



MoGua

叶友 1.5.1.APK 分析报告



APP名称:

叶友

包名:	com.miliaoapp.live
域名线索:	74条
URL线索:	98条
邮箱线索:	2条
分析日期:	2025年8月23日
分析平台:	摸瓜APK反编译平台

文件名: 叶友_1.5.1_0727.apk
文件大小: 131.56MB
MD5值: c36aa89708b607aeddca359427ae28bb
SHA1值: 480089cd87c945a30f2c436bd5955a32db805796
SHA256值: f2b4b29b52956ed518c275e16bf7baf5d2925396809f04319072563481a0ad13

i APP 信息

App名称: 叶友
包名: com.miliaoapp.live
主活动Activity: com.miliaoapp.live.activity.SplashActivity
安卓版本名称: 1.5.1
安卓版本: 151

🔍 域名线索

域名	服务器信息
api-cn.faceplusplus.com	IP: 60.205.234.99 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
	IP: 203.119.169.174 所属国家: China 地区: Beijing

restapi.amap.com	城市: Beijing 纬度: 39.907501 经度: 116.397232
wb.amap.com	IP: 59.82.31.104 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
com.thoughtworks.xstream	没有服务器地理信息.
mpsapi.amap.com	IP: 59.82.112.213 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
fusion.qq.com	IP: 175.27.9.24 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
open.weixin.qq.com	IP: 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
lbs.amap.com	IP: 59.82.29.231 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650

	经度: 120.161423
mobilegw.alipaydev.com	IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
api.weixin.qq.com	IP: 175.27.5.221 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
xmlpull.org	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
news-at.zhihu.com	IP: 42.81.26.128 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
app.ylshow.cn	IP: 212.129.231.22 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

picsum.photos	IP: 172.67.74.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
license.vod2.myqcloud.com	IP: 119.167.131.102 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
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
m5.amap.com	IP: 59.82.113.187 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
vod2.qcloud.com	IP: 43.156.86.191 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
apilocate.amap.com	IP: 59.82.31.183 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397232
aomedia.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
tsis.jpush.cn	IP: 60.204.210.215 所属国家: China 地区: Jiangxi 城市: Nanchang 纬度: 28.683331 经度: 115.883331
www.yiwens.ren	IP: 111.230.93.21 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
apiinit.amap.com	IP: 203.119.169.174 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
mcgw.alipay.com	IP: 124.239.239.237 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
	IP: 150.138.36.16 所属国家: China 地区: Shandong

buy.cloud.tencent.com	城市: Jinan 纬度: 36.668331 经度: 116.997223
demo.ylshow.cn	IP: 212.129.231.22 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
top.ylshow.cn	IP: 212.129.231.22 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
192.168.1.5	IP: 192.168.1.5 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
mta.oa.com	IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690
tb.53kf.com	IP: 61.130.25.238 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658

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
mobilegw.alipay.com	IP: 203.209.245.77 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
www.slf4j.org	IP: 83.173.251.158 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366669 经度: 8.550000
wappaygw.alipay.com	IP: 124.239.239.237 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
xml.org	IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
mobilegw.stable.alipay.net	没有服务器地理信息.
	IP: 221.204.165.203 所属国家: China

qzs.qq.com	地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.560280
vodreport.qcloud.com	IP: 150.138.36.16 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
h5.m.taobao.com	IP: 111.225.210.165 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
pingma.qq.com	IP: 119.45.78.184 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
huatuocode.huatuo.qq.com	没有服务器地理信息.
wap.amap.com	IP: 42.81.21.166 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666
www.1-liao.com	IP: 3.209.25.139 所属国家: United States of America 地区: Virginia 城市: Ashburn

	纬度: 39.043720 经度: -77.487488
mobilegw.aaa.alipay.net	没有服务器地理信息.
api-us.faceplusplus.com	IP: 35.182.97.149 所属国家: Canada 地区: Quebec 城市: Montreal 纬度: 45.508839 经度: -73.587807
yuntuapi.amap.com	没有服务器地理信息.
wprd0d.is.autonavi.com	没有服务器地理信息.
192.168.1.7	IP: 192.168.1.7 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
paygate-yf.meituan.com	IP: 101.236.69.63 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
adiu.amap.com	IP: 59.82.29.231 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
	IP: 40.70.71.156

playready.directtaps.net	所属国家: United States of America 地区: Virginia 城市: Boydton 纬度: 36.667641 经度: -78.387497
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
room.qcloud.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
schemas.microsoft.com	IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
api.usercenter.3ttech.cn	IP: 47.95.165.170 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
tempa.3ttech.cn	IP: 120.78.31.4 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

exoplayer.dev	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
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
graph.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
mclient.alipay.com	IP: 27.128.221.243 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
mobile.unionpay.com	没有服务器地理信息.
182.92.20.189	IP: 182.92.20.189 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
	IP: 17.253.85.206 所属国家: Hong Kong

developer.apple.com	地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
mta.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
pv.sohu.com	IP: 42.81.26.128 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666
49.235.214.62	IP: 49.235.214.62 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
m.alipay.com	IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
sandcash.mixienet.com.cn	IP: 203.107.86.172 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

192.168.1.4	IP: 192.168.1.4 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
cgi.connect.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
bjuser.jpush.cn	IP: 122.9.15.248 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

 URL线索

URL信息	Url所在文件
http://www.slf4j.org/codes.html	org.slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html	org.slf4j/MDC.java

http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tvt/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tvt/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	q/a/s.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	q/a/b0.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	q/a/l.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	q/a/c.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	q/a/k0.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	q/a/v0/d.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	q/a/v0/f.java
https://tsis.jpush.cn	cn/jiguang/ad/i.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/aa/b.java
http://182.92.20.189:9099/	cn/jiguang/o/c.java
https://adiu.amap.com/ws/device/adius	j/c/a/a/a/h2.java
http://restapi.amap.com/v3	j/c/a/a/a/s3.java
https://restapi.amap.com/v3	j/c/a/a/a/s3.java
http://restapi.amap.com/v4	j/c/a/a/a/s3.java
https://restapi.amap.com/v4	j/c/a/a/a/s3.java
http://yuntuapi.amap.com	j/c/a/a/a/s3.java

https://yuntuapi.amap.com	j/c/a/a/a/s3.java
http://m5.amap.com/ws/mapapi/shortaddress/transform	j/c/a/a/a/s3.java
https://m5.amap.com/ws/mapapi/shortaddress/transform	j/c/a/a/a/s3.java
http://restapi.amap.com	j/c/a/a/a/p0.java
http://apiinit.amap.com/v3/log/init	j/c/a/a/a/j0.java
https://restapi.amap.com/v3/iasdkauth	j/c/a/a/a/i0.java
http://restapi.amap.com/v3/iasdkauth	j/c/a/a/a/i0.java
http://wb.amap.com/? r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0	j/c/a/a/a/c0.java
http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0	j/c/a/a/a/c0.java
http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0	j/c/a/a/a/c0.java
http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0	j/c/a/a/a/c0.java
http://restapi.amap.com/v3/geocode/regeo	j/k/h2.java
https://restapi.amap.com/v3/iasdkauth	j/k/e3.java
http://restapi.amap.com/v3/iasdkauth	j/k/e3.java
http://restapi.amap.com	j/k/l3.java
http://abroad.apilocate.amap.com/mobile/binary	j/k/r2.java
http://apilocate.amap.com/mobile/binary	j/k/m2.java

http://abroad.apilocate.amap.com/mobile/binary	j/k/m2.java
https://adiu.amap.com/ws/device/adius	j/k/n0.java
http://restapi.amap.com/v3/place/text?	j/k/a.java
http://restapi.amap.com/v3/place/around?	j/k/a.java
http://restapi.amap.com/v3/config/district?	j/k/a.java
http://abroad.apilocate.amap.com/mobile/binary	j/k/f2.java
http://app.ylshow.cn/app/	j/o/a/a.java
http://www.1-liao.com	j/o/a/f/a.java
https://api.weixin.qq.com/sns/oauth2/access_token	j/o/a/f/a.java
https://api.weixin.qq.com/sns/userinfo	j/o/a/f/a.java
http://pv.sohu.com/cityjson?ie=utf-8	j/o/a/f/a.java
http://top.ylshow.cn/ip.php	j/o/a/f/a.java
https://license.vod2.myqcloud.com/license/v2/1314311834_1/v_cube.license	j/o/a/f/b.java
http://app.ylshow.cn/user_use.html	j/o/a/f/b.java
http://app.ylshow.cn/user_secrect.html	j/o/a/f/b.java
http://app.ylshow.cn/app_permission.html	j/o/a/f/b.java
https://vod2.qcloud.com/v3/index.php?Action=	j/o/a/q/c/i.java
https://vodreport.qcloud.com/ugcupload	j/o/a/q/c/j.java

https://exoplayer.dev/issues/player-accessed-on-wrong-thread	j/i/a/a/d1.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	j/i/a/a/l1/b0.java
https://aomedia.org/emsg/ID3	j/i/a/a/o1/h/a.java
https://developer.apple.com/streaming/emsg-id3	j/i/a/a/o1/h/a.java
http://www.w3.org/ns/ttml	j/i/a/a/r1/s/a.java
http://com.thoughtworks.xstream/sax/property/configured-xstream	j/q/a/i/t/d0.java
http://com.thoughtworks.xstream/sax/property/source-object-list	j/q/a/i/t/d0.java
http://com.thoughtworks.xstream/sax/property/source-object-list\	j/q/a/i/t/d0.java
http://xml.org/sax/features/namespaces	j/q/a/i/t/d0.java
http://xml.org/sax/features/namespace-prefixes	j/q/a/i/t/d0.java
http://com.thoughtworks.xstream/sax/property/configured-xstream\	j/q/a/i/t/d0.java
http://com.thoughtworks.xstream/XStreamSource/feature	j/q/a/i/t/j0.java
https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple\	j/b/d/a.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&	j/b/b/c/a.java
https://mcgw.alipay.com/sdklog.do	j/b/b/f/f/c.java
https://mobilegw.alipay.com/mgw.htm	j/b/b/b/a.java
https://mobilegw.alipaydev.com/mgw.htm	j/b/b/b/a.java

http://m.alipay.com/?action=h5quit	j/b/b/b/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	j/b/b/b/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	j/b/b/b/a.java
http://www.yiwens.ren/app/	com/miliaoapp/live/dialogfragment/SwitchingLinesFragment.java
http://demo.ylshow.cn/app/	com/miliaoapp/live/dialogfragment/HostDialogFragment.java
http://192.168.1.4:81/app/	com/miliaoapp/live/dialogfragment/HostDialogFragment.java
http://192.168.1.5:8080/app/	com/miliaoapp/live/dialogfragment/HostDialogFragment.java
http://192.168.1.7/app/	com/miliaoapp/live/dialogfragment/HostDialogFragment.java
http://app.ylshow.cn/app/agree.jsp	com/miliaoapp/live/dialog/a.java
http://app.ylshow.cn/app/private.jsp	com/miliaoapp/live/dialog/a.java
https://room.qcloud.com/weapp/utis/report	com/miliaoapp/live/txlive/http/HttpRequests.java
https://buy.cloud.tencent.com/avc	com/miliaoapp/live/txlive/im/IMMessageMgr.java
http://app.ylshow.cn/app/charge.jsp	com/miliaoapp/live/activity/ChargeActivity.java
http://app.ylshow.cn/app/private.jsp	com/miliaoapp/live/activity/SettingActivity.java
http://app.ylshow.cn/app/agree.jsp	com/miliaoapp/live/activity/SettingActivity.java
http://app.ylshow.cn/app/agreement.jsp	com/miliaoapp/live/activity/AlipayAccountActivity.java
http://app.ylshow.cn/app/agree.jsp	com/miliaoapp/live/activity/ScrollLoginActivity.java
http://app.ylshow.cn/app/private.jsp	com/miliaoapp/live/activity/ScrollLoginActivity.java

https://tb.53kf.com/code/client/10188492/1?device=android	com/miliaoapp/live/activity/KeFuWebViewActivity.java
http://app.ylshow.cn/app/agree.jsp	com/miliaoapp/live/activity/PhoneLoginActivity.java
http://49.235.214.62:8081/push/read	com/miliaoapp/live/im/ChatFragment.java
http://app.ylshow.cn/	com/miliaoapp/live/network/b.java
http://news-at.zhihu.com/api/4/	com/miliaoapp/live/network/f.java
http://app.ylshow.cn/auth/webLogin?userCode=%1\$s&userPwd=%2\$s	com/miliaoapp/live/network/f.java
http://app.ylshow.cn/	com/miliaoapp/live/network/f.java
http://wap.amap.com/	com/amap/api/maps/AMapUtils.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.java
http://wprd0%d.is.autonavi.com/appmaptile?	com/amap/api/mapcore/util/q3.java
http://restapi.amap.com/v4/gridmap?	com/amap/api/mapcore/util/q3.java
https://adiu.amap.com/ws/device/adius	com/amap/api/mapcore/util/o8.java
http://restapi.amap.com/v4	com/amap/api/mapcore/util/c7.java
https://restapi.amap.com/v3/iasdkauth	com/amap/api/mapcore/util/u5.java
http://restapi.amap.com/v3/iasdkauth	com/amap/api/mapcore/util/u5.java
http://apiinit.amap.com/v3/log/init	com/amap/api/mapcore/util/v5.java
http://restapi.amap.com	com/amap/api/mapcore/util/d6.java

http://apilocate.amap.com/mobile/binary	com/amap/api/mapcore/util/va.java
http://restapi.amap.com/v4	com/amap/api/mapcore/util/c3.java
http://restapi.amap.com/v4/graspoad/driving?	com/amap/api/mapcore/util/o5.java
http://tempa.3ttech.cn:18000/live/record/queryserverid?appid=	com/wushuangtech/wstechapi/internal/TTTRtcEngineImpl.java
http://api.usercenter.3ttech.cn/verify.php?token=	com/wushuangtech/api/EnterConfApiImpl.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/b/a/e.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/b/a/a.java
https://sandcash.mixienet.com.cn/h5/?	com/pay/paytypelibrary/PayUtil.java
https://api-cn.faceplusplus.com/sdk/v3/auth	com/meihu/beautylibrary/utls/h.java
https://api-us.faceplusplus.com/sdk/v3/auth	com/meihu/beautylibrary/utls/h.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/autonavi/amap/mapcore/Inner_3dMap_location.java
http://m5.amap.com/	com/autonavi/amap/mapcore/maploader/AMapLoader.java
http://mpsapi.amap.com/	com/autonavi/ae/gmap/GLMapEngine.java
http://m5.amap.com/	com/autonavi/ae/gmap/GLMapEngine.java

http://49.235.214.62:8081/push/read	com/tencent/qcloud/tim/uikit/modules/chat/base/ChatManagerKit.java
http://49.235.214.62:8081/push/getRead	com/tencent/qcloud/tim/uikit/modules/chat/layout/message/MessageListAdapter.java
https://picsum.photos/id/%d/200/200	com/tencent/qcloud/tim/uikit/modules/group/info/GroupInfoLayout.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://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiImpl.java

http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApilml.java
http://qzs.qq.com	com/tencent/open/SocialApilml.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApilml.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utis/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×tamp=%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://xmlpull.org/v1/doc/features.html	com/tencent/cos/xml/transfer/XmlBuilder.java
http://xmlpull.org/v1/doc/features.html	com/tencent/cos/xml/transfer/XmlSlimBuilder.java
https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\	com/unionpay/UPPayAssistEx.java
https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\	com/unionpay/mobile/android/utis/c.java

邮箱线索

邮箱地址	所在文件
null@null.xml	j/q/a/k/b.java
tt01@2x.png	com/miliaoapp/live/im/e.java

☰ 手机线索

手机号	所在文件
17179869184	tvt/ijk/media/player/IjkMediaMeta.java
17179869184	com/faceunity/wrapper/faceunity.java
15060355040	com/unionpay/UPPayAssistEx.java
17179869184	tv/danmaku/ijk/media/player/i.java

☀ 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: CN=hxm

签名算法: rsassa_pkcs1v15

有效期自: 2021-07-26 02:17:14+00:00

有效期至: 2046-07-20 02:17:14+00:00

发行人: CN=hxm

序列号: 0x61efcb33

哈希算法: sha256

md5值: 67d620f50f63ffba7239fcbc9165cd8

sha1值: 0faa9fc743304c6676865afb39c411d8550f118d

sha256值: 4b24b53735803e804604dcce3ce07b940c7fe3c2125feecfd55647e87d7e3a69

sha512值: 8e2216399122aa098b52dc1079a98a1fa7e2b01acc49635013ba0bc8a2b608e981d0c7919a74c01334bef1ad0753327330132accd3aa9c79eb546af4bc538742

公钥算法: rsa

密钥长度: 2048

指纹: 21c44a2f642034ea4420270056e33264507ca753fe6b0cbc35fef197af4c8ebc

硬编码敏感信息

可能的敏感信息
"account_password" : "账号密码登录"
"active_user" : "活跃用户:"
"chat_user" : "叶友:"
"forget_password" : "忘记密码?"
"input_password" : "输入密码"
"need_independent_password" : "启动未成年模式,需要设置独立密码"
"online_user" : "当前在线用户: 5562次"
"password" : "密 码:"
"phone_private" : "私密(不公开)"
"please_input_active_user" : "请输入您的活跃用户"
"please_input_long_password" : "密码长度不够"
"please_input_password" : "请输入密码"
"private_agree" : " 《隐私协议》 "
"private_chat_switch" : "私信聊天"
"private_detail" : "隐私协议"

"private_image" : "私密照片"
"private_video" : "私密视频"
"see_user" : "观众"
"swtich_off_alert_private" : "关闭后你将收不到私聊消息"
"token_invalid" : "登录失效，请重新登录"
"user_secret" : "用户隐私政策"
"verify_password" : "验证密码"
"wrong_password" : "密码不正确,请重新输入"

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.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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
com.miliaoapp.live.permission.JPUSH_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。
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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.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_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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent101://,