MoGua

金魁花 2.0.APK 分析报告

APP名称:	金魁花

包名:	wrwtr.fdmbxvydzs.ajdtpr
域名线索:	4条
URL线索:	4条
邮箱线索:	0条
分析日期:	2025年8月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: jkh-1754227695459.apk
文件大小: 2.74MB
MD5值: 373769b1fe401626a37b138803f833d9
SHA1值: 66129dd69e5246ad94e0ce2d2bc437fe5907e3b8
SHA256值: 4b29abae8fbe3b57bfb260dd414655ec64b7d887d98caa064355a8df36d527c7

APP 信息

App名称: 金魁花
包名: wrwtr.fdmbxvydzs.ajdtpr
主活动Activity: wrwtr.fdmbxvydzs.ajdtpr.QWEActivity
安卓版本名称: 2.0
安卓版本: 2

域名线索

域名	服务器信息
work.weixin.qq.com	**IP**: 106.55.127.35 **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.
47.96.70.39	**IP**: 47.96.70.39 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 8.136.102.154

jkhh5.leyangkj.com	**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://jkhh5.leyangkj.com	wrwtr/fdmbxvydzs/ajdtpr/QWEActivity.java
https://work.weixin.qq.com	wrwtr/fdmbxvydzs/ajdtpr/QWEActivity.java
http://47.96.70.39:9888/mCenter/app/api/upload	wrwtr/fdmbxvydzs/ajdtpr/QWEActivity$onCreate$2$2$onReceivedError$1.java
http://schemas.android.com/apk/res/android	y2/b.java
http://schemas.android.com/apk/res/android	b0/l.java

邮箱线索

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=beijing, ST=beijing, L=beijing, O=tq1754226150294, OU=ee1754226150294, CN=efdu
签名算法: rsassa_pkcs1v15
有效期自: 2025-08-03 13:02:30+00:00
有效期至: 2075-07-22 13:02:30+00:00
发行人: C=beijing, ST=beijing, L=beijing, O=tq1754226150294, OU=ee1754226150294, CN=efdu
序列号: 0x72b20b65
哈希算法: sha512
md5值: 4b6fcba7d8431602ef4ae7366da892d6
sha1值: 11361a3b7834f22e6ba48cb131b4c447a283aa8e
sha256值: d51a58ef070605b0c07e69b73c482179c4509637753b1f61f482b23fd71d9660
sha512值: 7b83d067104a0d07e3b50db35fb433b8de50de6066d9e015c5b00bc4889ac72d4ed774112ad643d2b267cf6bee48220a93edb356914d1cbc254c496634f65110
公钥算法: rsa
密钥长度: 4096
指纹: 90e21cfb583f6acb75fd1b60db414bb7f895c95c3fbaab6f1f2146beb2d88b33

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.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_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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference

应用内通信