MoGua

抖阴漫画 1.3.APK 分析报告

APP名称: 抖阴漫画

包名:	dymh-tdymh668.apk
域名线索:	24条
URL线索:	24条
邮箱线索:	4条
分析日期:	2025年5月14日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: dymh-tdymh668.apk
文件大小: 14.69MB
MD5值: a94eb6367050e2c9f7204aa94dc507ff
SHA1值: 6a089f2b2e9991097f3f56a15b14ff29d92dfb7f
SHA256值: 4f0ae6bc161e54e345e47c3e615f83ae0e21695bc448c4ce72e0c8ca98b7af62

APP 信息

App名称: 抖阴漫画
包名: dymh-tdymh668.apk
主活动Activity: []
安卓版本名称: 1.3
安卓版本: 1

域名线索

域名	服务器信息
api-dymh.kicfoakjvf.com	**IP**: 104.21.50.212 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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
api.dymh0geq4v1u.com	**IP**: 8.218.16.26 **所属国家**: Hong Kong **地区**: Hong Kong

	城市: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
dashif.org	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
h5.m.taobao.com	**IP**: 220.181.135.167 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ns.adobe.com	没有服务器地理信息.
loggw-exsdk.alipay.com	**IP**: 110.76.3.1 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
playready.directtaps.net	**IP**: 104.45.231.79 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
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
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
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
schemas.android.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
api.dymhcyklr90m.com	IP: 8.218.16.26 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
mobilegw.aaa.alipay.net	没有服务器地理信息.
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
	IP: 203.209.255.238 **所属国家**: China **地区**: Zhejiang

mobilegw.alipay.com	**城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
api-dymh.sljghdlqpa.com	IP: 172.67.193.117 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.dymhszgt59qz.com	IP: 8.218.16.26 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
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
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**: 120.161583
mobilegw.stable.alipay.net	没有服务器地理信息.
api.dymh3oj510di.com	IP: 8.218.16.26 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521

	经度: 114.157692
api.dymh4fnkozsr.com	**IP**: 8.218.16.26 **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://m.alipay.com/?action=h5quit	v2/g.java
http://api-dymh.sljghdlqpa.com/cxapi	r8/k.java
http://api-dymh.kicfoakjvf.com/cxapi	r8/k.java
http://api.dymh3oj510di.com/cxapi	r8/k.java
http://api.dymhcyklr90m.com/cxapi	r8/k.java
http://api.dymh4fnkozsr.com/cxapi	r8/k.java
http://api.dymh0geq4v1u.com/cxapi	r8/k.java
http://api.dymhszgt59qz.com/cxapi	r8/k.java
https://h5.m.taobao.com/mlapp/olist.html	n2/a.java
https://mobilegw.alipay.com/mgw.htm	n2/d.java

http://www.w3.org/ns/ttml	l6/a.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	jb/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	jb/d.java
http://dashif.org/guidelines/last-segment-number	b6/c.java
http://ns.adobe.com/xap/1.0/\u0000	r0/a.java
http://schemas.android.com/apk/res/android	g0/h.java
https://github.com/danikula/AndroidVideoCache/issues/43.	m4/h.java
https://github.com/danikula/AndroidVideoCache/issues.	m4/h.java
https://github.com/danikula/AndroidVideoCache/issues/88.	m4/h.java
http://%s:%d/%s	m4/k.java
http://%s:%d/%s	m4/f.java
https://github.com/danikula/AndroidVideoCache/issues/134.	m4/f.java
https://mobilegw.alipay.com/mgw.htm	q2/c.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/ShitTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.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
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://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
https://mcgw.alipay.com/sdklog.do	r2/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	r2/c.java

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	m4/h.java
this@videodetailactivity.id	z9/c.java
this@videodetailactivity.id	z9/d.java
dymhv555@outlook.com	v8/b.java

手机线索

手机号	所在文件
15222222222	com/alipay/apmobilesecuritysdk/d/c.java
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: 2023-08-22 04:05:02+00:00
有效期至: 2051-01-07 04:05:02+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x3cbb5387
哈希算法: sha256
md5值: 22543e0df300442fa1a733e94826e28c
sha1值: 9a230fcd65311e8f81c0fe8de8254cbde4f23a1f
sha256值: 38f19c14025afa633117d746034be5c259df432e3569768c32c5b2a153d52b3e
sha512值: 7f6e462b76d8f98af7913ccfcc39465e5715684978acdc677ae87c1bf94d11ce2fb4177ceaacfed933a37fac4e0c5bcfcb9f79e5f08beaf679faafe25600a637
公钥算法: rsa
密钥长度: 2048
指纹: 4f23ca4fc220892c33c9ab3313bd67521ceaa75ca6828533b39cfec3e74e8e1e

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.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.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