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

**OKPAY（ 2.3.0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 | OKPAY |
| 版本 | 2.3.0 |
| 包名 | com.gogoppp.com |
| 域名线索 | 29条 |
| URL线索 | 24条 |
| APP图标 |  |
| 分析日期 | 2025年2月22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 | OKPAY.apk |
| 文件大小 | 31.51MB |
| MD5值 | 6582899a862b4e42b39c044a4c405515 |
| SHA1值 | 6ef93d29783a46b345adf2e6860139c1840c631b |
| SHA256值 | 497228aa81a8dd53be28ccb606df12b2affc87167d792ea00199efb22aae245a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | OKPAY |
| 包名 | com.gogoppp.com |
| 主活动Activity | com.leo.okp.MainActivity |
| 安卓版本名称 | 2.3.0 |
| 安卓版本 | 2300 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| d392zskyvppgok.cloudfront.net | 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  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| a2402e.okfy8899.com | IP: 172.66.40.212 所属国家: United States of America 地区: California 城市: San Francisco  |
| developer.apple.com | IP: 17.253.85.205 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| developer.android.com | IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| goo.gl | IP: 142.250.69.206 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.google-analytics.com | IP: 114.250.70.33 所属国家: China 地区: Beijing 城市: Beijing  |
| d1ezmc44834wik.cloudfront.net | 没有服务器地理信息.  |
| 47.108.253.50 | IP: 47.108.253.50 所属国家: China 地区: Sichuan 城市: Chengdu  |
| ns.adobe.com | 没有服务器地理信息.  |
| 8.134.90.244 | IP: 8.134.90.244 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| schemas.microsoft.com | IP: 13.107.253.49 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| www.example.com | IP: 92.122.244.51 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| www.gok4lfahgh2bfasdfasd.live | 没有服务器地理信息.  |
| ssl.google-analytics.com | IP: 114.250.64.41 所属国家: China 地区: Beijing 城市: Beijing  |
| www.okpneway777.com | 没有服务器地理信息.  |
| pagead2.googlesyndication.com | IP: 114.250.63.38 所属国家: China 地区: Beijing 城市: Beijing  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| plus.google.com | IP: 108.160.167.147 所属国家: United States of America 地区: California 城市: San Francisco  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| dartbug.com | IP: 216.239.38.21 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| default.url | 没有服务器地理信息.  |
| schemas.android.com | 没有服务器地理信息.  |
| aomedia.org | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| dl7237s.hudsb4.xyz | 没有服务器地理信息.  |
| www.ibm.com | IP: 23.35.121.153 所属国家: Japan 地区: Tokyo 城市: Tokyo  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | i1/n.java  |
| http://www.google-analytics.com  | i4/n0.java  |
| https://ssl.google-analytics.com  | i4/n0.java  |
| http://goo.gl/8Rd3yj  | i4/d1.java  |
| http://goo.gl/8Rd3yj  | i4/s.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://developer.android.com/reference/javax/net/ssl/SSLSocket  | io/flutter/plugins/videoplayer/VideoPlayerPlugin.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | l3/z.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | p0/a.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | t7/m.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | p1/x0.java  |
| https://plus.google.com/  | y3/j0.java  |
| http://dashif.org/guidelines/last-segment-number  | v2/d.java  |
| http://dashif.org/guidelines/trickmode  | v2/d.java  |
| http://dashif.org/thumbnail\_tile  | v2/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | v2/d.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | p3/b.java  |
| https://x</LA\_URL>  | t1/k0.java  |
| https://default.url  | t1/k0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | t1/l0.java  |
| http://schemas.android.com/apk/res/android  | y/k.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | u7/o.java  |
| http://ns.adobe.com/xap/1.0/  | z1/a.java  |
| https://aomedia.org/emsg/ID3  | j2/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | j2/a.java  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://dartbug.com/52121.  | lib/arm64-v8a/libflutter.so  |
| http://47.108.253.50/api/507e69upb88f00347  | lib/armeabi-v7a/libapp.so  |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status  | lib/armeabi-v7a/libapp.so  |
| http://8.134.90.244/api/64cacupb524741a5d  | lib/armeabi-v7a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/armeabi-v7a/libapp.so  |
| https://i923847m.oo17lom.xyz./api/4e0679e423b9fd5up  | lib/armeabi-v7a/libapp.so  |
| https://i923847m.oo17lom.xyz./api/473bb50ef131aup24  | lib/armeabi-v7a/libapp.so  |
| https://www.okpneway777.com  | lib/armeabi-v7a/libapp.so  |
| https://d392zskyvppgok.cloudfront.net/YBdfpTjAv2inYBdfpTjA  | lib/armeabi-v7a/libapp.so  |
| https://d1ezmc44834wik.cloudfront.net/MGiAEr9Wimgv2MGiAEr9W  | lib/armeabi-v7a/libapp.so  |
| https://dl7237s.hudsb4.xyz/J7v6kAv2inJ7v6kA  | lib/armeabi-v7a/libapp.so  |
| https://www.gok4lfahgh2bfasdfasd.live/client/chat/home.html?code=55b8b6748a2caab189d3347bf1808f6b65e506f53187f904&vavatar=%s&vname=%s&order\_id=%s  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://a2402e.okfy8899.com/DZgv2inDZg  | lib/armeabi-v7a/libapp.so  |
| https://i923847m.oo17lom.xyz./api/788eeb9c55a4b81up  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://dartbug.com/52121.  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/x86\_64/libflutter.so  |
| https://dartbug.com/52121.  | lib/x86\_64/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | u3/u.java  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| \_httpparser@13463476.responsepa \_assetmanifestbin@311287047.fromstanda \_double@0150898.fromintege \_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_growablelist@0150898.\_literal6 \_receiveportimpl@1026248.fromrawrec \_colorfilter@15065589.mode \_imagefilter@15065589.composed \_list@0150898.\_ofarray \_timer@1026248.periodic \_growablelist@0150898.\_literal2 \_list@0150898.empty \_directory@14069316.fromrawpat \_invocationmirror@0150898.\_withtype \_colorfilter@15065589.lineartosr \_growablelist@0150898.\_literal1 \_uri@0150898.file \_imagefilter@15065589.blur \_growablelist@0150898.\_literal4 \_growablelist@0150898.\_ofgrowabl channelcontroller@33156646.implementa \_growablelist@0150898.of \_pointerpanzoomdata@527213599.fromupdate \_hashcollisionnode@70137193.fromcollis authenticationscheme@13463476.fromstring \_list@0150898.of \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_growablelist@0150898.\_literal3 \_growablelist@0150898.\_ofother \_timer@1026248.\_internal androidstorage@31339836.implementa \_growablelist@0150898.\_literal5 \_list@0150898.\_ofother \_bytebuffer@7027147.\_new channelcontroller@30238507.implementa ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_nativesocket@14069316.normal \_imagefilter@15065589.fromcolorf \_colorfilter@15065589.srgbtoline \_uri@0150898.directory \_growablelist@0150898.\_literal8 \_file@14069316.fromrawpat \_compressednode@70137193.single \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |
| appro@openssl.org  | lib/x86\_64/libflutter.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | p4/a.java  |

## **5. 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=sh, L=sh, O=sh, OU=abcd, CN=abc 签名算法: rsassa\_pkcs1v15 有效期自: 2023-08-10 09:53:37+00:00 有效期至: 2050-12-26 09:53:37+00:00 发行人: C=cn, ST=sh, L=sh, O=sh, OU=abcd, CN=abc 序列号: 0x24eca69b 哈希算法: sha256 md5值: 58ccd18a2db451a6e30a5a558ba6f411 sha1值: a1642cd220a1b4cb897bc4fb61badfb04fe7c830 sha256值: 43517a6e9910c71168fc67b82f4a8f09371e490dcf79a8cd2cb8b1303747efc1 sha512值: 2a4410385863183f1d287c633a540d90b0fbadd5356ca6cc85a42a32626ac44ec3dcc895246b75afd20111b7a9cc31b18523caf24f9a3cc96448ce52ffca9ca6 公钥算法: rsa 密钥长度: 2048 指纹: 859401e99c78efb60c1194e001bb1ec1b4decd5d2195587c98a2fb8dbe2f37ce**

## **6. 硬编码敏感信息**

## **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.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\_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\_PRIVILEGED\_PHONE\_STATE | 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 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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\_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.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\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ASSISTED\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_LOCATION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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。 |
| 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.gogoppp.com.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.gogoppp.com.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.leo.okp.MainActivity | **Schemes**: okpay://,  |

**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。**