



MoGua

荣昇金业 1.2.0.APK 分析报告



APP名称:

荣昇金业

包名:	uni.UNI1F0B3DC
域名线索:	17条
URL线索:	23条
邮箱线索:	1条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件名: 荣昇金业.apk
文件大小: 62.63MB
MD5值: 10b033b3b895c7752989def0b9cdc0c1
SHA1值: ab8119b5f50a097f68e575c900dd2add67ff30ef
SHA256值: bd632f230a1fb6c475fede357d6ab4e88749e07ce57b04ae41b949c38b4fe0cf

i APP 信息

App名称: 荣昇金业
包名: uni.UNI1F0B3DC
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.2.0
安卓版本: 120

🔍 域名线索

域名	服务器信息
www.google.com	IP: 31.13.94.41 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
quilljs.com	IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
rstrader.vip	没有服务器地理信息.
	IP: 69.147.80.12

developer.yahoo.com	所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089
www.baidu.com	IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
github.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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
er.dcloud.io	没有服务器地理信息.
www.uvui.cn	IP: 61.48.83.227 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ask.dcloud.net.cn	IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin

	纬度: 39.142181 经度: 117.176102
schemas.android.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
service.dcloud.net.cn	IP: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
apis.map.qq.com	IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
d3bhzipiwsopde2.cloudfront.net	IP: 3.165.84.142 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
ns.adobe.com	没有服务器地理信息.

www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
------------	---

 URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.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/35627	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java

https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.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/36199	摸瓜V1引擎
https://rstrader.vip/invest-server	摸瓜V2引擎
https://rstrader.vip/	摸瓜V2引擎
https://rstrader.vip/file	摸瓜V2引擎
https://www.uvui.cn	摸瓜V2引擎
https://www.baidu.com	摸瓜V2引擎
https://d3bhziwpsopde2.cloudfront.net/talk/82175658b8a21447392357sa0b.html	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
http://developer.yahoo.com/yui/license.html	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎

https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com	摸瓜V2引擎

 手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书

主题: C=CN, ST=, L=, O=Android, OU=Android, CN=PvsalzHngLxKAgTkT0ZG1oET1i0Wale8e3MB3ZZGLNLKlbEwbv94Bf55KTcUZSPZ%2F6xkqe5NKGfXr%2B9a35YSTw%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-04 12:20:11+00:00
有效期至: 2125-03-11 12:20:11+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=PvsalzHngLxKAgTkT0ZG1oET1i0Wale8e3MB3ZZGLNLKlbEwbv94Bf55KTcUZSPZ%2F6xkqe5NKGfXr%2B9a35YSTw%3D%3D
序列号: 0x2e7cf167
哈希算法: sha256
md5值: c4b979c6df634dcea89cf033fdf2b5df
sha1值: 4560e9891e6a308d119253bd485571dfa2573aa9
sha256值: 6ddef3d16ae0d626b890ac54f9d8af7cecbf1a48c7ea384b7a726ec46e8fc8be
sha512值: bfbef13de211d4c9342ab799509e25ac309637f2029d1b68e31cc06d0f6915527aee96be8b3163698167344db066b5d0276136ed291eabfbe18e87311daae6d23
公钥算法: rsa
密钥长度: 2048
指纹: cb5b2a3e9054f041d383d82b5ffb7ec0eaf6665ffbed0331a2586b49267adf83

 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_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"
"dcloud_tips_certificate" : "certificate"

dcloud_tips_certificate : certificate
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"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"
"dcloud_tips_certificate" : "证书"

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
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
uni.UNI1F0B3DC.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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。

应用内通信

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。