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

**Tolpar（ 1.5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 | Tolpar |
| 版本 | 1.5 |
| 包名 | tolpar.cn |
| 域名线索 | 2条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年10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 | b4398a753aceb98ad59249fd572d9ccc.apk |
| 文件大小 | 6.37MB |
| MD5值 | b4398a753aceb98ad59249fd572d9ccc |
| SHA1值 | 81970559f7891891a13d776a31d729e57848cf18 |
| SHA256值 | a7284253c73703bcf854236ce051109ae0cad174b420220bf0782541b4c02625 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Tolpar |
| 包名 | tolpar.cn |
| 主活动Activity | com.iapp.app.run.mian |
| 安卓版本名称 | 1.5 |
| 安卓版本 | 100001 |

## **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.  |
| iappzy.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://iappzy.com/a.png  | com/mx/MainActivity.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/f.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| pat@pat.net  | bsh/Interpreter.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179878401  | bsh/ParserTokenManager.java  |
| 17179869184  | bsh/ParserTokenManager.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=cn, ST=bj, L=bj, O=ipuser, OU=ipuser, CN=ipuser 签名算法: rsassa\_pkcs1v15 有效期自: 2016-07-02 11:43:26+00:00 有效期至: 2098-08-21 11:43:26+00:00 发行人: C=cn, ST=bj, L=bj, O=ipuser, OU=ipuser, CN=ipuser 序列号: 0x3435f5c4 哈希算法: sha256 md5值: c118816b9a0f406ba5ba053c67638185 sha1值: ae773917cc7a7523b41e1eb95bed61cf0aa8e3b0 sha256值: ac0d0777ca24956f8d584c69a7fd5d2e4fb88e276d953aec9e29ceeb9aa78e32 sha512值: 4667da273fe54297d8c90136e189f721a4bf15ba360aac00f095756e2ed09e59edcf69e08cddd20c379bff78f3b4d59c0fcb3ad5ed3c93dc472c8a85a40a21f5 公钥算法: rsa 密钥长度: 2048 指纹: 8bbf61332bce2af8264b5b6a580609a347650411f6732d955346f9f5fe76cf86**

## **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.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 |
| 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.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 |
| i.app | 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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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。 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |

## **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。**