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

**森木财经（ 6.2.0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 | 森木财经 |
| 版本 | 6.2.0 |
| 包名 | skdhruhnrur.dbduierhr.idndhrht |
| 域名线索 | 94条 |
| URL线索 | 90条 |
| APP图标 |  |
| 分析日期 | 2025年7月7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 | 森木财经.apk |
| 文件大小 | 53.83MB |
| MD5值 | 3027c6992bdf0168a74e5e5863db4a00 |
| SHA1值 | 357ae5eb08231ac23e9988fe6a31555da8ac9160 |
| SHA256值 | 4031f596e5f22525f12a97e78edf75fe3cbfcab48b88a735495445fa4a85398e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 森木财经 |
| 包名 | skdhruhnrur.dbduierhr.idndhrht |
| 主活动Activity | com.tiocloud.chat.feature.splash.SplashActivity |
| 安卓版本名称 | 6.2.0 |
| 安卓版本 | 620 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| fr.register.xmpush.global.xiaomi.com | IP: 98.64.182.160 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| ai.login.umeng.com | IP: 59.82.31.160 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| open.weibo.cn | IP: 123.125.107.13 所属国家: China 地区: Beijing 城市: Beijing  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| service.weibo.com | IP: 123.125.107.13 所属国家: China 地区: Beijing 城市: Beijing  |
| 182.16.27.50 | IP: 182.16.27.50 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| ucc.umeng.com | IP: 203.119.169.43 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| wap.cmpassport.com | IP: 120.232.169.168 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| loc.map.baidu.com | IP: 111.206.209.174 所属国家: China 地区: Beijing 城市: Beijing  |
| fusion.qq.com | IP: 116.130.229.204 所属国家: China 地区: Beijing 城市: Beijing  |
| qzs.qq.com | IP: 221.204.15.88 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| graph.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.tiocloud.com | IP: 61.136.232.38 所属国家: China 地区: Hubei 城市: Shiyan  |
| store.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| open.weixin.qq.com | IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai  |
| a.app.xx.com | 没有服务器地理信息.  |
| schemas.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| register.xmpush.global.xiaomi.com | IP: 47.237.96.1 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| playready.directtaps.net | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| alogsus.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| qa-webox-api.5upay.com | 没有服务器地理信息.  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| dev-merchant.5upay.com | IP: 172.24.2.175 所属国家: - 地区: - 城市: -  |
| daup.map.baidu.com | IP: 110.242.74.236 所属国家: China 地区: Hebei 城市: Baoding  |
| ulogs.umengcloud.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| pv.sohu.com | IP: 123.125.244.28 所属国家: China 地区: Beijing 城市: Beijing  |
| opencloud.wostore.cn | IP: 210.22.123.92 所属国家: China 地区: Shanghai 城市: Shanghai  |
| px.ucweb.com | IP: 116.132.217.40 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| store3.hispace.hicloud.com | IP: 23.200.55.51 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| play.google.com | IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam  |
| developer.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.weixin.qq.com | IP: 116.128.184.169 所属国家: China 地区: Shanghai 城市: Shanghai  |
| appr.tc | 没有服务器地理信息.  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| merchant.5upay.com | IP: 39.106.92.227 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| dev-webox-api.ehking.com | 没有服务器地理信息.  |
| cgi.connect.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| new.api.ad.xiaomi.com | 没有服务器地理信息.  |
| store1.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| imtt.dd.qq.com | IP: 221.204.217.51 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| api.weibo.com | IP: 116.133.8.18 所属国家: China 地区: Beijing 城市: Beijing  |
| webox.5upay.com | IP: 47.95.113.116 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ai-login.aliplus.test | 没有服务器地理信息.  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| wallet.95516.com | IP: 116.196.139.42 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| ofloc.map.baidu.com | IP: 110.242.70.118 所属国家: China 地区: Hebei 城市: Baoding  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| uat-webox-api.5upay.com | 没有服务器地理信息.  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| plbslog.umeng.com | IP: 36.156.202.68 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| res.t-io.org | 没有服务器地理信息.  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mirror.anji-plus.com | 没有服务器地理信息.  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| store-drru.hispace.hicloud.com | IP: 159.138.201.153 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| idmb.register.xmpush.global.xiaomi.com | IP: 20.219.205.9 所属国家: India 地区: Maharashtra 城市: Pune  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| g.cn | IP: 114.250.64.34 所属国家: China 地区: Beijing 城市: Beijing  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.asia | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| deeplink.umeng.com | IP: 59.82.29.163 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| id6.me | IP: 42.123.76.150 所属国家: China 地区: Beijing 城市: Beijing  |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| openmobile.qq.com | IP: 60.28.215.27 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  |
| ulogs.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| e.189.cn | IP: 42.123.76.65 所属国家: China 地区: Beijing 城市: Beijing  |
| pre-ailogin.umeng.com | IP: 203.119.204.83 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| uat-merchant.5upay.com | IP: 172.16.10.248 所属国家: - 地区: - 城市: -  |
| store2.hispace.hicloud.com | IP: 18.155.68.98 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.xmpush.xiaomi.com | IP: 101.126.23.136 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| ug.edm.weibo.cn | IP: 116.133.8.18 所属国家: China 地区: Beijing 城市: Beijing  |
| collect.ux.21cn.com | IP: 222.93.106.185 所属国家: China 地区: Jiangsu 城市: Suzhou  |
| bbs.lbsyun.baidu.com | 没有服务器地理信息.  |
| appsupport.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| qa-merchant.5upay.com | IP: 172.24.2.179 所属国家: - 地区: - 城市: -  |
| www.baidu.com | IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding  |
| api.weibo.cn | IP: 123.125.107.16 所属国家: China 地区: Beijing 城市: Beijing  |
| www.jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach  |
| appgallery.cloud.huawei.com | IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| eco.taobao.com | IP: 59.82.122.172 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet  | com/baidu/location/indoor/mapversion/b/a.java  |
| http://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/d/h.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| http://g.cn/generate\_204  | com/ehking/sdk/wepay/utlis/CheckWifiLoginTask.java  |
| http://pv.sohu.com/cityjson?ie=utf-8  | com/ehking/sdk/wepay/utlis/NetUtils.java  |
| https://wallet.95516.com/s/wl/webV3/activity/yhtzB/insB2c/html/b2cIndex.html?institutionId=E00000295038  | com/ehking/sdk/wepay/constant/Constants.java  |
| https://webox.5upay.com/  | com/ehking/sdk/wepay/constant/Constants.java  |
| https://merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/constant/Constants.java  |
| https://merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/constant/Constants.java  |
| https://qa-webox-api.5upay.com/  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://qa-merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://qa-merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://webox.5upay.com/  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://uat-webox-api.5upay.com/  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://uat-merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://uat-merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://dev-webox-api.ehking.com/  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://dev-merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://dev-merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| http://wap.cmpassport.com/resources/html/contract.html  | com/cmic/sso/sdk/activity/LoginAuthActivity.java  |
| https://e.189.cn/sdk/agreement/detail.do  | com/cmic/sso/sdk/activity/LoginAuthActivity.java  |
| https://eco.taobao.com/router/rest  | com/mobile/auth/BuildConfig.java  |
| https://wap.cmpassport.com/resources/html/contract.html  | com/mobile/auth/gatewayauth/Constant.java  |
| https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118  | com/mobile/auth/gatewayauth/Constant.java  |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true  | com/mobile/auth/gatewayauth/Constant.java  |
| https://opencloud.wostore.cn/openapi/netauth/precheck/wp?  | com/mobile/auth/aa/b.java  |
| https://collect.ux.21cn.com/collect/custom/accountMsg  | com/mobile/auth/c/d.java  |
| https://id6.me/auth/preauth.do  | com/mobile/auth/d/a.java  |
| https://id6.me/auth/preauth.do  | com/mobile/auth/p/c.java  |
| https://px.ucweb.com/upload  | com/nirvana/tools/crash/BuildConfig.java  |
| https://api.weibo.cn/2/sdk/login  | com/sina/weibo/sdk/network/intercept/GuestParamInterception.java  |
| http://api.weibo.cn/2/sdk/login  | com/sina/weibo/sdk/network/intercept/GuestParamInterception.java  |
| https://api.weibo.cn/2/sdk/login  | com/sina/weibo/sdk/network/intercept/CommonParamInterception.java  |
| https://ug.edm.weibo.cn/api/gettoken  | com/sina/weibo/sdk/network/intercept/RequestTokenInterception.java  |
| https://ug.edm.weibo.cn/api/refreshtoken  | com/sina/weibo/sdk/network/intercept/RequestTokenInterception.java  |
| https://open.weibo.cn/oauth2/authorize?  | com/sina/weibo/sdk/auth/BaseSsoHandler.java  |
| https://api.weibo.com/oauth2/access\_token  | com/sina/weibo/sdk/auth/AccessTokenKeeper.java  |
| https://api.weibo.com/2/proxy/sdk/statistic.json  | com/sina/weibo/sdk/statistic/LogReport.java  |
| http://service.weibo.com/share/mobilesdk.php  | com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java  |
| http://service.weibo.com/share/mobilesdk\_uppic.php  | com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java  |
| https://api.weibo.com/oauth2/getaid.json  | com/sina/weibo/sdk/utils/AidTask.java  |
| http://qzs.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| http://qzs.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| http://qzs.qq.com  | com/tencent/open/SocialApiIml.java  |
| http://qzs.qq.com/open/mobile/request/sdk\_request.html?  | com/tencent/open/SocialApiIml.java  |
| https://huatuocode.huatuo.qq.com  | com/tencent/open/b/d.java  |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/f.java  |
| https://graph.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.java  |
| http://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | com/tencent/connect/common/BaseApi.java  |
| http://qzs.qq.com/open/mobile/login/qzsjump.html?  | com/tencent/connect/common/BaseApi.java  |
| http://qzs.qq.com/open/mobile/login/qzsjump.html?  | com/tencent/connect/auth/a.java  |
| https://openmobile.qq.com/v3/user/get\_info  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | com/tencent/connect/auth/AuthAgent.java  |
| http://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | com/tencent/connect/auth/AuthAgent.java  |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1  | com/tencent/connect/share/QQShare.java  |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1  | com/tencent/connect/share/QzoneShare.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.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/d.java  |
| http://182.16.27.50:6060  | com/tiocloud/chat/TioApplication.java  |
| http://182.16.27.50:6060/tioim/register?inviteUid=%s&inviteCode=%s  | com/tiocloud/chat/yanxun/share/ShareActivity.java  |
| http://182.16.27.50:6060  | com/tiocloud/chat/test/TestActivity.java  |
| https://res.t-io.org/wx/upload/video/22/9010/1119563/88097616/74541310984/33/180013/1290950731423162368.m4a  | com/tiocloud/chat/test/activity/RecordTestActivity.java  |
| https://www.tiocloud.com/2/index.html  | com/tiocloud/social/TioSocialDemoActivity.java  |
| https://www.tiocloud.com/2/imgs/header/logo.png  | com/tiocloud/social/TioSocialDemoActivity.java  |
| https://deeplink.umeng.com/deeplink/match  | com/umeng/analytics/b.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/i.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/analytics/pro/ai.java  |
| https://pslog.umeng.com/ablog  | com/umeng/analytics/pro/ai.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| http://ai-login.aliplus.test/api/umed/cache  | com/umeng/umverify/utils/g.java  |
| https://pre-ailogin.umeng.com/api/umed/cache  | com/umeng/umverify/utils/g.java  |
| https://ai.login.umeng.com/api/umed/cache  | com/umeng/umverify/utils/g.java  |
| https://ai.login.umeng.com/api/umed/mobile/log  | com/umeng/umverify/b/a.java  |
| https://merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/watayouxiang/wallet/feature/open/OpenWalletActivity.java  |
| https://merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/watayouxiang/wallet/feature/open/OpenWalletActivity.java  |
| https://api.weixin.qq.com/sns/oauth2/access\_token?appid=  | com/watayouxiang/social/WXHelper.java  |
| https://api.weixin.qq.com/sns/userinfo?access\_token=  | com/watayouxiang/social/WXHelper.java  |
| https://api.weibo.com/2/users/show.json?access\_token=  | com/watayouxiang/social/WBHelper.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fy.java  |
| http://new.api.ad.xiaomi.com/logNotificationAdActions  | com/xiaomi/push/cq.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | com/xiaomi/push/gj.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gq.java  |
| http://%1$s/gslb/?ver=4.0  | com/xiaomi/push/cz.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gr.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fo.java  |
| http://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bf.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  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | p/a/y/e/a/s/e/net/rc.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | p/a/y/e/a/s/e/net/rc.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | p/a/y/e/a/s/e/net/sc.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | p/a/y/e/a/s/e/net/sc.java  |
| http://182.16.27.50:6060  | p/a/y/e/a/s/e/net/um1.java  |
| http://182.16.27.50:7070  | p/a/y/e/a/s/e/net/um1.java  |
| http://loc.map.baidu.com/indoorlocbuildinginfo.php  | p/a/y/e/a/s/e/net/v4.java  |
| https://api.map.baidu.com/sdkcs/verify  | p/a/y/e/a/s/e/net/n1.java  |
| http://loc.map.baidu.com/sdk.php  | p/a/y/e/a/s/e/net/u4.java  |
| http://loc.map.baidu.com/sdk\_ep.php  | p/a/y/e/a/s/e/net/u4.java  |
| http://loc.map.baidu.com/tcu.php  | p/a/y/e/a/s/e/net/u4.java  |
| https://loc.map.baidu.com/sdk.php  | p/a/y/e/a/s/e/net/u4.java  |
| https://daup.map.baidu.com/cltr/rcvr  | p/a/y/e/a/s/e/net/u4.java  |
| http://loc.map.baidu.com/cc.php  | p/a/y/e/a/s/e/net/l2.java  |
| http://itsdata.map.baidu.com/long-conn-gps/sdk.php  | p/a/y/e/a/s/e/net/n2.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | p/a/y/e/a/s/e/net/zn.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | p/a/y/e/a/s/e/net/zn.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | p/a/y/e/a/s/e/net/zn.java  |
| http://%s:%d/%s  | p/a/y/e/a/s/e/net/bo.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | p/a/y/e/a/s/e/net/bo.java  |
| https://ofloc.map.baidu.com/offline\_loc  | p/a/y/e/a/s/e/net/z3.java  |
| http://%s/%s  | p/a/y/e/a/s/e/net/t3.java  |
| https://ofloc.map.baidu.com/offline\_loc  | p/a/y/e/a/s/e/net/t3.java  |
| https://api.xmpush.xiaomi.com/upload/xmsf\_log?file=  | p/a/y/e/a/s/e/net/b22.java  |
| https://api.xmpush.xiaomi.com/upload/app\_log?file=  | p/a/y/e/a/s/e/net/b22.java  |
| http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n=============================================\n  | p/a/y/e/a/s/e/net/nb.java  |
| http://loc.map.baidu.com/gpsz  | p/a/y/e/a/s/e/net/e3.java  |
| https://api.xmpush.xiaomi.com/upload/crash\_log?file=  | p/a/y/e/a/s/e/net/d22.java  |
| https://a.app.xx.com/o/simple.jsp?pkgname=com.xxx.xx  | p/a/y/e/a/s/e/net/qq1.java  |
| https://a.app.xx.com/o/simple.jsp?pkgname=com.xxx.xx  | p/a/y/e/a/s/e/net/hq1.java  |
| https://ofloc.map.baidu.com/offline\_loc  | p/a/y/e/a/s/e/net/w3.java  |
| https://imtt.dd.qq.com/16891/apk/5CACCB57E3F02E46404D27ABAA85474C.apk  | p/a/y/e/a/s/e/net/nj1.java  |
| https://a.app.xx.com/o/simple.jsp  | p/a/y/e/a/s/e/net/op1.java  |
| http://%s:%d/%s  | p/a/y/e/a/s/e/net/xn.java  |
| https://www.baidu.com  | p/a/y/e/a/s/e/net/bn0.java  |
| https://mirror.anji-plus.com/captcha-api/  | p/a/y/e/a/s/e/net/pg1.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://play.google.com/store  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com/app/  | 摸瓜V1引擎  |
| https://play.google.com/store/apps/details?id=  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com  | 摸瓜V1引擎  |
| https://appr.tc  | 摸瓜V1引擎  |
| https://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V1引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://store1.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| liwei31@staff.weibo  | com/sina/weibo/sdk/network/intercept/RequestTokenInterception.java  |
| watayouxiang@qq.com  | com/tiocloud/chat/test/activity/HttpTestActivity.java  |
| permission@gmail.com  | p/a/y/e/a/s/e/net/k32.java  |
| danikula@gmail.com  | p/a/y/e/a/s/e/net/zn.java  |
| 邮箱watayouxian@qq.com  | p/a/y/e/a/s/e/net/xa1.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13000000000  | com/ehking/sdk/wepay/constant/Constants.java  |
| 18345352118  | p/a/y/e/a/s/e/net/rb.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=oukygcltkpurjzv, ST=ruphzxqmamontkv, L=itussyikcudfouj, O=ups1751439980724, OU=pcu1751439980724, CN=Xvpc1751439980724 签名算法: rsassa\_pkcs1v15 有效期自: 2025-07-02 07:06:20+00:00 有效期至: 2075-06-20 07:06:20+00:00 发行人: C=oukygcltkpurjzv, ST=ruphzxqmamontkv, L=itussyikcudfouj, O=ups1751439980724, OU=pcu1751439980724, CN=Xvpc1751439980724 序列号: 0x75bea277 哈希算法: sha1 md5值: af7ecc252e20ed69b6a6f2f4dd7e2617 sha1值: 72f40d7e1e5867ae1a4ae02e460fe16fa67ac5ac sha256值: 4a58646a45b6dda59d83c4f41ad156ed06b59e31ff97f5c67c0da3307cbad8c1 sha512值: 7633f8086afa2e6515066efc7ad731b2f75706940ac4fe3023922bb3f4fc6a63e4be2484b8dde8c25f4404407aadc591fbbdfc1929f94a6a0ff0c8e0a59113be 公钥算法: rsa 密钥长度: 1024 指纹: bea2df46189035008b72ecef338fe2a9ecfb1073ae7e63a69646406405317c6c**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "add\_me\_friend\_need\_auth" : "加我为好友时需要验证"  |
| "double\_input\_pwd\_unsame" : "两次输入密码不一致"  |
| "easy\_password" : "密码过于简单"  |
| "fail\_pwd\_input" : "密码为6到16位数字和字母的组合"  |
| "fail\_pwd\_input\_identical" : "两次输入密码不一致"  |
| "fail\_pwd\_login\_input" : "密码格式不正确"  |
| "find\_pwd" : "找回密码"  |
| "forget\_password" : "忘记密码"  |
| "forget\_pwd" : "忘记密码"  |
| "get\_session\_fail" : "获取会话失败"  |
| "input\_password" : "No不需要翻译"  |
| "input\_six\_pwd" : "请输入至少6位新密码"  |
| "jihuo\_session\_fail" : "激活会话失败"  |
| "liangcimimabuyizhi" : "两次输入密码不一致，请重新输入!"  |
| "mail\_find\_pwd" : "邮箱号找回密码"  |
| "mark\_auth" : "提醒:后续只能绑定该持卡人的银行卡"  |
| "modify\_pwd" : "修改密码"  |
| "opening\_authroizon\_page" : "正在唤起授权页"  |
| "phone\_find\_pwd" : "手机号找回密码"  |
| "pref\_aecdump\_key" : "aecdump\_preference"  |
| "pref\_audiocodec\_key" : "audiocodec\_preference"  |
| "pref\_audiosettings\_key" : "audio\_settings\_key"  |
| "pref\_camera2\_key" : "camera2\_preference"  |
| "pref\_capturequalityslider\_key" : "capturequalityslider\_preference"  |
| "pref\_data\_id\_key" : "data\_id\_preference"  |
| "pref\_data\_protocol\_key" : "Subprotocol"  |
| "pref\_datasettings\_key" : "data\_settings\_key"  |
| "pref\_disable\_built\_in\_aec\_key" : "disable\_built\_in\_aec\_preference"  |
| "pref\_disable\_built\_in\_agc\_key" : "disable\_built\_in\_agc\_preference"  |
| "pref\_disable\_built\_in\_ns\_key" : "disable\_built\_in\_ns\_preference"  |
| "pref\_disable\_webrtc\_agc\_and\_hpf\_key" : "disable\_webrtc\_agc\_and\_hpf\_preference"  |
| "pref\_displayhud\_key" : "displayhud\_preference"  |
| "pref\_enable\_datachannel\_key" : "enable\_datachannel\_preference"  |
| "pref\_enable\_rtceventlog\_key" : "enable\_rtceventlog\_key"  |
| "pref\_enable\_save\_input\_audio\_to\_file\_key" : "enable\_key"  |
| "pref\_flexfec\_key" : "flexfec\_preference"  |
| "pref\_fps\_key" : "fps\_preference"  |
| "pref\_hwcodec\_key" : "hwcodec\_preference"  |
| "pref\_max\_retransmit\_time\_ms\_key" : "max\_retransmit\_time\_ms\_preference"  |
| "pref\_max\_retransmits\_key" : "max\_retransmits\_preference"  |
| "pref\_maxvideobitrate\_key" : "maxvideobitrate\_preference"  |
| "pref\_maxvideobitratevalue\_key" : "maxvideobitratevalue\_preference"  |
| "pref\_miscsettings\_key" : "misc\_settings\_key"  |
| "pref\_negotiated\_key" : "negotiated\_preference"  |
| "pref\_noaudioprocessing\_key" : "audioprocessing\_preference"  |
| "pref\_opensles\_key" : "opensles\_preference"  |
| "pref\_ordered\_key" : "ordered\_preference"  |
| "pref\_resolution\_key" : "resolution\_preference"  |
| "pref\_room\_key" : "room\_preference"  |
| "pref\_room\_list\_key" : "room\_list\_preference"  |
| "pref\_room\_server\_url\_key" : "room\_server\_url\_preference"  |
| "pref\_screencapture\_key" : "screencapture\_preference"  |
| "pref\_speakerphone\_key" : "speakerphone\_preference"  |
| "pref\_startaudiobitrate\_key" : "startaudiobitrate\_preference"  |
| "pref\_startaudiobitratevalue\_key" : "startaudiobitratevalue\_preference"  |
| "pref\_tracing\_key" : "tracing\_preference"  |
| "pref\_videocall\_key" : "videocall\_preference"  |
| "pref\_videocodec\_key" : "videocodec\_preference"  |
| "pref\_videosettings\_key" : "video\_settings\_key"  |
| "pwd" : "密码"  |
| "pwd\_login\_app" : "密码登录"  |
| "pwd\_null\_tip" : "密码不能为空"  |
| "pwd\_reset\_success\_relogin" : "密码修改成功，请重新登录"  |
| "pwd\_set\_success\_login" : "密码设置成功，请登录"  |
| "qingshezhizhifumima" : "请设置支付密码"  |
| "qingshuruzhifumima" : "请输入支付密码"  |
| "qingzaicishuruzhifumima" : "请再次输入支付密码"  |
| "repair\_pwd" : "修改密码"  |
| "report\_user" : "举报用户"  |
| "reset\_pwd" : "重置密码"  |
| "reset\_pwd\_success" : "修改密码成功"  |
| "retrieve\_pwd\_success" : "找回密码成功"  |
| "session\_group" : "群聊"  |
| "session\_top" : "会话置顶"  |
| "set\_login\_pwd" : "设置登录密码(至少6位)"  |
| "set\_password" : "设置密码"  |
| "set\_pwd" : "设置密码"  |
| "sure\_delete\_session" : "确定删除会话吗"  |
| "swicth\_to\_pwd" : "切换至密码登录"  |
| "tip\_alipay\_auth\_failed" : "支付宝授权失败"  |
| "unkown\_session\_type" : "未知会话类型"  |
| "use\_pwd" : "使用密码"  |
| "username" : "用户名"  |
| "xiugaimima" : "修改密码"  |
| "yuan\_pwd" : "原密码"  |
| "add\_me\_friend\_need\_auth" : "cần xác minh khi thêm tôi làm bạn"  |
| "double\_input\_pwd\_unsame" : "Mật khẩu không khớp nhau"  |
| "find\_pwd" : "tàm lại mật khẩn"  |
| "forget\_pwd" : "quên mật khẩu"  |
| "get\_session\_fail" : "không lấy được đối thoại"  |
| "input\_password" : "No不需要翻译"  |
| "input\_six\_pwd" : "Vui lòng nhập ít nhất 6 ký tự"  |
| "jihuo\_session\_fail" : "không thể kích hoạt"  |
| "liangcimimabuyizhi" : "2 lần nhập mật khẩu không giống nhau, vui lòng nhập lại!"  |
| "mail\_find\_pwd" : "mail tìm lại mật khẩu"  |
| "modify\_pwd" : "thay đổi mật khẩu"  |
| "opening\_authroizon\_page" : "Đang đi đến trang uỷ quyền"  |
| "phone\_find\_pwd" : "số điện thoại tìm lại mật khẩu"  |
| "pref\_aecdump\_key" : "aecdump\_preference"  |
| "pref\_audiocodec\_key" : "audiocodec\_preference"  |
| "pref\_audiosettings\_key" : "audio\_settings\_key"  |
| "pref\_camera2\_key" : "camera2\_preference"  |
| "pref\_capturequalityslider\_key" : "capturequalityslider\_preference"  |
| "pref\_data\_id\_key" : "data\_id\_preference"  |
| "pref\_data\_protocol\_key" : "Subprotocol"  |
| "pref\_datasettings\_key" : "data\_settings\_key"  |
| "pref\_disable\_built\_in\_aec\_key" : "disable\_built\_in\_aec\_preference"  |
| "pref\_disable\_built\_in\_agc\_key" : "disable\_built\_in\_agc\_preference"  |
| "pref\_disable\_built\_in\_ns\_key" : "disable\_built\_in\_ns\_preference"  |
| "pref\_disable\_webrtc\_agc\_and\_hpf\_key" : "disable\_webrtc\_agc\_and\_hpf\_preference"  |
| "pref\_displayhud\_key" : "displayhud\_preference"  |
| "pref\_enable\_datachannel\_key" : "enable\_datachannel\_preference"  |
| "pref\_enable\_rtceventlog\_key" : "enable\_rtceventlog\_key"  |
| "pref\_enable\_save\_input\_audio\_to\_file\_key" : "enable\_key"  |
| "pref\_flexfec\_key" : "flexfec\_preference"  |
| "pref\_fps\_key" : "fps\_preference"  |
| "pref\_hwcodec\_key" : "hwcodec\_preference"  |
| "pref\_max\_retransmit\_time\_ms\_key" : "max\_retransmit\_time\_ms\_preference"  |
| "pref\_max\_retransmits\_key" : "max\_retransmits\_preference"  |
| "pref\_maxvideobitrate\_key" : "maxvideobitrate\_preference"  |
| "pref\_maxvideobitratevalue\_key" : "maxvideobitratevalue\_preference"  |
| "pref\_miscsettings\_key" : "misc\_settings\_key"  |
| "pref\_negotiated\_key" : "negotiated\_preference"  |
| "pref\_noaudioprocessing\_key" : "audioprocessing\_preference"  |
| "pref\_opensles\_key" : "opensles\_preference"  |
| "pref\_ordered\_key" : "ordered\_preference"  |
| "pref\_resolution\_key" : "resolution\_preference"  |
| "pref\_room\_key" : "room\_preference"  |
| "pref\_room\_list\_key" : "room\_list\_preference"  |
| "pref\_room\_server\_url\_key" : "room\_server\_url\_preference"  |
| "pref\_screencapture\_key" : "screencapture\_preference"  |
| "pref\_speakerphone\_key" : "speakerphone\_preference"  |
| "pref\_startaudiobitrate\_key" : "startaudiobitrate\_preference"  |
| "pref\_startaudiobitratevalue\_key" : "startaudiobitratevalue\_preference"  |
| "pref\_tracing\_key" : "tracing\_preference"  |
| "pref\_videocall\_key" : "videocall\_preference"  |
| "pref\_videocodec\_key" : "videocodec\_preference"  |
| "pref\_videosettings\_key" : "video\_settings\_key"  |
| "pwd" : "mật khẩu"  |
| "pwd\_login\_app" : "Mật mã đăng nhập"  |
| "pwd\_null\_tip" : "mật mã không được để trống"  |
| "pwd\_reset\_success\_relogin" : "đổi mật khẩu thành công ，mời đăng nhập lại"  |
| "pwd\_set\_success\_login" : "Thiết lập mật khẩu thành công, vui lòng đăng nhập"  |
| "qingshezhizhifumima" : "vui lòng cài đặt mật khẩu thanh toán"  |
| "qingshuruzhifumima" : "Vui lòng nhập mật khẩu thanh toán"  |
| "qingzaicishuruzhifumima" : "vui lòng nhập lại mật khẩu thanh toán"  |
| "repair\_pwd" : "Đổi mật khẩu"  |
| "report\_user" : "báo cáo người dùng"  |
| "reset\_pwd" : "Đặt lại mật khẩu"  |
| "reset\_pwd\_success" : "thay đổi mật khẩu thành công"  |
| "retrieve\_pwd\_success" : "tàm lại mật khẩu thành công"  |
| "session\_group" : "nhóm chat"  |
| "session\_top" : "thiết lập đối thoại"  |
| "set\_login\_pwd" : "Thiết lập mật khẩu (ít nhất 6 ký tự)"  |
| "set\_password" : "thiết lập mật khẩu"  |
| "set\_pwd" : "thiết lập mật mã"  |
| "sure\_delete\_session" : "Bạn có chắc sẽ xoá phiên chạy"  |
| "swicth\_to\_pwd" : "Chuyển đăng nhập mật khẩu"  |
| "tip\_alipay\_auth\_failed" : "truy cập zhifubao thất bại"  |
| "unkown\_session\_type" : "loại hình không xác định"  |
| "username" : "tên người dùng"  |
| "xiugaimima" : "sauwr mật mã"  |
| "yuan\_pwd" : "mật khẩu cũ"  |

## **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.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.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.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.USE\_FULL\_SCREEN\_INTENT  | 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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.READ\_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.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.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.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 |
| skdhruhnrur.dbduierhr.idndhrht.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.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.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.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 |
| skdhruhnrur.dbduierhr.idndhrht\_com.huawei.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| skdhruhnrur.dbduierhr.idndhrht.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| skdhruhnrur.dbduierhr.idndhrht\_com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| skdhruhnrur.dbduierhr.idndhrht\_com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| skdhruhnrur.dbduierhr.idndhrht.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| skdhruhnrur.dbduierhr.idndhrht.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| skdhruhnrur.dbduierhr.idndhrht\_com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent{qq\_app\_id}://,  |

**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。**