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

**RedotPay（ 2.0.6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 | RedotPay |
| 版本 | 2.0.6 |
| 包名 | com.redotpay |
| 域名线索 | 17条 |
| URL线索 | 17条 |
| APP图标 |  |
| 分析日期 | 2024年12月21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 | redotpay-latest.apk |
| 文件大小 | 130.8MB |
| MD5值 | bceb48cce446311e654d168df4efc896 |
| SHA1值 | 97e9b53576e961a8905a948834dd8320f6557567 |
| SHA256值 | f69471c30387b7c79ace5050b6de07fe1058e39e6120ecd676dfb2daf81ba784 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | RedotPay |
| 包名 | com.redotpay |
| 主活动Activity | com.redotpay.MainActivity |
| 安卓版本名称 | 2.0.6 |
| 安卓版本 | 40 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.binance.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| wanproxy.127.net | IP: 223.252.196.41  所属国家: China  地区: Guangdong  城市: Guangzhou |
| api.sumsub.com | IP: 76.223.74.24  所属国家: United States of America  地区: Washington  城市: Seattle |
| support.sumsub.com | IP: 46.51.152.13  所属国家: Ireland  地区: Dublin  城市: Dublin |
| android.asset | 没有服务器地理信息. |
| wannos.127.net | IP: 223.252.196.42  所属国家: China  地区: Guangdong  城市: Guangzhou |
| 223.252.196.38 | IP: 223.252.196.38  所属国家: China  地区: Guangdong  城市: Guangzhou |
| developer.android.com | IP: 142.251.43.14  所属国家: United States of America  地区: California  城市: Mountain View |
| crash.163.com | IP: 45.254.50.146  所属国家: China  地区: Guangdong  城市: Guangzhou |
| verify.dun.163.com | IP: 59.111.211.180  所属国家: China  地区: Guangdong  城市: Guangzhou |
| dev-in.sumsub.com | IP: 10.220.21.151  所属国家: -  地区: -  城市: - |
| sentry.sumsub.com | IP: 104.18.40.73  所属国家: United States of America  地区: California  城市: San Francisco |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| xml.org | IP: 104.239.240.11  所属国家: United States of America  地区: Texas  城市: Windcrest |
| da.dun.163.com | IP: 59.111.211.178  所属国家: China  地区: Guangdong  城市: Guangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://support.sumsub.com/hc/ | ILtALZMDt9mMFpj/r2tvh3xUM6NLrx2eU2vFh0qjB.java |
| https://github.com/Baseflow/flutter-permission-handler/issues | com/baseflow/permissionhandler/PermissionManager.java |
| https://www.binance.com/ | com/binance/android/binancepay/internal/activity/BinancePayActivity.java |
| http://www.w3.org/TR/SVG11/feature | com/caverock/androidsvg/SVGParser.java |
| http://www.w3.org/2000/svg | com/caverock/androidsvg/SVGParser.java |
| http://www.w3.org/1999/xlink | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/features/external-general-entities | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/features/external-parameter-entities | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/properties/lexical-handler | com/caverock/androidsvg/SVGParser.java |
| http://xmlpull.org/v1/doc/features.html | com/caverock/androidsvg/SVGParser.java |
| https://wannos.127.net/lbs;https://wannos-hz.127.net/lbs;https://wannos-bj.127.net/lbs;https://wannos-oversea.127.net/lbs | com/netease/cloud/nos/yidun/core/AcceleratorConf.java |
| http://223.252.196.38/lbs | com/netease/cloud/nos/yidun/core/AcceleratorConf.java |
| https://wannos.127.net | com/netease/cloud/nos/yidun/core/AcceleratorConf.java |
| http://wanproxy.127.net | com/netease/cloud/nos/yidun/monitor/MonitorConfig.java |
| https://verify.dun.163.com/v1/liveperson/check | com/netease/nis/alivedetected/a.java |
| https://verify.dun.163.com/v1/liveperson/getConf | com/netease/nis/alivedetected/a.java |
| https://da.dun.163.com/sn.gif?d= | com/netease/nis/alivedetected/e/d.java |
| https://crash.163.com/uploadCrashLogInfo.do | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java |
| https://crash.163.com/client/api/uploadStartUpInfo.do | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java |
| https://da.dun.163.com/sn.gif?d= | com/netease/nis/captcha/g.java |
| https://crash.163.com/uploadCrashLogInfo.do | com/netease/nis/crashreport/BaseNdkHandler.java |
| https://crash.163.com/client/api/uploadStartUpInfo.do | com/netease/nis/crashreport/BaseNdkHandler.java |
| https://sentry.sumsub.com/ | com/sumsub/sns/BuildConfig.java |
| https://api.sumsub.com/ | com/sumsub/sns/core/SNSMobileSDK.java |
| https://developer.android.com/guide/topics/permissions/overview | io/flutter/plugin/platform/PlatformPlugin.java |
| https://android.asset/ | io/noties/markwon/image/destination/ImageDestinationProcessorAssets.java |
| http://dev-in.sumsub.com/\ | sd8PpYvrQ9pq27nrQLqVNK2R2/qrdW8Q5Lxs3TMWrXBOy51gfzDXt.java |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | com/caverock/androidsvg/SVGAndroidRenderer.java |
| 17179869184 | com/caverock/androidsvg/SVG.java |
| 17179869184 | com/caverock/androidsvg/SVGParser.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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 签名算法: rsassa\_pkcs1v15 有效期自: 2023-06-07 10:54:25+00:00 有效期至: 2053-06-07 10:54:25+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0x22cf8d57e36aa685659323a8fcd5d28e3616fcfa 哈希算法: sha256 md5值: e6202e604ab438fc046a6a6cd5fd3320 sha1值: d27e5a6c17707077c134691f1663f90b35c6e1f8 sha256值: 9a54863421de226537e25f6374f82d5ba524e15c75826c0980ea34d15f1ad308 sha512值: fea0d1ea6f4bdaf0976bd22129b2e92bb978158d1206079acb7b495a714a152fbecf0f43709e28d4a00e226031050ab8483b050b3b8104d89035d50e00e4e744 公钥算法: rsa 密钥长度: 4096 指纹: 4970d5679b32a4a63080fe3e39d15e68d20383e05fafd53f9c51334f6f772f55**

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.READ\_MEDIA\_IMAGES | 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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_ATTRIBUTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.redotpay.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| 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.huawei.android.launcher.permission.READ\_SETTINGS | 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.huawei.android.launcher.permission.WRITE\_SETTINGS | 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.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.redotpay.MainActivity | **Schemes**: redotpay://,  **Hosts:** app.redotpay.com, |
| com.google.firebase.auth.internal.GenericIdpActivity | **Schemes**: genericidp://,  **Hosts:** firebase.auth,  **Paths:** /, |
| com.google.firebase.auth.internal.RecaptchaActivity | **Schemes**: recaptcha://,  **Hosts:** firebase.auth,  **Paths:** /, |

**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。**