



MoGua

妖精动漫 1.1.7.APK 分析报告



APP名称:

妖精动漫

包名: com.yjdm.shell.sign_1_1_7

域名线索: 12条

URL线索: 5条

邮箱线索: 1条

分析日期: 2025年6月15日

分析平台: [摸瓜APK反编译平台](#)

文件名: yjdm_1.1.7.apk
文件大小: 24.78MB
MD5值: 579f022c80578ac5cb0e1b78dc15326f
SHA1值: e03746e36db686d2413d302a8b48fee217a804d4
SHA256值: 8412fd9d15ce30d191505f905c41baba99878f5213c5a154c00c2359e157999b

i APP 信息

App名称: 妖精动漫
包名: com.yjdm.shell.sign_1_1_7
主活动Activity: com.yjdm.shell.MainActivity
安卓版本名称: 1.1.7
安卓版本: 22

🔍 域名线索

域名	服务器信息
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
123.56.28.222	IP: 123.56.28.222 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri

	城市: Kansas City 纬度: 39.099731 经度: -94.578568
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
m2uj1.cc	IP: 149.30.245.79 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
wx1k0.cc	IP: 172.67.189.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.jsdelivr.com	IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 154.197.19.116

is5x9.cc	所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
cdn.mxpnl.com	IP: 130.211.5.208 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590

 URL线索

URL信息	Url所在文件
https://cdn.mxpnl.com/libs/mixpanel-2-latest.min.js	Mogua Engine V2
https://www.jsdelivr.com/using-sri-with-dynamic-files	Mogua Engine V2

https://github.com/apvarun/toastify-js	Mogua Engine V2
https://github.com/richtr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	Mogua Engine V2
http://www.w3.org/XML/1998/namespace	lib/armeabi-v7a/libflutter.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/ .	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues .	lib/armeabi-v7a/libflutter.so
https://m2uj1.cc	lib/armeabi-v7a/libapp.so
https://wx1k0.cc	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
https://is5x9.cc	lib/armeabi-v7a/libapp.so
https://t.me/yaojingdm1	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
http://123.56.28.222:1111/yjdm	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android .	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new .	lib/armeabi-v7a/libapp.so

邮箱地址	所在文件
_double@0150898.fromintege _growablelist@0150898._literal _casterror@0150898._create _typeerror@0150898._create _bytebuffer@7027147._new _assertionerror@0150898._create	lib/armeabi-v7a/libapp.so

手机线索

✿ 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: C='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国'

签名算法: rsassa pkcs1v15

有效期自: 2023-10-18 15:30:00+00:00

有效期至: 2033-10-15 15:30:00+00:00

发行人: C='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国'

序列号: 0x2c78606b

哈希算法: sha256

md5值: 932861b41ceccfb935a7df98b81cb0e2

sha1值: fc5a64f2394dbcfbee1e817e1a1627039edabf96

sha256值: f63e38fef8b71c48d74fbcdb45e44cfc581a5b9eb1aa7380f3b472211c5f287d

sha512值: 995647f4a2a0f3c459d787030be887dd85ef7508ea8940dcd0a8c14f9ce617163dce868593296ea1618cb8bd8d129b576f23bc359250350fa1ecc420c202f103

公钥算法: rsa

密钥长度: 2048

指纹: 9802c2e4ea3ef8104903a600c6985cdd182de14a6092de79148cc28bdd823572

硬编码敏感信息

可能的敏感信息
"google_api_key" : "AlzaSyCQUAqLRqaulgOtizmF_95ywtG2TbEM2ml"
"google_crash_reporting_api_key" : "AlzaSyCQUAqLRqaulgOtizmF_95ywtG2TbEM2ml"

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.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.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_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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

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
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
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

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。