

# APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♣ 多爱迷 1.0.APK

APP名称: 多爱迷

包名: com.dolovmi2u.cn

域名线索: 9条

URL线索: 39条

邮箱线索: 0条

分析日期: 2022年1月22日 17:43

文件名: duoaimi547654.apk

文件大小: 4.54MB

MD5值: 94d777080e63e29c24e0d0ffdb0fe9c4

**SHA1**值: 5751282df8b528a1bbb24b070fff8453fc0a6d94

**\$HA256**值: b2c54c37a768d469eec6c0c5f56a493886748d4e4d89e3affa249742ae369e78

## i APP 信息

App名称: 多爱迷

包名: com.dolovmi2u.cn

主活动**Activity:** io.dcloud.PandoraEntry

安卓版本名称: 1.0 安卓版本: 1

### 0 域名线索

域名	是否危险域名	服务器信息
stream.dcloud.net.cn	good	P: 118.31.103.188 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 査看地图: Google Map
schemas.android.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
long.open.weixin.qq.com	good	IP: 109.244.217.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
m3w.cn	good	IP: 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	good	IP: 47.93.95.208 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
open.weixin.qq.com	good	IP: 175.24.219.72 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
stream.mobihtml5.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
service.dcloud.net.cn	good	IP: 47.97.36.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
ask.dcloud.net.cn	good	IP: 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map

# ₩URL线索

URL信息	Url所在文件
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/gg/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://ask.dcloud.net.cn/article/283	io/dcloud/i/b.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/g/b/c.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/g/b/h/a.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/36199	Android String Resource

# ₩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.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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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

向手机申请的权限	是否危险	类型	详细情况
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.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_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.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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上 显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference



APK is signed

v1 signature: True v2 signature: True v3 signature: True

Found 1 unique certificates

Subject: C=DOLOVMI, ST=SHUZHOU, L=CHINA, O=DOLOVMI, OU=DOLOVMI, CN=DOLOVMI

Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2021-03-19 03:45:35+00:00 Valid To: 2046-03-13 03:45:35+00:00

Issuer: C=DOLOVMI, ST=SHUZHOU, L=CHINA, O=DOLOVMI, OU=DOLOVMI, CN=DOLOVMI

Serial Number: 0x7dd3ab2e Hash Algorithm: sha256

md5: 24b95ba350da21e65d1269b247fb62fa

sha1: 2c5bacc34eed13fd9cee470cb7dd922203f91c9d

sha256: b9d1fe98b3bb556e61a0719c125e623f7fecb7f1792f478b683417c9b2c8fc78

sha512: 52d8b202f1f3cd33a6170b26982d001481073fbeedfafad0fcc495a4c7db02b9d7d0d24ed5c9f33fcc7946d45989ac74e05136cd091ad9f2d275b1cd5724e6c2

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 925d83979f27c3e623aba0816d1e3a58b171f60250724c2ecf95b2578d41a710



#### ₽ 硬编码敏感信息

#### 可能的敏感信息

"dcloud\_common\_user\_refuse\_api": "the user denies access to the API"

"dcloud\_feature\_confusion\_exception\_no\_key\_input": "no public key input"

"dcloud\_feature\_confusion\_exception\_no\_private\_key\_input": "no private key input"

"dcloud io without authorization": "not authorized"

# 可能的敏感信息 "dcloud\_oauth\_authentication\_failed": "failed to obtain authorization to log in to the authentication service" "dcloud\_oauth\_empower\_failed": "the Authentication Service operation to obtain authorized logon failed" "dcloud\_oauth\_logout\_tips" : "not logged in or logged out" "dcloud\_oauth\_oauth\_not\_empower": "oAuth authorization has not been obtained" "dcloud\_oauth\_token\_failed": "failed to get token" "dcloud\_permissions\_reauthorization": "reauthorize" "dcloud\_common\_user\_refuse\_api": "用户拒绝该API访问" "dcloud\_feature\_confusion\_exception\_no\_key\_input": "公钥数据为空" "dcloud\_feature\_confusion\_exception\_no\_private\_key\_input": "私钥数据为空" "dcloud\_io\_without\_authorization":"没有获得授权" "dcloud\_oauth\_authentication\_failed": "获取授权登录认证服务操作失败" "dcloud\_oauth\_empower\_failed":"获取授权登录认证服务操作失败" "dcloud\_oauth\_logout\_tips":"未登录或登录已注销" "dcloud\_oauth\_oauth\_not\_empower": "尚未获取oauth授权" "dcloud\_oauth\_token\_failed": "获取token失败"

#### 可能的敏感信息

"dcloud\_permissions\_reauthorization" : "重新授权"

## **命**加壳分析

文件列表	分析结果						
	売列表 详细情况						
classes.dex	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check SIM operator check subscriber ID check possible VM check						

报告由 摸瓜平台 自动生成,并非包含所有检测结果,有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析