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

**EZpay（ 2.0.3-normal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 | EZpay |
| 版本 | 2.0.3-normal |
| 包名 | com.flying.p96.normal |
| 域名线索 | 26条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2025年9月5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 | ezpay.apk |
| 文件大小 | 42.34MB |
| MD5值 | dd25f08b373449257300e61249336211 |
| SHA1值 | be7481f174a23b748096ce3a180fe68d0018b8e8 |
| SHA256值 | 035f5c3f49e43084bc3023df6ea066364ee795e956afee3bba5dc0d46a993f41 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | EZpay |
| 包名 | com.flying.p96.normal |
| 主活动Activity | com.flying.p96.MainActivity |
| 安卓版本名称 | 2.0.3-normal |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| uatproxy.caplw.com | IP: 104.18.203.224 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.jsdelivr.com | IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.22.19 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.  |
| stg-m.luckywlt.net | IP: 154.38.203.10 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| m.luckywlt.com | IP: 154.38.203.10 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| stg-proxy.capluckywlt.com | IP: 43.175.130.182 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| stg-m.luckywlt.com | IP: 154.38.203.10 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| 34.96.232.46 | IP: 34.96.232.46 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.tensorflow.org | IP: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto  |
| uatproxy.capluckywlt.com | IP: 104.18.203.224 所属国家: United States of America 地区: California 城市: San Francisco  |
| journeyapps.com | IP: 216.137.39.33 所属国家: United States of America 地区: California 城市: Los Angeles  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| proxy.capluckywlt.com | IP: 43.175.130.182 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| public-capital-lucky-proxy-fat.k8s-fat.com | 没有服务器地理信息.  |
| api.capeleph.com | IP: 10.227.5.18 所属国家: - 地区: - 城市: -  |
| www.example.com | IP: 23.48.5.17 所属国家: Japan 地区: Osaka 城市: Ibaraki  |
| proxy.caplw.com | IP: 43.175.130.182 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| developer.android.com | IP: 142.250.73.142 所属国家: United States of America 地区: California 城市: Mountain View  |
| 34.92.108.46 | IP: 34.92.108.46 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| plus.google.com | IP: 173.252.88.133 所属国家: United States of America 地区: Illinois 城市: Chicago  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://)([\\s\\S]+)  | com/huawei/hms/scankit/p/C0189bd.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://plus.google.com/  | d2/h1.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/h.java  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://github.com/nodeca/pica  | 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://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/arm64-v8a/libbarhopper\_v3.so  |
| http://http  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://api.capeleph.com  | lib/armeabi-v7a/libapp.so  |
| https://m.luckywlt.com  | lib/armeabi-v7a/libapp.so  |
| https://proxy.capluckywlt.com/  | lib/armeabi-v7a/libapp.so  |
| https://stg-proxy.capluckywlt.com/  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://34.92.108.46:8498/  | lib/armeabi-v7a/libapp.so  |
| https://uatproxy.capluckywlt.com/  | lib/armeabi-v7a/libapp.so  |
| https://34.96.232.46:8499  | lib/armeabi-v7a/libapp.so  |
| https://uatproxy.caplw.com/  | lib/armeabi-v7a/libapp.so  |
| http://public-capital-lucky-proxy-fat.k8s-fat.com/  | lib/armeabi-v7a/libapp.so  |
| https://proxy.caplw.com/  | lib/armeabi-v7a/libapp.so  |
| https://stg-m.luckywlt.net  | lib/armeabi-v7a/libapp.so  |
| https://stg-m.luckywlt.com  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| http://http  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/x86/libbarhopper\_v3.so  |
| http://http  | lib/x86/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/x86/libbarhopper\_v3.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/x86\_64/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/x86\_64/libbarhopper\_v3.so  |
| http://http  | lib/x86\_64/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/x86\_64/libbarhopper\_v3.so  |
| https://github.com/flutter/flutter/issues.  | 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  | a2/v.java  |
| android-sdk-releaser@vopo7.prod  | lib/arm64-v8a/libbarhopper\_v3.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| \_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring \_list@0150898.of \_httpparser@13463476.responsepa \_list@0150898.generate \_typeerror@0150898.\_create \_hashcollisionnode@60137193.fromcollis \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_double@0150898.fromintege \_growablelist@0150898.\_literal3 \_future@4048458.immediate \_growablelist@0150898.\_literal channelcontroller@37156646.implementa \_growablelist@0150898.\_ofother \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_timer@1026248.\_internal \_growablelist@0150898.\_literal6 \_growablelist@0150898.\_literal5 \_receiveportimpl@1026248.fromrawrec \_list@0150898.\_ofarray \_timer@1026248.periodic \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from \_list@0150898.empty \_list@0150898.\_ofother \_bytebuffer@7027147.\_new \_directory@14069316.fromrawpat \_invocationmirror@0150898.\_withtype ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_nativesocket@14069316.normal \_compressednode@60137193.single \_uri@0150898.file \_growablelist@0150898.\_literal1 \_uri@0150898.directory androidstorage@35339836.implementa \_growablelist@0150898.\_literal8 \_file@14069316.fromrawpat \_growablelist@0150898.\_literal4 \_growablelist@0150898.\_ofgrowabl \_growablelist@0150898.of channelcontroller@29195533.implementa \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |
| android-sdk-releaser@vopo7.prod  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| android-sdk-releaser@vopo7.prod  | lib/x86/libbarhopper\_v3.so  |
| android-sdk-releaser@vopo7.prod  | lib/x86\_64/libbarhopper\_v3.so  |
| appro@openssl.org  | lib/x86\_64/libflutter.so  |

### **4.4 手机号线索**

## **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=333, ST=mn, L=ph, O=it, OU=zf, CN=flying 签名算法: rsassa\_pkcs1v15 有效期自: 2024-07-27 01:32:13+00:00 有效期至: 2051-12-13 01:32:13+00:00 发行人: C=333, ST=mn, L=ph, O=it, OU=zf, CN=flying 序列号: 0x66fbdf51f605ee9 哈希算法: sha384 md5值: 2b3c8fd2290cb426699d81eae4405acc sha1值: 3276633e5da499648dc5c5838824830b0883605a sha256值: be40c1af20c3c6d2f4f86f1dbb8bab075773d6adb86165a8eb7545bf1bf9dcf6 sha512值: 5c8da6edd36f6751b86baf270d3289b34b1f7813aa61dfbc7562ba61b2d58e0d4ba09de12e32fb72efd5f95f3fffdde0766109ed84ab0c4fe02d917601a4053d 公钥算法: rsa 密钥长度: 2048 指纹: 9e559edb2675ae019b509be8dbd2077d0494fb74777d501c7f266336a4cbf668**

## **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.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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| 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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.flying.p96.normal.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.flying.p96.MainActivity | **Schemes**: ezpay://,  |

**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。**