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

**XiXi（ 1.0.1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 | XiXi |
| 版本 | 1.0.1 |
| 包名 | com.tiocloud.xixi.chat |
| 域名线索 | 69条 |
| URL线索 | 60条 |
| APP图标 |  |
| 分析日期 | 2025年1月27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 | base.apk |
| 文件大小 | 45.72MB |
| MD5值 | 5eaaf8030f3c0d8d47f65b786d49edd0 |
| SHA1值 | 9b9c1ea077a00328356d1b41e87ba9a86a1ea5d5 |
| SHA256值 | cec0a7cc762558987b66b01ca14c26adce13d3996f0cc70600395b3a0cc363a6 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | XiXi |
| 包名 | com.tiocloud.xixi.chat |
| 主活动Activity | com.tiocloud.chat.feature.splash.SplashActivity |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 47.110.157.169 | IP: 47.110.157.169 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  |
| cn.register.xmpush.xiaomi.com | IP: 118.26.252.220 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.android.com | 没有服务器地理信息.  |
| schemas.microsoft.com | IP: 13.107.237.49 所属国家: United States of America 地区: Washington 城市: Redmond  |
| www.tiocloud.com | IP: 122.112.214.244 所属国家: China 地区: Shanghai 城市: Shanghai  |
| grs.dbankcloud.com | IP: 121.36.119.243 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| store1.hispace.hicloud.com | IP: 118.194.33.169 所属国家: China 地区: Shanghai 城市: Shanghai  |
| qzs.qq.com | IP: 182.254.60.147 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| www.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: Texas 城市: Dallas  |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| open.weixin.qq.com | IP: 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing  |
| 20.239.94.99 | IP: 20.239.94.99 所属国家: United States of America 地区: Washington 城市: Redmond  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| play.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| open.weibo.cn | IP: 49.7.37.118 所属国家: China 地区: Beijing 城市: Beijing  |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.weibo.cn | IP: 180.149.139.248 所属国家: China 地区: Beijing 城市: Beijing  |
| new.api.ad.xiaomi.com | 没有服务器地理信息.  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| graph.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| appsupport.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |
| fr.register.xmpush.global.xiaomi.com | IP: 52.58.96.106 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| grs.dbankcloud.asia | 没有服务器地理信息.  |
| tx.t-io.org | IP: 129.211.52.247 所属国家: China 地区: Beijing 城市: Beijing  |
| ce3e75d5.jpush.cn | IP: 183.232.25.164 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| api.xmpush.xiaomi.com | IP: 118.26.252.230 所属国家: China 地区: Beijing 城市: Beijing  |
| aomediacodec.github.io | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| ug.edm.weibo.cn | IP: 49.7.37.77 所属国家: China 地区: Beijing 城市: Beijing  |
| www.openssl.org | IP: 104.71.138.221 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.jivesoftware.com | IP: 141.193.213.11 所属国家: United States of America 地区: Texas 城市: Austin  |
| mirror.anji-plus.com | IP: 203.156.222.138 所属国家: China 地区: Shanghai 城市: Shanghai  |
| long.open.weixin.qq.com | IP: 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing  |
| a.app.qq.com | IP: 175.27.12.121 所属国家: China 地区: Beijing 城市: Beijing  |
| store-drru.hispace.hicloud.com | IP: 159.138.202.186 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| xmlpull.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| hkflylinks.oss-cn-hongkong.aliyuncs.com | IP: 47.75.19.179 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| metrics-dra.dt.hicloud.com | IP: 94.74.84.62 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| openmobile.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |
| ns.adobe.com | 没有服务器地理信息.  |
| service.weibo.com | IP: 49.7.40.134 所属国家: China 地区: Beijing 城市: Beijing  |
| api.weibo.com | IP: 49.7.37.118 所属国家: China 地区: Beijing 城市: Beijing  |
| www.webrtc.org | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| appr.tc | IP: 216.239.34.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| gitee.com | IP: 212.64.63.190 所属国家: China 地区: Beijing 城市: Beijing  |
| imtt.dd.qq.com | IP: 61.49.23.135 所属国家: China 地区: Beijing 城市: Beijing  |
| resolver.msg.xiaomi.net | IP: 183.84.5.221 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.dbankcloud.cn | IP: 49.4.41.160 所属国家: China 地区: Beijing 城市: Beijing  |
| fusion.qq.com | IP: 175.27.9.125 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics1.data.hicloud.com | IP: 114.115.188.66 所属国家: China 地区: Beijing 城市: Beijing  |
| res.t-io.org | IP: 122.112.214.244 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.chinabite.com | IP: 125.76.231.66 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| store3.hispace.hicloud.com | IP: 23.56.113.54 所属国家: United States of America 地区: California 城市: San Jose  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| store.hispace.hicloud.com | IP: 49.4.38.106 所属国家: China 地区: Beijing 城市: Beijing  |
| store2.hispace.hicloud.com | IP: 13.225.183.77 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| playready.directtaps.net | IP: 40.70.71.156 所属国家: United States of America 地区: Virginia 城市: Boydton  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 110.42.1.64 | IP: 110.42.1.64 所属国家: China 地区: Zhejiang 城市: Ningbo  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| api.weixin.qq.com | IP: 109.244.145.152 所属国家: China 地区: Beijing 城市: Beijing  |
| idmb.register.xmpush.global.xiaomi.com | IP: 52.66.182.128 所属国家: India 地区: Maharashtra 城市: Mumbai  |
| store-at-dre.hispace.dbankcloud.com | IP: 80.158.5.6 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| cgi.connect.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | h/d/a/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | h/d/a/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | h/d/a/i.java  |
| http://%s:%d/%s  | h/d/a/g.java  |
| http://%s:%d/%s  | h/d/a/l.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | h/d/a/l.java  |
| https://a.app.qq.com/o/simple.jsp?pkgname=com.tiocloud.xixi.chat  | h/x/i/h/c/c/g.java  |
| https://a.app.qq.com/o/simple.jsp  | h/x/i/h/a/c.java  |
| https://a.app.qq.com/o/simple.jsp?pkgname=com.tiocloud.xixi.chat  | h/x/i/h/b/c/g.java  |
| https://hkflylinks.oss-cn-hongkong.aliyuncs.com  | h/x/f/e/b.java  |
| http://110.42.1.64:9099  | h/x/f/e/b.java  |
| https://gitee.com/jack-ccq/wangt062/raw/master/verification-code/what  | h/x/f/e/b.java  |
| http://20.239.94.99:6060  | h/x/f/e/b.java  |
| http://20.239.94.99:9092  | h/x/f/e/b.java  |
| https://imtt.dd.qq.com/16891/apk/5CACCB57E3F02E46404D27ABAA85474C.apk  | h/x/b/f.java  |
| https://www.tiocloud.com/2/h5down.html  | h/x/b/f.java  |
| https://mirror.anji-plus.com/captcha-api/  | h/v/g/i/d.java  |
| https://api.xmpush.xiaomi.com/upload/crash\_log?file=  | h/y/c/a/o1.java  |
| https://api.xmpush.xiaomi.com/upload/xmsf\_log?file=  | h/y/c/a/m1.java  |
| https://api.xmpush.xiaomi.com/upload/app\_log?file=  | h/y/c/a/m1.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | i/a/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | i/a/p/e.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | i/a/p/c.java  |
| https://ce3e75d5.jpush.cn/wi/cjc4sa  | cn/jiguang/at/c.java  |
| https://ce3e75d5.jpush.cn/wi/d8n3hj  | cn/jiguang/at/c.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/fo.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://new.api.ad.xiaomi.com/logNotificationAdActions  | com/xiaomi/push/cq.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gr.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fy.java  |
| http://%1$s/gslb/?ver=4.0  | com/xiaomi/push/cz.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://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bf.java  |
| https://api.weibo.com/2/proxy/sdk/statistic.json  | com/sina/weibo/sdk/statistic/LogReport.java  |
| https://api.weibo.com/oauth2/getaid.json  | com/sina/weibo/sdk/utils/AidTask.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://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://api.weibo.cn/2/sdk/login  | com/sina/weibo/sdk/network/intercept/CommonParamInterception.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.com/oauth2/access\_token  | com/sina/weibo/sdk/auth/AccessTokenKeeper.java  |
| https://open.weibo.cn/oauth2/authorize?  | com/sina/weibo/sdk/auth/BaseSsoHandler.java  |
| http://47.110.157.169:6060  | com/tiocloud/chat/test/TestActivity.java  |
| https://tx.t-io.org  | 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  |
| http://www.chinabite.com  | com/tiocloud/chat/feature/news/NewDetailActivity.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://graph.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.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  |
| 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  |
| 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://qzs.qq.com/open/mobile/login/qzsjump.html?  | com/tencent/connect/auth/a.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  |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/f.java  |
| https://huatuocode.huatuo.qq.com  | com/tencent/open/b/d.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  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | e/n/a/a.java  |
| http://schemas.android.com/apk/res/android  | e/j/i/c/g.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://appgallery.cloud.huawei.com/app/  | Mogua Engine V1  |
| https://play.google.com/store/apps/details?id=  | Mogua Engine V1  |
| https://appgallery.cloud.huawei.com  | Mogua Engine V1  |
| https://appr.tc  | Mogua Engine V1  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V1  |
| https://store.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V1  |
| 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://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://store1.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://metrics1.data.hicloud.com:6447  | 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  |
| http://www.openssl.org/support/faq.html  | lib/x86/libijkffmpeg.so  |
| https://crbug.com/1053756  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00  | lib/x86/libjingle\_peerconnection\_so.so  |
| https://aomediacodec.github.io/av1-rtp-spec/  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space  | lib/x86/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn  | lib/x86/libjingle\_peerconnection\_so.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | h/d/a/i.java  |
| liwei31@staff.weibo  | com/sina/weibo/sdk/network/intercept/RequestTokenInterception.java  |
| 发送到您的注册邮箱watayouxian@qq.com  | com/tiocloud/chat/test/activity/UITestActivity.java  |
| watayouxiang@qq.com  | com/tiocloud/chat/test/activity/HttpTestActivity.java  |
| o@netstream.failed  | lib/x86/librtmp-jni.so  |
| ffmpeg-devel@ffmpeg.org  | lib/x86/libijkplayer.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2008-02-29 01:33:46+00:00 有效期至: 2035-07-17 01:33:46+00:00 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0x936eacbe07f201df 哈希算法: sha1 md5值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569 公钥算法: rsa 密钥长度: 2048 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "clear\_session\_record" : "Clear chat"  |
| "clear\_shuangxiang\_session\_record" : "Two-way clear chat history"  |
| "confir\_remove\_user" : "Are you sure to remove this user from group chat？"  |
| "confir\_xinmima" : "Confirm new password"  |
| "confire\_jubao\_user" : "Are you sure you want to report this user?"  |
| "denglu\_mima" : "Login password"  |
| "find\_pwd" : "Retrieve password"  |
| "forget\_pwd" : "Forget password"  |
| "get\_token\_fail" : "Failed to get token"  |
| "has\_pingbi\_user" : "The user has been blocked"  |
| "input\_email\_zhanghaomima" : "Please input your email account password"  |
| "input\_login\_mima" : "Please input your password"  |
| "input\_nide\_password" : "input your password"  |
| "input\_password" : "Please enter the password, 6 ~ 20 letters or numbers"  |
| "input\_xinmima" : "Please input a new password"  |
| "input\_yuanmima" : "Please input the original password"  |
| "input\_zhifu\_mima" : "Please input the payment password"  |
| "input\_zhifumima\_yanzheng" : "Please input the payment password to verify your identity"  |
| "modify\_pwd" : "Change Password"  |
| "pwd" : "Password"  |
| "pwd\_null\_tip" : "Password cannot be empty"  |
| "queren\_xinmima" : "Confirm the new password"  |
| "report\_user" : "Report user"  |
| "retrieve\_pwd\_success" : "Retrieve password success"  |
| "session\_group" : "Group"  |
| "set\_login\_password" : "Please set login password"  |
| "set\_password" : "Set password"  |
| "set\_pwd" : "Set password"  |
| "token\_null" : "Token is empty"  |
| "xinmima" : "New password"  |
| "clear\_session\_record" : "Clear chat"  |
| "clear\_shuangxiang\_session\_record" : "Two-way clear chat history"  |
| "confir\_remove\_user" : "Are you sure to remove this user from group chat？"  |
| "confir\_xinmima" : "Confirm new password"  |
| "confire\_jubao\_user" : "Are you sure you want to report this user?"  |
| "denglu\_mima" : "Login password"  |
| "find\_pwd" : "Retrieve password"  |
| "forget\_pwd" : "Forget password"  |
| "get\_token\_fail" : "Failed to get token"  |
| "has\_pingbi\_user" : "The user has been blocked"  |
| "input\_email\_zhanghaomima" : "Please input your email account password"  |
| "input\_login\_mima" : "Please input your password"  |
| "input\_nide\_password" : "input your password"  |
| "input\_password" : "Please enter the password, 6 ~ 20 letters or numbers"  |
| "input\_xinmima" : "Please input a new password"  |
| "input\_yuanmima" : "Please input the original password"  |
| "input\_zhifu\_mima" : "Please input the payment password"  |
| "input\_zhifumima\_yanzheng" : "Please input the payment password to verify your identity"  |
| "modify\_pwd" : "Change Password"  |
| "pwd" : "Password"  |
| "pwd\_null\_tip" : "Password cannot be empty"  |
| "queren\_xinmima" : "Confirm the new password"  |
| "report\_user" : "Report user"  |
| "retrieve\_pwd\_success" : "Retrieve password success"  |
| "session\_group" : "Group"  |
| "set\_login\_password" : "Please set login password"  |
| "set\_password" : "Set password"  |
| "set\_pwd" : "Set password"  |
| "token\_null" : "Token is empty"  |
| "xinmima" : "New password"  |
| "clear\_session\_record" : "清空聊天记录"  |
| "clear\_shuangxiang\_session\_record" : "双向清除聊天记录"  |
| "confir\_remove\_user" : "确定将该用户移出群聊？"  |
| "confir\_xinmima" : "确认新密码"  |
| "confire\_jubao\_user" : "确定举报该用户吗？"  |
| "denglu\_mima" : "登录密码"  |
| "find\_pwd" : "找回密码"  |
| "forget\_pwd" : "忘记密码"  |
| "get\_token\_fail" : "获取token失败"  |
| "has\_pingbi\_user" : "已屏蔽该用户"  |
| "input\_email\_zhanghaomima" : "请输入邮箱账号密码"  |
| "input\_login\_mima" : "请输入登录密码"  |
| "input\_nide\_password" : "请输入您的密码"  |
| "input\_password" : "请输入密码，6~20位字母或者数字"  |
| "input\_xinmima" : "请输入新密码"  |
| "input\_yuanmima" : "请输入原密码"  |
| "input\_zhifu\_mima" : "请输入支付密码"  |
| "input\_zhifumima\_yanzheng" : "请输入支付密码，以验证身份"  |
| "modify\_pwd" : "修改密码"  |
| "pwd" : "密码"  |
| "pwd\_null\_tip" : "密码不能为空"  |
| "queren\_xinmima" : "确认新密码"  |
| "report\_user" : "举报用户"  |
| "retrieve\_pwd\_success" : "找回密码成功"  |
| "session\_group" : "群聊"  |
| "set\_login\_password" : "请设置登录密码"  |
| "set\_password" : "设置密码"  |
| "set\_pwd" : "设置密码"  |
| "token\_null" : "Token为空"  |
| "xinmima" : "新密码"  |

## **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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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。 |
| com.tiocloud.xixi.chat.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\_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\_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.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\_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 |
| 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.tiocloud.xixi.chat.permission.MIPUSH\_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.tiocloud.xixi.chat.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.tiocloud.xixi.chat.permission.PUSH\_PROVIDER | 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。 |
| 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。**