MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

好玩租号平台 2.0.0.APK

APP名称:	好玩租号平台
包名:	com.uliang.zuhao
域名线索:	7条
URL线索:	37条
邮箱线索:	0条
分析日期:	2022年2月4日 11:13

文件信息

文件名: haowanzuhao599110.apk
文件大小: 4.41MB
MD5值: e718492d03cf85c635d7ab9a234629bb
SHA1值: 46f4fa65a04c4381d9a5c12d010503b497615036
SHA256值: 075c086eb1fb66e7de704c9dcbe92bbdece640fd99d98c2dfa2201b89978913f

APP 信息

App名称: 好玩租号平台
包名: com.uliang.zuhao
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 2.0.0
安卓版本: 20211215

域名线索

域名	是否危险域名	服务器信息
schemas.android.com	good	没有服务器地理信息.
stream.dcloud.net.cn	good	**IP:** 118.31.103.188 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

域名	是否危险域名	服务器信息
ask.dcloud.net.cn	good	**IP:** 222.85.26.232 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613 查看地图: Google Map
stream.mobihtml5.com	good	没有服务器地理信息.
m3w.cn	good	**IP:** 222.85.26.230 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613 查看地图: Google Map
service.dcloud.net.cn	good	**IP:** 120.26.1.80 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
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

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
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

URL信息	Url所在文件
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。

向手机申请的权限	是否危险	类型	详细情况
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
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_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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=CN, ST=遵义, L=贵州, O=创韵网络科技有限公司, OU=创韵网络科技有限公司, CN=飞洋
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-02 11:09:48+00:00
Valid To: 2117-03-31 11:09:48+00:00
Issuer: C=CN, ST=遵义, L=贵州, O=创韵网络科技有限公司, OU=创韵网络科技有限公司, CN=飞洋
Serial Number: 0x1e1c2317

Hash Algorithm: sha256
md5: 9c4ef16bdbce4b16c2c530a6483199b3
sha1: d10adef9338b8cd05b5e72fd0b2d7a8a630bce6e
sha256: 1334893c81e44fd4b62ad866a10928babb2442ae24eb954d1292d7d79653e9b6
sha512: 0a66c684931fbec8d115a19913d97343300d6294faf1a271545df8ef3364a539f6755da1aaa6fcbb8015d834902cbfdaa1211c5b12b11c46ffffe72e70183ec2
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 2cb103c3c1c13170f619120a6852c842d84bd85b0b38a01fce13d79c9cbcd523

🔑 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"
"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"

可能的敏感信息
"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"
"dcloud_permissions_reauthorization" : "重新授权"

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>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</td></tr><tr><td>编译器</td><td>r8</td></tr></table>
