



囧次元 1.5.7.5.APK 分析报告



APP名称:

囧次元

包名:	com.lmm.huiyuanuxiang
域名线索:	29条
URL线索:	42条
邮箱线索:	2条
分析日期:	2025年6月25日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 1730481984xTTfpxlDT0keXZQ9QXO0w9486d136948a05c89a039fd4df8d682975ba96322c30c097315487c241d4071847fd.apk
文件大小: 54.88MB

MD5值: cc2ecdca7a3d7e7ba3760e87832c1454
SHA1值: 1f414921497ec89689999904a0fd5034a0ecc2be
SHA256值: 47dc5c47a324cb3e02aed7825006ba86a6d867ab9da15cca723388f8e5fb3d01

i APP 信息

App名称: 囡次元
包名: com.llmm.huiyuanuxiang
主活动Activity: com.maoyun.guoguo.MainActivity
安卓版本名称: 1.5.7.5
安卓版本: 79

🔍 域名线索

域名	服务器信息
apps.oceanengine.com	IP: 106.74.132.35 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
sf6-ttcdn-tos.pstatp.com	IP: 103.251.162.48 所属国家: China 地区: Qinghai 城市: Xining 纬度: 36.616669 经度: 101.766670
union.baidu.com	IP: 111.206.208.169 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

i.snssdk.com	IP: 125.39.135.110 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
open.e.kuaishou.com	IP: 116.136.202.194 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
open.weixin.qq.com	IP: 220.196.139.154 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
cpro.baidustatic.com	IP: 101.72.203.38 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
www.samsungapps.com	IP: 54.229.225.161 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151

	经度: -6.267249
open.weibo.cn	IP: 123.126.45.166 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
c.etooldads.cn	IP: 39.96.185.90 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
long.open.weixin.qq.com	IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
api.weibo.com	IP: 123.126.45.166 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
adservice.sigmob.cn	IP: 39.106.232.111 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.jsdelivr.com	IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco

	纬度: 37.775700 经度: -122.395203
apps.bytesfield.com	IP: 106.74.132.36 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
p1-lm.adkwai.com	IP: 114.66.246.206 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
apps.bytesfield-b.com	IP: 60.222.11.202 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
apps.samsung.com	IP: 104.17.142.17 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
211.151.146.65	IP: 211.151.146.65 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 39.106.166.112 所属国家: China

adxtool.sigmob.cn	地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
developer.android.com	IP: 172.217.14.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
login.sina.com.cn	IP: 202.108.0.130 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
c.tobidad.cn	IP: 39.96.185.90 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
static.yximgs.com	IP: 221.204.65.226 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
	IP: 47.94.5.41

dc.sigmob.cn	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
service.weibo.com	IP: 202.108.0.98 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
m.sigmob.com	IP: 39.107.65.119 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

 URL线索

URL信息	Url所在文件
https://cpro.baidustatic.com/cpro/logo/sdk/mob-adlcon_2x.png	com/baidu/mobads/sdk/api/XAdNativeResponse.java
https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png	com/baidu/mobads/sdk/api/XAdNativeResponse.java
http://union.baidu.com/	com/baidu/mobads/sdk/api/XAdNativeResponse.java
https://cpro.baidustatic.com/cpro/logo/sdk/mob-adlcon_2x.png	com/baidu/mobads/sdk/api/XAdEntryResponse.java
https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png	com/baidu/mobads/sdk/api/XAdEntryResponse.java
http://union.baidu.com/	com/baidu/mobads/sdk/api/XAdEntryResponse.java

http://211.151.146.65:8080/wlantest/shanghai_sun/mock_ad_server_interstitial_video.json	com/baidu/mobads/sdk/internal/ds.java
http://union.baidu.com	com/baidu/mobads/sdk/internal/ap.java
https://i.snssdk.com/	com/bytedance/sdk/openadsdk/downloadnew/core/AdBaseConstants.java
https://dc.sigmob.cn/log	com/czhj/sdk/common/models/Config.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/tk/ks_so-tachikomaNoSoRelease-3.3.64.1-30279a11a9-537.zip	com/kwad/components/offline/c/c.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v8_lite_3358	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v8_3358	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v7_lite_3358	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v7_3358	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/obiwan/ks_so-obiwanNoSoRelease-3.3.56-445ef4f109-409.zip	com/kwad/components/offline/b/b.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/adLive/ks_so-adLiveNoSoRelease-3.3.59-5a16210b94-483.zip	com/kwad/components/offline/a/b.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/adLive/ks_so-adLiveArm64v8aRelease-3.3.44.2-e8fbb3a5f8-666.apk	com/kwad/components/offline/a/a/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/adLive/ks_so-adLiveArmeabiv7aRelease-3.3.44.2-e8fbb3a5f8-666.apk	com/kwad/components/offline/a/a/a.java

https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/kwad/framework/filedownloader/services/a.java
https://open.e.kuaishou.com/rest/e/v3/open/sdk2	com/kwad/sdk/api/loader/u.java
http://%s:%d/%s	com/kwad/sdk/core/videocache/f.java
https://github.com/danikula/AndroidVideoCache/issues/88 .	com/kwad/sdk/core/videocache/h.java
https://github.com/danikula/AndroidVideoCache/issues/43 .	com/kwad/sdk/core/videocache/h.java
https://github.com/danikula/AndroidVideoCache/issues .	com/kwad/sdk/core/videocache/h.java
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArm64v8aRelease-3.3.14.apk	com/kwad/sdk/collector/d.java
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArmeabiv7aRelease-3.3.14.apk	com/kwad/sdk/collector/d.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArm64v8aRelease-3.3.47-e8fbb3a5f8-666.apk	com/kwad/sdk/crash/g.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArmeabiv7aRelease-3.3.47-e8fbb3a5f8-666.apk	com/kwad/sdk/crash/g.java
http://apps.samsung.com/appquery/appDetail.as?appld=	com/kwad/sdk/utils/d.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac64	com/kwad/sdk/kgeo/c.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac32	com/kwad/sdk/kgeo/c.java
https://c.etoolads.cn/s/config	com/sigmob/sdk/base/k.java
https://adservice.sigmob.cn/s/config	com/sigmob/sdk/base/k.java
https://adservice.sigmob.cn/s/config?	com/sigmob/sdk/base/l.java

https://adservice.sigmob.cn/ad/v4	com/sigmob/sdk/base/l.java
https://adxtool.sigmob.cn/debug/feedback	com/sigmob/sdk/base/l.java
https://adservice.sigmob.cn/hb/v2/ad	com/sigmob/sdk/base/l.java
https://dc.sigmob.cn/log	com/sigmob/sdk/base/l.java
http://127.0.0.1	com/sigmob/sdk/mraid/o.java
https://m.sigmob.com	com/sigmob/sdk/mraid/b.java
http://%s:%d/%s	com/sigmob/sdk/videocache/n.java
http://%s:%d/%s	com/sigmob/sdk/videocache/h.java
https://api.weibo.com/oauth2/access_token	com/sina/weibo/sdk/a/e.java
https://service.weibo.com/share/mobilesdk_uppik.php	com/sina/weibo/sdk/a/d.java
https://service.weibo.com/share/mobilesdk.php	com/sina/weibo/sdk/web/WebActivity.java
https://open.weibo.cn/oauth2/authorize?	com/sina/weibo/sdk/web/WebActivity.java
https://service.weibo.com/share/mobilesdk.php	com/sina/weibo/sdk/web/b/d.java
https://open.weibo.cn/oauth2/authorize?	com/sina/weibo/sdk/auth/a.java
https://www.samsungapps.com/appquery/appDetail.as?appId=	com/ss/android/downloadlib/z/hb.java
https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/downloadlib/addownload/compliance/wo.java
https://apps.bytesfield.com	com/ss/android/downloadlib/addownload/compliance/un.java

https://apps.bytesfield-b.com	com/ss/android/downloadlib/addownload/compliance/un.java
https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java
https://login.sina.com.cn/visitor/signin	com/weibo/ssosdk/WeiboSsoSdk.java
https://adservice.sigmob.cn/w/config	com/windmill/sdk/d/j.java
https://c.tobidad.cn/w/config	com/windmill/sdk/d/j.java
https://adservice.sigmob.cn/extconfig?	com/windmill/sdk/d/j.java
https://adservice.sigmob.cn/strategy/v6	com/windmill/sdk/d/j.java
https://adservice.sigmob.cn/waterfall/v1	com/windmill/sdk/d/j.java
https://dc.sigmob.cn/log	com/windmill/sdk/d/j.java
https://adservice.sigmob.cn/w/config?	com/windmill/sdk/d/j.java
https://c.tobidad.cn/w/config?	com/windmill/sdk/d/j.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
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://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/apvarun/toastify-js	摸瓜V2引擎

✉ 邮箱线索

邮箱地址	所在文件
.apk@classes.dex	com/kuaishou/weapon/p0/ac.java
danikula@gmail.com	com/kwad/sdk/core/videocache/h.java

☰ 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: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2023-05-17 03:01:49+00:00
有效期至: 2053-05-09 03:01:49+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha256
md5值: fd1695d368f882529400df91009650a0
sha1值: 9cc3c37983fd2b9901d9c9316011b588ca706802
sha256值: cb0c57d91fc3ae63f8e1806d3d66e281acefb72444f0b8452e8886ec3e1f63fe
sha512值: 128ed534debefd7c62c7323aa95911d8bd2ca9bb64d8d28ab923cafd70a15655d3b5a9d4582f2e1a2b8b5416c637f2506776d16019bf8323b974103ad87230a2
公钥算法: rsa
密钥长度: 2048
指纹: bcb0f4e6e28a24856d6feedb66987f46ef79c23422bb11d891489a48de744319

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.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
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.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
com.llmm.huiyuanuxiang.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
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.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_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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
android.Manifest.permission.LOCAL_MAC_ADDRESS	未知	Unknown permission	Unknown permission from android reference
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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

android.permission.QUERY_ALL_PACKAGES	正常		允许应用程序查询设备上所有应用包名,无论是否安装
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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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。
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
com.lmm.huiyuanuxiang.permission.KW_SDK_BROADCAST	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
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
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。