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

**蘑菇視頻（ 1.3.4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 | 蘑菇視頻 |
| 版本 | 1.3.4 |
| 包名 | com.apaz.cmoagdzg |
| 域名线索 | 24条 |
| URL线索 | 28条 |
| APP图标 |  |
| 分析日期 | 2025年5月15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 | mogu1.3.4gg.apk |
| 文件大小 | 14.87MB |
| MD5值 | 376fc868010a939596c9aecd9454cb46 |
| SHA1值 | c47c30660c52b620b68a3aa0c13ddac6bae27cbe |
| SHA256值 | e0613e278ad40ec7163ca7e2009554f26050673a16e6ae109eb783a8b778b77e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 蘑菇視頻 |
| 包名 | com.apaz.cmoagdzg |
| 主活动Activity | com.asdfg.camobgg.ui.LoadingActivity |
| 安卓版本名称 | 1.3.4 |
| 安卓版本 | 33 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.mgsp.ltd | IP: 137.175.44.132  所属国家: United States of America  地区: California  城市: San Jose |
| www.ijianji.com | IP: 47.115.44.41  所属国家: China  地区: Guangdong  城市: Shenzhen |
| www.slf4j.org | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| mogu.la | IP: 210.87.207.163  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| www.huishenghuiying.com.cn | IP: 42.193.217.87  所属国家: China  地区: Beijing  城市: Beijing |
| pslog.umeng.com | IP: 59.82.29.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ouplog.umeng.com | IP: 47.246.110.94  所属国家: Singapore  地区: Singapore  城市: Singapore |
| alogus.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| errlog.umeng.com | IP: 223.109.148.142  所属国家: China  地区: Jiangsu  城市: Nanjing |
| alogsus.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| px.ucweb.com | IP: 116.132.217.241  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| dns.alidns.com | IP: 223.5.5.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| miao.wondershare.cn | IP: 47.98.66.240  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulogs.umengcloud.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| kuai.360.cn | IP: 124.165.123.4  所属国家: China  地区: Shanxi  城市: Taiyuan |
| www.capcut.cn | IP: 202.108.29.205  所属国家: China  地区: Beijing  城市: Beijing |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| bcut.bilibili.cn | IP: 122.188.187.204  所属国家: China  地区: Hubei  城市: Tianmen |
| px-intl.ucweb.com | IP: 157.185.188.1  所属国家: Canada  地区: Ontario  城市: North York |
| plbslog.umeng.com | IP: 36.156.202.75  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| aaid.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ulogs.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| developer.umeng.com | IP: 59.82.31.210  所属国家: China  地区: Zhejiang  城市: Hangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://%s:%d/%s | OoooooO/o0000O.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | OoooooO/o0000O.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | OoooooO/o0000O0.java |
| https://github.com/danikula/AndroidVideoCache/issues. | OoooooO/o0000O0.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | OoooooO/o0000O0.java |
| http://%s:%d/%s | OoooooO/o0000O00.java |
| https://dns.alidns.com/resolve?name=apihost.mgsp.me&short=true&type=16 | com/asdfg/camobgg/api/ApiService.java |
| https://api.mgsp.ltd | com/asdfg/camobgg/main/App.java |
| https://mogu.la | com/asdfg/camobgg/model/GlobeAppData.java |
| https://www.ijianji.com | com/asdfg/camobgg/ui/activity/RecommendToolsActivity$initData$1$1.java |
| https://bcut.bilibili.cn/ | com/asdfg/camobgg/ui/activity/RecommendToolsActivity$initData$1$2.java |
| https://www.capcut.cn | com/asdfg/camobgg/ui/activity/RecommendToolsActivity$initData$1$3.java |
| https://miao.wondershare.cn/ | com/asdfg/camobgg/ui/activity/RecommendToolsActivity$initData$1$4.java |
| https://www.huishenghuiying.com.cn/ | com/asdfg/camobgg/ui/activity/RecommendToolsActivity$initData$1$5.java |
| https://kuai.360.cn/home.html | com/asdfg/camobgg/ui/activity/RecommendToolsActivity$initData$1$6.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://errlogos.umeng.com/upload | com/uc/crashsdk/e.java |
| https://errlog.umeng.com/upload | com/uc/crashsdk/e.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://px-intl.ucweb.com | com/uc/crashsdk/a/h.java |
| https://px.ucweb.com | com/uc/crashsdk/a/h.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ouplog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://aaid.umeng.com/api/updateZdata | com/umeng/umzid/ZIDManager.java |
| https://aaid.umeng.com/api/postZdata | com/umeng/umzid/ZIDManager.java |
| http://www.slf4j.org/codes.html | o00O0oOO/OooO0OO.java |
| https://github.com/vinc3m1 | Mogua Engine V1 |
| https://github.com/vinc3m1/RoundedImageView | Mogua Engine V1 |
| https://github.com/vinc3m1/RoundedImageView.git | Mogua Engine V1 |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/arm64-v8a/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/arm64-v8a/libcrashsdk.so |
| https://errlog.umeng.com | lib/arm64-v8a/libcrashsdk.so |
| https://errlogos.umeng.com | lib/arm64-v8a/libcrashsdk.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | OoooooO/o0000O0.java |
| mogudizhi@gmail.com | com/asdfg/camobgg/ui/activity/ContactActivity$initData$2.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099 | o00000o0/OooOOO.java |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **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: CN=asdasd 签名算法: rsassa\_pkcs1v15 有效期自: 2024-01-17 05:53:06+00:00 有效期至: 2049-01-10 05:53:06+00:00 发行人: CN=asdasd 序列号: 0x23e70cc3 哈希算法: sha256 md5值: 5c3a344aed477bfadc153a5adf70e911 sha1值: 1dde01ba2c5c868ba1901ae59537f61f33b1e25b sha256值: 0543af2015bca0a84b53e534b1c345138ceedbccdd0b720e9003e6b792cff835 sha512值: 5a066e9fb16a0134dd59bcce4fe385f4c2330d1968eac4b310d0ce301673cc6e71fc09b0d318ec6f55d21397dc640c109e9b1a6bb4c928e156bc54a29ab54f5a 公钥算法: rsa 密钥长度: 2048 指纹: 01c8b138f5e190eb9acd562090989f6d0737bf68c47fa36fab362c24a3d99db8**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_roundedimageview\_author" : "Vince Mi" |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1" |

## **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.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.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.ACCESS\_DOWNLOAD\_MANAGER | 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.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.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.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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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\_PACKAGE\_CHANGED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_INSTALL | 未知 | Unknown permission | Unknown permission from android reference |
| 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.samsung.android.providers.context.permission.WRITE\_USE\_APP\_FEATURE\_SURVEY | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_ADDED | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.asdfg.camobgg.MainActivity | **Schemes**: mgapp://,  **Hosts:** mainpage, |

**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。**