MoGua

游多多 2.1.APK 分析报告

APP名称:	游多多

包名:	com.skxaaalo.bskhqqop
域名线索:	4条
URL线索:	5条
邮箱线索:	1条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 游多多.apk
文件大小: 4.67MB
MD5值: fa61b0be181991ecdac8856bf7cb2b6e
SHA1值: cddef237c0b07a4d2df83564fff6ecadc1562305
SHA256值: 828514f0ea56f48da673a02a8b552cb1202007660701adceb6c4071e5f2aea0b

APP 信息

App名称: 游多多
包名: com.skxaaalo.bskhqqop
主活动Activity: com.xway.nav.MainActivity
安卓版本名称: 2.1
安卓版本: 2

域名线索

域名	服务器信息
mika6.com	**IP**: 154.93.105.210 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
schemas.android.com	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
api.onedrive.com	**IP**: 13.107.42.12 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	b/g/d/d/g.java
http://ns.adobe.com/xap/1.0/\u0000	b/j/a/a.java
http://schemas.android.com/apk/res/android	c/c/a/g.java
https://dummy/	com/xway/app/i0.java
https://api.onedrive.com/v1.0/drives/	com/xway/app/i0.java
https://mika6.com/navapp.apk	com/xway/nav/MainActivity.java

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libbumper.so

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: CN=DDDDA
签名算法: rsassa_pkcs1v15
有效期自: 2023-01-14 08:41:47+00:00
有效期至: 2048-01-14 08:41:47+00:00
发行人: CN=DDDDA
序列号: 0x63da25cb
哈希算法: sha256
md5值: 8a74de1e1889136e142828318a216f64
sha1值: 3b2934837409b8197900127e89b84ae2195ca5e0
sha256值: 0d8643c241ed4cf875d0a5b03cb2ab5a8872fb1fdff22c73f68eeb2a949b4144
sha512值: 3f2638152699fb4f1e17ad38fa628017a7a5ae9e43abcd8679c8d3f0baa51a5d7c33d1807d06e6a763f465d747f5fca726383fab745cce18f6061f6707635d54
公钥算法: rsa
密钥长度: 2048
指纹: 316d9adb6e25296b6777d58577ede33b03b2accde63d89bd63aa002139fdeec6

🔑 硬编码敏感信息

可能的敏感信息
"active_or_getkey" : "开通会员"
"auth_authagain" : "重试授权"
"no_try_key" : " 当前试用人数已达上线，请明日再来。 "
"register_sms_auth_code" : "短信验证码"
"reset_pwd_submit" : "确认"
"retrieve_pwd_email_label" : "点击这里"

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.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_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_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.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.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.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.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_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
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.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.xway.nav.MainActivity	Schemes: stacksapp://, Hosts: @string/app_scheme_host, Ports: 8000, Paths: /start,
com.xway.nav.ServiceActivity	Schemes: stacksapp://, Hosts: @string/app_scheme_host, Ports: 8000, Paths: /service,
com.xway.nav.MigrateActivity	Schemes: stacksapp://, Hosts: @string/app_scheme_host, Ports: 8000, Paths: /migrate,

---

报告由 **摸瓜**APK**反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。