



MoGua

动漫之家 2.02.APK 分析报告



APP名称:

动漫之家

包名:	com.qnmd.admzj.vs02ez
域名线索:	24条
URL线索:	22条
邮箱线索:	1条
分析日期:	2025年8月14日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 动漫之家.apk

文件大小: 24.13MB

MD5值: 2124a24daebdfa7dd81b56952f17a62e

SHA1值: 34cf75c2778f67dcb8060d7da68f43bf58ea9951
SHA256值: 2f7483ccd03dda2ca6072ca47ba6d316f392a3df489c27cbdd96f3ba4b807fe0

i APP 信息

App名称: 动漫之家
包名: com.qnmd.admzj.vs02ez
主活动Activity: com.jbzd.media.movecartoons.ui.splash.SplashActivity
安卓版本名称: 2.02
安卓版本: 202

🔍 域名线索

域名	服务器信息
api.05gsw5mz0z.com	IP: 3.165.39.28 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
schemas.android.com	没有服务器地理信息.
mcgw.alipay.com	IP: 218.61.165.219 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
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.telegram.org	IP: 108.160.165.189 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.axbly1sq8d.com	IP: 3.165.39.110 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
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
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
wappaygw.alipay.com	IP: 218.61.165.219 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
mobilegw.aaa.alipay.net	没有服务器地理信息.
api.xjyu06sesk.com	没有服务器地理信息.

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
api.voasivxqkz.com	IP: 3.165.39.110 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
api.2ujeptnmvz.com	IP: 3.165.39.28 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
mobilegw.stable.alipay.net	没有服务器地理信息.
mclient.alipay.com	IP: 116.136.185.217 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
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
	IP: 203.209.250.8 所属国家: China

mobilegw.alipay.com	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
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
api.8unb0gub0z.com	没有服务器地理信息.
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
h5.m.taobao.com	IP: 125.38.11.130 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102

 URL线索

URL信息	Url所在文件
-------	---------

https://api.telegram.org/bot6086117813:AAFwiL2Rn_qZbWa_a6DkegGeAx1glJorQzA/sendMessage	b/a/a/a/h.java
http://api.8unb0gub0z.com/mhapi/	b/a/a/a/q/i.java
http://api.xjyu06sesk.com/mhapi/	b/a/a/a/q/i.java
http://api.2ujeptnmvz.com/mhapi/	b/a/a/a/q/i.java
http://api.voasivxqkz.com/mhapi/	b/a/a/a/q/i.java
http://api.axbly1sq8d.com/mhapi/	b/a/a/a/q/i.java
http://api.05gsw5mz0z.com/mhapi/	b/a/a/a/q/i.java
http://api.2ujeptnmvz.com/mhapi/	b/a/a/a/q/m/c.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://loggw-exsdk.alipay.com/loggw/logUpload.do	b/c/b/f/d/d.java
https://mcgw.alipay.com/sdklog.do	b/c/b/f/d/c.java
https://github.com/danikula/AndroidVideoCache/issues/88.	b/g/a/i.java
https://github.com/danikula/AndroidVideoCache/issues/43.	b/g/a/i.java
https://github.com/danikula/AndroidVideoCache/issues.	b/g/a/i.java
http://%s:%d/%s	b/g/a/l.java

http://%s:%d/%s	b/g/a/g.java
https://github.com/danikula/AndroidVideoCache/issues/134.	b/g/a/g.java
http://dashif.org/guidelines/last-segment-number	b/k/a/a/k1/l0/k/c.java
http://xml.apache.org/xslt	b/e/a/b/e.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
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://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	b/g/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: 2024-09-09 20:00:03+00:00
有效期至: 2052-01-26 20:00:03+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x5ccea214
哈希算法: sha256
md5值: 500fc3e0af5f0f82f5b55e89ae451676
sha1值: 9b8e6c86bb32072ebba8d8345284ce1192509a46
sha256值: d7ded58a91aea752025a473c4528595f67a2b65a0ce93c580ab4d4a43c5b4eef
sha512值: ec05fe9e10563f1d9b8d2f2fa2037aee436fcad7caec9c534b7a635eeae5aebafb1afb1d00fa707c6e0ebb2f7653a5d7b214a2324da27f4cb7931adcdc8d3533
公钥算法: rsa
密钥长度: 2048
指纹: cd1e57fee5bc49e459f740f80d9ccd1cd035440811d0a60508f99ee64f7ef41e

 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，重复扫码，修改金额均无法到账。 2、付款后没有到账，请保存好付款截图，联系在线客服处理。 3、支付通道在夜间比较忙碌，为保证您的付款体验，您可以尽量选择白天支付，晚上观看，谢谢您的理解。"
"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