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

**圆通环球（ 1.0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 | 圆通环球 |
| 版本 | 1.0 |
| 包名 | plus.zlgf |
| 域名线索 | 23条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2025年7月4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 | plus.zlgf.apk |
| 文件大小 | 14.16MB |
| MD5值 | 6fcfd6971677e5465f9ad65fa03e9a94 |
| SHA1值 | 923ffa83708c360f168cf08123c75a479da12fe8 |
| SHA256值 | dbe3a6f3cef5dc0fac21e044340faf81b538fb7a647062d13ecb99585b2cc701 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 圆通环球 |
| 包名 | plus.zlgf |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| mths.be | IP: 83.137.145.144 所属国家: Netherlands 地区: Groningen 城市: Groningen  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| img01.yzcdn.cn | IP: 39.91.174.14 所属国家: China 地区: Shandong 城市: Linyi  |
| bit.ly | IP: 67.199.248.11 所属国家: United States of America 地区: New York 城市: New York City  |
| jquery.com | IP: 104.18.156.119 所属国家: United States of America 地区: California 城市: San Francisco  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| er.dcloud.net.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| m3w.cn | IP: 42.231.138.195 所属国家: China 地区: Henan 城市: Nanyang  |
| ns.adobe.com | 没有服务器地理信息.  |
| schemas.android.com | 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  |
| js.foundation | IP: 104.131.8.164 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| lodash.com | IP: 52.74.232.59 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| jquery.org | IP: 104.17.176.200 所属国家: United States of America 地区: California 城市: San Francisco  |
| element.eleme.io | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| er.dcloud.io | 没有服务器地理信息.  |
| npms.io | IP: 104.21.112.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| underscorejs.org | IP: 172.67.134.18 所属国家: United States of America 地区: California 城市: San Francisco  |
| ask.dcloud.net.cn | IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| openjsf.org | IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut  |
| admin.ggffcm.top | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| push2his.eastmoney.com | IP: 117.184.38.143 所属国家: China 地区: Shanghai 城市: Shanghai  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| https://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| https://er.dcloud.io/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://er.dcloud.net.cn/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/p/h1.java  |
| https://ask.dcloud.net.cn/article/35627  | io/dcloud/p/r.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/p/r.java  |
| https://er.dcloud.io/rv  | io/dcloud/p/d0.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/p/d0.java  |
| https://ask.dcloud.net.cn/article/287  | io/dcloud/share/IFShareApi.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifViewUtils.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| https://ask.dcloud.net.cn/article/36199  | 摸瓜V1引擎  |
| http://a  | 摸瓜V2引擎  |
| http://a/c%20d  | 摸瓜V2引擎  |
| https://push2his.eastmoney.com/api/qt/stock/trends2/get?fields1=f1,f2,f3,f4,f5,f6,f7,f8,f9,f10,f11,f12,f13&fields2=f51,f52,f53,f54,f55,f56,f57,f58&secid=  | 摸瓜V2引擎  |
| https://push2his.eastmoney.com/api/qt/stock/kline/get?fields1=f1,f2,f3,f4,f5,f6,f7,f8,f9,f10,f11,f12,f13&fields2=f51,f52,f53,f54,f55,f56,f57,f58,f59,f60,f61&beg=  | 摸瓜V2引擎  |
| https://push2his.eastmoney.com/api/qt/stock/kline/get?fields1=f1,f2,f3,f4,f5,f6,f7,f8,f9,f10,f11,f12,f13&fields2=f51,f52,f53,f54,f55,f56,f57,f58,f59,f60,f61&beg=20190909&end=20500101&ut=fa5fd1943c7b386f172d6893dbfba10b&rtntype=6&secid=  | 摸瓜V2引擎  |
| https://admin.ggffcm.top  | 摸瓜V2引擎  |
| http://127.0.0.1:8087  | 摸瓜V2引擎  |
| http://127.0.0.1:8080  | 摸瓜V2引擎  |
| http://127.0.0.1:8088  | 摸瓜V2引擎  |
| http://127.0.0.1:8080/API/StockHistoryDay  | 摸瓜V2引擎  |
| http://127.0.0.1:8080/API/FactorTiming  | 摸瓜V2引擎  |
| http://127.0.0.1:8080/API/MarketAttention  | 摸瓜V2引擎  |
| http://127.0.0.1:8080/API/MarketHeat  | 摸瓜V2引擎  |
| http://127.0.0.1:8080/API/QuadrantCalculate  | 摸瓜V2引擎  |
| https://github.com/jones2000/HQChart\n\*\n\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  | 摸瓜V2引擎  |
| https://jquery.com/  | 摸瓜V2引擎  |
| https://jquery.org/license  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| https://img01.yzcdn.cn/vant/coupon-empty.png  | 摸瓜V2引擎  |
| https://img01.yzcdn.cn/vant/empty-image-  | 摸瓜V2引擎  |
| https://img01.yzcdn.cn/vant/share-sheet-  | 摸瓜V2引擎  |
| https://img01.yzcdn.cn/upload\_files/2020/06/24/FmKWDg0bN9rMcTp9ne8MXiQWGtLn.png  | 摸瓜V2引擎  |
| https://lodash.com/>  | 摸瓜V2引擎  |
| https://openjsf.org/>  | 摸瓜V2引擎  |
| https://lodash.com/license>  | 摸瓜V2引擎  |
| http://underscorejs.org/LICENSE>  | 摸瓜V2引擎  |
| https://npms.io/search?q=ponyfill.  | 摸瓜V2引擎  |
| https://bit.ly/2ZqJzkp  | 摸瓜V2引擎  |
| http://127.0.0.1:8886  | 摸瓜V2引擎  |
| https://js.foundation/>  | 摸瓜V2引擎  |
| http://a  | 摸瓜V2引擎  |
| http://a/c%20d  | 摸瓜V2引擎  |
| https://feross.org/opensource>  | 摸瓜V2引擎  |
| https://mths.be/punycode  | 摸瓜V2引擎  |
| http://element.eleme.io/  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| jintongxue2018@163.com  | 摸瓜V2引擎  |
| hilongjw@gmail.com  | 摸瓜V2引擎  |

### **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: True 找到 1 个唯一证书 主题: C=chengdu, ST=chengdu, L=chengdu, O=pr1743832067393, OU=ra1743832067393, CN=zlfr 签名算法: rsassa\_pkcs1v15 有效期自: 2025-04-05 05:47:47+00:00 有效期至: 2075-03-24 05:47:47+00:00 发行人: C=chengdu, ST=chengdu, L=chengdu, O=pr1743832067393, OU=ra1743832067393, CN=zlfr 序列号: 0x4097aa0b 哈希算法: sha1 md5值: a7d7e815e0b65c19e6fd743869a6933e sha1值: 544326be22c87b2cedc13ae0c7e4ee501a695c06 sha256值: f4190b6ab9cf64d6033b49bad564f669847427d79e41cd159fd78c8dfc94311f sha512值: 4402b0bfddeecd4916b29914721008d5553fcde20cce05b27fb0300001fa66be3a458226bb8b3c18a103c2f021ce5ec01584e4c4a69e4480c23abe7cd2ac656f 公钥算法: rsa 密钥长度: 1024 指纹: 8c8fd340ba1eb34d4d7a7afc966404040ec8f8588e1bbe97cf1fcc9482163b38**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API"  |
| "dcloud\_io\_without\_authorization" : "not authorized"  |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service"  |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed"  |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained"  |
| "dcloud\_oauth\_token\_failed" : "failed to get token"  |
| "dcloud\_permissions\_reauthorization" : "reauthorize"  |
| "dcloud\_tips\_certificate" : "certificate"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_io\_without\_authorization" : "没有获得授权"  |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权"  |
| "dcloud\_oauth\_token\_failed" : "获取token失败"  |
| "dcloud\_permissions\_reauthorization" : "重新授权"  |
| "dcloud\_tips\_certificate" : "证书"  |

## **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.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\_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.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 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.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 |
| 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。 |
| com.vivo.notification.permission.BADGE\_ICON | 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.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.asus.msa.SupplementaryDID.ACCESS | 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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: h5904011c://,  |

**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。**