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

**TEST0627（ 1.2.1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 | TEST0627 |
| 版本 | 1.2.1 |
| 包名 | com.qxco3.baxe69lr |
| 域名线索 | 21条 |
| URL线索 | 4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 | TEST0627\_2.apk |
| 文件大小 | 2.43MB |
| MD5值 | 261ab27365a4b9bee0592572bd1e97c4 |
| SHA1值 | 998436fd0235c04dd3c542b6d30e419b01ffde0d |
| SHA256值 | 5abd2904951885b826b02b6ff13820fe1a14a3379d0907e274516becd3323828 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | TEST0627 |
| 包名 | com.qxco3.baxe69lr |
| 主活动Activity | com.example.myapplication.ui.webviewstudy.GameActivity |
| 安卓版本名称 | 1.2.1 |
| 安卓版本 | 4 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| gdpr.us.adjust.com | IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin  |
| app.adjust.net.in | IP: 185.151.204.31 所属国家: Germany 地区: Berlin 城市: Berlin  |
| subscription.us.adjust.com | IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin  |
| app.us.adjust.com | IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin  |
| app.adjust.cn | IP: 47.104.30.117 所属国家: China 地区: Shandong 城市: Qingdao  |
| gdpr.adjust.net.in | IP: 185.151.204.30 所属国家: Germany 地区: Berlin 城市: Berlin  |
| schemas.android.com | 没有服务器地理信息.  |
| gdpr.adjust.world | IP: 185.151.204.40 所属国家: Germany 地区: Berlin 城市: Berlin  |
| subscription.tr.adjust.com | IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir  |
| subscription.eu.adjust.com | IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin  |
| gdpr.eu.adjust.com | IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin  |
| subscription.adjust.com | IP: 185.151.204.52 所属国家: Germany 地区: Berlin 城市: Berlin  |
| app.tr.adjust.com | IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir  |
| app.adjust.com | IP: 185.151.204.9 所属国家: Germany 地区: Berlin 城市: Berlin  |
| subscription.adjust.world | IP: 185.151.204.44 所属国家: Germany 地区: Berlin 城市: Berlin  |
| gdpr.tr.adjust.com | IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir  |
| subscription.adjust.net.in | IP: 185.151.204.34 所属国家: Germany 地区: Berlin 城市: Berlin  |
| app.adjust.world | IP: 185.151.204.43 所属国家: Germany 地区: Berlin 城市: Berlin  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| gdpr.adjust.com | IP: 185.151.204.50 所属国家: Germany 地区: Berlin 城市: Berlin  |
| app.eu.adjust.com | IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://app.adjust.com  | com/adjust/sdk/Constants.java  |
| https://gdpr.adjust.com  | com/adjust/sdk/Constants.java  |
| https://subscription.adjust.com  | com/adjust/sdk/Constants.java  |
| https://github.com/adjust/android\_sdk  | com/adjust/sdk/ActivityHandler.java  |
| https://app.adjust.world  | com/adjust/sdk/network/UrlStrategy.java  |
| https://app.adjust.cn  | com/adjust/sdk/network/UrlStrategy.java  |
| https://app.eu.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://app.adjust.net.in  | com/adjust/sdk/network/UrlStrategy.java  |
| https://app.tr.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://app.us.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://gdpr.adjust.world  | com/adjust/sdk/network/UrlStrategy.java  |
| https://gdpr.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://gdpr.eu.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://gdpr.adjust.net.in  | com/adjust/sdk/network/UrlStrategy.java  |
| https://gdpr.tr.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://gdpr.us.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://subscription.adjust.world  | com/adjust/sdk/network/UrlStrategy.java  |
| https://subscription.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://subscription.eu.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://subscription.adjust.net.in  | com/adjust/sdk/network/UrlStrategy.java  |
| https://subscription.tr.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| https://subscription.us.adjust.com  | com/adjust/sdk/network/UrlStrategy.java  |
| http://schemas.android.com/apk/res/android  | s/h.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='CN', ST=''Beijing', L='Beijing', O='MyOrganization', OU='IT', CN='CN' 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-12 12:37:28+00:00 有效期至: 2124-09-18 12:37:28+00:00 发行人: C='CN', ST=''Beijing', L='Beijing', O='MyOrganization', OU='IT', CN='CN' 序列号: 0x6a98273868e4065 哈希算法: sha256 md5值: 6c0f44d57e342c3f36dd0c41e34ee67c sha1值: 15fcc99ec2f6885b8305c091ca8046fa258b00a4 sha256值: e92f19d675acbffec79edaebd8367570ea6fc95fae7d826855935848bfce0d77 sha512值: 94ffd254adf8b71348d7698f865025e8aa2c0900a1d5bda77b1211e7336492f286757937bcf2417d83d6ed50bf4c472e662d8e60b654f97bada3c532c3022c19 公钥算法: rsa 密钥长度: 2048 指纹: cf7128712b66ed15542165e62fef946c9e50ebe6440f1863a7637224cb935db7**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_high" : "HIGH"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_low" : "LOW"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_normal" : "NORMAL"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_silence" : "SILENCE"  |
| "google\_api\_key" : "AIzaSyAQg2m49WtDGByA9WJZCcKN6rq1YYzkfBA"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAQg2m49WtDGByA9WJZCcKN6rq1YYzkfBA"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_high" : "重要"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_low" : "不重要"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_normal" : "普通"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_silence" : "静默"  |

## **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.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.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\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.example.myapplication.ui.webviewstudy.GameActivity | **Schemes**: panda\_2://, **Hosts:** open,  |

**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。**