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

**母狗园（ 2.3.0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 | 母狗园 |
| 版本 | 2.3.0 |
| 包名 | com.androidjks.aw.d1735030412293165332 |
| 域名线索 | 20条 |
| URL线索 | 32条 |
| APP图标 |  |
| 分析日期 | 2025年10月2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 | shishidh\_2.3.0\_30539743.apk |
| 文件大小 | 40.4MB |
| MD5值 | 9268475e8b125fd1024674245be75bdd |
| SHA1值 | ae44a4e70d7d1975d3447265c3af40231cad9ebb |
| SHA256值 | c9a67930b0094eb92a9f1d183bcf35ab3c36b4d8d58759a0ac8e8a5b5f8fc0ff |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 母狗园 |
| 包名 | com.androidjks.aw.d1735030412293165332 |
| 主活动Activity | com.grass.mh.SplashActivity |
| 安卓版本名称 | 2.3.0 |
| 安卓版本 | 230 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| data.flurry.com | IP: 98.136.147.17 所属国家: United States of America 地区: New York 城市: New York City  |
| aw.vkdzygl0.xyz | 没有服务器地理信息.  |
| playready.directtaps.net | IP: 104.45.231.79 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.example.com | IP: 173.222.245.18 所属国家: Italy 地区: Lazio 城市: Rome  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.slf4j.org | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| freemarker.org | IP: 192.64.119.217 所属国家: United States of America 地区: Georgia 城市: Atlanta  |
| tc-bj-alijs-1324672756.cos.ap-beijing.myqcloud.com | IP: 153.3.46.162 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| freemarker.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| d56pev9tevmkv.cloudfront.net | IP: 3.169.8.196 所属国家: United States of America 地区: Washington 城市: Seattle  |
| schemas.android.com | 没有服务器地理信息.  |
| api.login.yahoo.com | IP: 74.6.160.138 所属国家: United States of America 地区: New York 城市: New York City  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| aw.vjgx0zd6.xyz | 没有服务器地理信息.  |
| aw.vekqdyjy.xyz | 没有服务器地理信息.  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| greenrobot.org | IP: 85.13.163.69 所属国家: Germany 地区: Thuringen 城市: Friedersdorf  |
| d12ilce452zs0c.cloudfront.net | IP: 18.65.214.130 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| cfg.flurry.com | IP: 69.147.80.12 所属国家: United States of America 地区: New York 城市: New York City  |
| clsp.fun | IP: 143.92.53.209 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/mp3cache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/mp3cache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/mp3cache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/mp3cache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/mp3cache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/mp3cache/HttpProxyCacheServer.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.java  |
| http://www.example.com  | com/flurry/sdk/ed.java  |
| https://cfg.flurry.com/sdk/v1/config  | com/flurry/sdk/cl.java  |
| https://cfg.flurry.com/sdk/v1/config  | com/flurry/sdk/by.java  |
| https://data.flurry.com/v1/flr.do  | com/flurry/sdk/br.java  |
| https://api.login.yahoo.com/oauth2/device\_session  | com/flurry/sdk/ef.java  |
| https://aw.vekqdyjy.xyz  | com/grass/mh/SplashActivity.java  |
| https://aw.vjgx0zd6.xyz  | com/grass/mh/SplashActivity.java  |
| https://aw.vkdzygl0.xyz  | com/grass/mh/SplashActivity.java  |
| https://d56pev9tevmkv.cloudfront.net/aw.json  | com/grass/mh/SplashActivity.java  |
| https://tc-bj-alijs-1324672756.cos.ap-beijing.myqcloud.com/aw.json  | com/grass/mh/SplashActivity.java  |
| https://d12ilce452zs0c.cloudfront.net/aw\_ldy.json  | com/grass/mh/SplashActivity.java  |
| https://clsp.fun  | com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java  |
| https://freemarker.apache.org/docs/ref\_builtins.html;  | freemarker/core/BuiltIn.java  |
| http://freemarker.org/docs/ref\_directive\_list.html).  | freemarker/core/FMParserTokenManager.java  |
| http://freemarker.org/docs/ref\_directive\_alphaidx.html;  | freemarker/core/FMParserTokenManager.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| http://schemas.android.com/apk/res/android  | org/dsq/library/widget/tablayout/SlidingTabLayout.java  |
| http://schemas.android.com/apk/res/android  | org/dsq/library/widget/tablayout/SegmentTabLayout.java  |
| http://schemas.android.com/apk/res/android  | org/dsq/library/widget/tablayout/CommonTabLayout.java  |
| https://greenrobot.org/greendao/documentation/database-encryption/  | org/greenrobot/greendao/database/DatabaseOpenHelper.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifViewUtils.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/mp3cache/HttpUrlSource.java  |
| danikula@gmail.com  | com/danikula/videocache/HttpUrlSource.java  |
| aw666me01@gmail.com  | com/grass/mh/SplashActivity.java  |
| aw666me01@gmail.com  | 摸瓜V1引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869185  | freemarker/core/FMParserTokenManager.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **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=86, ST=Hainan, L=Haikou, O=wujikeji, OU=CHN, CN=ChenXiaopeng 签名算法: rsassa\_pkcs1v15 有效期自: 2024-07-08 03:53:48+00:00 有效期至: 2049-07-02 03:53:48+00:00 发行人: C=86, ST=Hainan, L=Haikou, O=wujikeji, OU=CHN, CN=ChenXiaopeng 序列号: 0x1d9272ce 哈希算法: sha256 md5值: 6611eaf74372fd774c2e0599ebb2c5b3 sha1值: a735159e80a7445642fd7f8f506780d21e50f4a4 sha256值: ec46082daea84aac1dd4c81bb2b30d5f42bf332edd75bf9a0e577b6371c39363 sha512值: d4323dd601f8b2d81906a885b2ea5aa0e8311a90e05426430ceb88b20dd440c979ad5872f742516359e635b2028079748dd697e97865dc3f78517d31520747b5 公钥算法: rsa 密钥长度: 2048 指纹: 9bd3fbcbf530ffe3d8d5456295aa7f20e1535a2e2bc53d729056f38ba85ad51a**

## **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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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。**