



# MoGua

## 秋月 8.0.7.APK 分析报告



APP名称:

秋月

包名: com.k4sJ7LEQvdYw1lDa.XzvKZVILQXhg8lyi

域名线索: 6条

URL线索: 6条

邮箱线索: 0条

分析日期: 2025年6月21日

分析平台: [摸瓜APK反编译平台](#)

文件名: qiuyue-p8YiZ-v601d64ec.apk  
文件大小: 47.85MB  
MD5值: 691e26868d557b34208dfabd1d0a7931  
SHA1值: 1b902a600962e8e37158e6adfdabe1b22ef1360  
SHA256值: 8a73d156644674dd1000e6d998ae4775654aa051ec9f33f0b79a1aff447939fd

## i APP 信息

App名称: 秋月  
包名: com.k4sj7LEQvdYw1IDa.XzvKZVILQXhg8lyi  
主活动Activity: com.QxPdDbngNPQjISjV.IEhevSXLTzoiRPKQ.MainActivity  
安卓版本名称: 8.0.7  
安卓版本: 1

## 🔍 域名线索

| 域名                    | 服务器信息                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------|
| developer.mozilla.org | IP: 34.111.97.67<br>所属国家: United States of America<br>地区: Missouri<br>城市: Kansas City<br>纬度: 39.099731<br>经度: -94.578568 |
| github.com            | IP: 20.205.243.166<br>所属国家: Singapore<br>地区: Singapore<br>城市: Singapore<br>纬度: 1.289987<br>经度: 103.850281                |
| paulbakaus.com        | IP: 167.172.18.193<br>所属国家: United States of America<br>地区: New Jersey                                                   |

|                   |                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <b>城市:</b> Clifton<br><b>纬度:</b> 40.858585<br><b>经度:</b> -74.163605                                                                                                       |
| dev.w3.org        | <b>IP:</b> 104.18.23.19<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Francisco<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203   |
| stackoverflow.com | <b>IP:</b> 172.64.155.249<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Francisco<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203 |
| www.gnu.org       | <b>IP:</b> 209.51.188.116<br><b>所属国家:</b> United States of America<br><b>地区:</b> Massachusetts<br><b>城市:</b> Somerville<br><b>纬度:</b> 42.387600<br><b>经度:</b> -71.099503  |

 URL线索

| URL信息                                                   | Url所在文件 |
|---------------------------------------------------------|---------|
| https://github.com/nodeca/pica                          | 摸瓜V2引擎  |
| http://paulbikaus.com/tutorials/html5/web-audio-on-ios/ | 摸瓜V2引擎  |
| http://stackoverflow.com/questions/24119684             | 摸瓜V2引擎  |
|                                                         | ...     |

|                                                                             |        |
|-----------------------------------------------------------------------------|--------|
| https://www.gnu.org/licenses/>.                                             | 摸瓜V2引擎 |
| https://www.gnu.org/licenses/>.                                             | 摸瓜V2引擎 |
| https://www.gnu.org/licenses/>.                                             | 摸瓜V2引擎 |
| https://github.com/richtr/NoSleep.js/issues/15                              | 摸瓜V2引擎 |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released) | 摸瓜V2引擎 |

 邮箱线索

 手机线索

 签名证书

无法读取代码签名证书.

 硬编码敏感信息

 加壳分析

| 加壳类型      | 所属文件 |
|-----------|------|
| 登陆摸瓜网站后查看 |      |

# 第三方插件

| 名称        | 分类 | URL链接 |
|-----------|----|-------|
| 登陆摸瓜网站后查看 |    |       |

## 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.FOREGROUND_SERVICE                                          | 正常   |                    | 允许常规应用程序使用Service.startForeground。                      |
| com.k4sj7LEQvdYw1IDa.XzvKZVILQXhg8lyi.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | 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.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.READ_PRIVILEGED_PHONE_STATE                                 | 未知   | Unknown permission | Unknown permission from android reference               |
| android.permission.FLASHLIGHT                                                  | 正常   | 控制手电筒              | 允许应用程序控制手电筒                                             |

|                                           |    |                    |                                                               |
|-------------------------------------------|----|--------------------|---------------------------------------------------------------|
| 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.VIBRATE                | 正常 | 可控震源               | 允许应用程序控制振动器                                                   |
| 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.READ_PHONE_STATE       | 危险 | 读取电话状态<br>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.POST_NOTIFICATIONS     | 未知 | Unknown permission | Unknown permission from android reference                     |
| android.permission.WRITE_SETTINGS         | 危险 | 修改全局系统<br>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.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.READ_MEDIA_IMAGES      | 未知 | Unknown permission | Unknown permission from android reference                     |
| android.permission.SYSTEM_ALERT_WINDOW    | 危险 | 显示系统级警<br>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<br>器内容      | 允许应用程序从外部存储读取                                                 |
| 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                                              |
|                                           | 危  | 精细定位               | 访问精细位置源,例如手机上的全球定位系统,如果                                       |

|                                             |    |                      |                                                   |
|---------------------------------------------|----|----------------------|---------------------------------------------------|
| android.permission.ACCESS_FINE_LOCATION     | 险  | (GPS)                | 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.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_MEDIA_AUDIO         | 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.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.PACKAGE_USAGE_STATS      | 合法 | 更新组件使用统计             | 允许修改收集的组件使用统计。不供普通应用程序使用                          |
| 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.INTERNET                 | 正常 | 互联网接入                | 允许应用程序创建网络套接字                                     |
| 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.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                            |
|                                             | 未  | Unknown              |                                                   |

|                                                      |    |                    |                                           |
|------------------------------------------------------|----|--------------------|-------------------------------------------|
| android.permission.READ_MEDIA_VISUAL_USER_SELECTED   | 知  | 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_MEDIA_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| 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                    |



应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。