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

**信仁汇通（ 1.0.9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 | 信仁汇通 |
| 版本 | 1.0.9 |
| 包名 | com.xyy.android.ltxrht |
| 域名线索 | 85条 |
| URL线索 | 106条 |
| APP图标 |  |
| 分析日期 | 2025年6月19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 | xrht.apk |
| 文件大小 | 68.2MB |
| MD5值 | f175304212138e943ecaf6d6e4e28b76 |
| SHA1值 | cb6d3017df39cbb5dda75f0f5a95af30cc2c822e |
| SHA256值 | c082d2dc6066084e38921279e858034f00915bc488f58161096902621934d6e5 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 信仁汇通 |
| 包名 | com.xyy.android.ltxrht |
| 主活动Activity | com.xyy.android.ltxrht.ui.launch.LaunchActivity |
| 安卓版本名称 | 1.0.9 |
| 安卓版本 | 9 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| i.snssdk.com | IP: 123.125.216.197  所属国家: China  地区: Beijing  城市: Beijing |
| wap.cmpassport.com | IP: 120.232.169.168  所属国家: China  地区: Guangdong  城市: Guangzhou |
| cn.register.xmpush.xiaomi.com | IP: 123.125.102.39  所属国家: China  地区: Beijing  城市: Beijing |
| msv6.wosms.cn | IP: 124.64.196.28  所属国家: China  地区: Beijing  城市: Beijing |
| render.alipay.com | IP: 27.221.79.105  所属国家: China  地区: Shandong  城市: Qingdao |
| schemas.android.com | 没有服务器地理信息. |
| opencloud.wostore.cn | IP: 116.128.209.136  所属国家: China  地区: Beijing  城市: Beijing |
| msg.cmpassport.com | IP: 112.33.111.254  所属国家: China  地区: Anhui  城市: Hefei |
| license.vod2.myqcloud.com | IP: 221.204.18.229  所属国家: China  地区: Shanxi  城市: Taiyuan |
| api-access.pangolin-sdk-toutiao.com | IP: 175.17.20.140  所属国家: China  地区: Jilin  城市: Changchun |
| mobilegwpre.alipay.com | IP: 110.75.138.35  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| apps.oceanengine.com | IP: 116.136.186.204  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| im.sdk.qcloud.com | IP: 221.204.43.70  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 |
| apmplus.volces.com | IP: 116.196.135.220  所属国家: China  地区: Zhejiang  城市: Jinhua |
| mclient.alipay.com | IP: 116.142.235.203  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 |
| 10.38.162.35 | IP: 10.38.162.35  所属国家: -  地区: -  城市: - |
| gromore.pangolin-sdk-toutiao.com | IP: 218.11.15.212  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| cloud.tencent.com | IP: 60.28.220.199  所属国家: China  地区: Tianjin  城市: Tianjin |
| applog.snssdk.com | IP: 116.196.135.221  所属国家: China  地区: Zhejiang  城市: Jinhua |
| ye.dun.163yun.com | IP: 59.111.248.82  所属国家: China  地区: Guangdong  城市: Guangzhou |
| zhiliao.qq.com | IP: 116.196.150.252  所属国家: China  地区: Zhejiang  城市: Jinhua |
| apps.bytesfield.com | IP: 106.74.132.34  所属国家: China  地区: Shandong  城市: Jinan |
| demos.trtc.tencent-cloud.com | IP: 119.188.180.230  所属国家: China  地区: Shandong  城市: Jinan |
| playable.oceanengine.com | IP: 61.182.131.176  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| crash.163.com | IP: 45.254.50.146  所属国家: China  地区: Guangdong  城市: Guangzhou |
| scc.bytedance.com | IP: 116.136.186.203  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| rtapplog.snssdk.com | IP: 123.6.21.191  所属国家: China  地区: Henan  城市: Zhengzhou |
| xmlpull.org | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| loggw-exsdk.alipay.com | IP: 110.76.6.92  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| idasc-kyc.tencentcloudapi.com | IP: 193.112.232.253  所属国家: China  地区: Beijing  城市: Beijing |
| sf3-fe-tos.pglstatp-toutiao.com | IP: 218.11.15.213  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| resolver.msg.xiaomi.net | IP: 39.102.218.17  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| rtlog.snssdk.com | IP: 116.136.186.204  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| sf6-ttcdn-tos.pstatp.com | IP: 183.255.33.74  所属国家: China  地区: Hainan  城市: Haikou |
| open.e.kuaishou.com | IP: 116.136.202.194  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| open.weixin.qq.com | IP: 140.207.176.25  所属国家: China  地区: Shanghai  城市: Shanghai |
| work.weixin.qq.com | IP: 106.55.209.39  所属国家: China  地区: Beijing  城市: Beijing |
| kycwa.tencentcloudapi.com | IP: 42.193.129.64  所属国家: China  地区: Beijing  城市: Beijing |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| p1-lm.adkwai.com | IP: 114.66.246.207  所属国家: China  地区: Beijing  城市: Beijing |
| intl.cloud.tencent.com | IP: 60.28.220.199  所属国家: China  地区: Tianjin  城市: Tianjin |
| nisportal.10010.com | IP: 124.64.196.20  所属国家: China  地区: Beijing  城市: Beijing |
| cdn-tos-cn.bytedance.net | IP: 10.8.7.221  所属国家: -  地区: -  城市: - |
| id6.me | IP: 42.123.76.150  所属国家: China  地区: Beijing  城市: Beijing |
| kyc1.qcloud.com | IP: 106.55.218.89  所属国家: China  地区: Beijing  城市: Beijing |
| mcgw.alipay.com | IP: 123.125.216.192  所属国家: China  地区: Beijing  城市: Beijing |
| buy.cloud.tencent.com | IP: 123.125.244.81  所属国家: China  地区: Beijing  城市: Beijing |
| apps.samsung.com | IP: 104.17.143.17  所属国家: United States of America  地区: California  城市: San Francisco |
| mobilegw.alipay.com | IP: 203.209.243.98  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| style-browse-openapi.test.gifshow.com | IP: 103.102.202.41  所属国家: China  地区: Beijing  城市: Beijing |
| android.bugly.qq.com | IP: 124.95.225.169  所属国家: China  地区: Liaoning  城市: Shenyang |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api-e189.21cn.com | IP: 222.93.106.185  所属国家: China  地区: Jiangsu  城市: Suzhou |
| 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 |
| da.dun.163.com | IP: 59.111.248.82  所属国家: China  地区: Guangdong  城市: Guangzhou |
| cpro.baidustatic.com | IP: 101.72.203.38  所属国家: China  地区: Hebei  城市: Langfang |
| kyc1-test.qcloud.com | IP: 123.207.114.133  所属国家: China  地区: Beijing  城市: Beijing |
| tobapplog.ctobsnssdk.com | IP: 116.196.135.221  所属国家: China  地区: Zhejiang  城市: Jinhua |
| sf1-amtos-cdn.bytesmanager.com | IP: 123.125.46.42  所属国家: China  地区: Beijing  城市: Beijing |
| static.yximgs.com | IP: 61.182.131.226  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| union.baidu.com | IP: 111.206.208.169  所属国家: China  地区: Beijing  城市: Beijing |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| www.samsungapps.com | IP: 52.18.136.34  所属国家: Ireland  地区: Dublin  城市: Dublin |
| kyccdn.tencentcloudapi.com | IP: 116.196.150.252  所属国家: China  地区: Zhejiang  城市: Jinhua |
| toblog.ctobsnssdk.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| idasc-kyc-test.tencentcloudapi.com | IP: 123.207.114.133  所属国家: China  地区: Beijing  城市: Beijing |
| api.xinrenhuitong.com | IP: 82.157.135.168  所属国家: China  地区: Beijing  城市: Beijing |
| www.tencentcloud.com | IP: 43.175.93.11  所属国家: Singapore  地区: Singapore  城市: Singapore |
| tdid.m.qq.com | IP: 60.29.240.40  所属国家: China  地区: Tianjin  城市: Tianjin |
| open.e.189.cn | IP: 42.123.76.75  所属国家: China  地区: Beijing  城市: Beijing |
| log.snssdk.com | IP: 123.125.216.193  所属国家: China  地区: Beijing  城市: Beijing |
| wappaygw.alipay.com | IP: 123.125.216.192  所属国家: China  地区: Beijing  城市: Beijing |
| h5.xinrenhuitong.com | IP: 192.144.237.129  所属国家: China  地区: Beijing  城市: Beijing |
| h5.m.taobao.com | IP: 125.38.11.130  所属国家: China  地区: Tianjin  城市: Tianjin |
| mobilegw.dl.alipaydev.com | IP: 110.75.132.25  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| success.ctobsnssdk.com | IP: 116.196.135.219  所属国家: China  地区: Zhejiang  城市: Jinhua |
| apps.bytesfield-b.com | IP: 106.74.132.37  所属国家: China  地区: Shandong  城市: Jinan |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| phoniex.toutiao.com | IP: 61.182.131.160  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| www.pangle.cn | IP: 123.125.216.196  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 |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mobilegwpre.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mobilegw.dl.alipaydev.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/m/l/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | com/alipay/sdk/m/l/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | com/alipay/sdk/m/m/a.java |
| https://render.alipay.com/p/s/i?scheme=%s | com/alipay/sdk/app/OpenAuthTask.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| http://union.baidu.com/ | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png | com/baidu/mobads/sdk/api/XAdEntryResponse.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png | com/baidu/mobads/sdk/api/XAdEntryResponse.java |
| http://union.baidu.com/ | com/baidu/mobads/sdk/api/XAdEntryResponse.java |
| http://union.baidu.com | com/baidu/mobads/sdk/internal/ao.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| http://127.0.0.1 | com/bykv/vk/component/ttvideo/DataLoaderHelper.java |
| http://127.0.0.1 | com/bykv/vk/component/ttvideo/medialoader/MediaLoaderWrapper.java |
| https://apmplus.volces.com/apm/collect/crash | com/bytedance/dq/d/s/d.java |
| https://apmplus.volces.com/monitor/collect/c/session | com/bytedance/dq/d/s/d.java |
| https://log.snssdk.com/service/2/device\_register\_only/ | com/bytedance/embedapplog/util/d.java |
| https://log.snssdk.com/service/2/app\_log/ | com/bytedance/embedapplog/util/d.java |
| https://applog.snssdk.com/service/2/app\_log/ | com/bytedance/embedapplog/util/d.java |
| https://rtlog.snssdk.com/service/2/app\_log/ | com/bytedance/embedapplog/util/d.java |
| https://rtapplog.snssdk.com/service/2/app\_log/ | com/bytedance/embedapplog/util/d.java |
| https://log.snssdk.com/service/2/log\_settings/ | com/bytedance/embedapplog/util/d.java |
| https://toblog.ctobsnssdk.com/service/2/device\_register\_only/ | com/bytedance/embedapplog/util/d.java |
| https://toblog.ctobsnssdk.com/service/2/app\_log/ | com/bytedance/embedapplog/util/d.java |
| https://tobapplog.ctobsnssdk.com/service/2/app\_log/ | com/bytedance/embedapplog/util/d.java |
| https://toblog.ctobsnssdk.com/service/2/log\_settings/ | com/bytedance/embedapplog/util/d.java |
| https://toblog.ctobsnssdk.com/service/2/abtest\_config/ | com/bytedance/embedapplog/util/d.java |
| https://success.ctobsnssdk.com/service/2/app\_log/ | com/bytedance/embedapplog/util/d.java |
| https://gromore.pangolin-sdk-toutiao.com | com/bytedance/msdk/core/ox.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/swiper\_up\_star.json | com/bytedance/sdk/component/adexpress/dynamic/interact/o.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/brush\_mask.json | com/bytedance/sdk/component/adexpress/dynamic/interact/o.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/static/images/ | com/bytedance/sdk/component/adexpress/dynamic/p/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/static/lotties/ | com/bytedance/sdk/component/adexpress/widget/DynamicLottieView.java |
| https://playable.oceanengine.com/web-api/v1/coldstart | com/bytedance/sdk/openadsdk/core/ji.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/pattern-aggregation/pattern-aggregation-eCommerce-abtest/shoppingMall-defaultPage/index.html | com/bytedance/sdk/openadsdk/core/live/EcBackUpWebView.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/ugeno-source/download\_hand\_tap.json | com/bytedance/sdk/openadsdk/core/o/ox/ox/ox.java |
| https://scc.bytedance.com/scc\_sdk/url\_scan\_v4 | com/bytedance/sdk/openadsdk/core/r/n.java |
| https://cdn-tos-cn.bytedance.net/obj/archi/ad/play-comp/playable-component-sdk/dev/index.ecommerce.html | com/bytedance/sdk/openadsdk/core/ugeno/component/interact/no.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/ugen\_icon\_close.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/d/dq.java |
| http://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_logoAd.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/d/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_logoAd.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_mpNativebanner\_close.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_play.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_close\_gray.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/csj\_clear\_close.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_splashZoomOutClose.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_voice\_silent.png' | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_voice.png' | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_voice\_silent.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_voice.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/resources/bu\_coupon\_bg.png\ | com/bytedance/sdk/openadsdk/core/ugeno/dq/dq/dq.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/ | com/bytedance/sdk/openadsdk/core/mn/ox.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/ | com/bytedance/sdk/openadsdk/core/bl/mn.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/renderer/package.json | com/bytedance/sdk/openadsdk/core/bl/mn.java |
| https://api-access.pangolin-sdk-toutiao.com/v2/inspect/aegis/client/page/ | com/bytedance/sdk/openadsdk/core/bl/mn.java |
| https://msg.cmpassport.com/h5/getMobile | com/bytedance/sdk/openadsdk/core/op/dq.java |
| https://nisportal.10010.com:9001/api?appid=1554778161154 | com/bytedance/sdk/openadsdk/core/op/dq.java |
| https://id6.me/gw/preuniq.do | com/bytedance/sdk/openadsdk/core/op/dq.java |
| https://api-access.pangolin-sdk-toutiao.com | com/bytedance/sdk/openadsdk/core/ir/u.java |
| https://apps.bytesfield.com/app\_package\_ce/appIntro | com/bytedance/sdk/openadsdk/core/widget/d.java |
| https://sf1-amtos-cdn.bytesmanager.com/obj/ad-app-package/personal-privacy-page.html | com/bytedance/sdk/openadsdk/core/widget/p.java |
| https://www.pangle.cn/privacy/partner | com/bytedance/sdk/openadsdk/core/widget/ig.java |
| https://phoniex.toutiao.com | com/bytedance/sdk/openadsdk/core/widget/o.java |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/ | com/bytedance/sdk/openadsdk/core/nativeexpress/NativeExpressView.java |
| https://i.snssdk.com/ | com/bytedance/sdk/openadsdk/downloadnew/core/AdBaseConstants.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/cmic/gen/sdk/view/GenLoginAuthActivity.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | com/cmic/gen/sdk/view/GenLoginAuthActivity.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/cmic/gen/sdk/view/GenLoginAuthActivity.java |
| http://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.java |
| http://xml.org/sax/features/namespaces | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java |
| http://xml.org/sax/features/validation | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java |
| http://xml.org/sax/features/namespaces | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/namespace-prefixes | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/validation | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/external-general-entities | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/external-parameter-entities | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/string-interning | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xmlpull.org/v1/doc/features.html | com/huawei/secure/android/common/xml/XmlNewPullParserSecurity.java |
| http://xmlpull.org/v1/doc/features.html | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.71-2c1b8e2a82-567.zip | com/kwad/components/offline/c/c.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_lite\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_lite\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/obiwan/ks\_so-obiwanNoSoRelease-3.3.56-445ef4f109-409.zip | com/kwad/components/offline/b/b.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRelease-3.3.68-9a2e5abfa5-559.zip | com/kwad/components/offline/a/b.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArm64v8aRelease-3.3.44.2-e8fbb3a5f8-666.apk | com/kwad/components/offline/a/a/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArmeabiv7aRelease-3.3.44.2-e8fbb3a5f8-666.apk | com/kwad/components/offline/a/a/a.java |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | com/kwad/framework/filedownloader/services/a.java |
| https://style-browse-openapi.test.gifshow.com//rest/e/internal/adBrowse | com/kwad/sdk/h.java |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2 | com/kwad/sdk/api/loader/v.java |
| http://%s:%d/%s | com/kwad/sdk/core/videocache/f.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/kwad/sdk/core/videocache/h.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArm64v8aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArmeabiv7aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| http://apps.samsung.com/appquery/appDetail.as?appId= | com/kwad/sdk/utils/e.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202406211433/ks\_so-exceptionArm64v8aRelease-3.3.67-e8fbb3a5f8-666.apk | com/kwad/sdk/crash/g.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202406211433/ks\_so-exceptionArmeabiv7aRelease-3.3.67-e8fbb3a5f8-666.apk | com/kwad/sdk/crash/g.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/kmac/ks\_kmac64 | com/kwad/sdk/kgeo/c.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/kmac/ks\_kmac32 | com/kwad/sdk/kgeo/c.java |
| https://crash.163.com/uploadCrashLogInfo.do | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java |
| https://crash.163.com/client/api/uploadStartUpInfo.do | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java |
| https://ye.dun.163yun.com/v1/oneclick/preCheck | com/netease/nis/quicklogin/b.java |
| https://ye.dun.163yun.com/v1/preCheck | com/netease/nis/quicklogin/b.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/netease/nis/quicklogin/utils/e.java |
| https://msv6.wosms.cn/html/oauth/protocol2.html | com/netease/nis/quicklogin/utils/e.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | com/netease/nis/quicklogin/utils/e.java |
| https://da.dun.163.com/sn.gif?d= | com/netease/nis/quicklogin/utils/g.java |
| https://i.snssdk.com/ | com/ss/android/downloadad/api/constant/AdBaseConstants.java |
| https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java |
| https://apps.oceanengine.com/customer/api/app/pkg\_info? | com/ss/android/downloadlib/addownload/compliance/d.java |
| https://apps.bytesfield.com | com/ss/android/downloadlib/addownload/compliance/iw.java |
| https://apps.bytesfield-b.com | com/ss/android/downloadlib/addownload/compliance/iw.java |
| https://www.samsungapps.com/appquery/appDetail.as?appId= | com/ss/android/downloadlib/mn/ia.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 |
| https://h.trace.qq.com/kv | com/tencent/bugly/idasc/proguard/ad.java |
| https://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/idasc/proguard/ac.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/idasc/proguard/ac.java |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/idasc/crashreport/common/strategy/StrategyBean.java |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| https://kycwa.tencentcloudapi.com/rcrm-codcs/mob-data-collect | com/tencent/cloud/huiyansdkface/a/c/f.java |
| https://idasc-kyc.tencentcloudapi.com | com/tencent/cloud/huiyansdkface/a/c/d.java |
| https://idasc-kyc-test.tencentcloudapi.com | com/tencent/cloud/huiyansdkface/a/c/d.java |
| https://kyc1.qcloud.com | com/tencent/cloud/huiyansdkface/a/c/d.java |
| https://kyc1-test.qcloud.com | com/tencent/cloud/huiyansdkface/a/c/d.java |
| https://kyccdn.tencentcloudapi.com | com/tencent/cloud/huiyansdkface/a/a/a/c.java |
| https://kycwa.tencentcloudapi.com/rcrm-codcs/mob-data-collect | com/tencent/cloud/huiyansdkface/facelight/common/KycWaSDK.java |
| https://zhiliao.qq.com/ | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://cloud.tencent.com/document/product/269/32458 | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg= | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://buy.cloud.tencent.com/avc?activeId=plugin&regionId=1 | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://cloud.tencent.com/document/product/269/11673?from=17219 | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://www.tencentcloud.com/document/product/1047/34349 | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s.png | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s\_full.png | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png | com/tencent/qcloud/tuicore/TUIConstants.java |
| https://demos.trtc.tencent-cloud.com/prod/base/v1/events/stat | com/tencent/qcloud/tuicore/TUIConfig.java |
| https://cloud.tencent.com/document/product/269/3794 | com/tencent/qcloud/tuikit/tuichat/bean/CustomHelloMessage.java |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png | com/tencent/qcloud/tuikit/tuigroup/TUIGroupConstants.java |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png | com/tencent/qcloud/tuikit/tuigroup/minimalistui/page/GroupInfoMinimalistFragment.java |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png | com/tencent/qcloud/tuikit/tuigroup/classicui/page/GroupInfoFragment.java |
| https://cloud.tencent.com/product/im | com/tencent/qcloud/tuikit/tuicontact/TUIContactConstants.java |
| https://www.tencentcloud.com/products/im?lang=en&pg= | com/tencent/qcloud/tuikit/tuicontact/TUIContactConstants.java |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/CreateGroupMinimalistActivity.java |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/CreateGroupActivity.java |
| https://tdid.m.qq.com?mc=2 | com/tencent/turingcam/KKOXW.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://api.xinrenhuitong.com | com/xyy/android/ltxrht/BuildConfig.java |
| https://h5.xinrenhuitong.com | com/xyy/android/commom/BuildConfig.java |
| https://h5.xinrenhuitong.com/pages/message/message?type=4 | com/xyy/android/common/Api.java |
| https://h5.xinrenhuitong.com/pages/message/message?type=1 | com/xyy/android/common/Api.java |
| https://h5.xinrenhuitong.com/pages/downloadPage/downloadCheck?code= | com/xyy/android/common/Api.java |
| https://h5.xinrenhuitong.com/pages/message/message?type=3 | com/xyy/android/common/Api.java |
| https://h5.xinrenhuitong.com/pages/report/reportList | com/xyy/android/common/Api.java |
| https://h5.xinrenhuitong.com/pages/message/message?type=2 | com/xyy/android/common/Api.java |
| https://license.vod2.myqcloud.com/license/v2/1329502086\_1/v\_cube.license | com/xyy/android/common/AppData.java |
| https://work.weixin.qq.com/kfid/kfc605fd730c58b1b63 | com/xyy/android/common/AppData.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fh.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fw.java |
| https://%1$s/gslb/?ver=5.0 | com/xiaomi/push/ch.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fx.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/ex.java |
| http://10.38.162.35:9085 | com/xiaomi/push/service/q.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/q.java |
| https://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/ax.java |
| https://open.e.189.cn/openapi/special/getTimeStamp.do | cn/com/chinatelecom/account/api/d/g.java |
| https://api-e189.21cn.com/gw/client/accountMsg.do | cn/com/chinatelecom/account/api/d/g.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Maybe.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Observable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Flowable.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/rxjava3/exceptions/UndeliverableException.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| .apk@classes.dex | com/kuaishou/weapon/p0/ac.java |
| danikula@gmail.com | com/kwad/sdk/core/videocache/h.java |
| xxx@email.elided | com/tencent/liteav/base/PiiElider.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 19700101000 | com/bytedance/sdk/component/kk/ox/s.java |
| 15552000000 | com/bytedance/sdk/openadsdk/core/wp/dq/dq.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: CN=XYY, OU=XYY, O=XYY, L=CC, ST=ED, C=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-12 05:11:55+00:00 有效期至: 2049-10-06 05:11:55+00:00 发行人: CN=XYY, OU=XYY, O=XYY, L=CC, ST=ED, C=CN 序列号: 0x1 哈希算法: sha256 md5值: 76e0f625f1624accba19ee06a8211f3c sha1值: 2bf18a02ebd321fe2194a64713c5835dd0e8d95f sha256值: 74d8d8261a5cfd30e7eb8666351aa67d6b22ce21d927acaa33f22bbac8cb1c61 sha512值: bd438fb303a2e1a4eec00694021f8dc7abb1990c6de48856c7cbff7f36a6d0790ffe41361ce03b4b25080e3f0dba94ebbac535f8ba61490b04f867876b3f8d3c 公钥算法: rsa 密钥长度: 2048 指纹: 1c75cc6f4b20f2b167df056f3295432f915ce2ffd4fa4c55d072dcdc012ac352**

## **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 |
| --- | --- | --- | --- |
| 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.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.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.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.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.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 |
| 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。 |
| 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.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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。 |
| android.permission.FOREGROUND\_SERVICE\_MICROPHONE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| 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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| com.xyy.android.ltxrht.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| com.xyy.android.ltxrht.openadsdk.permission.TT\_PANGOLIN | 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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.xyy.android.ltxrht.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.xyy.android.ltxrht.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PROJECTION | 未知 | Unknown permission | Unknown permission from android reference |
| com.xyy.android.ltxrht.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tencent.qcloud.tim.push.TIMPushOpenActivity | **Schemes**: pushscheme://,  **Hosts:** com.tencent.qcloud.uniapp,  **Paths:** /detail, |

**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。**