MoGua

麻豆 3.2.8.APK 分析报告

APP名称:	麻豆

包名:	si0fh.n4ia6.gskv2
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年8月27日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 48.apk
文件大小: 61.38MB
MD5值: 2ad54b3ac0cf7c7a13a5b58347adf305
SHA1值: 4221025b9307c4b443ee07e8fb5cbe32303ad59c
SHA256值: 24586676abdb76eb9fc1512a713c4ccbca8b3ae8cebd2614fb895776cd13b2a4

APP 信息

App名称: 麻豆
包名: si0fh.n4ia6.gskv2
主活动Activity: com.yunbao.phonelive.activity.LauncherActivity
安卓版本名称: 3.2.8
安卓版本: 900038

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=admins94pi0, ST=admins94pi0, L=admins94pi0, O=admins94pi0, OU=admins94pi0, CN=admins94pi0

签名算法: rsassa_pkcs1v15
有效期自: 2024-11-29 09:42:56+00:00
有效期至: 2124-11-05 09:42:56+00:00
发行人: C=admins94pi0, ST=admins94pi0, L=admins94pi0, O=admins94pi0, OU=admins94pi0, CN=admins94pi0
序列号: 0x14c82bdf
哈希算法: sha256
md5值: a2b78080160f720f72f040c805ac5025
sha1值: ff23035bafb3c3e1211aceee385c16afdb26fd09
sha256值: ee46fe79a31247f76d30db232da92393ede22408e32317e35925827a6e1c4818
sha512值: e6d31465b78c7ef5e82771d7cc8bf56fe9537c5b53cbdf5f1ee20d052201657c7188c7f2f8bbe782b8abfecb8646481f6e586a20a8e64b60578e2eb2d6d0d51f
公钥算法: rsa
密钥长度: 1024
指纹: c6ef3da42b149203a63f31b79ffd0e87e64b79bf106ea0ec2b5f683119502ce3

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.NETWORK_PROVIDER	未	Unknown	Unknown permission from android reference

	知	permission	
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
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.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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.CHANGE_WIFI_STATE	正	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

	常		进行更改
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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.RECEIVE_USER_PRESENT	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。
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
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
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未	Unknown	Unknown permission from android reference

	知	permission	

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.yunbao.common.arouter.SchemeFilterActivity	Schemes: guming://, Hosts: com.guming,

---