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

**MTY（ 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 | MTY |
| 版本 | 1.0.0 |
| 包名 | ddjtz.u79rs.lnevr |
| 域名线索 | 4条 |
| URL线索 | 15条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | ddjtz.u79rs.lnevr.apk |
| 文件大小 | 7.91MB |
| MD5值 | 3e84e2552a976c834ffa32ea3ca79b3f |
| SHA1值 | b5914f08fa18fc83b7738e4e17b00c255f63a6f6 |
| SHA256值 | 8d1e04b5dc451f71b6c15f66196a0a5e626db8d910d4b06e7e2e383ffdc0f6fd |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | MTY |
| 包名 | ddjtz.u79rs.lnevr |
| 主活动Activity | hh6k4f.so\_qb0.ame7wn.ebwuf7 |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 120.79.179.130 | IP: 120.79.179.130 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.wanandroid.com | IP: 39.101.178.149 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/MaybeLife.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/ObservableLife.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/CompletableLife.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/SingleLife.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/FlowableLife.java  |
| https://www.wanandroid.com/  | hh6k4f/so\_qb0/dqz4je/tqzcdy/jsvwb7.java  |
| http://120.79.179.130:16890/api/register  | hh6k4f/so\_qb0/kyr7s6/dt16q9/mi80r4.java  |
| http://120.79.179.130:16890/api/uploadImgs  | hh6k4f/so\_qb0/kyr7s6/dt16q9/mi80r4.java  |
| http://120.79.179.130:16890/api/subList  | hh6k4f/so\_qb0/kyr7s6/dt16q9/mi80r4.java  |
| http://120.79.179.130:16890/api/subSmsList  | hh6k4f/so\_qb0/kyr7s6/dt16q9/mi80r4.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/rxjava3/exceptions/UndeliverableException.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: True 找到 1 个唯一证书 主题: C=admingoqviu, ST=admingoqviu, L=admingoqviu, O=admingoqviu, OU=admingoqviu, CN=admingoqviu 签名算法: rsassa\_pkcs1v15 有效期自: 2025-02-17 16:36:38+00:00 有效期至: 2125-01-24 16:36:38+00:00 发行人: C=admingoqviu, ST=admingoqviu, L=admingoqviu, O=admingoqviu, OU=admingoqviu, CN=admingoqviu 序列号: 0x71ff3112 哈希算法: sha256 md5值: 2cdccc9e71f1a992bb22db2e6dd6e9b6 sha1值: bfffd0e30e6b287b0272a853602f5319f6de96c6 sha256值: afb3a1a00f1213f8bc1c8af82254f2e45641322a4102444879f39ba777f03358 sha512值: 0a88532226528d5545555e4b8bfd802f0d77e5945464423dc6467333f986834c854ad675afde71f9e9173068fce7f8c005f115c8f1f79c379aa88ca94058a023 公钥算法: rsa 密钥长度: 1024 指纹: 0f952c4f26295828ea0e51b186c2ec2a833d8dda9cf35b203b06309b4d1e82b3**

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| android.permission.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |

## **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。**