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

**戏曲多多（ 1.0.6.0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 | 戏曲多多 |
| 版本 | 1.0.6.0 |
| 包名 | com.duoduo.opreatv |
| 域名线索 | 23条 |
| URL线索 | 25条 |
| APP图标 |  |
| 分析日期 | 2025年7月31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 | 7172.apk |
| 文件大小 | 7.7MB |
| MD5值 | d799501659766c27c34e1d83d62aacf5 |
| SHA1值 | 420849a03fca42944b0d4fcabf213bcb1e6fae17 |
| SHA256值 | 9bca9bc4958b912c2d94df08b1b323a93ae0bc45537385372bf0b37780a9da4b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 戏曲多多 |
| 包名 | com.duoduo.opreatv |
| 主活动Activity | com.duoduo.opreatv.ui.SplashActivity |
| 安卓版本名称 | 1.0.6.0 |
| 安卓版本 | 1060 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ucc.umeng.com | IP: 203.119.169.9 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| main.xiquduoduo.com | IP: 39.106.250.1 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| imtt.dd.qq.com | IP: 39.91.140.213 所属国家: China 地区: Shandong 城市: Linyi  |
| temai.taobao.com | IP: 59.82.23.172 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| aspect-upush.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| errlogos.umeng.com | IP: 47.246.110.18 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| errnewlogos.umeng.com | IP: 47.246.110.96 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| alogsus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| gcw.bdcdn.shoujiduoduo.com | IP: 150.138.110.41 所属国家: China 地区: Shandong 城市: Qingdao  |
| ulogs.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| developer.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| errlog.umeng.com | IP: 223.109.148.180 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ulogs.umengcloud.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| errnewlog.umeng.com | IP: 223.109.148.180 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| log.djduoduo.com | IP: 116.62.216.222 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m.baidu.com | IP: 110.242.71.103 所属国家: China 地区: Hebei 城市: Baoding  |
| pslog.umeng.com | IP: 59.82.60.44 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| plbslog.umeng.com | IP: 36.156.202.73 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| cdnbbbd.shoujiduoduo.com | IP: 123.117.132.35 所属国家: China 地区: Beijing 城市: Beijing  |
| utoken.umeng.com | IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://m.baidu.com  | a0/a.java  |
| http://cdnbbbd.shoujiduoduo.com/bb/games/rec/cartoonv2.png  | a0/a.java  |
| http://gcw.bdcdn.shoujiduoduo.com/bama/jar/duo\_baidu\_5.8.jpg  | a0/a.java  |
| http://gcw.bdcdn.shoujiduoduo.com/bama/jar/duo\_gdt\_4.28.902.jpg  | a0/a.java  |
| http://cdnbbbd.shoujiduoduo.com/bb/games/rec/babysong.png  | a0/a.java  |
| http://imtt.dd.qq.com/16891/A70202A499BF4A3121EB2781EFEE809D.apk?fsname=com.duoduo.duoduocartoon\_1.5.1.0\_1510.apk&csr=1bbd  | a0/a.java  |
| http://imtt.dd.qq.com/16891/9E7905202867A12D62B498D9F644905C.apk?fsname=com.duoduo.child.story\_3.8.2.1\_3821.apk&csr=1bbd  | a0/a.java  |
| http://cdnbbbd.shoujiduoduo.com/bb/games/rec/bamadance.png  | a0/a.java  |
| http://gcw.bdcdn.shoujiduoduo.com/bama/img/c\_opera\_ad\_logo.png  | a0/a.java  |
| http://temai.taobao.com/?pid=mm\_45015339\_6770250\_28434796  | a0/a.java  |
| https://main.xiquduoduo.com  | com/duoduo/opreatv/b.java  |
| http://img  | com/duoduo/opreatv/media/mvcache/MVCacheMgrImpl.java  |
| http://%s:%d  | com/duoduo/opreatv/media/mvcache/proxy/b.java  |
| http://imtt.dd.qq.com/16891/A70202A499BF4A3121EB2781EFEE809D.apk?fsname=com.duoduo.duoduocartoon\_1.5.1.0\_1510.apk&csr=1bbd  | com/duoduo/opreatv/utils/ServerConfig.java  |
| http://cdnbbbd.shoujiduoduo.com/bb/games/rec/cartoonv2.png  | com/duoduo/opreatv/utils/ServerConfig.java  |
| http://cdnbbbd.shoujiduoduo.com/bb/games/rec/babysong.png  | com/duoduo/opreatv/utils/ServerConfig.java  |
| http://imtt.dd.qq.com/16891/9E7905202867A12D62B498D9F644905C.apk?fsname=com.duoduo.child.story\_3.8.2.1\_3821.apk&csr=1bbd  | com/duoduo/opreatv/utils/ServerConfig.java  |
| http://cdnbbbd.shoujiduoduo.com/bb/games/rec/bamadance.png  | com/duoduo/opreatv/utils/ServerConfig.java  |
| http://gcw.bdcdn.shoujiduoduo.com/bama/img/c\_opera\_ad\_logo.png  | com/duoduo/opreatv/utils/ServerConfig.java  |
| https://main.xiquduoduo.com  | com/duoduo/opreatv/network/f.java  |
| https://main.xiquduoduo.com/bama/service/s.php?  | com/duoduo/opreatv/network/f.java  |
| https://main.xiquduoduo.com/bama.bak/service/s.php?  | com/duoduo/opreatv/network/f.java  |
| https://main.xiquduoduo.com/bama/apppage/usb\_copy.php?&prod=  | com/duoduo/opreatv/network/f.java  |
| http://log.djduoduo.com/logs/log.php  | com/duoduo/opreatv/network/f.java  |
| https://main.xiquduoduo.com/bama/private\_policy\_gcw.html  | com/duoduo/opreatv/network/f.java  |
| https://main.xiquduoduo.com/bama/private\_policy/opera\_tv.html  | com/duoduo/opreatv/network/f.java  |
| https://main.xiquduoduo.com/bama/service\_policy/opera\_tv.html  | com/duoduo/opreatv/network/f.java  |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/f/c.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/j.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/j.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/j.java  |
| http://%s:%d/%s  | com/danikula/videocache/l.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/l.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | com/umeng/analytics/pro/an.java  |
| https://ucc.umeng.com/v2/inn/fetch  | com/umeng/analytics/pro/ao.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://errnewlog.umeng.com  | com/umeng/umcrash/UMCrashContent.java  |
| https://errnewlogos.umeng.com  | com/umeng/umcrash/UMCrashContent.java  |
| https://errnewlogos.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlogos.umeng.com  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlog.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlog.umeng.com  | com/umeng/umcrash/UMCrash.java  |
| https://utoken.umeng.com  | com/umeng/umzid/ZIDManager.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/e.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/d.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/videocache/j.java  |
| permission@gmail.com  | com/yanzhenjie/permission/checker/c.java  |

### **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: C=inject, ST=inject, L=inject, O=inject, OU=inject, CN=inject.keystore 签名算法: rsassa\_pkcs1v15 有效期自: 2019-10-11 02:39:57+00:00 有效期至: 2841-02-23 02:39:57+00:00 发行人: C=inject, ST=inject, L=inject, O=inject, OU=inject, CN=inject.keystore 序列号: 0x47f931c3 哈希算法: sha256 md5值: 64843786c6ada15ca4254f4da77e4978 sha1值: b2e643d00042e8e23481794e88eedd3966c65dfa sha256值: 28afa96de62296ef3b7598b27d00b673920d3e0bf5fad9c95ad4ef8de5d8df99 sha512值: 2bcfcb9c6759eb8689d05d7f2393725c1ebea61bf8c4559c9057dc654ad28c1c776ddbe55a6f8a6af71968f2883555e7a74e6c588854a5a2c275ddb4cf0536d2**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "protocol\_user" : "用户协议"  |

## **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.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.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.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.PROCESS\_OUTGOING\_CALLS | 危险 | 拦截拨出电话 | 允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话 |
| 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 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.BIND\_VPN\_SERVICE | 合法 |  | VpnService 必须要求,以确保只有系统可以绑定到它 |
| 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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.duoduo.opreatv.ui.SplashActivity | **Schemes**: um.5d6f805d3fc195033c000b51://,  |

**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。**