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

**牧兰优选（ 1.1.6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 | 牧兰优选 |
| 版本 | 1.1.6 |
| 包名 | com.dbzvgk.stfttw |
| 域名线索 | 11条 |
| URL线索 | 8条 |
| APP图标 |  |
| 分析日期 | 2025年2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 | mlyx.apk |
| 文件大小 | 22.18MB |
| MD5值 | ee2a179b466b788c2284eed6f125ca7e |
| SHA1值 | 5fd4499f0815d9129ce3e01ac84cefac2ea6cacf |
| SHA256值 | 4490edd11bb1763958aed4fff87eddcbbcdb24ce7eb4106c56f7990ae39f7fd5 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 牧兰优选 |
| 包名 | com.dbzvgk.stfttw |
| 主活动Activity | com.googlecnx.androidcnx.MainActivity |
| 安卓版本名称 | 1.1.6 |
| 安卓版本 | 3 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| log.tbs.qq.com | IP: 109.244.244.32 所属国家: China 地区: Beijing 城市: Beijing  |
| h5.mulanny.com | IP: 211.149.185.85 所属国家: China 地区: Sichuan 城市: Chengdu  |
| tbsrecovery.imtt.qq.com | IP: 109.244.244.237 所属国家: China 地区: Beijing 城市: Beijing  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| cfg.imtt.qq.com | IP: 109.244.173.227 所属国家: China 地区: Beijing 城市: Beijing  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| debugx5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| debugtbs.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| pms.mb.qq.com | IP: 109.244.173.227 所属国家: China 地区: Beijing 城市: Beijing  |
| mdc.html5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| china-dna.com | IP: 116.62.238.180 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://china-dna.com  | com/googlecnx/androidcnx/MainActivityX.java  |
| http://h5.mulanny.com  | com/googlecnx/androidcnx/MainActivity.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/n.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/n.java  |
| https://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/n.java  |
| https://tbsrecovery.imtt.qq.com/getconfig  | com/tencent/smtt/utils/n.java  |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| https://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/m.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/ui/dialog/d.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=20bd0f88, ST=20bd0f88, L=20bd0f88, O=20bd0f88, OU=20bd0f88, CN=20bd0f88 签名算法: rsassa\_pkcs1v15 有效期自: 2023-03-25 02:00:13+00:00 有效期至: 2023-06-23 02:00:13+00:00 发行人: C=20bd0f88, ST=20bd0f88, L=20bd0f88, O=20bd0f88, OU=20bd0f88, CN=20bd0f88 序列号: 0x14f3cd40 哈希算法: sha256 md5值: 0067773a447159cd34ca4f101bbbee63 sha1值: af71f1e5b868acb77367f04f54a9f55989ba4e1d sha256值: 451ad875db773a07273eddbbb7e852718d9622f8a78a3498852c84968d121cb1 sha512值: 83dd46bf6cd0013d930faa033bd35cffe9053714c6c9dc6bbb54363a49d22455a2229ae5e41119cdac05549979f590505b51390225674c970430c2363f2938f7 公钥算法: rsa 密钥长度: 2048 指纹: d99ebf28b953c2ff5ceddd2021ed06f1bd5cc880c0c296ceef63163c9c297cea**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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 |

## **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。**