MoGua

XiXi 1.0.1.APK 分析报告

APP名称:	XiXi
包名:	com.tiocloud.xixi.chat

域名线索:	69条
URL线索:	60条
邮箱线索:	6条
分析日期:	2025年1月27日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 45.72MB
MD5值: 5eaaf8030f3c0d8d47f65b786d49edd0
SHA1值: 9b9c1ea077a00328356d1b41e87ba9a86a1ea5d5
SHA256值: cec0a7cc762558987b66b01ca14c26adce13d3996f0cc70600395b3a0cc363a6

APP 信息

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

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 **纬度**: 30.293650 **经度**: 120.161423
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321331 **经度**: 10.134890
cn.register.xmpush.xiaomi.com	**IP**: 118.26.252.220 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
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

	纬度: 47.682899 **经度**: -122.120903
www.tiocloud.com	**IP**: 122.112.214.244 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
grs.dbankcloud.com	**IP**: 121.36.119.243 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
store1.hispace.hicloud.com	**IP**: 118.194.33.169 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
qzs.qq.com	**IP**: 182.254.60.147 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545540 **经度**: 114.068298
www.ietf.org	**IP**: 104.16.44.99 **所属国家**: United States of America **地区**: Texas **城市**: Dallas **纬度**: 32.783058 **经度**: -96.806671
huatuocode.huatuo.qq.com	没有服务器地理信息.
	IP: 175.24.209.30 **所属国家**: China **地区**: Beijing

open.weixin.qq.com	**城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
20.239.94.99	**IP**: 20.239.94.99 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
github.com	**IP**: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
data-drru.push.dbankcloud.com	**IP**: 159.138.202.31 **所属国家**: Russian Federation **地区**: Moskva **城市**: Moscow **纬度**: 55.752220 **经度**: 37.615559
play.google.com	**IP**: 142.251.43.14 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
open.weibo.cn	**IP**: 49.7.37.118 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
register.xmpush.global.xiaomi.com	**IP**: 47.88.199.5 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore

	纬度: 1.289670 **经度**: 103.850067
api.weibo.cn	**IP**: 180.149.139.248 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
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 **纬度**: 55.752220 **经度**: 37.615559
graph.qq.com	**IP**: 175.27.9.43 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
ru.register.xmpush.global.xiaomi.com	**IP**: 107.155.52.56 **所属国家**: Russian Federation **地区**: Moskva **城市**: Moscow **纬度**: 55.752220 **经度**: 37.615559
appsupport.qq.com	**IP**: 175.27.9.14 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
fr.register.xmpush.global.xiaomi.com	**IP**: 52.58.96.106 **所属国家**: Germany **地区**: Hessen

	城市: Frankfurt am Main **纬度**: 50.115520 **经度**: 8.684170
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 **纬度**: 39.907501 **经度**: 116.397232
ce3e75d5.jpush.cn	**IP**: 183.232.25.164 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
api.xmpush.xiaomi.com	**IP**: 118.26.252.230 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
aomediacodec.github.io	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
ug.edm.weibo.cn	**IP**: 49.7.37.77 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 104.71.138.221 **所属国家**: Japan

www.openssl.org	**地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
www.jivesoftware.com	IP: 141.193.213.11 **所属国家**: United States of America **地区**: Texas **城市**: Austin **纬度**: 30.271158 **经度**: -97.741699
mirror.anji-plus.com	IP: 203.156.222.138 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
long.open.weixin.qq.com	IP: 109.244.216.15 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
a.app.qq.com	IP: 175.27.12.121 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
store-drru.hispace.hicloud.com	IP: 159.138.202.186 **所属国家**: Russian Federation **地区**: Moskva **城市**: Moscow **纬度**: 55.752220 **经度**: 37.615559
xmlpull.org	IP: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California

	纬度: 40.065632 **经度**: -79.891708
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 **纬度**: 22.285521 **经度**: 114.157692
metrics-dra.dt.hicloud.com	**IP**: 94.74.84.62 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
openmobile.qq.com	**IP**: 175.27.9.14 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
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 **纬度**: 39.907501 **经度**: 116.397232
api.weibo.com	**IP**: 49.7.37.118 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.webrtc.org	**IP**: 142.251.43.14 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514
appr.tc	**IP**: 216.239.34.21 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
gitee.com	**IP**: 212.64.63.190 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
imtt.dd.qq.com	**IP**: 61.49.23.135 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
resolver.msg.xiaomi.net	**IP**: 183.84.5.221 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
metrics2.data.hicloud.com	**IP**: 80.158.2.190 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321331 **经度**: 10.134890
grs.dbankcloud.cn	**IP**: 49.4.41.160 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501

	经度: 116.397232
fusion.qq.com	**IP**: 175.27.9.125 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
metrics1.data.hicloud.com	**IP**: 114.115.188.66 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
res.t-io.org	**IP**: 122.112.214.244 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
www.chinabite.com	**IP**: 125.76.231.66 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280
store3.hispace.hicloud.com	**IP**: 23.56.113.54 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.339390 **经度**: -121.894958
data-drcn.push.dbankcloud.com	**IP**: 121.36.117.8 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000

store.hispace.hicloud.com	**IP**: 49.4.38.106 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
store2.hispace.hicloud.com	**IP**: 13.225.183.77 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
crbug.com	**IP**: 216.239.32.29 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
playready.directtaps.net	**IP**: 40.70.71.156 **所属国家**: United States of America **地区**: Virginia **城市**: Boydton **纬度**: 36.667641 **经度**: -78.387497
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 **纬度**: 1.289670 **经度**: 103.850067
110.42.1.64	**IP**: 110.42.1.64 **所属国家**: China **地区**: Zhejiang **城市**: Ningbo **纬度**: 29.878189 **经度**: 121.549454

appgallery.cloud.huawei.com	**IP**: 121.36.118.136 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
api.weixin.qq.com	**IP**: 109.244.145.152 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
idmb.register.xmpush.global.xiaomi.com	**IP**: 52.66.182.128 **所属国家**: India **地区**: Maharashtra **城市**: Mumbai **纬度**: 19.014410 **经度**: 72.847939
store-at-dre.hispace.dbankcloud.com	**IP**: 80.158.5.6 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321331 **经度**: 10.134890
cgi.connect.qq.com	**IP**: 175.27.9.43 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

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

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

手机线索

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

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

🔑 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"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent{qq_app_id}://,

---