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

**猫爪（ 2.7.1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 | 猫爪 |
| 版本 | 2.7.1 |
| 包名 | com.xiyou.miao |
| 域名线索 | 60条 |
| URL线索 | 63条 |
| APP图标 |  |
| 分析日期 | 2024年9月18日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 202309071740534ldna.apk |
| 文件大小 | 8.89MB |
| MD5值 | c4049c3beb90d11ded4a3c7be90cb48e |
| SHA1值 | b195562d48b299192d747ab9ab4906c78f0f2e00 |
| SHA256值 | 1a86aa07b217119dd5683535b76ce96922478e33278ca5504b6eefa549635729 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 猫爪 |
| 包名 | com.xiyou.miao |
| 主活动Activity | com.xiyou.miao.SplashActivity |
| 安卓版本名称 | 2.7.1 |
| 安卓版本 | 2070101 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 203.107.1.1 | IP: 203.107.1.1  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| metrics5.data.hicloud.com | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| huatuocode.huatuo.qq.com | 没有服务器地理信息. |
| aaid.umeng.com | IP: 218.91.197.68  所属国家: China  地区: Jiangsu  城市: Nantong |
| grs.dbankcloud.eu | 没有服务器地理信息. |
| cgi.connect.qq.com | IP: 175.27.9.14  所属国家: China  地区: Beijing  城市: Beijing |
| grs.dbankcloud.cn | IP: 49.4.40.185  所属国家: China  地区: Guangdong  城市: Guangzhou |
| grs.dbankcloud.asia | 没有服务器地理信息. |
| metrics2.data.hicloud.com | IP: 80.158.2.190  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| 10.38.162.35 | IP: 10.38.162.35  所属国家: -  地区: -  城市: - |
| pslog.umeng.com | IP: 59.82.31.92  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| alogus.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| cn.register.xmpush.xiaomi.com | IP: 118.26.252.220  所属国家: China  地区: Beijing  城市: Beijing |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189  所属国家: Singapore  地区: Singapore  城市: Singapore |
| ucc.umeng.com | IP: 203.119.145.45  所属国家: China  地区: Beijing  城市: Beijing |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| open.weixin.qq.com | IP: 109.244.144.48  所属国家: China  地区: Beijing  城市: Beijing |
| metrics1-drcn.dt.dbankcloud.cn | IP: 114.115.188.183  所属国家: China  地区: Beijing  城市: Beijing |
| xmlpull.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| openmobile.qq.com | IP: 175.27.9.14  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 |
| grs.platform.dbankcloud.ru | 没有服务器地理信息. |
| login.imgcache.qq.com | IP: 182.254.59.164  所属国家: China  地区: Guangdong  城市: Shenzhen |
| ulogs.umengcloud.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| cgi.qplus.com | 没有服务器地理信息. |
| android.bugly.qq.com | IP: 109.244.244.35  所属国家: China  地区: Beijing  城市: Beijing |
| image.cnamedomain.com | 没有服务器地理信息. |
| aspect-upush.umeng.com | IP: 59.82.31.92  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| stat.api.tpns.tencent.com | IP: 42.194.154.20  所属国家: China  地区: Beijing  城市: Beijing |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| api.tpns.tencent.com | IP: 1.14.225.81  所属国家: China  地区: Beijing  城市: Beijing |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58  所属国家: China  地区: Guangdong  城市: Guangzhou |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| appsupport.qq.com | IP: 175.27.9.14  所属国家: China  地区: Beijing  城市: Beijing |
| alogsus.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| developer.umeng.com | IP: 59.82.31.92  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: - |
| ulogs.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| mp.weixin.qq.com | IP: 175.24.219.72  所属国家: China  地区: Beijing  城市: Beijing |
| log.tpns.tencent.com | IP: 1.14.225.56  所属国家: China  地区: Beijing  城市: Beijing |
| plbslog.umeng.com | IP: 36.156.202.73  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| resolver.msg.xiaomi.net | IP: 183.84.5.221  所属国家: China  地区: Beijing  城市: Beijing |
| www.52maozhua.com | IP: 175.178.206.98  所属国家: China  地区: Beijing  城市: Beijing |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| long.open.weixin.qq.com | IP: 109.244.217.35  所属国家: China  地区: Beijing  城市: Beijing |
| grs.dbankcloud.com | IP: 121.36.116.8  所属国家: China  地区: Beijing  城市: Beijing |
| h.trace.qq.com | IP: 109.244.244.61  所属国家: China  地区: Beijing  城市: Beijing |
| www.slf4j.org | IP: 83.173.251.158  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| miaozhua-test.oss-cn-hangzhou.aliyuncs.com | IP: 47.110.23.84  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 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 |
| platform-preprod.52mengdong.com | IP: 1.14.227.133  所属国家: China  地区: Beijing  城市: Beijing |
| platform.52mengdong.com | IP: 42.193.238.190  所属国家: China  地区: Beijing  城市: Beijing |
| platform-test.52mengdong.com | IP: 1.14.227.133  所属国家: China  地区: Beijing  城市: Beijing |
| oss.aliyuncs.com | IP: 118.178.29.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| image.52mengdong.com | IP: 106.116.171.238  所属国家: China  地区: Hebei  城市: Tangshan |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.huawei.com | IP: 106.38.242.116  所属国家: China  地区: Beijing  城市: Beijing |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection | org/java\_websocket/AbstractWebSocket.java |
| http://www.slf4j.org/codes.html | org/slf4j/LoggerFactory.java |
| http://www.slf4j.org/codes.html | org/slf4j/MDC.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| https://www.52maozhua.com/fish/detail | com/xiyou/miao/user/mine/g.java |
| https://www.52maozhua.com/ruleview | com/xiyou/miao/user/mine/sport/b.java |
| https://www.52maozhua.com/fish/detail | com/xiyou/miao/user/mine/sport/b.java |
| https://www.52maozhua.com/rankings | com/xiyou/miao/user/mine/sport/b.java |
| https://www.52maozhua.com/user\_level?level= | com/xiyou/miao/user/mine/level/WebviewBottomDialog.java |
| https://www.52maozhua.com/personaleula | com/xiyou/miao/dialog/SignInDialog$rbAgree$2$1.java |
| https://www.52maozhua.com/secret\_privacy | com/xiyou/miao/dialog/SignInDialog$rbAgree$2$2.java |
| https://www.52maozhua.com/secret\_privacy | com/xiyou/miao/dialog/PrivacyDialog$init$1$2.java |
| https://www.52maozhua.com/personaleula | com/xiyou/miao/dialog/PrivacyDialog$init$1$1.java |
| https://www.52maozhua.com/personaleula | com/xiyou/miao/account/AboutActivity$initView$1$1.java |
| http://platform-preprod.52mengdong.com | com/xiyou/miao/account/DevelopViewModel.java |
| https://www.52maozhua.com/secret\_privacy | com/xiyou/miao/account/AboutActivity$initView$1$2.java |
| https://www.52maozhua.com/secret\_privacy | com/xiyou/miao/account/phone/LoginPhoneActivity$initView$4.java |
| https://platform-test.52mengdong.com | com/xiyou/maozhua/api/GlobalConfig.java |
| https://miaozhua-test.oss-cn-hangzhou.aliyuncs.com | com/xiyou/maozhua/api/GlobalConfig.java |
| http://platform-preprod.52mengdong.com | com/xiyou/maozhua/api/GlobalConfig.java |
| https://platform.52mengdong.com | com/xiyou/maozhua/api/GlobalConfig.java |
| https://image.52mengdong.com | com/xiyou/maozhua/api/GlobalConfig.java |
| https://image.52mengdong.com | com/xiyou/maozhua/api/GlobalConfig$OSS\_HOST$2.java |
| https://miaozhua-test.oss-cn-hangzhou.aliyuncs.com | com/xiyou/maozhua/api/GlobalConfig$OSS\_HOST$2.java |
| https://platform.52mengdong.com | com/xiyou/maozhua/api/GlobalConfig$API\_HOST$2.java |
| https://platform-test.52mengdong.com | com/xiyou/maozhua/api/GlobalConfig$API\_HOST$2.java |
| http://platform-preprod.52mengdong.com | com/xiyou/maozhua/api/GlobalConfig$API\_HOST$2.java |
| https://miaozhua-test.oss-cn-hangzhou.aliyuncs.com | com/xiyou/maozhua/api/ali/AliOss.java |
| https://image.52mengdong.com | com/xiyou/maozhua/api/ali/AliOss.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/hi.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/gb.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/go.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/hg.java |
| https://%1$s/gslb/?ver=5.0 | com/xiaomi/push/ch.java |
| https://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/ba.java |
| http://10.38.162.35:9085 | com/xiaomi/push/service/ct.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/ct.java |
| https://ip. | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| https://203.107.1.1/181345/d?host= | com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java |
| http://oss.aliyuncs.com | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://127.0.0.1 | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| https://www.huawei.com/auth/account/nonincludegranted | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/base.profile/accesstoken | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/carrierid | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/base.profile/serviceauthcode | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/base.profile | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/country | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/games | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/shipping.address | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/age.range | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/assisttoken | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/homezone | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/age.groupflag | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/mobile.flag | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/mobile.number | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/auth/account/realname.anonymous | com/huawei/hms/support/api/entity/common/CommonConstant.java |
| https://www.huawei.com/healthkit/oxygensaturation.both | com/huawei/hms/hihealth/HuaweiHiHealth.java |
| https://www.huawei.com/healthkit/oxygensaturation.read | com/huawei/hms/hihealth/HuaweiHiHealth.java |
| https://www.huawei.com/healthkit/oxygensaturation.write | com/huawei/hms/hihealth/HuaweiHiHealth.java |
| https://www.huawei.com/healthkit/oxygensaturation.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/activity.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/activity.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/activityrecord.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/activityrecord.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/activityrecord.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/activity.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bloodglucose.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bloodglucose.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bloodglucose.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bloodpressure.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bloodpressure.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bloodpressure.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bodyfat.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bodyfat.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bodyfat.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bodytemperature.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bodytemperature.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/bodytemperature.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/calories.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/calories.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/calories.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/distance.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/distance.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/distance.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/hearthealth.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/hearthealth.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/hearthealth.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/heartrate.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/heartrate.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/heartrate.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/heightweight.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/heightweight.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/heightweight.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/historydata.open.month | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/historydata.open.week | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/historydata.open.year | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/huaweihealth.link | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/location.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/location.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/location.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/nutrition.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/nutrition.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/nutrition.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/oxygensaturation.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/oxygensaturation.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/pulmonary.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/pulmonary.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/pulmonary.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/reproductive.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/reproductive.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/reproductive.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/sleep.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/sleep.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/sleep.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/speed.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/speed.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/speed.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/step.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/step.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/step.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/strength.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/strength.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/strength.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/stress.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/stress.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/stress.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/uricacid.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/uricacid.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/uricacid.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/urineroutine.both | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/urineroutine.read | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/urineroutine.write | com/huawei/hms/hihealth/data/Scopes.java |
| https://www.huawei.com/healthkit/oxygensaturation.read | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://www.huawei.com/healthkit/oxygensaturation.write | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://www.huawei.com/healthkit/oxygensaturation.both | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://www.huawei.com/healthkit/uricacid.read | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://www.huawei.com/healthkit/uricacid.write | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://www.huawei.com/healthkit/uricacid.both | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://www.huawei.com/healthkit/urineroutine.read | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://www.huawei.com/healthkit/urineroutine.write | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://www.huawei.com/healthkit/urineroutine.both | com/huawei/hms/hihealth/data/HealthDataTypes.java |
| https://aaid.umeng.com/api/updateZdata | com/umeng/umzid/ZIDManager.java |
| https://aaid.umeng.com/api/postZdata | com/umeng/umzid/ZIDManager.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.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 |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://aspect-upush.umeng.com/occa/v1/event/report | com/umeng/analytics/pro/an.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://ucc.umeng.com/v2/inn/fetch | com/umeng/analytics/pro/ao.java |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| https://h.trace.qq.com/kv | com/tencent/bugly/proguard/ad.java |
| https://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/proguard/ac.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/proguard/ac.java |
| https://log.tpns.tencent.com/device/v4/sdk/list | com/tencent/android/tpush/common/i.java |
| https://openmobile.qq.com/oauth2.0/me | com/tencent/connect/UnionInfo.java |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version? | com/tencent/connect/common/BaseApi.java |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | com/tencent/connect/common/BaseApi.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 |
| https://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 |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | com/tencent/connect/auth/a.java |
| https://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/open/SocialApiIml.java |
| https://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/open/SocialApiIml.java |
| https://login.imgcache.qq.com | com/tencent/open/SocialApiIml.java |
| https://login.imgcache.qq.com/open/mobile/request/sdk\_request.html? | com/tencent/open/SocialApiIml.java |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group | com/tencent/open/SocialOperation.java |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind | com/tencent/open/SocialOperation.java |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | com/tencent/open/utils/g.java |
| https://cgi.qplus.com/report/report | com/tencent/open/utils/l.java |
| https://huatuocode.huatuo.qq.com?domain=mobile.opensdk.com&cgi=opensdk&type= | com/tencent/open/a/d.java |
| https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.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://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/c.java |
| https://guid. | com/tencent/tpns/baseapi/core/a.java |
| https://api.tpns.tencent.com/guid/v4/register\_device | com/tencent/tpns/baseapi/core/a.java |
| https://stat. | com/tencent/tpns/baseapi/core/a.java |
| https://stat.api.tpns.tencent.com/log/v4/statistics/push | com/tencent/tpns/baseapi/core/a.java |
| https://log. | com/tencent/tpns/baseapi/core/a.java |
| https://log.tpns.tencent.com/log/v4/statistics/push | com/tencent/tpns/baseapi/core/a.java |
| https://stat.api.tpns.tencent.com/v3/mobile/log/upload | com/tencent/tpns/baseapi/core/a.java |
| https://api.tpns.tencent.com/device/v4/account/batch\_operate | com/tencent/tpns/baseapi/core/a.java |
| https://data-drcn.push.dbankcloud.com | Mogua Engine V2 |
| https://data-dra.push.dbankcloud.com | Mogua Engine V2 |
| https://data-dre.push.dbankcloud.com | Mogua Engine V2 |
| https://data-drru.push.dbankcloud.com | Mogua Engine V2 |
| https://grs.dbankcloud.com | Mogua Engine V2 |
| https://grs.dbankcloud.cn | Mogua Engine V2 |
| https://grs.dbankcloud.asia | Mogua Engine V2 |
| https://grs.platform.dbankcloud.ru | Mogua Engine V2 |
| https://grs.dbankcloud.eu | Mogua Engine V2 |
| https://metrics1-drcn.dt.dbankcloud.cn:443 | Mogua Engine V2 |
| https://metrics-dra.dt.hicloud.com:6447 | Mogua Engine V2 |
| https://metrics2.data.hicloud.com:6447 | Mogua Engine V2 |
| https://metrics5.data.hicloud.com:6447 | Mogua Engine V2 |
| https://metrics5.dt.dbankcloud.ru:6447 | Mogua Engine V2 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| this@activity.supportfra | com/xiyou/miao/home/bottle/CommentListFragment$showCommentErrorDialog$1$2$1.java |
| this@showleveltipdialog.supportfra | com/xiyou/miao/extension/AppViewExtensionKt$showLevelTipDialog$1$1.java |

### **4.4 手机号线索**

## **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: ST=zhengdu, L=cn, O=xiyou, OU=xiyou, CN=miaozhua 签名算法: rsassa\_pkcs1v15 有效期自: 2018-12-20 07:24:48+00:00 有效期至: 2043-12-14 07:24:48+00:00 发行人: ST=zhengdu, L=cn, O=xiyou, OU=xiyou, CN=miaozhua 序列号: 0xe901c01 哈希算法: sha256 md5值: 6f19ccdc12b8c4489258110ef1c650d3 sha1值: 5a85260ef0cd63114be483a8ff296ee3ba1472e7 sha256值: 244fe2ad5cc2cc4d1760abd9ffb770c0877e190e4b2241acd9435b82a6a2927f sha512值: 31308cf5f27af4892aebec1b262796f038fcbf602b6cfb78e17d61b90895ab7033abf28622f88bd8ac9a795cf25c441eee5b286a61f59af499730adf9610eda2 公钥算法: rsa 密钥长度: 2048 指纹: be956e67034ba7aa9ecebb39a585200a84c4e18e83fe42627e54098b5e5790ad**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_login\_auth\_denied" : "拒绝授权" |
| "edit\_user" : "编辑资料" |
| "edit\_user\_name" : "昵称" |

## **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.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.READ\_MEDIA\_IMAGES | 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.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\_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\_DOWNLOAD\_MANAGER | 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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 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。 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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 |
| miui.permission.READ\_STEPS | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.xiyou.miao.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.xiyou.miao.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.xiyou.miao.permission.PUSH\_PROVIDER | 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 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| android.permission.POST\_NOTIFICATIONS | 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.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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 |
| com.xiyou.miao.permission.XGPUSH\_RECEIVE | 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.xiyou.miao.permission.MIPUSH\_RECEIVE | 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://, |
| com.tencent.android.tpush.TpnsActivity | **Schemes**: tpns://,  **Hosts:** com.xiyou.miao, |
| com.tencent.android.tpush.InnerTpnsActivity | **Schemes**: stpns://,  **Hosts:** com.xiyou.miao, |

**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。**