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

**九州群将录（ 2.1.7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 | 九州群将录 |
| 版本 | 2.1.7 |
| 包名 | com.hb01.dev |
| 域名线索 | 4条 |
| URL线索 | 3条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | 安卓.apk |
| 文件大小 | 452.02MB |
| MD5值 | f2ee29209c83ed2d86f6f212057ed2a0 |
| SHA1值 | 0001e4b65e3dd5015783dcb323c8717f0cab627f |
| SHA256值 | 4e710197d7374146b93e4f2ed402ca6c7a6768a2759c56effb3deb7bea0b2121 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 九州群将录 |
| 包名 | com.hb01.dev |
| 主活动Activity | org.cocos2dx.javascript.AppActivity |
| 安卓版本名称 | 2.1.7 |
| 安卓版本 | 23112802 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| h.trace.qq.com | IP: 113.56.189.162  所属国家: China  地区: Hubei  城市: Huangshi |
| android.bugly.qq.com | IP: 124.95.225.169  所属国家: China  地区: Liaoning  城市: Shenyang |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26  所属国家: United States of America  地区: California  城市: San Francisco |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| https://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| https://h.trace.qq.com/kv | com/tencent/bugly/proguard/r.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ٯ@qz.xri  ig@o0.gf2 | 摸瓜V2引擎 |
| k@1.njme | 摸瓜V2引擎 |
| rnsn@i-i.15 | 摸瓜V2引擎 |
| rnsn@s.r5 | 摸瓜V2引擎 |
| rnsn@i.i6 | 摸瓜V2引擎 |
| n@4.p0  n@q.s3w  n@u7.qq3  n@42i.57v  n@v.0467s  n@wq.iz5  n@u.qs  n@7.pq  n@10.s5wz  n@0.m32  n@p14.zq8  n@m.t15 | 摸瓜V2引擎 |
| n@u7.qq3 | 摸瓜V2引擎 |
| n@0.m32 | 摸瓜V2引擎 |
| n@4.p0 | 摸瓜V2引擎 |
| n@m.t15 | 摸瓜V2引擎 |
| i@9.ծw  x@bٷt5d.auӽo  k@\_-x.iy  o@x.vgh  qϊ@ox.eeܖx  my5@zta.a2  lscv@bqn.vbx  i@g.ks  yu@r.3m  mic@ѝʧczxd.yi  1@om.hi | 摸瓜V2引擎 |
| n@q3.3z86  n@-.tqr  n@is.rs  n@4w0.vrrw  n@u.vz  n@uw.p6  n@5s.s0i  n@mu.zs4  n@m.6u7  n@2.3z  n@-tus.80 | 摸瓜V2引擎 |
| rnsn@u.2w  n@2.3z | 摸瓜V2引擎 |
| sn@q.iu | 摸瓜V2引擎 |
| n@-.tqr | 摸瓜V2引擎 |
| rnsn@1.m7 | 摸瓜V2引擎 |
| rnsn@v.0z | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| sn@6.i1 | 摸瓜V2引擎 |
| nppnppn@rl4.bχ | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| rnsn@6.t5 | 摸瓜V2引擎 |
| rnsn@q.iu | 摸瓜V2引擎 |
| rnsn@z.i6 | 摸瓜V2引擎 |
| n@5s.s0i | 摸瓜V2引擎 |
| sn@6.i1 | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| rnsn@t.8i4 | 摸瓜V2引擎 |
| rnsn@i.15 | 摸瓜V2引擎 |
| rnsn@8.3u | 摸瓜V2引擎 |
| rnsn@z.i6 | 摸瓜V2引擎 |
| sn@7.wp8z6 | 摸瓜V2引擎 |
| n@is.rs | 摸瓜V2引擎 |
| rnsn@wq.s2 | 摸瓜V2引擎 |
| rnsn@q.iu | 摸瓜V2引擎 |
| n@uw.p6 | 摸瓜V2引擎 |
| rnsn@0.85p | 摸瓜V2引擎 |
| rnsn@3.si | 摸瓜V2引擎 |
| rnsn@3.8w | 摸瓜V2引擎 |
| rnsn@i.tpi | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| n@-.tqr | 摸瓜V2引擎 |
| nppnppn@rl4.bχ | 摸瓜V2引擎 |
| sn@5.m5 | 摸瓜V2引擎 |
| rnsn@z.mv | 摸瓜V2引擎 |
| rnsn@r3.mr | 摸瓜V2引擎 |
| n@4w0.vrrw | 摸瓜V2引擎 |
| rnsn@s4.vz | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| rnsn@0.85p | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| rnsn@z.zm | 摸瓜V2引擎 |
| rnsn@8.w8p | 摸瓜V2引擎 |
| rnsn@628.uw | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| rnsn@-.8q | 摸瓜V2引擎 |
| rnsn@4.25 | 摸瓜V2引擎 |
| rnsn@z.pt | 摸瓜V2引擎 |
| rnvon@v.4m | 摸瓜V2引擎 |
| rnsn@0.50 | 摸瓜V2引擎 |
| rnsn@w.32 | 摸瓜V2引擎 |
| rnsn@8.3u | 摸瓜V2引擎 |
| n@4w0.vrrw | 摸瓜V2引擎 |
| rnsn@6.sz | 摸瓜V2引擎 |
| rnsn@zm.mw | 摸瓜V2引擎 |
| rnsn@i.28i | 摸瓜V2引擎 |
| rnsn@1.33 | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| rnsn@s4.vz | 摸瓜V2引擎 |
| rnsn@2.1m | 摸瓜V2引擎 |
| nppnppn@rl4.bχ | 摸瓜V2引擎 |
| rnsn@q.iu | 摸瓜V2引擎 |
| rnpn@8.sq | 摸瓜V2引擎 |
| rnsn@v34.sq | 摸瓜V2引擎 |
| rnsn@8.38 | 摸瓜V2引擎 |
| n@2.3z | 摸瓜V2引擎 |
| rnsn@i.1v | 摸瓜V2引擎 |
| -@ek.ifbhbfryvd  мwbu@o.dll | 摸瓜V2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: True 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**

## **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.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\_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.RESTART\_PACKAGES | 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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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。 |
| com.asus.msa.SupplementaryDID.ACCESS | 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 |

## **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。**