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

**嘿嘿连载（ 3.1.5.2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 | 嘿嘿连载 |
| 版本 | 3.1.5.2 |
| 包名 | com.hhhhlianzai.app |
| 域名线索 | 82条 |
| URL线索 | 74条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | 嘿嘿连载\_3.1.5.2.apk |
| 文件大小 | 48.5MB |
| MD5值 | a56906f92162863a966847904cb98c8b |
| SHA1值 | dce476d46a692a13888505700b35605f743ff3c0 |
| SHA256值 | 84bad89dea4a5d9a137908e0c1bb094a1339ad8c60c5710f3db8ebe9e8ce6922 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 嘿嘿连载 |
| 包名 | com.hhhhlianzai.app |
| 主活动Activity | com.heiheilianzai.app.ui.activity.SplashActivity |
| 安卓版本名称 | 3.1.5.2 |
| 安卓版本 | 20220802 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5  所属国家: Singapore  地区: Singapore  城市: Singapore |
| api-push.meizu.com | IP: 125.94.213.129  所属国家: China  地区: Guangdong  城市: Guangzhou |
| mclient.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| api.orbopv.com | IP: 23.59.252.195  所属国家: United States of America  地区: California  城市: Los Angeles |
| uatapi3.08bea5.com | IP: 54.177.221.121  所属国家: United States of America  地区: California  城市: San Francisco |
| en.wikipedia.org | IP: 173.244.209.150  所属国家: United States of America  地区: Utah  城市: Providence |
| ulogs.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Beijing  城市: Beijing |
| playready.directtaps.net | IP: 40.70.71.156  所属国家: United States of America  地区: Virginia  城市: Boydton |
| raw.githubusercontent.com | IP: 185.199.109.133  所属国家: United States of America  地区: Pennsylvania  城市: California |
| log.umsns.com | IP: 59.82.60.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mobile.umeng.com | IP: 59.82.31.160  所属国家: China  地区: Beijing  城市: Beijing |
| bjuser.jpush.cn | IP: 122.9.15.248  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| long.open.weixin.qq.com | IP: 109.244.216.15  所属国家: China  地区: Beijing  城市: Beijing |
| api.he0jys.com | IP: 23.59.252.200  所属国家: United States of America  地区: California  城市: Los Angeles |
| paygate-yf.meituan.com | IP: 101.236.9.32  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.alipay.com | IP: 203.209.247.65  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| rqd.uu.qq.com | IP: 109.244.173.225  所属国家: China  地区: Beijing  城市: Beijing |
| api.weixin.qq.com | IP: 109.244.145.152  所属国家: China  地区: Beijing  城市: Beijing |
| m.alipay.com | IP: 203.209.245.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| schemas.microsoft.com | IP: 13.107.238.49  所属国家: United States of America  地区: Washington  城市: Redmond |
| idmb.register.xmpush.global.xiaomi.com | IP: 43.204.76.177  所属国家: Australia  地区: Queensland  城市: Brisbane |
| alogus.umeng.com | IP: 223.109.148.178  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 |
| api.scyfnq.com | IP: 52.52.130.136  所属国家: United States of America  地区: California  城市: San Francisco |
| uatapi4.08bea5.com | IP: 54.177.221.121  所属国家: United States of America  地区: California  城市: San Francisco |
| api-push.in.meizu.com | IP: 206.161.233.191  所属国家: United States of America  地区: Virginia  城市: Herndon |
| www.tcsygnlw.com | IP: 154.86.178.125  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.jivesoftware.com | IP: 141.193.213.10  所属国家: United States of America  地区: Texas  城市: Austin |
| alogsus.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| openmobile.qq.com | IP: 175.27.9.14  所属国家: China  地区: Beijing  城市: Beijing |
| www.slf4j.org | IP: 159.100.250.151  所属国家: Switzerland  地区: Vaud  城市: Lausanne |
| metok.sys.miui.com | IP: 124.251.100.14  所属国家: China  地区: Beijing  城市: Beijing |
| norma-external-collect.meizu.com | IP: 113.106.27.98  所属国家: China  地区: Guangdong  城市: Zhongshan |
| uatapi.08bea5.com | IP: 172.67.218.96  所属国家: United States of America  地区: California  城市: San Francisco |
| fr.register.xmpush.global.xiaomi.com | IP: 18.193.154.21  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| resolver.msg.xiaomi.net | IP: 183.84.5.221  所属国家: China  地区: Beijing  城市: Beijing |
| schemas.xmlsoap.org | IP: 13.107.237.49  所属国家: United States of America  地区: Washington  城市: Redmond |
| api.08bea5.com | IP: 54.177.221.121  所属国家: United States of America  地区: California  城市: San Francisco |
| cmnsguider.yunos.com | IP: 203.119.175.203  所属国家: China  地区: Beijing  城市: Beijing |
| 182.92.20.189 | IP: 182.92.20.189  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| applog.uc.cn | IP: 123.182.50.230  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| android.bugly.qq.com | IP: 109.244.244.137  所属国家: China  地区: Beijing  城市: Beijing |
| api.xmpush.xiaomi.com | IP: 183.84.7.230  所属国家: China  地区: Beijing  城市: Beijing |
| d.iqt.ai | IP: 104.21.6.202  所属国家: United States of America  地区: California  城市: San Francisco |
| www.qq.com | IP: 175.27.8.138  所属国家: China  地区: Beijing  城市: Beijing |
| mcgw.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| cn.register.xmpush.xiaomi.com | IP: 220.181.106.176  所属国家: China  地区: Beijing  城市: Beijing |
| h5.m.taobao.com | IP: 111.225.210.165  所属国家: China  地区: Hebei  城市: Langfang |
| gjapplog.ucweb.com | IP: 168.235.204.12  所属国家: United States of America  地区: California  城市: Monrovia |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| uatapi5.08bea5.com | IP: 54.177.221.121  所属国家: United States of America  地区: California  城市: San Francisco |
| tsis.jpush.cn | IP: 183.232.58.227  所属国家: China  地区: Guangdong  城市: Guangzhou |
| api.askoc8.com | IP: 156.251.141.52  所属国家: United States of America  地区: California  城市: Los Angeles |
| scapi.tdqtnuvpci.com | IP: 23.59.252.195  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.baidu.com | IP: 110.242.68.3  所属国家: China  地区: Hebei  城市: Baoding |
| rjk.qq-5.com | IP: 124.222.191.192  所属国家: China  地区: Beijing  城市: Beijing |
| ulogs.umengcloud.com | IP: 223.109.148.179  所属国家: China  地区: Beijing  城市: Beijing |
| pv.sohu.com | IP: 42.81.15.45  所属国家: China  地区: Tianjin  城市: Tianjin |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| uatapi2.08bea5.com | IP: 23.59.252.203  所属国家: United States of America  地区: California  城市: Los Angeles |
| ouplog.umeng.com | IP: 47.246.110.94  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| graph.qq.com | IP: 175.27.9.14  所属国家: China  地区: Beijing  城市: Beijing |
| plbslog.umeng.com | IP: 36.156.202.78  所属国家: China  地区: Beijing  城市: Beijing |
| developer.umeng.com | IP: 59.82.31.210  所属国家: China  地区: Beijing  城市: Beijing |
| ccc.sys.miui.com | IP: 124.251.34.42  所属国家: China  地区: Beijing  城市: Beijing |
| errlog.umeng.com | IP: 223.109.148.129  所属国家: China  地区: Beijing  城市: Beijing |
| log-report.com | IP: 172.67.199.50  所属国家: United States of America  地区: California  城市: San Francisco |
| wappaygw.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| open.weixin.qq.com | IP: 109.244.144.48  所属国家: China  地区: Beijing  城市: Beijing |
| www.umeng.com | IP: 59.82.60.44  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| verification.voiceware.co.kr | IP: 210.205.55.5  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| www.boshanguan.cn | IP: 69.165.67.174  所属国家: United States of America  地区: Wyoming  城市: Cheyenne |
| api.x51d23.com | IP: 172.247.109.203  所属国家: United States of America  地区: California  城市: Los Angeles |
| domain.260b18.com | IP: 104.21.86.15  所属国家: United States of America  地区: California  城市: San Francisco |
| api.1rephm.com | IP: 23.59.252.203  所属国家: United States of America  地区: California  城市: Los Angeles |
| manual.sensorsdata.cn | IP: 221.204.166.202  所属国家: China  地区: Shanxi  城市: Taiyuan |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.slf4j.org/codes.html | org/slf4j/LoggerFactory.java |
| http://www.slf4j.org/codes.html | org/slf4j/MDC.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | a/a/a/h/i.java |
| https://github.com/danikula/AndroidVideoCache/issues. | a/a/a/h/i.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | a/a/a/h/i.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | a/a/a/h/g.java |
| http://%s:%d/%s | a/a/a/h/l.java |
| https://tsis.jpush.cn | cn/jiguang/ad/i.java |
| https://bjuser.jpush.cn/v1/appawake/status | cn/jiguang/aa/b.java |
| http://182.92.20.189:9099/ | cn/jiguang/o/c.java |
| http://rjk.qq-5.com/tc.php | com/hanbing/wltc/han.java |
| https://log-report.com/report | com/cloudinject/feature/̗̖/C0244.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 |
| http://%s:%d/%s | com/danikula/videocache/Pinger.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/Pinger.java |
| http://%s:%d/%s | com/danikula/videocache/HttpProxyCacheServer.java |
| https://api.scyfnq.com/index.php | com/tinstall/tinstall/TInstall.java |
| http://www.baidu.com/ | com/tinstall/tinstall/TInstall.java |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | com/liulishuo/filedownloader/services/BaseFileServiceUIGuard.java |
| https://api.xmpush.xiaomi.com/upload/xmsf\_log?file= | com/xiaomi/mipush/sdk/w.java |
| https://api.xmpush.xiaomi.com/upload/app\_log?file= | com/xiaomi/mipush/sdk/w.java |
| https://api.xmpush.xiaomi.com/upload/crash\_log?file= | com/xiaomi/mipush/sdk/y.java |
| https://metok.sys.miui.com | com/xiaomi/push/bl.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/gu.java |
| http://ccc.sys.miui.com | com/xiaomi/push/br.java |
| http://www.jivesoftware.com/xmlns/xmpp/properties\ | com/xiaomi/push/hf.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/hn.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/hm.java |
| http://%1$s/gslb/?ver=4.0 | com/xiaomi/push/ds.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/gk.java |
| http://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/bb.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/l.java |
| https://register.xmpush.global.xiaomi.com | com/xiaomi/push/service/l.java |
| https://fr.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/l.java |
| https://ru.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/l.java |
| https://idmb.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/l.java |
| https://errlog.umeng.com/upload | com/uc/crashsdk/e.java |
| https://applog.uc.cn/collect | com/uc/crashsdk/a/h.java |
| https://gjapplog.ucweb.com/collect | com/uc/crashsdk/a/h.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| http://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/cons/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/cons/a.java |
| http://m.alipay.com/?action=h5quit | com/alipay/sdk/cons/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$& | com/alipay/sdk/data/a.java |
| http://mcgw.alipay.com/sdklog.do | com/alipay/sdk/packet/impl/c.java |
| https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple\ | com/alipay/test/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.aaa.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.stable.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://xml.apache.org/xslt | com/elvishew/xlog/formatter/message/xml/DefaultXmlFormatter.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/live/eggplant/player/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/live/eggplant/player/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/live/eggplant/player/videocache/HttpUrlSource.java |
| http://%s:%d/%s | com/live/eggplant/player/videocache/Pinger.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/live/eggplant/player/videocache/Pinger.java |
| http://%s:%d/%s | com/live/eggplant/player/videocache/HttpProxyCacheServer.java |
| https://en.wikipedia.org/wiki/Hostname | com/sensorsdata/analytics/android/sdk/SensorsDataAPI.java |
| https://manual.sensorsdata.cn/sa/latest/tech\_sdk\_client\_web\_access-7545017.html\ | com/sensorsdata/analytics/android/sdk/visual/ViewSnapshot.java |
| https://api.x51d23.com | com/heiheilianzai/app/BuildConfig.java |
| https://api.orbopv.com | com/heiheilianzai/app/BuildConfig.java |
| https://api.he0jys.com | com/heiheilianzai/app/BuildConfig.java |
| https://api.1rephm.com | com/heiheilianzai/app/BuildConfig.java |
| https://api.askoc8.com | com/heiheilianzai/app/BuildConfig.java |
| https://uatapi.08bea5.com | com/heiheilianzai/app/BuildConfig.java |
| https://uatapi2.08bea5.com | com/heiheilianzai/app/BuildConfig.java |
| https://uatapi3.08bea5.com | com/heiheilianzai/app/BuildConfig.java |
| https://uatapi4.08bea5.com | com/heiheilianzai/app/BuildConfig.java |
| https://uatapi5.08bea5.com | com/heiheilianzai/app/BuildConfig.java |
| http://api.08bea5.com | com/heiheilianzai/app/BuildConfig.java |
| https://domain.260b18.com | com/heiheilianzai/app/BuildConfig.java |
| https://scapi.tdqtnuvpci.com/sa?project=YDA44 | com/heiheilianzai/app/BuildConfig.java |
| https://scapi.tdqtnuvpci.com/sa?project=BLGtest | com/heiheilianzai/app/BuildConfig.java |
| https://d.iqt.ai/tts/Android/verification.txt | com/heiheilianzai/app/utils/manager/ReadSpeakManager.java |
| https://www.boshanguan.cn | com/heiheilianzai/app/component/http/PreparedDomain.java |
| https://www.tcsygnlw.com | com/heiheilianzai/app/component/http/PreparedDomain.java |
| https://raw.githubusercontent.com/leolee001/PPText/master/androidText.txt | com/heiheilianzai/app/constant/AppConfig.java |
| https://raw.githubusercontent.com/2116245820/hhlz-uat/main/hhlzuatapi.json | com/heiheilianzai/app/constant/RabbitConfig.java |
| https://raw.githubusercontent.com/tdopops/heiheilianzhai/main/hhlzline.json | com/heiheilianzai/app/constant/RabbitConfig.java |
| https://raw.githubusercontent.com/tdopops/heiheilianzhai/main/uat-jk.json | com/heiheilianzai/app/constant/RabbitConfig.java |
| https://raw.githubusercontent.com/tdopops/heiheilianzhai/main/live-jk.json | com/heiheilianzai/app/constant/RabbitConfig.java |
| http://pv.sohu.com/cityjson?ie=utf-8 | com/heiheilianzai/app/constant/ReaderConfig.java |
| http://api-push.meizu.com/garcia/api/server/getPublicKey | com/meizu/cloud/pushsdk/handler/a/a.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 |
| http://norma-external-collect.meizu.com/android/exchange/getpublickey.do | com/meizu/cloud/pushsdk/a/a/a.java |
| http://norma-external-collect.meizu.com/push/android/external/add.do | com/meizu/cloud/pushsdk/a/a/b.java |
| https://api-push.meizu.com | com/meizu/cloud/pushsdk/b/c/e.java |
| http://%s:%d?%s | com/mobi/xad/bean/Material.java |
| https://graph.qq.com/oauth2.0/me?access\_token= | com/umeng/qq/handler/UmengQQHandler.java |
| https://openmobile.qq.com/user/get\_simple\_userinfo?status\_os= | com/umeng/qq/handler/UmengQQHandler.java |
| http://log.umsns.com/link/qq/download/ | com/umeng/qq/handler/UmengQQHandler.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ouplog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com/unify\_logs | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com/unify\_logs | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com/unify\_logs | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com/unify\_logs | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://cmnsguider.yunos.com:443/genDeviceToken | com/umeng/commonsdk/statistics/idtracking/s.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/socialize/utils/UrlUtil.java |
| https://log.umsns.com/ | com/umeng/socialize/view/OauthDialog.java |
| https://log.umsns.com/ | com/umeng/socialize/common/SocializeConstants.java |
| https://log.umsns.com/link/qq/download/ | com/umeng/socialize/common/SocializeConstants.java |
| https://log.umsns.com/link/weixin/download/ | com/umeng/socialize/common/SocializeConstants.java |
| http://www.umeng.com/social | com/umeng/socialize/common/SocializeConstants.java |
| https://mobile.umeng.com/images/pic/home/social/img-1.png | com/umeng/socialize/net/LinkcardRequest.java |
| https://log.umsns.com/ | com/umeng/socialize/net/base/SocializeRequest.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/h.java |
| https://api.weixin.qq.com/sns/userinfo?access\_token= | com/umeng/weixin/handler/UmengWXHandler.java |
| https://api.weixin.qq.com/sns/oauth2/access\_token? | com/umeng/weixin/handler/UmengWXHandler.java |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token? | com/umeng/weixin/handler/UmengWXHandler.java |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token?appid= | com/umeng/weixin/handler/UmengWXHandler.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://www.qq.com/s? | com/tencent/mm/opensdk/openapi/WXApiImplV10.java |
| http://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/d.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/f.java |
| http://www.w3.org/2001/XMLSchema-instance\ | kr/co/voiceware/vtlicensemodule/VwCertificateBySoap.java |
| http://www.w3.org/2001/XMLSchema\ | kr/co/voiceware/vtlicensemodule/VwCertificateBySoap.java |
| http://schemas.xmlsoap.org/soap/envelope/\ | kr/co/voiceware/vtlicensemodule/VwCertificateBySoap.java |
| http://verification.voiceware.co.kr/ws\ | kr/co/voiceware/vtlicensemodule/VwCertificateBySoap.java |
| http://verification.voiceware.co.kr/ws/get\_license\ | kr/co/voiceware/vtlicensemodule/VwCertificateBySoap.java |
| https://github.com/grandcentrix/tray/wiki/Custom-Authority | net/grandcentrix/tray/provider/TrayContract.java |
| https://github.com/grandcentrix/tray/issues | net/grandcentrix/tray/provider/TrayContract.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://applog.uc.cn/collect | lib/armeabi/libcrashsdk.so |
| https://gjapplog.ucweb.com/collect | lib/armeabi/libcrashsdk.so |
| https://errlog.umeng.com | lib/armeabi/libcrashsdk.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | a/a/a/h/i.java |
| 854366888@qq.com | com/minusoneapp/PackageSignatureHooker.java |
| danikula@gmail.com | com/danikula/videocache/HttpUrlSource.java |
| danikula@gmail.com | com/live/eggplant/player/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: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2008-02-29 01:33:46+00:00 有效期至: 2035-07-17 01:33:46+00:00 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0x936eacbe07f201df 哈希算法: sha1 md5值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569 公钥算法: rsa 密钥长度: 2048 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "read\_license\_key\_null" : "read book license key is NULL" |
| "tray\_\_authority" : "com.hhhhlianzai.app.tray" |

## **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。**