



MoGua

老司鸡 1.0.0.APK 分析报告



APP名称:

老司鸡

包名:	com.PtZgZ.jdNhs
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件名: 老司鸡.apk

文件大小: 17.87MB

MD5值: 37f7435d903b6477a3f6d90ee8e1812a

SHA1值: 8e834f5cf93850f3e6d174903f65560019da0d3e

SHA256值: cab1c9cfe302197988fe9abe7cfab1cf7f8fb5e472d23b596f053c31885b1084

i APP 信息

App名称: 老司鸡

包名: com.PtZgZ.jdNhs

主活动Activity: com.example.laosijiclient.MainActivity

安卓版本名称: 1.0.0

安卓版本: 12

🔍 域名线索

🌐 URL线索

✉ 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='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: 2025-06-04 08:38:18+00:00
 有效期至: 2035-06-02 08:38:18+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: 0x20312e7c
 哈希算法: sha256
 md5值: 5efd0954430ecf7baf96fa510cfe806f
 sha1值: 5aa662acb53616ddc52b95dcdf54c851fa0746d3
 sha256值: d89ed7387570739b032722676e591caebb1ac048110f229bf7eca262b7ecb6db
 sha512值: 07e1615c64bc159aa9d486474b0f7fc1ea678682c8671bd875ffc0231e4c1c68f683f63f546032d09b96495647d413489f093b1dd15539a6a777732d42d58172
 公钥算法: rsa
 密钥长度: 2048
 指纹: 1b0691b9e887eb8e196a0ad87793708a1fc5f69c2d8df24e31785881c88f0b94

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
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。
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.PtZgZ.jdNhs.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。

com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,