Evaluation Warning: The document was created with Spire.Doc for Python.

**国创筑梦（ 1.0.1版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 国创筑梦 |
| 版本 | 1.0.1 |
| 包名 | glatpi.egnyuk.wqmjwg.hsxphx |
| 域名线索 | 63条 |
| URL线索 | 46条 |
| APP图标 |  |
| 分析日期 | 2025年6月18日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | CXFDT678.apk |
| 文件大小 | 109.73MB |
| MD5值 | 1bda428cd1a411da01b05c27024f93f0 |
| SHA1值 | c824995970b6a1338b20879903e475517da3e94b |
| SHA256值 | ccc0661274a3069aac35e18674d8c7686049119db7b4addc0dbb45ad1dd46d37 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 国创筑梦 |
| 包名 | glatpi.egnyuk.wqmjwg.hsxphx |
| 主活动Activity | com.yingqiang.zumeng.v1.MainActivity |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 162.14.3.250 | IP: 162.14.3.250  所属国家: China  地区: Beijing  城市: Beijing |
| h.trace.qq.com | IP: 113.56.189.246  所属国家: China  地区: Hubei  城市: Huangshi |
| cos-android-sdk-doc-1253960454.cos.ap-shanghai.myqcloud.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| aomedia.org | IP: 173.255.213.90  所属国家: United States of America  地区: California  城市: Fremont |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| schemas.microsoft.com | IP: 13.107.253.39  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| 119.29.29.99 | IP: 119.29.29.99  所属国家: Singapore  地区: Singapore  城市: Singapore |
| grs.dbankcloud.asia | IP: 121.36.117.149  所属国家: China  地区: Beijing  城市: Beijing |
| otheve.beacon.qq.com | IP: 113.56.189.125  所属国家: China  地区: Hubei  城市: Huangshi |
| 119.29.29.98 | IP: 119.29.29.98  所属国家: Singapore  地区: Singapore  城市: Singapore |
| playvideo.qcloud.com | IP: 220.194.123.111  所属国家: China  地区: Tianjin  城市: Tianjin |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252  所属国家: China  地区: Beijing  城市: Beijing |
| api-push.in.meizu.com | IP: 206.161.233.191  所属国家: United States of America  地区: Virginia  城市: Herndon |
| demos.trtc.tencent-cloud.com | IP: 123.125.244.81  所属国家: China  地区: Beijing  城市: Beijing |
| 162.14.19.114 | IP: 162.14.19.114  所属国家: China  地区: Beijing  城市: Beijing |
| en.wikipedia.org | IP: 31.13.112.9  所属国家: Ireland  地区: Dublin  城市: Dublin |
| grs.dbankcloud.cn | IP: 124.70.116.153  所属国家: China  地区: Guangdong  城市: Guangzhou |
| cloud.tencent.com | IP: 116.196.155.61  所属国家: China  地区: Zhejiang  城市: Jinhua |
| console.intl.cloud.tencent.com | IP: 124.163.195.89  所属国家: China  地区: Shanxi  城市: Taiyuan |
| im.sdk.qcloud.com | IP: 116.196.151.15  所属国家: China  地区: Zhejiang  城市: Jinhua |
| ns.adobe.com | 没有服务器地理信息. |
| tun-cos-1258344701.file.myqcloud.com | IP: 116.196.151.15  所属国家: China  地区: Zhejiang  城市: Jinhua |
| www.tencentcloud.com | IP: 43.175.93.11  所属国家: Singapore  地区: Singapore  城市: Singapore |
| test.snowflake.qq.com | IP: 221.198.69.15  所属国家: China  地区: Tianjin  城市: Tianjin |
| 10.38.162.35 | IP: 10.38.162.35  所属国家: -  地区: -  城市: - |
| grs.dbankcloud.com | IP: 60.28.200.159  所属国家: China  地区: Tianjin  城市: Tianjin |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52  所属国家: China  地区: Hebei  城市: Langfang |
| bkplayvideo.qcloud.com | IP: 157.148.63.81  所属国家: China  地区: Guangdong  城市: Guangzhou |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160  所属国家: China  地区: Shanghai  城市: Shanghai |
| norma-external-collect.meizu.com | 没有服务器地理信息. |
| metrics2.data.hicloud.com | IP: 80.158.2.190  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| othstr.beacon.qq.com | IP: 112.65.194.211  所属国家: China  地区: Shanghai  城市: Shanghai |
| resolver.msg.xiaomi.net | IP: 110.43.0.169  所属国家: China  地区: Beijing  城市: Beijing |
| dashif.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| console.cloud.tencent.com | IP: 60.28.220.193  所属国家: China  地区: Tianjin  城市: Tianjin |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| api.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| buy.tencentcloud.com | IP: 43.175.52.13  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| accounts.google.com | IP: 46.82.174.69  所属国家: Germany  地区: Niedersachsen  城市: Braunschweig |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| grs.dbankcloud.eu | 没有服务器地理信息. |
| journeyapps.com | IP: 216.137.39.6  所属国家: United States of America  地区: California  城市: Los Angeles |
| htrace.wetvinfo.com | IP: 220.194.118.67  所属国家: China  地区: Tianjin  城市: Tianjin |
| buy.cloud.tencent.com | IP: 60.28.220.193  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.jsdelivr.com | IP: 104.21.23.24  所属国家: United States of America  地区: California  城市: San Francisco |
| snowflake.qq.com | IP: 116.130.220.107  所属国家: China  地区: Beijing  城市: Beijing |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189  所属国家: Singapore  地区: Singapore  城市: Singapore |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| 1255566655.vod2.myqcloud.com | IP: 60.220.213.225  所属国家: China  地区: Shanxi  城市: Taiyuan |
| developer.apple.com | IP: 17.253.87.196  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| vodreport.qcloud.com | IP: 123.12.235.54  所属国家: China  地区: Henan  城市: Hebi |
| default.url | 没有服务器地理信息. |
| metrics5.data.hicloud.com | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| intl.cloud.tencent.com | IP: 60.28.220.193  所属国家: China  地区: Tianjin  城市: Tianjin |
| 162.14.13.170 | IP: 162.14.13.170  所属国家: China  地区: Beijing  城市: Beijing |
| api-push.meizu.com | IP: 221.5.93.66  所属国家: China  地区: Guangdong  城市: Foshan |
| developer.android.com | IP: 142.250.217.110  所属国家: United States of America  地区: California  城市: Mountain View |
| grs.platform.dbankcloud.ru | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| open.res.flyme.cn | IP: 221.5.93.54  所属国家: China  地区: Guangdong  城市: Foshan |
| zhiliao.qq.com | IP: 119.188.149.190  所属国家: China  地区: Shandong  城市: Jinan |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | a5/o0.java |
| https://x</LA\_URL> | a5/n0.java |
| https://default.url | a5/n0.java |
| https://accounts.google.com/o/oauth2/revoke?token= | c7/f.java |
| https://htrace.wetvinfo.com/kv | com/tencent/beacon/a/b/c.java |
| https://h.trace.qq.com/kv | com/tencent/beacon/a/b/c.java |
| https://otheve.beacon.qq.com/analytics/v2\_upload | com/tencent/beacon/base/net/b/b.java |
| https://othstr.beacon.qq.com/analytics/v2\_upload | com/tencent/beacon/base/net/b/b.java |
| https://cos-android-sdk-doc-1253960454.cos.ap-shanghai.myqcloud.com/beacon\_cc/android/ | com/tencent/cos/xml/CloudControl.java |
| http://xmlpull.org/v1/doc/features.html | com/tencent/cos/xml/transfer/XmlSlimBuilder.java |
| http://xmlpull.org/v1/doc/features.html | com/tencent/cos/xml/transfer/XmlBuilder.java |
| https://www.tencentcloud.com/document/product/1047/50032 | com/tencent/flutter/tim\_ui\_kit\_push\_plugin/ChannelPushManager.java |
| https://cloud.tencent.com/document/product/269/74605 | com/tencent/flutter/tim\_ui\_kit\_push\_plugin/ChannelPushManager.java |
| http://open.res.flyme.cn/fileserver/upload/file/202109/7bf101e2843642709c7a11f4b57861cd.pdf | com/tencent/flutter/tim\_ui\_kit\_push\_plugin/channelUtils/MeizuUtils.java |
| https://cloud.tencent.com/act/event/License | com/tencent/liteav/a.java |
| http://playvideo.qcloud.com/getplayinfo/v2 | com/tencent/liteav/txcvodplayer/b/d.java |
| https://playvideo.qcloud.com/getplayinfo/v2 | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/coverBySnapshot/1513156403\_1311093072.100\_0.jpg?t=5c08d9fa&us=someus&sign=95f34beb353fe32cfe7f8b5e79cc28b1\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058\_533711271\_00001.jpg?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058\_533711271.vtt?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/uAnXX0OMLSAA.wmv?t=5c08d9fa&us=someus&sign=659af5dd3f27eb92dc4ed74eb561daa4\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/master\_playlist.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f220.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f230.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f240.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f210.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f10.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f20.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| https://playvideo.qcloud.com/getplayinfo/v4 | com/tencent/liteav/txcvodplayer/b/c.java |
| https://bkplayvideo.qcloud.com/getplayinfo/v4 | com/tencent/liteav/txcvodplayer/b/c.java |
| https://vodreport.qcloud.com/describeControlInfos/v1/ | com/tencent/liteav/txcvodplayer/a/b.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/tencent/qcloud/qcloudxml/core/QCloudXml.java |
| https://console.cloud.tencent.com/im/detail | com/tencent/qcloud/tuikit/tuicallengine/a.java |
| https://console.intl.cloud.tencent.com/im/detail | com/tencent/qcloud/tuikit/tuicallengine/a.java |
| https://buy.cloud.tencent.com/avc?addRavLicense=1 | com/tencent/qcloud/tuikit/tuicallengine/e/o.java |
| https://buy.tencentcloud.com/avc?addRavLicense=1 | com/tencent/qcloud/tuikit/tuicallengine/e/o.java |
| https://tun-cos-1258344701.file.myqcloud.com/my.html | com/tencent/qimei/s/c.java |
| https://tun-cos-1258344701.file.myqcloud.com/fp.js | com/tencent/qimei/s/c.java |
| https://tun-cos-1258344701.file.myqcloud.com/fp.js | com/tencent/qimei/s/a.java |
| https://test.snowflake.qq.com/ola | com/tencent/qimei/e/a.java |
| https://snowflake.qq.com/ola | com/tencent/qimei/e/a.java |
| https://en.wikipedia.org/wiki/Blend\_modes\n// | com/tencent/ugc/videoprocessor/transitions/StereoViewerFilter.java |
| https://api-push.meizu.com/garcia/api/server/getPublicKey | 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 |
| http://10.38.162.35:9085 | com/xiaomi/push/service/v2.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/v2.java |
| https://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/b1.java |
| http://dashif.org/guidelines/last-segment-number | d6/d.java |
| http://dashif.org/guidelines/trickmode | d6/d.java |
| http://dashif.org/thumbnail\_tile | d6/d.java |
| http://dashif.org/guidelines/thumbnail\_tile | d6/d.java |
| https://developer.android.com/guide/topics/permissions/overview | io/flutter/plugin/platform/h.java |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted | t6/z.java |
| http://xmlpull.org/v1/doc/features.html | tf/v6.java |
| http://xmlpull.org/v1/doc/features.html | tf/n7.java |
| https://%1$s/gslb/?ver=5.0 | tf/f2.java |
| http://xmlpull.org/v1/doc/features.html | tf/p7.java |
| http://xmlpull.org/v1/doc/features.html | tf/i6.java |
| https://github.com/Baseflow/flutter-permission-handler/issues | w0/t.java |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread | w4/c1.java |
| http://ns.adobe.com/xap/1.0/ | g5/a.java |
| https://aomedia.org/emsg/ID3 | q5/a.java |
| https://developer.apple.com/streaming/emsg-id3 | q5/a.java |
| https://api-push.meizu.com/garcia/api/client/ | oe/a.java |
| https://api-push.in.meizu.com/garcia/api/client/ | oe/a.java |
| https://api-push.meizu.com/garcia/api/client/log/upload | oe/a.java |
| 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 |
| 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://162.14.13.170/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| http://162.14.3.250/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| https://119.29.29.99/d?token=353599313 | lib/arm64-v8a/libImSDK.so |
| http://119.29.29.98/d?id=39662 | lib/arm64-v8a/libImSDK.so |
| http://162.14.19.114/ | lib/arm64-v8a/libImSDK.so |
| https://api.flutter.dev/flutter/material/Scaffold/of.html | lib/arm64-v8a/libapp.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided | com/tencent/liteav/base/PiiElider.java |
| u0013android@android.com0  u0013android@android.com | e7/q.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 16222222222 | com/tencent/imsdk/common/HttpClient.java |
| 17222222222 | com/tencent/imsdk/common/HttpClient.java |
| 18222222222 | com/tencent/imsdk/common/HttpClient.java |
| 14159265358 | com/tencent/ugc/videoprocessor/transitions/BounceFilter.java |
| 17512775099 | w8/a.java |

## **5. 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=chengdu, ST=chengdu, L=chengdu, O=gy1747965835425, OU=or1747965835425, CN=itez 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-23 02:03:55+00:00 有效期至: 2075-05-11 02:03:55+00:00 发行人: C=chengdu, ST=chengdu, L=chengdu, O=gy1747965835425, OU=or1747965835425, CN=itez 序列号: 0x3fe0f13 哈希算法: sha1 md5值: cd68c182dcec5697084a369375a0d13d sha1值: 597223736678cf3ce7a92fd75f8044620a11ba8d sha256值: b9390e34bd291535da5cc5100b8445df18b2f5e7cb1b6cad0cb25991ae0402c8 sha512值: d089d4c2126deec064fcb0909b3ebab155083e5e3cd3f93d84417c89ac9e7ff250d6dcebf41a584ae0424e6ad35bbf0a392188e4499bd0b9c66b754221f4a780 公钥算法: rsa 密钥长度: 1024 指纹: 538aaa793a12d43b75685e01841639377b0fc9d488bceb21df047114b8b78c54**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps" |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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.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 |
| 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.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.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.FOREGROUND\_SERVICE\_CAMERA | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MICROPHONE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_CONNECTED\_DEVICE | 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.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.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.POST\_NOTIFICATIONS | 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.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.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 |
| glatpi.egnyuk.wqmjwg.hsxphx.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 |
| glatpi.egnyuk.wqmjwg.hsxphx.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| glatpi.egnyuk.wqmjwg.hsxphx.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| glatpi.egnyuk.wqmjwg.hsxphx.permission.MIPUSH\_RECEIVE | 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.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.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。 |

## **10. 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:** glatpi.egnyuk.wqmjwg.hsxphx,  **Paths:** /message, |
| com.tencent.flutter.tim\_ui\_kit\_push\_plugin.pushActivity.HONORMessageActivity | **Schemes**: tencent\_im\_push://,  **Hosts:** glatpi.egnyuk.wqmjwg.hsxphx,  **Paths:** /honorMessage, |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**