



MoGua

九幽神原 1.0.1.APK 分析报告



APP名称:

九幽神原

包名:	com.oskrivl.cc
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18日
分析平台:	摸瓜APK反编译平台

文件名: jysy_20406.apk

文件大小: 27.15MB

MD5值: 334cdbb3dac882658c0aeb2ef18e3082

SHA1值: eb976ac721877b2f47e30534711a79b78da5f686

SHA256值: 16b87d3fcd406721c536bf953d1a4c6bd325b96137dae7f022f35cda844d9f1d

i APP 信息

App名称: 九幽神原

包名: com.oskrivl.cc

主活动Activity: org.cocos2dx.javascript.AppActivity

安卓版本名称: 1.0.1

安卓版本: 1

🔍 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=adf, ST=ad, L=d, O=asdf, OU=adf, CN=adafs

签名算法: rsassa_pkcs1v15
 有效期自: 2025-01-07 07:28:11+00:00
 有效期至: 2025-04-07 07:28:11+00:00
 发行人: C=adf, ST=ad, L=d, O=asdf, OU=adf, CN=adafs
 序列号: 0x3bab3a10
 哈希算法: sha256
 md5值: b781b1bcef07206ddb7b9205bc40998e
 sha1值: 3052a87a64c69b787699a6d4c43e3f1a447af4cc
 sha256值: c87052b2a3e959c2a81c2b16df95bd98fdd6dd4c40151f87fd68d7829991aaa0
 sha512值: 1ff1e713d5f1a1f8d0d31e85de0c9f838d8777987201e7af9b0277e4d82ee9f41c0b3c0a1cdf14acbce4cb4f06d4a37e0cef905b05a5eb861d0f793f55c2edeb
 公钥算法: rsa
 密钥长度: 2048
 指纹: c614c2a14b1bfa8561a030aba3d168c060766f609f064ba929a881e4a5a3e199

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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作

			蓝牙设备
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由

应用内通信

活动(ACTIVITY)	通信(INTENT)
org.cocos2dx.javascript.AppActivity	Schemes: comsuperchesshnwwjj://,