MoGua

대한통운 1.0.APK 分析报告

APP名称: 대한통운

包名:	com.han001.cn
域名线索:	4条
URL线索:	1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

文件信息

文件名: test1.apk
文件大小: 1.2MB
MD5值: ebfd36fd2f64cb21c288b687b9f80ccf
SHA1值: d4d0d5035ad8df5384b997c0cc28bf74dc65e9b8
SHA256值: f46f222f250537f573fb8ba5ead4c1a925685baf5528b3c128371b8111f6d63b

APP 信息

App名称: 대한통운
包名: com.han001.cn
主活动Activity: com.myfoot.cn.MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
s.appjiagu.com	**IP**: 112.64.200.254 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
a.appjiagu.com	没有服务器地理信息.
zoa.zedaok.com	没有服务器地理信息.
c.appjiagu.com	**IP**: 123.125.81.24 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
s.appjiagu.com	摸瓜V3引擎
a.appjiagu.com	摸瓜V3引擎
zoa.zedaok.com	摸瓜V3引擎
c.appjiagu.com	摸瓜V3引擎

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=rwerewr, ST=rewrew, L=erewr, O=uae, OU=usa, CN=year
签名算法: rsassa_pkcs1v15
有效期自: 2016-06-26 11:58:39+00:00
有效期至: 2046-06-19 11:58:39+00:00
发行人: C=rwerewr, ST=rewrew, L=erewr, O=uae, OU=usa, CN=year

序列号: 0x3060a742
哈希算法: sha256
md5值: c2a86938ca640d1b7c48c70011cdcb5e
sha1值: fc4c8c09b4f204a0c4bbc8277d190da5e3207d9c
sha256值: c73787024e49dc1d6e031c0cd33fe827a16c4579f44bb80e4f717f2728e8edc9
sha512值: eee6ac9a80108b412cd29aa07a67b963d231b5b0dd11408e2ffb053e2a46f22f3770bf0a52fbe22ba6a0845324a32e8607e96ea0cdcc0e4af996215648d9ffe8

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.MOUNT_FORMAT_FILESYSTEMS	危险	格式化外部存储器	允许应用程序格式化可移动存储
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_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.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.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
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_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
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.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
		装载和卸载文	

android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	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.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.WRITE_CALL_LOG	危险		允许应用程序写入（但不读取）用户号召日志数据。
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.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_MOCK_LOCATION	危险	用于测试的模拟位置源	创建模拟位置源进行测试。恶意应用程序可以使用它来覆盖由真实位置源（如 GPS 或网络提供商）返回的位置和/或状态
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.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.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_FIND_LOCATION	未知	Unknown permission	Unknown permission from android reference

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.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。

应用内通信
