MoGua

抖阴 7.1.2.APK 分析报告

APP名称:	抖阴

包名:	com.tiktok.dy20250310
域名线索:	35条
URL线索:	28条
邮箱线索:	1条
分析日期:	2025年4月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: douyin_zjdy7046_7.1.2.apk
文件大小: 17.85MB
MD5值: 246525407278d2c32be8e9db3837741c
SHA1值: 5d5f32bf9c90190d32e61fccbd2ab55242c9993d
SHA256值: 934e5541a299db8df96d7403db2f87d31c7411045ceda0c8316b5fe0f2625e65

APP 信息

App名称: 抖阴
包名: com.tiktok.dy20250310
主活动Activity: com.niming.weipa.ui.splash.SplashActivity
安卓版本名称: 7.1.2
安卓版本: 1

域名线索

域名	服务器信息
ddos26.4dmsexybg.com	**IP**: 172.67.200.73 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
pagead2.googlesyndication.com	**IP**: 114.250.69.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mcgw.alipay.com	**IP**: 123.125.216.191 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
mclient.alipay.com	**IP**: 116.136.165.42 **所属国家**: China **地区**: Nei Mongol **城市**: Hohhot **纬度**: 40.810650 **经度**: 111.650665
wappaygw.alipay.com	**IP**: 123.125.216.191 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.qq.com	**IP**: 221.198.70.47 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
ddosbak.p2jgys50gvb.com	**IP**: 104.21.19.176 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
bk123.x32rv8mm4.com	没有服务器地理信息.

bk123.ji9karm0m.com	没有服务器地理信息.
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
app.dylite.ipx.mx	没有服务器地理信息.
bak.dyfa3xmzzvd6ewigf7ywz79uf.com	没有服务器地理信息.
playready.directtaps.net	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
h5.m.taobao.com	**IP**: 125.38.11.131 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
app.8dy.me	**IP**: 157.240.7.8 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
	IP: 203.209.245.120 **所属国家**: China **地区**: Zhejiang

m.alipay.com	**城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
api.telegram.org	**IP**: 88.191.249.182 **所属国家**: France **地区**: Ile-de-France **城市**: Paris **纬度**: 48.859077 **经度**: 2.293486
schemas.android.com	没有服务器地理信息.
mobilegw.alipay.com	**IP**: 203.209.250.8 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
render.alipay.com	**IP**: 122.156.129.94 **所属国家**: China **地区**: Heilongjiang **城市**: Heihe **纬度**: 50.266670 **经度**: 127.466667
bk123.5k8zbwod0.com	没有服务器地理信息.
bak.uogx0xftbl.com	**IP**: 104.21.48.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 85.13.163.69 **所属国家**: Germany

greenrobot.org	**地区**: Thuringen **城市**: Friedersdorf **纬度**: 50.604919 **经度**: 11.035770
schemas.microsoft.com	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
mobilegw.aaa.alipay.net	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**: 120.161583
bak.dy4bzju8p2tzhhmaf9sc95qpj.com	没有服务器地理信息.
bak.wtk5y8b2jo.com	**IP**: 104.21.22.221 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
bk123.ec8r200g7.com	没有服务器地理信息.
mobilegw.stable.alipay.net	没有服务器地理信息.
loggw-exsdk.alipay.com	**IP**: 119.42.231.4 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650

	经度: 120.161583
api.buzhidaoxiesha.com	没有服务器地理信息.
tmapi.tmsangewg.com	没有服务器地理信息.
mobilegw-1-64.test.alipay.net	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	c/c/a/a/b/a/b.java
https://mobilegw.alipay.com/mgw.htm	c/a/b/c/a.java
https://mobilegw.alipaydev.com/mgw.htm	c/a/b/c/a.java
https://mcgw.alipay.com/sdklog.do	c/a/b/c/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	c/a/b/c/a.java
http://m.alipay.com/?action=h5quit	c/a/b/c/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	c/a/b/c/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	c/a/b/c/a.java
https://h5.m.taobao.com/mlapp/olist.html	c/a/b/d/a.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://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
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/k.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/k.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/k.java
http://%s:%d/%s	com/danikula/videocache/m.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/m.java

http://%s:%d/%s	com/danikula/videocache/i.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/liulishuo/filedownloader/services/a.java
http://app.dylite.ipx.mx	com/niming/weipa/c.java
http://app.8dy.me	com/niming/weipa/c.java
http://tmapi.tmsangewg.com/cxapi/	com/niming/weipa/newnet/NetConfig.java
http://api.buzhidaoxiesha.com/cxapi/	com/niming/weipa/utils/v.java
http://api.	com/niming/weipa/utils/m0.java
https://ddos26.4dmsexybg.com/mmapi/	com/niming/weipa/utils/m0.java
https://bk123.5k8zbwod0.com/mmapi/	com/niming/weipa/utils/m0.java
https://bk123.ec8r200g7.com/mmapi/	com/niming/weipa/utils/m0.java
https://bk123.ji9karm0m.com/mmapi/	com/niming/weipa/utils/m0.java
https://bk123.x32rv8mm4.com/mmapi/	com/niming/weipa/utils/m0.java
http://app.8dy.me	com/niming/weipa/utils/y.java
http://www.qq.com	com/niming/weipa/utils/n0.java

https://api.telegram.org/bot6086117813:AAFwiL2Rn_qZbWa_a6DkegGeAx1glJorQzA/sendMessage	com/niming/weipa/utils/d0.java
http://www.qq.com	com/niming/weipa/f/b.java
http://app.8dy.me	com/niming/weipa/base/BaseActivity.java
http://ddosbak.p2jgys50gvb.com	com/niming/weipa/g/c.java
http://bak.uogx0xftbl.com	com/niming/weipa/g/c.java
http://bak.wtk5y8b2jo.com	com/niming/weipa/g/c.java
http://bak.dyfa3xmzzvd6ewigf7ywz79uf.com	com/niming/weipa/g/c.java
http://bak.dy4bzju8p2tzhhmaf9sc95qpj.com	com/niming/weipa/g/c.java
http://app.dylite.ipx.mx	com/niming/weipa/g/c.java
https://api.telegram.org/bot743083118:AAFcQa9POAvUhMcS2_AGFR6BKBf_nj_vGbE/sendMessage	com/niming/weipa/g/b.java
https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/c/b.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/c/b.java

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/k.java

手机线索

手机号	所在文件
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: True
找到 1 个唯一证书
主题: CN=Jhon, OU=a, O=b, L=c, ST=d, C=e
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-10 09:17:13+00:00
有效期至: 2050-03-04 09:17:13+00:00
发行人: CN=Jhon, OU=a, O=b, L=c, ST=d, C=e
序列号: 0x1
哈希算法: sha256
md5值: 1effc92ac5458c5e2f6643b76beccbec
sha1值: 8aced0e8a1c198a9c2c5208564a242a400845c5f
sha256值: 4b6ad83c985a314cfbcaa685c886fb64e9411a108b0cae4fc1f403e3c996c2c2
sha512值: fc0a991ba254b4063afc6b1e35f5feaa700fa9c0f3ef3a2b7091e361a2cfca17c39dad89a7906336009c19bff098235d883c54d7281e714faf1a5be3801a7478
公钥算法: rsa
密钥长度: 2048
指纹: 9a0bef210040e1772d058c2d718174ba002fd5439b68597cd1adf5027bebe746

硬编码敏感信息

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.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
com.qti.permission.PROFILER	未知	Unknown permission	Unknown permission from android reference
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_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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
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。
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.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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

应用内通信
