll&copyright=1&dpiType=ph  | im/rightkinghts/messenger/AndroidUtilities.java  |
| https://instagram.com/  | im/rightkinghts/messenger/MessageObject.java  |
| https://www.instagram.com/explore/tags/  | im/rightkinghts/messenger/MessageObject.java  |
| https://twitter.com/  | im/rightkinghts/messenger/MessageObject.java  |
| https://twitter.com/hashtag/  | im/rightkinghts/messenger/MessageObject.java  |
| https://m12345.cc/dl  | im/rightkinghts/messenger/ContactsController.java  |
| https://static-maps  | im/rightkinghts/messenger/ImageLoader.java  |
| https://maps.googleapis  | im/rightkinghts/messenger/ImageLoader.java  |
| https://m12345.cc/install.html?appkey=7HDA8K35WHGPO4  | im/rightkinghts/messenger/MessagesController.java  |
| http://www.shareinstall.com.cn/js-test.html?appkey=7HDA8K35WHGPO4  | im/rightkinghts/messenger/MessagesController.java  |
| http://www.example.com  | im/rightkinghts/messenger/support/customtabsclient/shared/CustomTabsHelper.java  |
| https://www.youtube.com/embed/  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| https://youtube.googleapis.com/v/  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| https://www.youtube.com/get\_video\_info?  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| https://www.youtube.com  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| https://player.vimeo.com/video/%s/config  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| https://api.twitch.tv/kraken/streams/%s?stream\_type=all  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| https://api.twitch.tv/api/channels/%s/access\_token  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| https://coub.com/api/v2/coubs/%s.json  | im/rightkinghts/messenger/utils/PlayerUtils.java  |
| http://www.google.com  | im/rightkinghts/messenger/browser/Browser.java  |
| https://m12345.cc/deactivate?phone=  | im/rightkinghts/ui/TwoStepVerificationActivity.java  |
| http://maps.google.com/maps?saddr=%f,%f&daddr=%f,%f  | im/rightkinghts/ui/LocationActivity.java  |
| http://youtube.com  | im/rightkinghts/ui/ArticleViewer.java  |
| https://m12345.cc/embed  | im/rightkinghts/ui/ArticleViewer.java  |
| https://m12345.cc/deactivate?phone=  | im/rightkinghts/ui/PassportActivity.java  |
| https://m12345.cc/proxy?  | im/rightkinghts/ui/ProxySettingsActivity.java  |
| https://m12345.cc/socks?  | im/rightkinghts/ui/ProxySettingsActivity.java  |
| https://m12345.cc  | im/rightkinghts/ui/ChatActivity.java  |
| http://m12345.cc  | im/rightkinghts/ui/ChatActivity.java  |
| https://m12345.cc/authtoken/  | im/rightkinghts/ui/ChatActivity.java  |
| https://openapi.baidu.com/oauth/2.0/token  | im/rightkinghts/ui/ChatActivity.java  |
| https://vop.baidu.com/pro\_api  | im/rightkinghts/ui/ChatActivity.java  |
| https://www.youtube.com/iframe\_api\  | im/rightkinghts/ui/components/EmbedBottomSheet.java  |
| http://youtube.com  | im/rightkinghts/ui/components/EmbedBottomSheet.java  |
| https://www.youtube.com  | im/rightkinghts/ui/components/EmbedBottomSheet.java  |
| https://m12345.cc/  | im/rightkinghts/ui/components/URLSpanNoUnderline.java  |
| https://www.youtube.com/embed/  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://youtube.googleapis.com/v/  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://www.youtube.com/get\_video\_info?  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://www.youtube.com  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://player.vimeo.com/video/%s/config  | im/rightkinghts/ui/components/WebPlayerView.java  |
| http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://api.twitch.tv/kraken/streams/%s?stream\_type=all  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://api.twitch.tv/api/channels/%s/access\_token  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://coub.com/api/v2/coubs/%s.json  | im/rightkinghts/ui/components/WebPlayerView.java  |
| https://192.168.31.38:8080/v1/token  | im/rightkinghts/ui/hui/visualcall/AliRtcConstants.java  |
| https://m12345.cc  | im/rightkinghts/ui/hui/discovery/QrScanActivity.java  |
| http://m12345.cc  | im/rightkinghts/ui/hui/discovery/QrScanActivity.java  |
| https://m12345.cc/authtoken/  | im/rightkinghts/ui/hui/discovery/QrScanActivity.java  |
| http://shibatch.sourceforge.net/\n\n  | im/rightkinghts/ui/utils/translate/ssrc/SSRC.java  |
| http://www.ntsc.ac.cn  | im/rightkinghts/ui/utils/timer/OrderCountDownHelper.java  |
| https://d.alipay.com  | im/rightkinghts/ui/wallet/WalletRechargeH5Activity.java  |
| https://attheme.org?slug=  | im/rightkinghts/ui/actionbar/Theme.java  |
| https://ss3.4sqi.net/img/categories\_v2/  | im/rightkinghts/ui/adapters/BaseLocationAdapter.java  |
| https://www.google.com/resolve?name=  | im/rightkinghts/tgnet/ConnectionsManager.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/videocache/HttpUrlSource.java  |
| support@stripe.com  | com/stripe/android/net/StripeApiHandler.java  |
| sms@stel.com  | im/rightkinghts/ui/ChangePhoneActivity.java  |
| login@stel.com sms@stel.com  | im/rightkinghts/ui/LoginActivity.java  |
| sms@stel.com  | im/rightkinghts/ui/PassportActivity.java  |
| sms@stel.com  | im/rightkinghts/ui/CancelAccountDeletionActivity.java  |
| login@stel.com sms@stel.com  | im/rightkinghts/ui/hui/login/HloginActivity.java  |
| login@stel.com  | im/rightkinghts/ui/hui/login/LoginVerifyActivity.java  |
| login@stel.com  | im/rightkinghts/ui/hui/login/LoginContronllerBaseActivity.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18345352118  | com/baidu/mapsdkplatform/comapi/util/b.java  |
| 14058229493  | im/rightkinghts/messenger/Utilities.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=TG@apksigner, ST=TG@apksigner, L=TG@apksigner, O=as1721981005610, OU=sg1721981005610, CN=cwlt 签名算法: rsassa\_pkcs1v15 有效期自: 2024-07-26 08:03:25+00:00 有效期至: 2074-07-14 08:03:25+00:00 发行人: C=TG@apksigner, ST=TG@apksigner, L=TG@apksigner, O=as1721981005610, OU=sg1721981005610, CN=cwlt 序列号: 0x4d1ca17 哈希算法: sha1 md5值: da0a91ab32270ff1481ffe3f3c4d4f9a sha1值: b2a0c50bc352cdbd2f026cfa66e4136f14e5e19a sha256值: dc031554bc01b54140f8bdabfedf4bf5e12604049d8a8b6df8d98ba38b92b90c sha512值: 333ce32f87f3969aa3ba2e789905f14e2cf5a6488f77ea42c9a20fdbb36edcd88bf402d02a98d1619926480b913964419fa2d61e698b8dbfced24bf2c39a4786 公钥算法: rsa 密钥长度: 1024 指纹: 8f030008a8bd1fd4e41343579b63a6b6454808d8e198dcb5a5aa26f8d35eb132**

## **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**

## **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。**