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

**瓜子影视（ 1.9.2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 | 瓜子影视 |
| 版本 | 1.9.2 |
| 包名 | com.secondhand.money |
| 域名线索 | 8条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年5月28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 | gzys.apk |
| 文件大小 | 39.81MB |
| MD5值 | 53174d7628937c8824e0825317cfce9b |
| SHA1值 | bf773a4eb212937d4e6c3b03d969f7124bfedc39 |
| SHA256值 | eb8ffda1f3d6680f598ee81eafbf89dc1a27eb2192be1f9ee4e7eaedaef90453 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 瓜子影视 |
| 包名 | com.secondhand.money |
| 主活动Activity | com.movie.firstIn.activity.splash.SplashActivity |
| 安卓版本名称 | 1.9.2 |
| 安卓版本 | 2406025 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| gcc.gnu.org | IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| android.googlesource.com | IP: 172.253.117.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.hpplay.com.cn | IP: 123.6.82.136 所属国家: China 地区: Henan 城市: Zhengzhou  |
| tvapp-openclient.yiboapp.tv | 没有服务器地理信息.  |
| errlogos.umeng.com | IP: 47.246.110.18 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.gstatic.com | IP: 203.208.43.66 所属国家: China 地区: Beijing 城市: Beijing  |
| errlog.umeng.com | IP: 223.109.148.143 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://www.hpplay.com.cn/  | 摸瓜V1引擎  |
| https://tvapp-openclient.yiboapp.tv  | 摸瓜V1引擎  |
| https://android.googlesource.com/toolchain/llvm  | 摸瓜V3引擎  |
| infinitedata-pa.googleapis.com  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/clang  | 摸瓜V3引擎  |
| http://schemas.android.com/aapt  | 摸瓜V3引擎  |
| firebaseinstallations.googleapis.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| instantmessaging-pa.googleapis.com  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| gmscompliance-pa.googleapis.com  | 摸瓜V3引擎  |
| clientservices.googleapis.com  | 摸瓜V3引擎  |
| www.gstatic.com  | 摸瓜V3引擎  |
| http://gcc.gnu.org/bugs.html):  | 摸瓜V3引擎  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlogos.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libijkffmpeg.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |

### **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: OU=sdfsa, CN=asdf 签名算法: rsassa\_pkcs1v15 有效期自: 2020-11-09 07:23:09+00:00 有效期至: 2045-11-03 07:23:09+00:00 发行人: OU=sdfsa, CN=asdf 序列号: 0x3d5b3b4 哈希算法: sha256 md5值: c23806ba4be69398a7b44012e2f51159 sha1值: 2f5e572e64b4ed3082e9e80cc8035c7115cd67fb sha256值: 2daa94115dc5c48038693654ffcc3aa095cbd093165b47bd7f15c8f83ca1bc9b sha512值: f621288c5e699a5ac4e194ed9d69ab3f5c8bfee87d68617e48b9491d7afecf6722c5eecbbf067cd587422b70dc071a39b92a25ecd6db12ca722a443cab64ddc9 公钥算法: rsa 密钥长度: 2048 指纹: 3fbc293e16e09bb71de852db54edc480858c60ff956b0b851bdc53781612950f**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "comment\_reply\_user\_name" : "回复@%s:"  |
| "google\_api\_key" : "AIzaSyBuIOzfKN-XAI1UJ5HisclnXI1WH0Y2F7M"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyBuIOzfKN-XAI1UJ5HisclnXI1WH0Y2F7M"  |
| "login\_forger\_password" : "忘记密码"  |
| "login\_input\_password" : "请输入您的密码"  |
| "setEmail\_input\_password" : "请输入您的密码"  |

## **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 |
| --- | --- | --- | --- |
| com.secondhand.money.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 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.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.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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| 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.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.RESTART\_PACKAGES | 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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.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 |
| android.permission.GET\_PACKAGE\_SIZE | 正常 | 测量应用程序存储空间 | 允许应用程序找出任何包使用的空间 |
| 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.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\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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。 |
| com.secondhand.money.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.secondhand.money.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.movie.firstIn.activity.homepage.HomepageActivity | **Schemes**: puvideo://, **Hosts:** video,  |
| com.movie.firstIn.activity.splash.SplashActivity | **Schemes**: ay56to://, sa13f27bec://,  |

**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。**