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

**下载工具（ 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 | 下载工具 |
| 版本 | 1.5 |
| 包名 | com.downloadtool |
| 域名线索 | 3条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年8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 | DownloadTool.apk |
| 文件大小 | 0.1MB |
| MD5值 | 17eb0ce927cf08ffbb7a9a4c55080b66 |
| SHA1值 | 19dd4e07673bffe8815ac939fa8eb935d54582e9 |
| SHA256值 | c825523cb17a024141c3e58c433cee78aeeb67017b284040bf6a3c785833cb63 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 下载工具 |
| 包名 | com.downloadtool |
| 主活动Activity | .StartActivity |
| 安卓版本名称 | 1.5 |
| 安卓版本 | 5 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| package.minghui.org | IP: 103.214.168.106 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.minghui.org | IP: 162.125.8.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.mhradio.org | IP: 199.59.149.203 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.minghui.org/mh/articles/%d/%d/%d/%d-%d-%d  | com/downloadtool/MainActivity.java  |
| http://package.minghui.org/dafa\_baozhang/mhweekly/%d/mhweekly%d  | com/downloadtool/MainActivity.java  |
| http://www.mhradio.org/news\_images/audio01/%d/%d/%d/mhzk%d-1.mp3  | com/downloadtool/MainActivity.java  |
| http://www.mhradio.org/news\_images/audio01/%d/%d/%d/mhzk%d-1.wma  | com/downloadtool/MainActivity.java  |
| http://package.minghui.org/dafa\_baozhang/mhzb/%d/MHZB\_%d  | com/downloadtool/MainActivity.java  |
| http://package.minghui.org/dafa\_baozhang/mhzb/%d/mhzb-%d  | com/downloadtool/MainActivity.java  |
| http://www.minghui.org/mh/fenlei/217/217.zip  | com/downloadtool/MainActivity.java  |
| http://www.minghui.org/  | com/downloadtool/MainActivity.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: False v3 签名: False 找到 1 个唯一证书 主题: CN=name 签名算法: rsassa\_pkcs1v15 有效期自: 2013-03-16 13:23:02+00:00 有效期至: 2038-03-10 13:23:02+00:00 发行人: CN=name 序列号: 0x7f5e63f2 哈希算法: sha256 md5值: b7f4a6c11d723612a9d274bc213aa4d6 sha1值: a012f932413721877ac78513da944a587fcefc88 sha256值: c1199c9ee3632461b1f9c061130e1d63f33d0dbc4cb154b6bea457d47608e960 sha512值: 0e2d4ac372a5107f2af5aad6a1addbf7bfc2c2ad8a6500ee580f9dc6ac9c0dc53f06954cc6761364ac0f97ffd2f9fa5caa48e3689c15bdd9501e8888b44e7fd4**

## **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\_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.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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.ACCESS\_SUPERUSER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.ACCESS\_BLUETOOTH\_SHARE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.HARDWARE\_TEST | 合法 | 测试硬件 | 允许应用程序控制各种外围设备以进行硬件测试 |

## **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。**