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

**媚娘（ 8.0.7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 | 媚娘 |
| 版本 | 8.0.7 |
| 包名 | com.fltwgynech.mwfiqdmbcc |
| 域名线索 | 8条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年6月18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 | 136295780\_sign.apk |
| 文件大小 | 46.48MB |
| MD5值 | 67d2a9af6d0be17f8bcde6cea9df2b35 |
| SHA1值 | 024ea4e8b29ab5ccac400b85a62aa9b44eb9526a |
| SHA256值 | 8c7541bbabace6a5f2b93c2cf2b98bc345834e561c7e7f19fce00c096aacee37 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 媚娘 |
| 包名 | com.fltwgynech.mwfiqdmbcc |
| 主活动Activity | com.fltwgynech.mwfiqdmbcc.MainActivity |
| 安卓版本名称 | 8.0.7 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.jd.co.th | 没有服务器地理信息.  |
| uranus.jd.com | IP: 120.52.83.70 所属国家: China 地区: Hebei 城市: Langfang  |
| beta-api.jd.co.th | 没有服务器地理信息.  |
| 11.50.163.13 | IP: 11.50.163.13 所属国家: United States of America 地区: Ohio 城市: Columbus  |
| stream-outside.jd.com | IP: 211.144.27.35 所属国家: China 地区: Beijing 城市: Beijing  |
| heracles.jd.com | IP: 60.9.5.193 所属国家: China 地区: Hebei 城市: Hengshui  |
| api.m.jd.com | IP: 120.52.83.22 所属国家: China 地区: Hebei 城市: Langfang  |
| beta-api.m.jd.com | IP: 172.18.255.235 所属国家: - 地区: - 城市: -  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://api.m.jd.com/api  | com/jingdong/aura/sdk/update/request/c.java  |
| https://beta-api.m.jd.com/api  | com/jingdong/aura/sdk/update/request/c.java  |
| https://beta-api.jd.co.th/api  | com/jingdong/aura/sdk/update/request/c.java  |
| https://api.jd.co.th/api  | com/jingdong/aura/sdk/update/request/c.java  |
| http://11.50.163.13:8088/microAppPlugin  | com/jingdong/aura/sdk/update/request/c.java  |
| https://heracles.jd.com/download/policy\_eids/  | com/jingdong/jdma/record/JDMAEngineImpl.java  |
| https://uranus.jd.com/log/m/v2  | com/jingdong/jdma/common/utils/Constant.java  |
| https://heracles.jd.com/download/policy\_eids/  | com/jingdong/jdma/strategy/ConfigBean.java  |
| https://heracles.jd.com/download/policy\_eids/  | com/jingdong/jdma/strategy/ConfigManager.java  |
| https://stream-outside.jd.com/track/verify  | com/jingdong/jdma/d/g.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**无法读取代码签名证书.**

## **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\_MEDIA\_VISUAL\_USER\_SELECTED | 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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 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\_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.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| 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.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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.PACKAGE\_USAGE\_STATS | 合法 | 更新组件使用统计 | 允许修改收集的组件使用统计。不供普通应用程序使用 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| 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.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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 |
| com.fltwgynech.mwfiqdmbcc.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**