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

**Project slimBOXtv（ 1.7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 | Project slimBOXtv |
| 版本 | 1.7 |
| 包名 | slim.box.tv.project |
| 域名线索 | 4条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年8月22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 | SBXproject\_9.apk |
| 文件大小 | 0.38MB |
| MD5值 | c3da535cb8c7ecd66fe43d07d9961ed7 |
| SHA1值 | 2bbb4348138224d80620f549ef8128500214b1b4 |
| SHA256值 | 6d1db535bf1695e4d0da7cc07fa3cfb1cb40e4c44f8b74405434599319e11810 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Project slimBOXtv |
| 包名 | slim.box.tv.project |
| 主活动Activity | slim.box.tv.project.MainActivity |
| 安卓版本名称 | 1.7 |
| 安卓版本 | 5 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| slimboxtv.ru | IP: 46.30.40.108 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| qiwi.com | IP: 91.232.230.50 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| t.me | IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington  |
| yoomoney.ru | IP: 185.71.78.222 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://t.me/mrSlimHouse  | Mogua Engine V1  |
| http://qiwi.com/n/SLIMBOX  | Mogua Engine V1  |
| https://yoomoney.ru/to/410012101149856  | Mogua Engine V1  |
| http://slimboxtv.ru  | Mogua Engine V1  |
| https://t.me/slimbox\_chat  | Mogua Engine V1  |

### **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=RU, ST=slimBOXtv, L=krasnodar, O=slimBOXtv, OU=slimBOXtv, CN=slim, E=shbboxx@gmail.com 签名算法: rsassa\_pkcs1v15 有效期自: 2021-10-28 21:18:06+00:00 有效期至: 2053-04-22 21:18:06+00:00 发行人: C=RU, ST=slimBOXtv, L=krasnodar, O=slimBOXtv, OU=slimBOXtv, CN=slim, E=shbboxx@gmail.com 序列号: 0xfb0e3489bac93ffa 哈希算法: sha1 md5值: acb38f8cdd553553743a9d199cde0c6b sha1值: c06940b454fd9f909ddd9c25838d118d1daeb73b sha256值: 414adf3f599b84ba52ef7f9e02e09363a9e421084683030389956be80d007df0 sha512值: 2f122912fa01c8176435a56c0297d49cac3a5ad4035e721be40f70bd154227a9ee5111071ac180e814725597bfe38937cfe6e7b99696e53f3902152d6e605b53 公钥算法: rsa 密钥长度: 1024 指纹: 8be8a6320be44fb238245a0b89ae6618109b8e22747c54f0d23ab20611ff40fd**

## **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.ACCESS\_SUPERUSER | 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\_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.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.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.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\_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.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.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| 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.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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.REAL\_GET\_TASKS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FORCE\_STOP\_PACKAGES | 合法 | 强制停止其他应用程序 | 允许一个应用程序强行停止其他应用程序 |

## **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。**