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

**南瓜视频（ 1.0.2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 | 南瓜视频 |
| 版本 | 1.0.2 |
| 包名 | com.hjmore.wuyu |
| 域名线索 | 42条 |
| URL线索 | 3条 |
| APP图标 |  |
| 分析日期 | 2025年7月7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 | 南瓜视频.apk |
| 文件大小 | 93.57MB |
| MD5值 | f0a3cd7aeeba8487f69d1abae6747c84 |
| SHA1值 | d73827e87596cbab6eb83f6bc4b96753fb83aedc |
| SHA256值 | 459c2c74855033756f4f01b4d215a55c5117d5fe228e7382c2b47424ffc58771 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 南瓜视频 |
| 包名 | com.hjmore.wuyu |
| 主活动Activity | com.lanlanys.app.view.SplashActivity |
| 安卓版本名称 | 1.0.2 |
| 安卓版本 | 58 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| xx.xx.xx.xx | 没有服务器地理信息. |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| union.eff.qq.com | IP: 157.255.219.214  所属国家: China  地区: Guangdong  城市: Shenzhen |
| hmma.baidu.com | IP: 110.242.68.195  所属国家: China  地区: Hebei  城市: Baoding |
| qzonestyle.gtimg.cn | IP: 42.231.138.64  所属国家: China  地区: Henan  城市: Nanyang |
| 46a79741.fyeds3.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| snowflake.qq.com | IP: 125.36.181.166  所属国家: China  地区: Tianjin  城市: Tianjin |
| tdid.m.qq.com | IP: 60.29.240.40  所属国家: China  地区: Tianjin  城市: Tianjin |
| ads.oneway.mobi | IP: 47.98.52.71  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| e.qq.com | IP: 220.194.116.85  所属国家: China  地区: Tianjin  城市: Tianjin |
| cpu-openapi.baidu.com | IP: 153.3.238.225  所属国家: China  地区: Jiangsu  城市: Nanjing |
| 47.98.52.71 | IP: 47.98.52.71  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| java.sun.com | IP: 23.215.212.52  所属国家: Australia  地区: Western Australia  城市: Perth |
| mobads-pre-config.bj.bcebos.com | IP: 113.200.2.111  所属国家: China  地区: Shaanxi  城市: Yulin |
| qzs.gdtimg.com | IP: 61.49.23.102  所属国家: China  地区: Beijing  城市: Beijing |
| m.baidu.com | IP: 110.242.71.103  所属国家: China  地区: Hebei  城市: Baoding |
| sdk.e.qq.com | IP: 220.194.116.72  所属国家: China  地区: Tianjin  城市: Tianjin |
| owads.audioadx.com | IP: 47.98.52.71  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| aden.baidu.com | IP: 110.242.68.230  所属国家: China  地区: Hebei  城市: Baoding |
| ads.oway.mobi | 没有服务器地理信息. |
| adsmind.ugdtimg.com | IP: 116.153.74.16  所属国家: China  地区: Jiangxi  城市: Nanchang |
| c2.gdt.qq.com | IP: 220.194.116.42  所属国家: China  地区: Tianjin  城市: Tianjin |
| schemas.xmlsoap.org | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| qzs.qq.com | IP: 116.196.150.247  所属国家: China  地区: Zhejiang  城市: Jinhua |
| glassfish.dev.java.net | IP: 137.254.56.48  所属国家: United States of America  地区: California  城市: Belmont |
| sf3-fe-tos.pglstatp-toutiao.com | IP: 121.17.122.82  所属国家: China  地区: Hebei  城市: Hengshui |
| mobads.baidu.com | IP: 111.206.208.180  所属国家: China  地区: Beijing  城市: Beijing |
| mobads-pre-config.cdn.bcebos.com | IP: 123.117.132.38  所属国家: China  地区: Beijing  城市: Beijing |
| 100000189777.retail.n.weimob.com | IP: 212.64.63.139  所属国家: China  地区: Beijing  城市: Beijing |
| cpu.baidu.com | IP: 153.3.238.55  所属国家: China  地区: Jiangsu  城市: Nanjing |
| bes-mtj.baidu.com | IP: 103.211.221.124  所属国家: China  地区: Jiangsu  城市: Nanjing |
| cpro.baidustatic.com | IP: 101.72.203.38  所属国家: China  地区: Hebei  城市: Langfang |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| render-server.cdn.bcebos.com | IP: 123.117.132.38  所属国家: China  地区: Beijing  城市: Beijing |
| upload.ffmpeg.org | IP: 213.36.253.119  所属国家: France  地区: Ile-de-France  城市: Paris |
| haokan.baidu.com | IP: 111.206.209.29  所属国家: China  地区: Beijing  城市: Beijing |
| mobads-logs.baidu.com | IP: 153.3.237.160  所属国家: China  地区: Jiangsu  城市: Nanjing |
| union.baidu.com | IP: 111.206.208.169  所属国家: China  地区: Beijing  城市: Beijing |
| i.gtimg.cn | IP: 111.161.120.102  所属国家: China  地区: Tianjin  城市: Tianjin |
| android.googlesource.com | IP: 192.178.163.82  所属国家: United States of America  地区: California  城市: Mountain View |
| mi.gdt.qq.com | IP: 220.194.116.121  所属国家: China  地区: Tianjin  城市: Tianjin |
| win.gdt.qq.com | IP: 220.194.116.80  所属国家: China  地区: Tianjin  城市: Tianjin |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/shake.webp | 摸瓜V2引擎 |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/shake\_text.png | 摸瓜V2引擎 |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/swipe\_right.webp | 摸瓜V2引擎 |
| https://win.gdt.qq.com/win\_notice.fcg?viewid=1 | 摸瓜V3引擎 |
| http://%s:%d/%s?timestamp=%s&cachefactor=%.2f&sign=%s | 摸瓜V3引擎 |
| https://snowflake.qq.com/ola/v2 | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_icon\_5.png | 摸瓜V3引擎 |
| http://m.baidu.com | 摸瓜V3引擎 |
| http://cfhp://commentlibavformat/check\_hijack.chijack: | 摸瓜V3引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_dark\_fb.png | 摸瓜V3引擎 |
| https://mobads-pre-config.cdn.bcebos.com/sdk/feed/slide\_all.json | 摸瓜V3引擎 |
| https://haokan.baidu.com/activity/h5/chaihongbao?productid=2&inviteCode=736CCC5X010&pd=lu&tab=guide& | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_white\_transparent\_fb.png | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/webview-cover.png | 摸瓜V3引擎 |
| https://c2.gdt.qq.com/ | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_white\_transparent\_fw.png | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_gray\_transparent.png | 摸瓜V3引擎 |
| https://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android01/download.html | 摸瓜V3引擎 |
| https://hmma.baidu.com/app.gif | 摸瓜V3引擎 |
| https://mobads-pre-config.cdn.bcebos.com/sdk/feed/slide\_finger.png | 摸瓜V3引擎 |
| http://schemas.xmlsoap.org/wsdl/soap/http?mtom=true | 摸瓜V3引擎 |
| https://mi.gdt.qq.com/ | 摸瓜V3引擎 |
| https://46a79741.fyeds3.com/ | 摸瓜V3引擎 |
| https://bes-mtj.baidu.com/auto.gif | 摸瓜V3引擎 |
| https://sdk.e.qq.com/mediation?version=2 | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_white\_transparent.png | 摸瓜V3引擎 |
| http://mobads.baidu.com/query\_ad | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android..io.github.rockerhieu.emojicon.EmojiconEditText | 摸瓜V3引擎 |
| https://aden.baidu.com/ | 摸瓜V3引擎 |
| https://sdk.e.qq.com/open/v1.1/dns/resolve | 摸瓜V3引擎 |
| https://cpu-openapi.baidu.com/api/v2/aggregation/channels | 摸瓜V3引擎 |
| http://mobads-pre-config.cdn.bcebos.com/sdk/iadex/full\_iadex.php | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_light\_fb.png | 摸瓜V3引擎 |
| http://m.baidu.com/baidu.php?sc | 摸瓜V3引擎 |
| http://mobads.baidu.com/cpro/ui/mads.php | 摸瓜V3引擎 |
| https://m.baidu.com/baidu.php?sc | 摸瓜V3引擎 |
| https://union.baidu.com | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/coupon/flip/coupon\_flip\_page.json | 摸瓜V3引擎 |
| https://mi.gdt.qq.com/gdt\_mview.fcg | 摸瓜V3引擎 |
| https://glassfish.dev.java.net/public/CDDL | 摸瓜V3引擎 |
| https://ads.oneway.mobi/diagnosis | 摸瓜V3引擎 |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_icon\_4.png | 摸瓜V3引擎 |
| http://47.98.52.71 | 摸瓜V3引擎 |
| http://union.baidu.com/ | 摸瓜V3引擎 |
| https://qzs.qq.com/union/res/union\_cdn/page/images/loading\_2x.gif | 摸瓜V3引擎 |
| http://java.sun.com/xml/ns/javaee/javaee\_web\_services\_1\_2.xsd | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_dark.png | 摸瓜V3引擎 |
| https://mobads.baidu.com/ads/preload.php | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_bg.png | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_1.json | 摸瓜V3引擎 |
| https://sdk.e.qq.com/activate | 摸瓜V3引擎 |
| https://xx.xx.xx.xx | 摸瓜V3引擎 |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png | 摸瓜V3引擎 |
| http://ads.oway.mobi | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_4.json | 摸瓜V3引擎 |
| http://127.0.0.1 | 摸瓜V3引擎 |
| http://mobads.baidu.com/ads/index.htm | 摸瓜V3引擎 |
| http://mobads.baidu.com/ | 摸瓜V3引擎 |
| https://100000189777.retail.n.weimob.com/saas/retail/100000189777/21036777/goods/detail | 摸瓜V3引擎 |
| https://union.eff.qq.com/v2/query/gdtmview | 摸瓜V3引擎 |
| https://mobads-pre-config.cdn.bcebos.com/sdk/splash/mix\_interact\_slide.json | 摸瓜V3引擎 |
| www.googleapis.com | 摸瓜V3引擎 |
| https://mobads-pre-config.cdn.bcebos.com/tools/lp\_hor.jpg | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_gray\_transparent\_fb.png | 摸瓜V3引擎 |
| https://sdk.e.qq.com/mediation?version=1 | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_light\_1.png | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android..io.github.rockerhieu.emojicon.EmojiconTextView | 摸瓜V3引擎 |
| https://sdk.e.qq.com/launch | 摸瓜V3引擎 |
| https://cpu-openapi.baidu.com/api/bes/s | 摸瓜V3引擎 |
| https://render-server.cdn.bcebos.com/static/images/20201231/zhongcao.png | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_gray\_transparent\_fw.png | 摸瓜V3引擎 |
| https://mobads-pre-config.cdn.bcebos.com/sdk/splash/bd\_splash\_shake\_lottie\_red\_package\_common.json | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/coupon/coupon\_default\_618.png | 摸瓜V3引擎 |
| http://hmma.baidu.com/app.gif | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/tools/toolsvideohor.mp4 | 摸瓜V3引擎 |
| https://tdid.m.qq.com?mc=2 | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_2.json | 摸瓜V3引擎 |
| http://schemas.android.com/tools | 摸瓜V3引擎 |
| https://i.gtimg.cn/ams-web/page-performance/page-performance.min.js?v=1 | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_icon\_2.png | 摸瓜V3引擎 |
| https://cpu-openapi.baidu.com/api/v2/data/list | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_dark\_fw.png | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_5.json | 摸瓜V3引擎 |
| http://owads.audioadx.com | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_3.json | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/bubble/bubble\_icon\_3.png | 摸瓜V3引擎 |
| https://cpu-openapi.baidu.com/api/v2/data/ads | 摸瓜V3引擎 |
| https://qzs.gdtimg.com/union/res/union\_cdn/page/temp\_v2/ams\_logo\_light\_fw.png | 摸瓜V3引擎 |
| https://mobads-logs.baidu.com/brwhis.log | 摸瓜V3引擎 |
| http://cpu-openapi.baidu.com/api/v2/data/novel/detail/ads | 摸瓜V3引擎 |
| https://mobads-logs.baidu.com/dz.zb?type=425 | 摸瓜V3引擎 |
| https://ads.oneway.mobi | 摸瓜V3引擎 |
| http://java.sun.com/xml/ns/javaee | 摸瓜V3引擎 |
| http://aden.baidu.com/ | 摸瓜V3引擎 |
| https://adsmind.ugdtimg.com | 摸瓜V3引擎 |
| https://cpu.baidu.com/block/app/ | 摸瓜V3引擎 |
| https://mobads-pre-config.bj.bcebos.com/sdk/dynamicBarrage/bd\_barrage\_emoji | 摸瓜V3引擎 |
| ftp://upload.ffmpeg.org/incoming/ | 摸瓜V3引擎 |
| https://e.qq.com/dev/index.html | 摸瓜V3引擎 |
| https://mobads-pre-config.cdn.bcebos.com/sdk/splash/mix\_interact\_shake.json | 摸瓜V3引擎 |

### **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: True 找到 1 个唯一证书 主题: CN=hjmore 签名算法: rsassa\_pkcs1v15 有效期自: 2024-05-28 15:04:04+00:00 有效期至: 2049-05-22 15:04:04+00:00 发行人: CN=hjmore 序列号: 0x1 哈希算法: sha256 md5值: 00ff7cff4b311975aa4e1db52dc7471c sha1值: e34a6948c26efc6026ba58eaeb36eac5b52271ee sha256值: 7837c509a890174424fff39c3da3fc72fdf029feaf9859cb861b3e327a6d7386 sha512值: 77951f2c8e27673dfd0f3b4343502c2a37c701d42203b998ff0d328ceb277c93649c60ef60f83e9a897b84167182d47d1db3f3862e471e67b5960d51b00ba32f 公钥算法: rsa 密钥长度: 2048 指纹: 0ad4f97ccf8453e04e92fc5542446407908569b6ec24be53d8b0dbe2d686e3bd**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "djx\_author\_desc\_more" : "更多" |
| "djx\_author\_loadmore\_no" : "暂无更多内容" |
| "djx\_author\_loadmore\_yes" : "加载更多…" |
| "djx\_author\_works\_count" : "作品 %1$s" |
| "djx\_block\_author" : "拉黑" |
| "djx\_block\_author\_failed" : "拉黑失败请重试" |
| "djx\_block\_author\_success" : "已拉黑" |
| "djx\_follow\_when\_author\_blocked" : "请解除拉黑后再关注哦" |
| "djx\_unblock\_author" : "解除拉黑" |
| "djx\_unblock\_author\_failed" : "解除失败请重试" |
| "djx\_unblock\_author\_success" : "已解除拉黑" |
| "privateKeyP2" : "#e$r" |

## **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.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.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.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.FOREGROUND\_SERVICE\_REMOTE\_MESSAGING | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 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.READ\_MEDIA\_VIDEO | 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.AUTHENTICATE\_ACCOUNTS | 危险 | 充当帐户验证器 | 允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码 |
| 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.WRITE\_SYNC\_SETTINGS | 正常 | 写入同步设置 | 允许应用程序修改同步设置,例如是否为联系人启用同步 |
| app.permission.OPEN\_MAIN\_PAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.USES\_POLICY\_FORCE\_LOCK | 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\_CLIPBOARD | 未知 | Unknown permission | Unknown permission from android reference |
| 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.hjmore.wuyu.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.EXPAND\_STATUS\_BAR | 正常 | 展开/折叠状态栏 | 允许应用程序展开或折叠状态栏 |
| 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 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 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.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.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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| 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.KILL\_BACKGROUND\_PROCESSES | 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.ACCESS\_ACCELEROMETER | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| android.permission.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| com.hjmore.wuyu.permission.KW\_SDK\_BROADCAST | 未知 | Unknown permission | Unknown permission from android reference |
| com.hjmore.wuyu.andpermission.bridge | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.lanlanys.app.view.activity.classification.SpecialActivity | **Schemes**: um.62b07eec05844627b5bc4d2d://, |
| com.lanlanys.app.view.SplashActivity | **Schemes**: lanlanys://,  **Hosts:** www.lanlanys.com,  **Ports:** 8888,  **Paths:** /startApp, |

**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。**