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

**1001夜（ 1.0.0.0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 | 1001夜 |
| 版本 | 1.0.0.0 |
| 包名 | com.sadas.o9iij3.maasd.asz.yh09jmb |
| 域名线索 | 0条 |
| URL线索 | 0条 |
| APP图标 |  |
| 分析日期 | 2025年5月14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 | night\_release\_2022\_11\_23\_16-12\_v1.0.0.0\_221124.apk |
| 文件大小 | 40.39MB |
| MD5值 | 19bcb9c60991e36c0d47eefca0b76c2e |
| SHA1值 | d82daa4391b1588831cc33f43027cc149892c213 |
| SHA256值 | 5513b22ee4e5d6858bbfe43bd217ddd490c5ce2374bf4a3f2964446d00acdac6 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 1001夜 |
| 包名 | com.sadas.o9iij3.maasd.asz.yh09jmb |
| 主活动Activity | com.hello.regular.activity.SplashActivity |
| 安卓版本名称 | 1.0.0.0 |
| 安卓版本 | 221124 |

## **4. 线索情况**

### **4.1 域名线索**

### **4.2 URL线索**

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| qiezishipin@gmail.com qiezishangwu@gmail.com  | Mogua Engine V1  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: True Found 1 unique certificates Subject: C=86, ST=CHINA, L=BEIJING, O=AG, OU=AG, CN=GA Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2022-11-23 05:28:15+00:00 Valid To: 2047-11-17 05:28:15+00:00 Issuer: C=86, ST=CHINA, L=BEIJING, O=AG, OU=AG, CN=GA Serial Number: 0x77d4e850 Hash Algorithm: sha256 md5: c0d63fe251b60eff13c1908a5ed9a112 sha1: fa82c2a5afe090457925e2067dbd975a1821a065 sha256: 22a642132ad528e603fc93774686fecc3ae030c2eedab3bdb688a54b1f57888b sha512: 996f45a9de74ee1473f73967c9ceb75781508747c348bed5f360a032ebf7f38e477688574acd25833476da88845608996b54e14132e256b01e82578e00dee22e PublicKey Algorithm: rsa Bit Size: 2048 Fingerprint: 10a81b159daa471b4dfaa45bd58ba45be0ac3cf2059958d1198bb1ea9ac6cb9d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "app\_not\_find\_key" : "尝试换个关键词吧 另外为主人推荐以下精彩影片"  |
| "integral\_re\_authorize\_save\_picture" : "请重新授权以保存图片"  |
| "mine\_author\_load" : "登录授权"  |
| "mine\_private" : "隐私保护"  |
| "no\_more\_session" : "没有更多会话了"  |
| "re\_authorize\_save\_er\_code\_picture" : "请重新授权以保存二维码图片"  |
| "reset\_password" : "重置密码"  |
| "team\_authentication" : "身份验证"  |
| "team\_invitee\_authentication" : "被邀请人身份验证"  |
| "team\_invitee\_need\_authen" : "需要验证"  |
| "team\_invitee\_not\_need\_authen" : "不需要验证"  |
| "team\_need\_authentication" : "需要身份验证"  |
| "video\_authorization\_failed\_operate" : "授权失败,悬浮小窗播放功能可在“我的-设置”中操作"  |

## **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.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.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.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.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\_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.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.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.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 |
| com.sadas.o9iij3.maasd.asz.yh09jmb.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.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\_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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.sadas.o9iij3.maasd.asz.yh09jmb.permission.RECEIVE\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| 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.INTERACT\_ACROSS\_USERS | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| android.permission.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 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 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.hello.regular.activity.SplashActivity | **Schemes**: s8pn91://, sa65df155c://, https://, night://, **Hosts:** smt33.app, smt55.app, smt66.app, smt77.app, smt88.app, qz999.app,  |
| com.hello.regular.activity.games.GameWebViewActivity2 | **Schemes**: @string/app\_scheme://, **Hosts:** @string/app\_host, **Paths:** @string/app\_path\_as,  |
| com.hello.regular.activity.games.GameWebViewActivity3 | **Schemes**: @string/app\_scheme://, **Hosts:** @string/app\_host, **Paths:** @string/app\_path,  |
| com.hello.regular.activity.games.GamePortraitActivity | **Schemes**: @string/app\_scheme://, **Hosts:** @string/app\_host, **Paths:** @string/app\_path\_portrait,  |

**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。**