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

**Scene（ 8.1.0 Beta2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 | Scene |
| 版本 | 8.1.0 Beta2 |
| 包名 | com.omarea.vtools |
| 域名线索 | 17条 |
| URL线索 | 26条 |
| APP图标 |  |
| 分析日期 | 2025年9月13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 | xgScene\_8.1.0 Beta2\_sign.apk |
| 文件大小 | 8.41MB |
| MD5值 | 4e1185cbd3a0e14c766773573c4b675f |
| SHA1值 | 92d56dad5950fa5c11b179cabacd25ffe27f7130 |
| SHA256值 | bba73e328cba071d1e95de1fae0f677d81419ee80f9bb916679c8d09a870e87c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Scene |
| 包名 | com.omarea.vtools |
| 主活动Activity | com.omarea.vtools.activities.ActivityPowerModeTile |
| 安卓版本名称 | 8.1.0 Beta2 |
| 安卓版本 | 820241219 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| fa.hsfaka.net | IP: 118.123.202.88 所属国家: China 地区: Sichuan 城市: Chengdu  |
| tinyurl.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| 119.91.234.23 | IP: 119.91.234.23 所属国家: China 地区: Beijing 城市: Beijing  |
| vtools.online | IP: 141.11.139.132 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| download.omarea.com | IP: 141.11.139.132 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| pd.qq.com | IP: 60.29.238.114 所属国家: China 地区: Tianjin 城市: Tianjin  |
| scene7.omarea.com | IP: 119.91.234.23 所属国家: China 地区: Beijing 城市: Beijing  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| vtools.oss-cn-beijing.aliyuncs.com | IP: 61.135.144.199 所属国家: China 地区: Beijing 城市: Beijing  |
| magisk-modules-repo.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| vtools.omarea.com | IP: 119.91.234.23 所属国家: China 地区: Beijing 城市: Beijing  |
| helloklf.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.paypal.me | IP: 151.101.89.21 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| source.android.com | IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto  |
| schemas.android.com | 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: -  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | c/g/d/d/r.java  |
| http://127.0.0.1:  | com/omarea/common/net/Daemon.java  |
| https://magisk-modules-repo.github.io/submission/modules.json  | com/omarea/library/basic/MagiskModulesRepo.java  |
| https://www.paypal.me/duduski  | com/omarea/vtools/dialogs/DialogPaymentMethods.java  |
| https://vtools.oss-cn-beijing.aliyuncs.com/  | com/omarea/vtools/dialogs/DialogPaymentMethods.java  |
| https://play.google.com/store/apps/details?id=  | com/omarea/vtools/dialogs/i4.java  |
| http://vtools.omarea.com/  | com/omarea/vtools/dialogs/f3.java  |
| https://fa.hsfaka.net/orderquery  | com/omarea/vtools/dialogs/w2.java  |
| https://fa.hsfaka.net/orderquery  | com/omarea/vtools/dialogs/x2.java  |
| https://vtools.oss-cn-beijing.aliyuncs.com/  | com/omarea/vtools/activities/ActivityAddinOnline.java  |
| https://vtools.omarea.com/  | com/omarea/vtools/activities/ActivityAddinOnline.java  |
| https://helloklf.github.io/vtools-online.html  | com/omarea/vtools/activities/ActivityAddinOnline.java  |
| http://vtools.omarea.com/  | com/omarea/vtools/activities/ActivityAppXposedDetails.java  |
| http://vtools.omarea.com/scene-policy.html  | com/omarea/vtools/activities/ActivityStartSplash.java  |
| https://github.com/Magisk-Modules-Repo/  | com/omarea/vtools/activities/ActivityModules.java  |
| http://vtools.omarea.com/scene-policy.html  | com/omarea/vtools/activities/ActivityOtherSettings.java  |
| https://github.com/helloklf/vtools/blob/scene3/docs/MIUI%E6%B8%A9%E6%8E%A7%E8%AF%B4%E6%98%8E.md  | com/omarea/vtools/activities/ActivityMiuiThermal.java  |
| https://play.google.com/store/apps/details?id=  | com/omarea/vtools/fragments/FragmentUser.java  |
| https://pd.qq.com/s/92rqbetny  | com/omarea/vtools/fragments/FragmentUser.java  |
| https://github.com/shadow3aaa/fas-rs/releases/  | com/omarea/vtools/fragments/FragmentPerf.java  |
| https://github.com/yc9559/uperf  | com/omarea/vtools/fragments/FragmentPerf.java  |
| https://github.com/yinwanxi/Uperf-Game-Turbo/releases  | com/omarea/vtools/fragments/FragmentPerf.java  |
| http://vtools.omarea.com/  | com/omarea/vtools/fragments/FragmentHome.java  |
| http://vtools.omarea.com/  | com/omarea/vtools/fragments/f.java  |
| http://vtools.oss-cn-beijing.aliyuncs.com/app-release  | com/omarea/net/h.java  |
| https://vtools.oss-cn-beijing.aliyuncs.com/vi/  | com/omarea/net/g.java  |
| http://download.omarea.com/toolkit/  | com/omarea/net/ScenePerf.java  |
| http://scene7.omarea.com:8080  | com/omarea/net/SceneServer.java  |
| http://119.91.234.23:8080  | com/omarea/net/SceneServer.java  |
| http://vtools.online  | com/omarea/net/SceneServer.java  |
| https://vtools.oss-cn-beijing.aliyuncs.com/addin/auto-skip-config-v1.json  | com/omarea/net/AutoSkipCloudData$updateConfig$1.java  |
| https://source.android.com/devices/tech/dalvik/jit-compiler?hl=zh-cn  | 摸瓜V1引擎  |
| https://vtools.oss-cn-beijing.aliyuncs.com/addin/swap-controller-3.6.5.zip  | 摸瓜V1引擎  |
| https://tinyurl.com/y3j7vszf  | 摸瓜V1引擎  |
| http://vtools.omarea.com/  | 摸瓜V1引擎  |
| http://vtools.omarea.com/  | 摸瓜V2引擎  |
| http://vtools.omarea.com/  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 1191634433@qq.com helloklf@outlook.com  | com/omarea/vtools/dialogs/c4.java  |
| helloklf@outlook.com  | com/omarea/vtools/dialogs/g3.java  |
| helloklf@outlook.com  | com/omarea/vtools/fragments/FragmentUser.java  |
| helloklf@outlook.com  | com/omarea/net/SceneMagisk.java  |
| helloklf@outlook.com  | 摸瓜V1引擎  |

### **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: False 找到 1 个唯一证书 主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2008-02-29 01:33:46+00:00 有效期至: 2035-07-17 01:33:46+00:00 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0x936eacbe07f201df 哈希算法: sha1 md5值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569 公钥算法: rsa 密钥长度: 2048 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "ACCESS\_SUPERUSER" : "访问超级用户权限"  |
| "app\_user" : "User"  |
| "apps\_op\_clear\_user" : "Current User only"  |
| "apps\_op\_uninstall\_user" : "Uninstall(Current user)"  |
| "dialog\_addin\_wlan\_pwd" : "Password:"  |
| "source\_author" : "Source/Author:"  |
| "user\_pwd\_input" : "password"  |
| "user\_reset\_password" : "Reset password"  |
| "app\_user" : "用户"  |
| "apps\_op\_clear\_user" : "仅限当前用户"  |
| "apps\_op\_uninstall\_user" : "从当前用户卸载"  |
| "dialog\_addin\_wlan\_pwd" : "密码："  |
| "source\_author" : "配置源/作者："  |
| "user\_pwd\_input" : "密码"  |
| "user\_reset\_password" : "忘了账号/密码？"  |
| "app\_user" : "用户"  |
| "apps\_op\_clear\_user" : "仅限当前用户"  |
| "apps\_op\_uninstall\_user" : "从当前用户卸载"  |
| "dialog\_addin\_wlan\_pwd" : "密码："  |
| "source\_author" : "配置源/作者："  |
| "user\_pwd\_input" : "密码"  |
| "user\_reset\_password" : "忘了账号/密码？"  |
| "app\_user" : "用户"  |
| "apps\_op\_clear\_user" : "仅限当前用户"  |
| "apps\_op\_uninstall\_user" : "从当前用户卸载"  |
| "dialog\_addin\_wlan\_pwd" : "密码："  |
| "source\_author" : "配置源/作者："  |
| "user\_pwd\_input" : "密码"  |
| "user\_reset\_password" : "忘了账号/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 |
| --- | --- | --- | --- |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 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.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.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.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.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.permiactivty\_module\_detailssion.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.REQUEST\_COMPANION\_RUN\_IN\_BACKGROUND | 正常 |  | 允许配套应用在后台运行。 |
| 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.BIND\_NOTIFICATION\_LISTENER\_SERVICE | 合法 |  | NotificationListenerService 必须要求,以确保只有系统可以绑定到它 |
| android.permission.WRITE\_SECURE\_SETTINGS | 系统需要 | 修改安全系统设置 | 允许应用程序修改系统固定好设置数据。不供普通应用程序使用 |
| 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.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| android.permission.BIND\_ACCESSIBILITY\_SERVICE | 合法 |  | AccessibilityService 必须要求,以确保只有系统可以绑定到它 |
| android.permission.GET\_APP\_OPS\_STATS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INTERACT\_ACROSS\_USERS | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **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。**