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

**鬼谷八荒（ 1.1.142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 | 鬼谷八荒 |
| 版本 | 1.1.142 |
| 包名 | com.guigugame.guigubahuang |
| 域名线索 | 25条 |
| URL线索 | 23条 |
| APP图标 |  |
| 分析日期 | 2025年6月14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 | 鬼谷八荒---12-22.apk |
| 文件大小 | 1494.39MB |
| MD5值 | 3965cfcd5c79ee6d6c8c5baa829c54c6 |
| SHA1值 | 872b98f5b4674b53ae856467d4d131f2c256cdad |
| SHA256值 | 64006fa50ecf531ad36e997e266ad284f923b234ded94da60416aab633cdad40 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 鬼谷八荒 |
| 包名 | com.guigugame.guigubahuang |
| 主活动Activity | com.unity3d.player.PrivacyActivity |
| 安卓版本名称 | 1.1.142 |
| 安卓版本 | 142 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| moment.intl.tapapis.com | IP: 104.18.11.208 所属国家: United States of America 地区: California 城市: San Francisco  |
| l.taptap.io | IP: 104.18.0.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| tds-tapsdk0.intl.tapapis.com | IP: 104.18.10.208 所属国家: United States of America 地区: California 城市: San Francisco  |
| accounts.tapapis.com | IP: 104.18.19.10 所属国家: United States of America 地区: California 城市: San Francisco  |
| tds-moment.taptap.cn | IP: 203.107.32.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| accounts.taptap.cn | IP: 203.107.32.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.tapapis.com | IP: 104.18.19.10 所属国家: United States of America 地区: California 城市: San Francisco  |
| tds-moment.tap.io | IP: 104.18.19.218 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.taptap.com | IP: 39.107.195.45 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  |
| tds.taptap-api.com | 没有服务器地理信息.  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| tds-moment.taptap-api.com | IP: 39.96.128.107 所属国家: China 地区: Beijing 城市: Beijing  |
| www.xdrnd.com | IP: 47.101.131.115 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.api.xdrnd.cn | IP: 8.153.206.29 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dahuangwangluo.com | IP: 8.134.86.187 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| l.taptap.com | IP: 104.18.26.242 所属国家: United States of America 地区: California 城市: San Francisco  |
| accounts.tapapis.cn | IP: 203.107.32.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| store-release.tapapis.cn | IP: 39.107.195.23 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| astat.bugly.cros.wr.pvp.net | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| tds-tapsdk.cn.tapapis.com | IP: 47.93.94.172 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  |
| accounts.taptap.io | IP: 104.18.1.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| open.tapapis.cn | IP: 203.107.32.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://tds-tapsdk.cn.tapapis.com  | com/tapsdk/antiaddiction/BuildConfig.java  |
| https://tds-tapsdk.cn.tapapis.com  | com/tapsdk/antiaddiction/AntiAddictionImpl.java  |
| https://tds-tapsdk.cn.tapapis.com  | com/tapsdk/antiaddiction/models/IdentifyModel.java  |
| https://tds-tapsdk.cn.tapapis.com  | com/tapsdk/antiaddiction/constants/Constants.java  |
| https://open.tapapis.cn  | com/tapsdk/antiaddictionui/constant/Constants.java  |
| https://open.api.xdrnd.cn  | com/tapsdk/antiaddictionui/constant/Constants.java  |
| https://tds-tapsdk.cn.tapapis.com  | com/tapsdk/tapconnect/constants/ServerApi.java  |
| https://tds-tapsdk0.intl.tapapis.com  | com/tapsdk/tapconnect/constants/ServerApi.java  |
| https://tds-moment.taptap-api.com/  | com/tapsdk/moment/NoticeHandler.java  |
| https://moment.intl.tapapis.com/  | com/tapsdk/moment/NoticeHandler.java  |
| https://tds-moment.taptap.cn  | com/tapsdk/moment/view/MomentDialog.java  |
| https://tds-moment.tap.io  | com/tapsdk/moment/view/MomentDialog.java  |
| https://www.taptap.com/mobile  | com/taptap/pay/sdk/library/DLCManager.java  |
| https://www.taptap.com/mobile  | com/taptap/pay/sdk/library/TapTapLicense.java  |
| https://accounts.taptap.cn  | com/taptap/sdk/RegionType.java  |
| https://accounts.tapapis.cn  | com/taptap/sdk/RegionType.java  |
| https://open.tapapis.com  | com/taptap/sdk/RegionType.java  |
| https://accounts.taptap.io  | com/taptap/sdk/RegionType.java  |
| https://accounts.tapapis.com  | com/taptap/sdk/RegionType.java  |
| https://www.xdrnd.com/  | com/taptap/sdk/ui/WebBlock.java  |
| https://open.tapapis.cn/friends/v1/list  | com/taptap/sdk/friends/TapFriends.java  |
| https://open.tapapis.com/friends/v1/list  | com/taptap/sdk/friends/TapFriends.java  |
| https://store-release.tapapis.cn  | com/taptap/services/update/TapUpdateAPI.java  |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection  | com/tds/common/websocket/conn/AbstractWebSocket.java  |
| https://l.taptap.com/5d1NGyET  | com/tds/common/utils/TapGameUtil.java  |
| https://l.taptap.io/GNYwFaZr  | com/tds/common/utils/TapGameUtil.java  |
| https://l.taptap.com/5d1NGyET?subc1=%s  | com/tds/common/utils/TapGameUtil.java  |
| https://l.taptap.io/GNYwFaZr?subc1=%s  | com/tds/common/utils/TapGameUtil.java  |
| https://tds.taptap-api.com/tool/check\_ip\_region  | com/tds/common/region/TdsRegionHelper.java  |
| https://accounts.taptap.cn  | com/tds/common/oauth/RegionType.java  |
| https://accounts.tapapis.cn  | com/tds/common/oauth/RegionType.java  |
| https://open.tapapis.com  | com/tds/common/oauth/RegionType.java  |
| https://accounts.taptap.io  | com/tds/common/oauth/RegionType.java  |
| https://accounts.tapapis.com  | com/tds/common/oauth/RegionType.java  |
| https://tds-tapsdk.cn.tapapis.com/achievement/api/v1/clients/  | com/tds/achievement/AchievementImpl.java  |
| https://tds-tapsdk0.intl.tapapis.com/achievement/api/v1/clients/  | com/tds/achievement/AchievementImpl.java  |
| 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  |
| http://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  |
| http://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/crashreport/common/strategy/a.java  |
| https://dahuangwangluo.com/user.html\  | com/unity3d/player/PrivacyActivity.java  |
| https://dahuangwangluo.com/notice.html\  | com/unity3d/player/PrivacyActivity.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: 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 |
| --- |
| "antiaddictionui\_dialog\_tap\_authorization\_title" : "TapTap 快速认证服务"  |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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\_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 |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| 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\_MEDIA\_IMAGES | 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.BIND\_VPN\_SERVICE | 合法 |  | VpnService 必须要求,以确保只有系统可以绑定到它 |
| 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.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 |

## **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。**