



抖漫 1.3.APK 分析报告



APP名称:

抖漫

包名:	com.qnmd.adm.cb02ts
域名线索:	25条
URL线索:	24条
邮箱线索:	2条
分析日期:	2025年9月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 抖漫.apk

文件大小: 21.25MB

MD5值: 1e533f7b2fadc6d3847fcec963b8a538

SHA1值: 237efb0d5cf8a80b988ff1702f87fe3512c8c446
SHA256值: db11828683b7a956df5344a5d4eb4df52e2f721689ecf544746284abfa62aef1

i APP 信息

App名称: 抖漫
包名: com.qnmd.adm.cb02ts
主活动Activity: com.jbzd.media.movecartoons.ui.splash.SplashActivity
安卓版本名称: 1.3
安卓版本: 12

🔍 域名线索

域名	服务器信息
wappaygw.alipay.com	IP: 111.202.5.210 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
schemas.android.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.
api.8kfzsu8vos.com	IP: 13.33.88.80 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
	IP: 203.209.243.98 所属国家: China 地区: Zhejiang

mobilegw.alipay.com	城市: Hangzhou 纬度: 30.293650 经度: 120.161583
douman.net	IP: 13.35.202.8 所属国家: India 地区: Telangana 城市: Hyderabad 纬度: 17.375290 经度: 78.474388
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
dashif.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
api.9bd8imhg53.com	IP: 13.33.88.103 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
api.pbmazltwbn.com	IP: 13.33.88.80 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
	IP: 116.142.235.203 所属国家: China

mclient.alipay.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
h5.m.taobao.com	IP: 125.39.135.147 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.khs3mg0xvp.com	IP: 13.33.88.99 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
schemas.microsoft.com	IP: 13.107.253.49 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
api.telegram.org	IP: 199.16.158.190 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
api.dc93i0tkfh.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
mobilegw.aaa.alipay.net	没有服务器地理信息.
playready.directtaps.net	IP: 13.107.253.39 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
mobilegw.stable.alipay.net	没有服务器地理信息.
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: 120.161583
api.gnwtldgm7h.com	没有服务器地理信息.
mcgw.alipay.com	IP: 111.202.5.210 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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: 120.161583

URL线索

URL信息	Url所在文件
https://api.telegram.org/bot6086117813:AAFwiL2Rn_qZbWa_a6DkegGeAx1glJorQzA/sendMessage	b/a/a/a/i.java
http://api.gnwtldgm7h.com/mhapi/	b/a/a/a/r/i.java
http://api.dc93i0tkfh.com/mhapi/	b/a/a/a/r/i.java
http://api.pbmazltwbn.com/mhapi/	b/a/a/a/r/i.java
http://api.khs3mg0xvp.com/mhapi/	b/a/a/a/r/i.java
http://api.8kfzsu8vos.com/mhapi/	b/a/a/a/r/i.java
http://api.9bd8imhg53.com/mhapi/	b/a/a/a/r/i.java
http://m.alipay.com/?action=h5quit	b/c/b/j/h.java
https://h5.m.taobao.com/mlapp/olist.html	b/c/b/c/a.java
https://mobilegw.alipay.com/mgw.htm	b/c/b/c/d.java
https://mobilegw.alipay.com/mgw.htm	b/c/b/f/c.java
https://mcgw.alipay.com/sdklog.do	b/c/b/f/d/c.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	b/c/b/f/d/d.java
http://dashif.org/guidelines/last-segment-number	b/l/a/a/k1/l0/k/c.java
http://schemas.android.com/apk/res/android	b/l/a/a/p1/n.java
https://github.com/danikula/AndroidVideoCache/issues/88	b/h/a/i.java

https://github.com/danikula/AndroidVideoCache/issues/43.	b/h/a/i.java
https://github.com/danikula/AndroidVideoCache/issues.	b/h/a/i.java
http://%s:%d/%s	b/h/a/l.java
http://%s:%d/%s	b/h/a/g.java
https://github.com/danikula/AndroidVideoCache/issues/134.	b/h/a/g.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://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.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://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
http://api.	com/jbzd/media/movecartoons/ui/splash/SplashViewMode.java
https://douman.net	com/jbzd/media/movecartoons/ui/splash/SplashActivity.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	g/b/a/c/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	g/b/a/c/d.java
http://xml.apache.org/xslt	d/a/a/b/a/m.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

邮箱线索

邮箱地址	所在文件
sagjcm886@gmail.com	b/a/a/a/h.java
danikula@gmail.com	b/h/a/i.java

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: False
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-18 20:00:29+00:00
有效期至: 2052-10-03 20:00:29+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x52ca32b2
哈希算法: sha256
md5值: 13f58b880982e6ea99e19692eda73698
sha1值: 3a7d9e417257d3f209fef682bf2c19179fe14e6c
sha256值: 0704048e2d95fc5be7e31c983669012188b919da0d4e3c91a6b36cbf3645b7b9
sha512值: 40ee66737d6d1351ca8bb0d5072aeb606870bba51b0009c85a3fb82fc2fb2516294c44572a6dd70e60785bc600423c5c514ff7b591507c4704391fad7191aa3a
公钥算法: rsa
密钥长度: 2048
指纹: 043ee57267b0653663af42cd634378bde00f4b23204b4e85ce6c0825be55a402

🔑 硬编码敏感信息

可能的敏感信息
"account_certificate" : "账号凭证"
"account_credentials" : "账号凭证"
"credentials_notice_tips" : "1. 请您保存二维码凭证，以便找回您的账号 2. 请妥善保管此账号凭证，不要随意透露给任何人 3. 若此账号不慎丢失，可通过app账号安全扫取该二维码凭证账

号登录"
"credentials_tips": "请到设置—找回账号—账号凭证找回或者扫描凭证"
"merchant_credentials_tips": "支付小贴士 1、跳转后请及时付款，超时支付无法到账，要重新发起。 2、每天发起支付不能超过5次，连续发起且未支付，账号可能被加入黑名单"
"mine_account_credentials": "账号凭证"
"scan_credentials": "扫描二维码"
"upload_credentials": "从相册选择"

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.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.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.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.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.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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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。

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。