MoGua

经链 1.0.7.APK 分析报告

APP名称: 经链

包名:	com.jingnian.jinglian
域名线索:	22条
URL线索:	10条
邮箱线索:	7条
分析日期:	2025年2月6日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 125_ef9ff1c5ac8a742a6ee5f547600735b0.apk
文件大小: 91.26MB
MD5值: 7ec6c592bc5ce88d1ae2b65036e0f1bc
SHA1值: 3c3dd3e07473e1488b1d200fe00d1781b8f4fbb7
SHA256值: 92076610f1bda3dc1e5e6f4899bde32b96b24e836788bd759059da7b9521919c

APP 信息

App名称: 经链
包名: com.jingnian.jinglian
主活动Activity: com.jingnian.jinglian.MainActivity
安卓版本名称: 1.0.7
安卓版本: 7

域名线索

域名	服务器信息
grs.dbankcloud.asia	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics1-drcn.dt.dbankcloud.cn	**IP**: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.dbankcloud.cn	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong

	城市: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
paulbakaus.com	IP: 167.172.18.193 **所属国家**: United States of America **地区**: New Jersey **城市**: Clifton **纬度**: 40.858585 **经度**: -74.163605
metrics5.data.hicloud.com	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
www.jsdelivr.com	IP: 104.21.23.24 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
stackoverflow.com	IP: 104.18.32.7 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
metrics2.data.hicloud.com	IP: 80.158.2.190 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
	IP: 20.205.243.166

github.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.com	IP: 60.28.193.195 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
data-dre.push.dbankcloud.com	IP: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
data-dra.push.dbankcloud.com	IP: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
data-drcn.push.dbankcloud.com	IP: 49.4.40.58 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
grs.dbankcloud.eu	没有服务器地理信息.
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore

	纬度: 1.289987 **经度**: 103.850281
data-drru.push.dbankcloud.com	IP: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
www.gnu.org	IP: 209.51.188.116 **所属国家**: United States of America **地区**: Massachusetts **城市**: Somerville **纬度**: 42.387600 **经度**: -71.099503
journeyapps.com	IP: 18.65.168.24 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
developer.mozilla.org	IP: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
grs.platform.dbankcloud.ru	没有服务器地理信息.
dev.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

metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499

URL线索

URL信息	Url所在文件
https://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1-drcn.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎

https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
http://paulbakaus.com/tutorials/html5/web-audio-on-ios/	摸瓜V2引擎
http://stackoverflow.com/questions/24119684	摸瓜V2引擎
https://www.gnu.org/licenses/>.	摸瓜V2引擎
https://www.gnu.org/licenses/>.	摸瓜V2引擎
https://www.gnu.org/licenses/>.	摸瓜V2引擎
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
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件

menu@2x.png
yz00@2x.png
yz01@2x.png
yz02@2x.png
yz03@2x.png
yz04@2x.png
yz05@2x.png
yz06@2x.png
yz07@2x.png
yz08@2x.png
yz09@2x.png
yz10@2x.png
yz11@2x.png
yz12@2x.png
yz13@2x.png
yz14@2x.png
yz15@2x.png
yz16@2x.png
yz17@2x.png
ys00@2x.png
ys01@2x.png
ys02@2x.png
ys03@2x.png
ys04@2x.png
ys05@2x.png
ys06@2x.png
ys07@2x.png
ys08@2x.png
ys09@2x.png
ys10@2x.png
ys11@2x.png
ys12@2x.png
ys13@2x.png
ys14@2x.png
ys15@2x.png
gcs00@2x.png
gcs01@2x.png

gcs02@2x.png
gcs03@2x.png
gcs04@2x.png
gcs05@2x.png

摸瓜V2引擎

gcs06@2x.png gcs07@2x.png gcs08@2x.png gcs09@2x.png gcs10@2x.png gcs11@2x.png gcs12@2x.png gcs13@2x.png gcs14@2x.png gcs15@2x.png gcs16@2x.png	
1@3x.png 2@3x.png 3@3x.png 4@3x.png 5@3x.png 6@3x.png 椭圆形@3x.png	摸瓜V2引擎
前景@3x.png 瓶子@3x.png 背景@3x.png	摸瓜V2引擎
1@3x.png 2@3x.png 3@3x.png 4@3x.png 5@3x.png 6@3x.png 形@3x.png logo2@3x.png	摸瓜V2引擎
1@3x.png 2@3x.png 3@3x.png 4@3x.png 5@3x.png 6@3x.png 形@3x.png	摸瓜V2引擎

logo3@3x.png	
1@3x.png 2@3x.png 3@3x.png 4@3x.png 5@3x.png 6@3x.png 形@3x.png logo1@3x.png	摸瓜V2引擎
1@3x.png 2@3x.png 5@3x.png 6@3x.png 4@3x.png 3@3x.png 7@3x.png 气泡@3x.png logo@3x.png 雷达扫描@3x.png 雷达底@3x.png	摸瓜V2引擎

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=86, ST=China, L=Beijing, O=jingnian, OU=jingnian, CN=jinglian
签名算法: rsassa_pkcs1v15
有效期自: 2022-12-22 09:27:30+00:00
有效期至: 2047-12-16 09:27:30+00:00

发行人: C=86, ST=China, L=Beijing, O=jingnian, OU=jingnian, CN=jinglian
序列号: 0x2c4e02d3
哈希算法: sha256
md5值: 7eb57ab652141c923266592283dfd407
sha1值: 4e0e430a0156f411d9816381fc6cf754c6388a16
sha256值: c8e80365dc59924bc46b74451e5f3da203f924e080725a689d09ca65f2002d49
sha512值: 896108c2d38a5b37df8b9b7a17508801e89ca1bbc5eac7b7e409e2d40d6b35fb3db4378c9216464a004e832c8f0a4f73400aa69830e2a14337d26e7664fe8771
公钥算法: rsa
密钥长度: 2048
指纹: d9cafd8398297fdf0ffd8aa13a0977d06bc0d39c08671aeb4fa188bb02480e39

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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.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.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.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.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.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.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
com.jingnian.jinglian.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
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.jingnian.jinglian.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
com.jingnian.jinglian.permission.C2D_MESSAGE	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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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
	未	Unknown	

android.permission.READ_MEDIA_IMAGES	知	permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	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_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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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.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.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.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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
	危		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

android.permission.ACCESS_FINE_LOCATION	险	精细定位（GPS）	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
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.jingnian.jinglian.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
com.jingnian.jinglian.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
com.jingnian.jinglian.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.jingnian.jinglian.permission.PUSH_PROVIDER	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
com.google.android.gms.permission.AD_ID	未	Unknown	Unknown permission from android reference

	知	permission	
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.flutter.tim_ui_kit_push_plugin.pushActivity.VIVOMessageActivity	Schemes: tencent_im_push://, Hosts: com.jingnian.jinglian, Paths: /message,
com.tencent.flutter.tim_ui_kit_push_plugin.pushActivity.HONORMessageActivity	Schemes: tencent_im_push://, Hosts: com.jingnian.jinglian, Paths: /honorMessage,

---