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

**手工小镇（ 1.0.0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 | 手工小镇 |
| 版本 | 1.0.0 |
| 包名 | dsf.tyr.retye.apk |
| 域名线索 | 1条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年1月31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 | dsf.tyr.retye.apk |
| 文件大小 | 3.47MB |
| MD5值 | f5a8d8168861f99b6584a73b5e6566f8 |
| SHA1值 | a0fc4f868d598c14682a94b49bdf15b8b6cd4b53 |
| SHA256值 | d267d87025afa6ac4b20f1db4230068c0f6601b641beea273b92486c3a269900 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 手工小镇 |
| 包名 | dsf.tyr.retye.apk |
| 主活动Activity | [] |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| schemas.android.com | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android | e/g/d/f/k.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: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, O=COM, OU=IT, CN=BUPA 签名算法: rsassa\_pkcs1v15 有效期自: 2023-08-17 05:53:12+00:00 有效期至: 2123-07-24 05:53:12+00:00 发行人: C=CN, O=COM, OU=IT, CN=BUPA 序列号: 0x128d1ae7 哈希算法: sha256 md5值: 822c8a7d12b318f635f91f6ebd8cefda sha1值: 8d6b37760bd2dfc445a08b613e9f331fd13f55a7 sha256值: 9f773b748a1fd04dbcde591cb0e5b4cd25c2ad85a3f9f8d7065c5b5c00cacaec sha512值: f82d93d33b6ead323e752eb6381a12df4cbfede88aac449abf0d1f43cfa5bf892b35d39439c1e5b610b1a8186122799d3db33ebae4298e68b284f40b4d1e3e5a 公钥算法: rsa 密钥长度: 2048 指纹: 8baaf0d4180336817a4f23a6cba1931c58405d129c62716d79ff6ed54a40969c**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "p\_rcpush\_mzAppKey" : "" |
| "p\_rcpush\_opAppKey" : "" |
| "p\_rcpush\_opAppSecret" : "" |
| "p\_rcpush\_vvAppKey" : "" |
| "p\_rcpush\_xmAppKey" : "" |
| "p\_weibo\_appkey" : "" |

## **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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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。 |
| dsf.tyr.retye.permission.YM\_APP | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.lt.app.JumpActivity | **Schemes**: ltapp364673://, |

**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。**