MoGua

便捷商家版 1.0.26.APK 分析报告

APP名称: 便捷商家版

包名:	uni.UNI694700C
域名线索:	21条
URL线索:	32条
邮箱线索:	0条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 覃彩妮uni.UNI694700C.apk
文件大小: 35.08MB
MD5值: 2d52796dc12f98771388f32940355774
SHA1值: cec5fdc59d7457b3a3e605f21a19e009994c3898
SHA256值: 05c2d6cdc85e0e0fd77e16a60219b225ea78e8afa414eaae9bd08c74ddefcb7e

APP 信息

App名称: 便捷商家版
包名: uni.UNI694700C
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.26
安卓版本: 1026

域名线索

域名	服务器信息
ask.dcloud.net.cn	**IP**: 124.163.195.89 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
buy.cloud.tencent.com	**IP**: 60.28.220.193 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
resolver.msg.xiaomi.net	**IP**: 39.102.218.17 **所属国家**: China **地区**: Zhejiang

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
er.dcloud.net.cn	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
cloud.tencent.com	**IP**: 60.28.220.193 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
zhiliao.qq.com	**IP**: 116.196.151.14 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
demos.trtc.tencent-cloud.com	**IP**: 221.204.14.83 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
api-push.in.meizu.com	**IP**: 206.161.233.191 **所属国家**: United States of America **地区**: Virginia **城市**: Herndon **纬度**: 38.978210 **经度**: -77.386993
	IP: 43.175.52.13

www.tencentcloud.com	**所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
intl.cloud.tencent.com	**IP**: 60.28.220.193 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
cn.register.xmpush.xiaomi.com	**IP**: 221.194.179.52 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
m3w.cn	**IP**: 221.204.20.165 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
api-push.meizu.com	**IP**: 221.5.93.66 **所属国家**: China **地区**: Guangdong **城市**: Foshan **纬度**: 23.026770 **经度**: 113.131477
xml.org	**IP**: 104.239.142.8 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246

im.sdk.qcloud.com	**IP**: 116.196.151.14 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
er.dcloud.io	没有服务器地理信息.
xmlpull.org	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
schemas.android.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
ns.adobe.com	没有服务器地理信息.
norma-external-collect.meizu.com	没有服务器地理信息.
10.38.162.35	**IP**: 10.38.162.35 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/35627	b/a.java
https://ask.dcloud.net.cn/article/35877	b/a.java
http://xml.org/sax/features/namespaces	com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java
http://xml.org/sax/features/validation	com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java
http://xml.org/sax/features/namespaces	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/namespace-prefixes	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/validation	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/external-general-entities	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/external-parameter-entities	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/string-interning	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html	com/huawei/secure/android/common/xml/XmlNewPullParserSecurity.java
http://xmlpull.org/v1/doc/features.html	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://api-push.meizu.com/garcia/api/server/getPublicKey	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com/garcia/api/server/getPushConf	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.in.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java

https://api-push.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/f0/a.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/f0/a.java
https://api-push.meizu.com/garcia/api/client/log/upload	com/meizu/f0/a.java
https://zhiliao.qq.com/	com/tencent/qcloud/tuicore/TUIConstants.java
https://cloud.tencent.com/document/product/269/32458	com/tencent/qcloud/tuicore/TUIConstants.java
https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg=	com/tencent/qcloud/tuicore/TUIConstants.java
https://buy.cloud.tencent.com/avc?activeId=plugin&regionId=1	com/tencent/qcloud/tuicore/TUIConstants.java
https://cloud.tencent.com/document/product/269/11673?from=17219	com/tencent/qcloud/tuicore/TUIConstants.java
https://www.tencentcloud.com/document/product/1047/34349	com/tencent/qcloud/tuicore/TUIConstants.java
https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage_%s.png	com/tencent/qcloud/tuicore/TUIConstants.java
https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage_%s_full.png	com/tencent/qcloud/tuicore/TUIConstants.java
https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group_avatar_%s.png	com/tencent/qcloud/tuicore/TUIConstants.java
https://demos.trtc.tencent-cloud.com/prod/base/v1/events/stat	com/tencent/qcloud/tuicore/TUIConfig.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/fg.java

http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/fv.java
https://%1$s/gslb/?ver=5.0	com/xiaomi/push/cg.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/fw.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/ew.java
http://10.38.162.35:9085	com/xiaomi/push/service/q.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/q.java
https://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/ax.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://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://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/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	j/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=u3h5sPMsqmFsH8sMH5FCfb12yQ0axdyrOSlQMAVcC%2FJuN5IwPM3fAboZrFaUCRANQqhpwV9kn0v%2F0RTwx9txIQ%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-29 13:45:10+00:00
有效期至: 2125-03-05 13:45:10+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=u3h5sPMsqmFsH8sMH5FCfb12yQ0axdyrOSlQMAVcC%2FJuN5IwPM3fAboZrFaUCRANQqhpwV9kn0v%2F0RTwx9txIQ%3D%3D
序列号: 0x35564faf
哈希算法: sha256
md5值: b5a46a2297c80d37e177cdd5a23fadb2
sha1值: 6a8bf727e472d6e2473d1b170cb4e2ca93cf4d3f
sha256值: 76eef365c6b2d5a0d92d7eb363f8701da9452d07af3661076a810ea7f1387ed9
sha512值: e006fa3ec87ab308876d10bc4a60fb8dc27949253e52c86a9735d2763e96380527610d24a9a77076c370e2df413e2ea7496678f832276c92cdfd2ee2b57fa46a
公钥算法: rsa
密钥长度: 2048
指纹: a2e040b105a0183fae0aa0949470de89cfb97960b473b2676fa6db721c6bd579

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.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
uni.UNI694700C.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
		Unknown	

com.meizu.flyme.push.permission.RECEIVE	未知	permission	Unknown permission from android reference
uni.UNI694700C.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
uni.UNI694700C.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
uni.UNI694700C.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
uni.UNI694700C.permission.PUSH_PROVIDER	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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	Unknown permission	Unknown permission from android reference
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.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。
	危险	装载和卸载文	

android.permission.MOUNT_UNMOUNT_FILESYSTEMS		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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.qcloud.tim.push.TIMPushOpenActivity	Schemes: pushscheme://, Hosts: com.tencent.qcloud.uniapp, Paths: /detail,

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。