MoGua

卡贝资本 1.0.9.APK 分析报告

APP名称: 卡贝资本

包名:	uni.UNIG44C04B3
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年6月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 卡贝资本.apk
文件大小: 31.65MB
MD5值: fed35f854e107d57e444d9ad484b633c
SHA1值: b64f6e35ad43104c944b98347055ddcafcaedf5f
SHA256值: 2e94bde20652f25eb46e19d64a6aa7f04f2e29bf6e7beb366a1eeefa2b2e450b

APP 信息

App名称: 卡贝资本
包名: uni.UNIG44C04B3
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.9
安卓版本: 118

域名线索

域名	服务器信息
schemas.android.com	没有服务器地理信息.
ask.dcloud.net.cn	**IP**: 116.136.188.184 **所属国家**: China **地区**: Nei Mongol **城市**: Hohhot **纬度**: 40.810650 **经度**: 111.650665
er.dcloud.net.cn	**IP**: 43.142.57.168 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

er.dcloud.io	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
m3w.cn	IP: 116.196.152.179 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://ask.dcloud.net.cn/article/35627	b/a.java
https://ask.dcloud.net.cn/article/35877	b/a.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java

https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://er.dcloud.io/rv	d/c.java
https://er.dcloud.net.cn/rv	d/c.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.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
https://ask.dcloud.net.cn/article/283	i/b.java

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: False
找到 1 个唯一证书
主题: C=CN, ST=, L=, O=Android, OU=Android, CN=gsg9y2Sk9m%2Biwan1gmgCeMkpl%2BGGEKbdrEczcWqq4SwAVozw1%2BHIYh%2F52x1OxZtu
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-03 11:40:03+00:00
有效期至: 2124-12-10 11:40:03+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=gsg9y2Sk9m%2Biwan1gmgCeMkpl%2BGGEKbdrEczcWqq4SwAVozw1%2BHIYh%2F52x1OxZtu

序列号: 0x5868f3a1
哈希算法: sha256
md5值: 22ff3d1b5f9e74f6348d186e0851ff60
sha1值: 7fc1b62acce38b1b3230d71e520657cb5758a04d
sha256值: 829db605d78736d602c0bba7c305039cc8a7206f6666626836536967bc77b2dd
sha512值: 300b62125f1831925305cd4ed9ab8be15571d11d3229d2d6257865cfce132ac9440f4b77c5e05a6d7e7aa1213714c8704386753e4e64a4ade804b997c20115bc
公钥算法: rsa
密钥长度: 2048
指纹: c14a44d76ca4f06496098726fa94b5a40115e14b74c4f8284fa36892e405e882

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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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.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.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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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_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_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.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.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
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

应用内通信