MoGua

91porn null.APK 分析报告

APP名称: 91porn

包名:	cktaskw.abobgqa.dvqzgkqj
域名线索:	51条
URL线索:	37条
邮箱线索:	0条
分析日期:	2025年4月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 91porn v1.0.1.apk
文件大小: 23.74MB
MD5值: ecccede9d6e97f080154e8563fecb82c
SHA1值: 9b9822400ad981c47ff58fe7a6235dc08e18d658
SHA256值: 14dba8cd0b7304857d5d4a2201c5d03c312cb632f64ed7fce4d88f9f0796aa11

APP 信息

App名称: 91porn
包名: cktaskw.abobgqa.dvqzgkqj
主活动Activity: com.fuerdai.tiktok.activity.SplashActivity
安卓版本名称: null
安卓版本:

域名线索

域名	服务器信息
greenrobot.org	**IP**: 85.13.163.69 **所属国家**: Germany **地区**: Thuringen **城市**: Friedersdorf **纬度**: 50.604919 **经度**: 11.035770
rtt2.map.qq.com	**IP**: 109.244.173.174 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
apikey.map.qq.com	**IP**: 109.244.173.174 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397232
api.scyfnq.com	IP: 54.193.54.180 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
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
raw.githubusercontent.com	IP: 185.199.109.133 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
mobilegw.stable.alipay.net	没有服务器地理信息.
render.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
cmnsguider.yunos.com	IP: 203.119.169.246 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

alogsus.umeng.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
plbslog.umeng.com	**IP**: 36.156.202.78 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
h5.m.taobao.com	**IP**: 220.181.135.168 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mobilegw.aaa.alipay.net	没有服务器地理信息.
pr.map.qq.com	**IP**: 109.244.173.174 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
open.weixin.qq.com	**IP**: 109.244.144.48 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 122.9.9.94

bjuser.jpush.cn	**所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
m3.map.gtimg.com	IP: 220.194.122.47 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
p2.map.gtimg.com	IP: 60.28.220.78 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
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
s1.map.gtimg.com	IP: 221.204.43.82 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280
loggw-exsdk.alipay.com	IP: 110.76.6.71 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650

	经度: 120.161423
alogus.umeng.com	IP: 223.109.148.178 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mcgw.alipay.com	IP: 124.239.239.236 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
ulogs.umengcloud.com	IP: 223.109.148.130 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
apis.map.qq.com	IP: 109.244.244.223 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
m1.map.gtimg.com	IP: 220.194.123.57 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666

developer.umeng.com	**IP**: 59.82.31.160 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
p0.map.gtimg.com	**IP**: 116.136.171.223 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
wappaygw.alipay.com	**IP**: 124.239.239.236 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
m.alipay.com	**IP**: 203.209.245.120 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
s0.map.gtimg.com	**IP**: 221.204.20.230 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280
tsis.jpush.cn	**IP**: 120.46.154.158 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671

	经度: 113.250000
ouplog.umeng.com	IP: 47.246.110.94 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
s2.map.gtimg.com	IP: 119.167.223.60 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
confinfo.map.qq.com	IP: 109.244.173.174 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
s3.map.gtimg.com	IP: 221.204.20.230 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280
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
	IP: 120.233.50.108 **所属国家**: China

ce3e75d5.jpush.cn	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
m2.map.gtimg.com	**IP**: 220.194.123.57 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
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
mobilegw.alipay.com	**IP**: 203.209.247.65 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
rtt2c.map.qq.com	**IP**: 175.27.9.21 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
rtt2b.map.qq.com	**IP**: 109.244.173.174 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

p3.map.gtimg.com	IP: 221.204.43.107 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280
p1.map.gtimg.com	IP: 60.28.220.78 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
rtt2a.map.qq.com	IP: 175.27.9.21 **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.
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
m0.map.gtimg.com	IP: 220.194.122.136 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
	IP: 223.109.148.178 **所属国家**: China

ulogs.umeng.com	**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://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/L-JINBIN/ApkSignatureKillerEx	bin/mt/signature/KillerApplication.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/aj/d.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/ai/b.java
http://182.92.20.189:9099/	cn/jiguang/r/a.java

https://tsis.jpush.cn	cn/jiguang/ao/i.java
https://api.scyfnq.com/index.php	com/tinstall/tinstall/TInstall.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java

http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.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
https://apis.map.qq.com/ws/geocoder/v1/	com/fuerdai/tiktok/dagger/http/server/Apis.java
http://schemas.android.com/apk/res/android	com/kun/brother/base/widget/SmsCodeInputWidget.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.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
https://apikey.map.qq.com/mkey/index.php/mkey/check?	com/tencent/mapsdk/rastercore/a.java
https://confinfo.map.qq.com/confinfo?apikey=	com/tencent/mapsdk/rastercore/d.java
https://pr.map.qq.com/pingd?	com/tencent/mapsdk/rastercore/d/e.java
https://m0.map.gtimg.com/hwap	com/tencent/mapsdk/rastercore/tile/b/e.java
https://m1.map.gtimg.com/hwap	com/tencent/mapsdk/rastercore/tile/b/e.java
https://m2.map.gtimg.com/hwap	com/tencent/mapsdk/rastercore/tile/b/e.java
https://m3.map.gtimg.com/hwap	com/tencent/mapsdk/rastercore/tile/b/e.java
https://s0.map.gtimg.com/oversea	com/tencent/mapsdk/rastercore/tile/b/b.java
https://s1.map.gtimg.com/oversea	com/tencent/mapsdk/rastercore/tile/b/b.java
https://s2.map.gtimg.com/oversea	com/tencent/mapsdk/rastercore/tile/b/b.java
https://s3.map.gtimg.com/oversea	com/tencent/mapsdk/rastercore/tile/b/b.java
https://p0.map.gtimg.com/sateTiles	com/tencent/mapsdk/rastercore/tile/b/d.java
https://p1.map.gtimg.com/sateTiles	com/tencent/mapsdk/rastercore/tile/b/d.java
https://p2.map.gtimg.com/sateTiles	com/tencent/mapsdk/rastercore/tile/b/d.java
https://p3.map.gtimg.com/sateTiles	com/tencent/mapsdk/rastercore/tile/b/d.java
https://rtt2.map.qq.com	com/tencent/mapsdk/rastercore/tile/b/f.java
https://rtt2a.map.qq.com	com/tencent/mapsdk/rastercore/tile/b/f.java

https://rtt2b.map.qq.com	com/tencent/mapsdk/rastercore/tile/b/f.java
https://rtt2c.map.qq.com	com/tencent/mapsdk/rastercore/tile/b/f.java
https://github.com/vinc3m1	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView.git	Mogua Engine V1
https://raw.githubusercontent.com/tdopops/dsp/main/live/cjbjiu1.json	Mogua Engine V1
https://raw.githubusercontent.com/tdopops/91porn/main/uat/91porn.json	Mogua Engine V1

邮箱线索

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
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"search_user" : "用户搜索"

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.NETWORK_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。
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.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.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.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.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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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

应用内通信