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

**龙啸九天（ 1.0.11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 | 龙啸九天 |
| 版本 | 1.0.11 |
| 包名 | ljcap.zc7je.st6oq |
| 域名线索 | 9条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年8月10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 | 九天.apk |
| 文件大小 | 498.4MB |
| MD5值 | 702986551fcf30ae3b328352878e963b |
| SHA1值 | b8775d11101da4e6e4bf796e926405f8e6fd823c |
| SHA256值 | 8ef8611b72551c8e567ea333d823d3f9e3e90b18da7443913db0e0156486fe15 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 龙啸九天 |
| 包名 | ljcap.zc7je.st6oq |
| 主活动Activity | org.cocos2dx.lua.SplashActivity |
| 安卓版本名称 | 1.0.11 |
| 安卓版本 | 11 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 203.107.1.1 | IP: 203.107.1.1 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| 203.107.1.67 | IP: 203.107.1.67 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| storecdn2.aiwaya.cn | 没有服务器地理信息.  |
| 203.107.1.33 | IP: 203.107.1.33 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| rqd.uu.qq.com | IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin  |
| msoftdl.360.cn | IP: 61.240.129.15 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| rizhi.aiwaya.cn | 没有服务器地理信息.  |
| example.com | IP: 96.7.128.198 所属国家: United States of America 地区: California 城市: El Segundo  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://rqd.uu.qq.com/rqd/sync  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://203.107.1.67/161083/resolve  | com/yunva/im/sdk/lib/YvLoginInit.java  |
| http://storecdn2.aiwaya.cn/amr5bd67ebd9faef20cbc113f99.amr  | com/yunva/im/sdk/lib/YvLoginInit.java  |
| http://203.107.1.67/161083/resolve  | com/yunva/im/sdk/lib/YvLoginInit.java  |
| https://203.107.1.33/161083/resolve  | com/yunva/im/sdk/lib/YvLoginInit.java  |
| http://203.107.1.33/161083/resolve  | com/yunva/im/sdk/lib/YvLoginInit.java  |
| https://203.107.1.1/161083/resolve?host  | com/yunva/im/sdk/lib/YvLoginInit.java  |
| http://203.107.1.1/161083/resolve?host  | com/yunva/im/sdk/lib/YvLoginInit.java  |
| http://rizhi.aiwaya.cn/index  | com/yunva/im/sdk/lib/YvLoginInit.java  |
| http://msoftdl.360.cn/mobilesafe/shouji360/360safesis/360MobileSafe\_6.5.0.1069.apk  | com/quicksdk/c/d.java  |
| http://example.com/  | cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java  |

### **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: C=15abedec, ST=15abedec, L=15abedec, O=15abedec, OU=15abedec, CN=15abedec 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-28 15:14:44+00:00 有效期至: 2125-05-04 15:14:44+00:00 发行人: C=15abedec, ST=15abedec, L=15abedec, O=15abedec, OU=15abedec, CN=15abedec 序列号: 0x62aed556 哈希算法: sha256 md5值: f5aed6601bb1308dbead825f47dbf27b sha1值: 65aa13b6c0e93a4fc20548a1d0502a6733d56563 sha256值: fc9fc8a198b5b6761ad4eff1892965f541c59f6376cf7bc4a15bbccb9d373f9e sha512值: 361c90a2220efb2e699a45989f676bac4050525dc4429369f2ce41f3619e249afd6291a84245f9276f7910aa5b9c014fdc62970f7b1579a683cea07432cfabcd 公钥算法: rsa 密钥长度: 1024 指纹: 409e0419414b3d5db5cb5a09c69ec8579f15c0515038fdf6d4a9279ca8d7858e**

## **6. 硬编码敏感信息**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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\_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.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.PROCESS\_OUTGOING\_CALLS | 危险 | 拦截拨出电话 | 允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话 |
| 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.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.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.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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| 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.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.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\_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.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| 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.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.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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| com.qti.permission.PROFILER | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**