



MoGua

抖音服务 cs04wv2a.APK 分析报告



APP名称:

抖音服务

包名: rs0lcqk6si.ha8vg6byaj.flvb8am6ec

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12日

分析平台: [摸瓜APK反编译平台](#)

文件信息

文件名: rs0lcqk6si.apk

文件大小: 23.34MB

MD5值: d12ccc8765b950ba4186da786c0d5f24

SHA1值: 30ebcfefb14cca5fd3e7c3e7367709c4cee9b70f5

SHA256值: 4bad63a59b3b9a193de1a248475b3d1e18971222c5874d27152d806e69035b10

i APP 信息

App名称: 抖音服务

包名: rs0lcqk6si.ha8vg6byaj.flvb8am6ec

主活动Activity: rs0lcqk6si.ha8vg6byaj.flvb8am6ec.MainActivity

安卓版本名称: cso4wv2a

安卓版本: 18634597

🔍 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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

签名算法: rsassa_pkcs1v15

有效期自: 2025-05-27 06:49:28+00:00

有效期至: 2125-05-03 06:49:28+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
 序列号: 0xca02821598344526
 哈希算法: sha384
 md5值: a21ac2597e1b954eea906f8fd0eb81ff
 sha1值: c861b847d74f98794e576b03765b3ef6f927fb09
 sha256值: ddb5f5dcfe4362f79a69334ec314995435049bd5a3dac1a7cd34a57a1b4d869e
 sha512值: d8c6ad41f8406730f2d22ad61b7b1cc6b7d97a8430c2bf9452a7b76f7b2f9d86367536b50c66ed45613d9a863c89d618a7d084e0ce62b6c2f89b7e0f62bd41c7
 公钥算法: rsa
 密钥长度: 2048
 指纹: 12aa00149d853afeb8f16e37961deeb6fac8026a2f7b81a7328656675a5b1854

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

	是		
--	---	--	--

向手机申请的权限	否 危 险	类型	详细情况
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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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
	正	开机时自动	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

android.permission.RECEIVE_BOOT_COMPLETED	常	启动	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.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
rs0lcqk6si.ha8vg6byaj.flvb8am6ec.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

活动(ACTIVITY)	通信(INTENT)
rs0lcqk6si.ha8vg6byaj.flvb8am6ec.MainActivity	Schemes: vzuqplcr://,