MoGua

妖精动漫 2.07.APK 分析报告

APP名称:	妖精动漫

包名:	com.mh.cartoon.yjdma
域名线索:	20条
URL线索:	21条
邮箱线索:	1条
分析日期:	2025年7月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: yjdm_zwmog1yjmh_2.07.apk
文件大小: 21.7MB
MD5值: deaba988318a31e9035fce83385fb3e9

SHA1值: 89d9a0a3ef6ae2c948f1c64dd741aa062da09444
SHA256值: 723d5882e16e85716f392fb47495414bfb5ee6a5c91dacd650760364ad977e4a

APP 信息

App名称: 妖精动漫
包名: com.mh.cartoon.yjdma
主活动Activity: com.jbzd.media.yjdm.ui.splash.SplashActivity
安卓版本名称: 2.07
安卓版本: 207

域名线索

域名	服务器信息
schemas.microsoft.com	**IP**: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
mcgw.alipay.com	**IP**: 116.142.245.206 **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
schemas.android.com	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
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
mobilegw.stable.alipay.net	没有服务器地理信息.
wappaygw.alipay.com	**IP**: 116.142.245.205 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
tmapi.tmsangewg.com	没有服务器地理信息.
mobilegw.alipay.com	**IP**: 203.209.250.2 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
mclient.alipay.com	**IP**: 116.142.245.227 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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.
h5.m.taobao.com	**IP**: 221.194.162.215 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
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
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
	IP: 157.240.7.8 **所属国家**: Singapore

api.telegram.org	**地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
api.buzhidaoxiesha.com	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**
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://m.alipay.com/?action=h5quit	g/a/b/j/h.java
https://h5.m.taobao.com/mlapp/olist.html	g/a/b/c/a.java
https://mobilegw.alipay.com/mgw.htm	g/a/b/c/d.java
https://mobilegw.alipay.com/mgw.htm	g/a/b/f/c.java
https://mcgw.alipay.com/sdklog.do	g/a/b/f/d/c.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	g/a/b/f/d/d.java
https://github.com/danikula/AndroidVideoCache/issues/88.	g/f/a/i.java
https://github.com/danikula/AndroidVideoCache/issues/43.	g/f/a/i.java
https://github.com/danikula/AndroidVideoCache/issues.	g/f/a/i.java
http://%s:%d/%s	g/f/a/l.java
http://%s:%d/%s	g/f/a/g.java
https://github.com/danikula/AndroidVideoCache/issues/134.	g/f/a/g.java
http://dashif.org/guidelines/last-segment-number	g/j/a/a/k1/l0/k/c.java

https://api.telegram.org/bot6086117813:AAFwiL2Rn_qZbWa_a6DkegGeAx1gIJorQzA/sendMessage	g/o/a/a/g.java
http://api.buzhidaoxiesha.com/cxapi/	g/o/a/a/q/m.java
http://tmapi.tmsangewg.com/cxapi/	g/o/a/a/q/m.java
http://xml.apache.org/xslt	e/a/a/b/a/m.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	i/b/a/c/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	i/b/a/c/d.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
danikula@gmail.com	g/f/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: True
找到 1 个唯一证书
主题: CN=yjmanhua, OU=yjmanhua, O=yjmanhua, L=yjmanhua, ST=yjmanhua, C=yjmanhua
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-31 07:11:48+00:00
有效期至: 2049-10-25 07:11:48+00:00
发行人: CN=yjmanhua, OU=yjmanhua, O=yjmanhua, L=yjmanhua, ST=yjmanhua, C=yjmanhua
序列号: 0x1
哈希算法: sha256
md5值: 7af2dca6f13c246a3f58dbe85a239a87
sha1值: 687a1141ec5a26c746e3391180904670eb7726c3
sha256值: e0c5040745b4b29be2a60d3d441c8d47a46656422581e5944b2ff58da082348c
sha512值: 13043fff637403fb40bd97d74854965750b020832e602789c4443c60d5e8ada2ca8f17eea0fd9c0a43473361dced13c4b76962be08be9a7927a68604510dabca
公钥算法: rsa
密钥长度: 2048
指纹: 7c6e5932627dddccf02da32f75bdc7fb7e59ea426f8e2200e66d90bd4896e8ff

🔑 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
		读取/修改/删除外	

android.permission.WRITE_EXTERNAL_STORAGE	危险	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