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

**欢乐游戏（ 1.0.0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 | 欢乐游戏 |
| 版本 | 1.0.0 |
| 包名 | com.hlyxnb.otogas |
| 域名线索 | 54条 |
| URL线索 | 49条 |
| APP图标 |  |
| 分析日期 | 2025年1月27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 | hlan.apk |
| 文件大小 | 43.68MB |
| MD5值 | f4ea4bdb83e1eef7c1f0408fa3a39603 |
| SHA1值 | d77a21e83d6e22836fa5e069e1576d4ede9b68be |
| SHA256值 | 78e4949e094f3566d28a08213ceec9976dce091b6e41250840c7c905e5f8945c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 欢乐游戏 |
| 包名 | com.hlyxnb.otogas |
| 主活动Activity | com.hlyxnb.otogas.MainActivity |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 11 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| cfg.imtt.qq.com | IP: 175.27.12.246  所属国家: China  地区: Beijing  城市: Beijing |
| log.tbs.qq.com | IP: 109.244.244.32  所属国家: China  地区: Beijing  城市: Beijing |
| huatuocode.huatuo.qq.com | 没有服务器地理信息. |
| api.sharetrace.com | IP: 39.98.67.122  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cgi.connect.qq.com | IP: 175.27.9.43  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.alipay.com | IP: 203.209.247.65  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 120.24.210.161 | IP: 120.24.210.161  所属国家: China  地区: Guangdong  城市: Shenzhen |
| apilocate.amap.com | IP: 59.82.31.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| debugtbs.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| mta.oa.com | IP: 193.123.33.15  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mcgw.alipay.com | IP: 124.239.239.237  所属国家: China  地区: Hebei  城市: Langfang |
| upl.baidu.com | IP: 110.242.68.242  所属国家: China  地区: Hebei  城市: Baoding |
| ssgw.updrips.com | 没有服务器地理信息. |
| apilocatesrc.amap.com | IP: 59.82.31.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mdc.html5.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| api.uca.cloud.unity3d.com | IP: 101.32.104.143  所属国家: Singapore  地区: Singapore  城市: Singapore |
| debugx5.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| open.weixin.qq.com | IP: 175.24.219.72  所属国家: China  地区: Beijing  城市: Beijing |
| vse.baidu.com | IP: 110.242.68.242  所属国家: China  地区: Hebei  城市: Baoding |
| graph.qq.com | IP: 175.27.9.43  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| tsis.jpush.cn | IP: 121.36.74.75  所属国家: China  地区: Beijing  城市: Beijing |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| adiu.amap.com | IP: 59.82.29.231  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| m.alipay.com | IP: 203.209.245.74  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| openmobile.qq.com | IP: 175.27.9.14  所属国家: China  地区: Beijing  城市: Beijing |
| pms.mb.qq.com | IP: 109.244.173.227  所属国家: China  地区: Beijing  城市: Beijing |
| config.uca.cloud.unity3d.com | IP: 34.111.113.40  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| wup.imtt.qq.com | IP: 42.187.184.221  所属国家: China  地区: Beijing  城市: Beijing |
| h5.m.taobao.com | IP: 220.181.135.167  所属国家: China  地区: Beijing  城市: Beijing |
| mse.baidu.com | IP: 180.101.49.124  所属国家: China  地区: Jiangsu  城市: Nanjing |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| fusion.qq.com | IP: 175.27.9.24  所属国家: China  地区: Beijing  城市: Beijing |
| abroad.apilocate.amap.com | IP: 59.82.44.11  所属国家: China  地区: Shanghai  城市: Shanghai |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| qzs.qq.com | IP: 221.204.18.250  所属国家: China  地区: Shanxi  城市: Taiyuan |
| appsupport.qq.com | IP: 175.27.9.14  所属国家: China  地区: Beijing  城市: Beijing |
| splash-ads.unitychina.cn | IP: 60.220.213.168  所属国家: China  地区: Shanxi  城市: Taiyuan |
| mta.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| 182.92.20.189 | IP: 182.92.20.189  所属国家: China  地区: Beijing  城市: Beijing |
| yuyin.baidu.com | IP: 153.3.237.166  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pingma.qq.com | IP: 119.45.78.184  所属国家: China  地区: Beijing  城市: Beijing |
| mclient.alipay.com | IP: 220.181.135.162  所属国家: China  地区: Beijing  城市: Beijing |
| cdp.cloud.unity3d.com | IP: 101.32.113.127  所属国家: Singapore  地区: Singapore  城市: Singapore |
| long.open.weixin.qq.com | IP: 109.244.217.35  所属国家: China  地区: Beijing  城市: Beijing |
| wappaygw.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| splash.unity.cn | IP: 172.81.232.209  所属国家: China  地区: Beijing  城市: Beijing |
| openapi.baidu.com | IP: 110.242.69.36  所属国家: China  地区: Hebei  城市: Baoding |
| restapi.amap.com | IP: 106.11.43.113  所属国家: China  地区: Beijing  城市: Beijing |
| vop.baidu.com | IP: 111.206.209.68  所属国家: China  地区: Beijing  城市: Beijing |
| lbs.amap.com | IP: 59.82.29.232  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://ssgw.updrips.com/oauth2/checkAppInfo | org/xianliao/im/sdk/net/model/LoginInfoRequest.java |
| http://120.24.210.161:52234/gateway/red/dispatcher | org/xianliao/im/sdk/net/model/GetBilIdlRequest.java |
| https://api.sharetrace.com | 肌緭/肌緭/肌緭/肌緭/葋申湋骶映鍮秄憁鎓羭/C0033.java |
| https://tsis.jpush.cn | cn/jiguang/c/a.java |
| http://182.92.20.189:9099/ | cn/jiguang/a/a/c/i.java |
| http://yuyin.baidu.com/voice?osname=voiceopen&action=usereventflow& | com/baidu/speech/utils/analysis/Analysis.java |
| http://vop.baidu.com/v2 | com/baidu/speech/core/ASREngine.java |
| https://upl.baidu.com//words/add | com/baidu/speech/asr/SlotControl.java |
| https://vse.baidu.com/v2 | com/baidu/speech/asr/SpeechConstant.java |
| https://vse.baidu.com/echo.fcgi | com/baidu/speech/asr/SpeechConstant.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/ | com/amap/api/location/AMapLocation.java |
| https://splash-ads.unitychina.cn/webview/release/native/config.json | com/unity3d/splash/services/core/properties/SdkProperties.java |
| https://splash.unity.cn/api/register-game-launch | com/unity3d/player/UnityPlayer.java |
| https://splash.unity.cn/api/diagnosis | com/unity3d/player/k.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/cons/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/cons/a.java |
| http://m.alipay.com/?action=h5quit | com/alipay/sdk/cons/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$& | com/alipay/sdk/data/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/packet/impl/c.java |
| http://mobilegw.stable.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.aaa.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/dn.java |
| https://restapi.amap.com/v3/iasdkauth | com/loc/m.java |
| http://restapi.amap.com/v3/iasdkauth | com/loc/m.java |
| https://adiu.amap.com/ws/device/adius | com/loc/bj.java |
| http://restapi.amap.com | com/loc/s.java |
| http://apilocate.amap.com/mobile/binary | com/loc/di.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/di.java |
| http://restapi.amap.com/v3/place/text? | com/loc/a.java |
| http://restapi.amap.com/v3/place/around? | com/loc/a.java |
| http://restapi.amap.com/v3/config/district? | com/loc/a.java |
| http://restapi.amap.com/v3/geocode/regeo | com/loc/dd.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/db.java |
| http://apilocatesrc.amap.com/mobile/binary | com/loc/db.java |
| http://xmlpull.org/v1/doc/features.html | com/ta/utdid2/b/a/e.java |
| http://xmlpull.org/v1/doc/features.html | com/ta/utdid2/b/a/a.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/v.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/v.java |
| http://wup.imtt.qq.com:8080 | com/tencent/smtt/utils/v.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/v.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/v.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/v.java |
| http://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/v.java |
| https://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/v.java |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs | com/tencent/smtt/utils/i.java |
| http://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/ag.java |
| http://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| http://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| http://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| http://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/a/d.java |
| https://graph.qq.com/oauth2.0/me | com/tencent/connect/UnionInfo.java |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1 | com/tencent/connect/share/QQShare.java |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1 | com/tencent/connect/share/QzoneShare.java |
| http://openmobile.qq.com/oauth2.0/m\_jump\_by\_version? | com/tencent/connect/common/BaseApi.java |
| http://qzs.qq.com/open/mobile/login/qzsjump.html? | com/tencent/connect/common/BaseApi.java |
| https://openmobile.qq.com/oauth2.0/m\_authorize? | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/user/user\_login\_statis | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/v3/user/get\_info | com/tencent/connect/auth/AuthAgent.java |
| http://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | com/tencent/connect/auth/AuthAgent.java |
| http://qzs.qq.com/open/mobile/login/qzsjump.html? | com/tencent/connect/auth/a.java |
| http://mta.qq.com/ | com/tencent/wxop/stat/StatServiceImpl.java |
| http://mta.oa.com/ | com/tencent/wxop/stat/StatServiceImpl.java |
| http://pingma.qq.com:80/mstat/report | com/tencent/wxop/stat/common/StatConstants.java |
| http://qzs.qq.com/open/mobile/request/sdk\_request.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com | com/tencent/open/SocialApiIml.java |
| https://openmobile.qq.com/ | com/tencent/open/utils/HttpUtils.java |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | com/tencent/open/utils/f.java |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report | com/tencent/open/b/g.java |
| https://huatuocode.huatuo.qq.com | com/tencent/open/b/d.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/d.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/f.java |
| https://api.uca.cloud.unity3d.com/v1/events | lib/armeabi-v7a/libunity.so |
| https://cdp.cloud.unity3d.com/v1/events | lib/armeabi-v7a/libunity.so |
| https://config.uca.cloud.unity3d.com | lib/armeabi-v7a/libunity.so |
| https://vse.baidu.com/echo.fcgi | lib/armeabi-v7a/libBaiduSpeechSDK.so |
| https://mse.baidu.com/echo.fcgi | lib/armeabi-v7a/libBaiduSpeechSDK.so |
| https://vop.baidu.com/echo.fcgi | lib/armeabi-v7a/libBaiduSpeechSDK.so |
| https://openapi.baidu.com/oauth/2.0/token | lib/armeabi-v7a/libBaiduSpeechSDK.so |
| http://upl.baidu.com/auth.php | lib/armeabi-v7a/libBaiduSpeechSDK.so |

### **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=c, ST=cd, L=cd, O=ycj, OU=ycj, CN=ycj 签名算法: rsassa\_pkcs1v15 有效期自: 2017-01-21 12:30:21+00:00 有效期至: 2071-10-25 12:30:21+00:00 发行人: C=c, ST=cd, L=cd, O=ycj, OU=ycj, CN=ycj 序列号: 0x6d7ffd50 哈希算法: sha256 md5值: aa57a9d10715452db8edbc3bbfa59995 sha1值: 8f70f8b691bd72e48c84dffb0be9c6c80e66d0b4 sha256值: 45ea0600010de79c1229d47e184ce527b6c9d9f715967e7df8627c7aa8a8103d sha512值: e17119b492bad182a247a694f06ee18983f56f3a22ab5572337c7e9177b68426e63be62f5df88f4834c988db4eaae051df0b31d4ac01bfb8bd969a5b3c2ca330 公钥算法: rsa 密钥长度: 2048 指纹: 6a9281c4ccc7e86685234b39d9c3cc8178232e4e8d5a616b593b6fc1761c89ef**

## **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.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\_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.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\_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.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.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.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.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.hlyxnb.otogas.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| 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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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\_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.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.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.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.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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.hlyxnb.otogas.MainActivity | **Schemes**: dtkwx://,  **Hosts:** dthy,  **Ports:** 8888,  **Paths:** /join, |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1107228740://, |
| com.hlyxnb.otogas.sgapi.SGEntryActivity | **Schemes**: paraches://,  **Hosts:** xianliaoIdL9CsA0EtAfm8HR, |

**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。**