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

**RF（ 2.18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 | RF |
| 版本 | 2.18 |
| 包名 | tw.twhawk.reversedfront |
| 域名线索 | 1条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年6月3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 | tw.twhawk.reversedfront.apk |
| 文件大小 | 93.12MB |
| MD5值 | 4133b362296ec53aaf809771a11781da |
| SHA1值 | 27cf67945e4636fa6735f5bc2fbac3e03f590ad4 |
| SHA256值 | ddb9c50c2c4f68186cec319f854ba3aa1cd27ad23a265f3e4645118d4de53ced |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | RF |
| 包名 | tw.twhawk.reversedfront |
| 主活动Activity | tw.twhawk.reversedfront.MainActivity |
| 安卓版本名称 | 2.18 |
| 安卓版本 | 84 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| appleid.apple.com | IP: 17.23.96.16 所属国家: United States of America 地区: California 城市: Cupertino  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://appleid.apple.com/auth/authorize  | com/RNAppleAuthentication/SignInWithAppleService.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False 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: 2023-08-30 06:55:15+00:00 有效期至: 2053-08-30 06:55:15+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0xbecc5b88d6a3c909beef3e7836a038916380a632 哈希算法: sha256 md5值: 34add9dc0826a3a53daf3a09ec7e6915 sha1值: d2d7e7124da4734f13c9deb1ba1985c0aca32869 sha256值: 20ac52b5cbe59b8f97f88d868e1e8462a769a768426e050425bb86f2f480eaa5 sha512值: 2a193a0c8458240182653e985d0ba0d52fb384afbf2fee0e80f54481c92002aa2a7c34bd7c2c83481b297cbc9a8b253f25890f73750184a2b07e1008333e4626 公钥算法: rsa 密钥长度: 4096 指纹: dd007c08b4d4ac67438bd751b05f797581e11667ce8e57b622077c530c60b8c1**

## **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.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 |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_DATA\_SYNC | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| tw.twhawk.reversedfront.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.facebook.CustomTabActivity | **Schemes**: fbconnect://, **Hosts:** cct.tw.twhawk.reversedfront,  |

**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。**