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

**天风国际（ 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 | 天风国际 |
| 版本 | 1.0 |
| 包名 | com.tfengg2uoij1.app |
| 域名线索 | 1条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2024年11月7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 | base.apk |
| 文件大小 | 5.41MB |
| MD5值 | 26bd90599b5c451aaa6a87dd5c445c9c |
| SHA1值 | ee9c6f242be6ff253220ae2941a631306b64ab08 |
| SHA256值 | adf6cebe938b49d5d67b5c6edef446ba318e00bc827d261f0ac1647329cfc301 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 天风国际 |
| 包名 | com.tfengg2uoij1.app |
| 主活动Activity | com.tfgainter.app.SplActivity |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 43.154.110.166 | IP: 43.154.110.166 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://43.154.110.166:9633/mmmmmm  | com/tfgainter/app/WebActivity.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| android.studio@android.com  | 摸瓜V1引擎  |

### **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: False 找到 1 个唯一证书 主题: CN=2, OU=2, O=3, L=3, ST=4, C=4 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-04 03:51:12+00:00 有效期至: 2049-09-28 03:51:12+00:00 发行人: CN=2, OU=2, O=3, L=3, ST=4, C=4 序列号: 0x1 哈希算法: sha256 md5值: afc3189eb010ef11be01b7f19b360fb3 sha1值: 5c1373cd2460912120cf9329f44ccc2ad482a61f sha256值: a3be833072d4522b7188ecba85c83e45d118fd809b09f7d06b8d7a0689388a11 sha512值: 63dd847929e42e8e7869d49ae286847c2999f906078411019a3f18faaff92dcdaacac524915f0cc7d619553ba4f7faf2c54533f8b658885cb03607c552c38f2b 公钥算法: rsa 密钥长度: 2048 指纹: 6d5c15b63ce74412ad60292b226cae0b32b635d2f5eb594034a7695b5ca965ac**

## **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.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.READ\_MEDIA\_VIDEO | 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.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.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.tfengg2uoij1.app.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**