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

**玩物（ 1.2.8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 | 玩物 |
| 版本 | 1.2.8 |
| 包名 | com.player.liveww |
| 域名线索 | 48条 |
| URL线索 | 57条 |
| APP图标 |  |
| 分析日期 | 2025年6月26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 | wwv1.2.8.apk |
| 文件大小 | 130.91MB |
| MD5值 | a095b75827f2ccdb03368c1cd27e5a67 |
| SHA1值 | b15aca6adbd07e2f1c0d43e730a6ddc2345378dd |
| SHA256值 | 2a8be4c8a57af340f19aee17032b46ddc675aba8716490c56d61068ff9af3fa3 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 玩物 |
| 包名 | com.player.liveww |
| 主活动Activity | com.player.liveww.MainActivity |
| 安卓版本名称 | 1.2.8 |
| 安卓版本 | 30 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| cloudcontrol.rongcloud.net | IP: 47.94.224.40 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| s3.amazonaws.com | IP: 16.15.185.48 所属国家: United States of America 地区: Washington 城市: Seattle  |
| full.hx-jt.cn | 没有服务器地理信息.  |
| game.hx-jt.cn | 没有服务器地理信息.  |
| cell.hx-jt.cn | 没有服务器地理信息.  |
| alogsus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| en.wikipedia.org | IP: 31.13.94.49 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| www.tinsyexyz.com | 没有服务器地理信息.  |
| e.hx-jt.cn | 没有服务器地理信息.  |
| feedback.rong-edge.com | IP: 101.200.58.95 所属国家: China 地区: Beijing 城市: Beijing  |
| www.baidu.com | IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding  |
| youtrack.jetbrains.com | IP: 63.35.30.167 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| test-bootstrapprofile-c-1.oss-cn-beijing.aliyuncs.com | IP: 123.125.18.57 所属国家: China 地区: Beijing 城市: Beijing  |
| ucc.umeng.com | IP: 203.119.169.9 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| stats.cn.ronghub.com | IP: 47.94.172.98 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| firebase.google.com | IP: 74.125.20.139 所属国家: United States of America 地区: California 城市: Mountain View  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| doll.hx-jt.cn | 没有服务器地理信息.  |
| schemas.android.com | 没有服务器地理信息.  |
| resolve.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.tensorflow.org | IP: 142.250.99.113 所属国家: United States of America 地区: California 城市: Mountain View  |
| issuetracker.google.com | IP: 74.125.20.113 所属国家: United States of America 地区: California 城市: Mountain View  |
| g.co | IP: 74.125.142.102 所属国家: United States of America 地区: California 城市: Mountain View  |
| utoken.umeng.com | IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| bei.hx-jt.cn | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| test-bootstrapprofile-b-2.s3.ap-southeast-1.amazonaws.com | IP: 3.5.148.149 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ns.adobe.com | 没有服务器地理信息.  |
| exoplayer.dev | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| developer.umeng.com | IP: 59.82.60.43 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| default.url | 没有服务器地理信息.  |
| www.example.com | IP: 23.220.70.41 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| aspect-upush.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| developer.android.com | IP: 108.177.98.139 所属国家: United States of America 地区: California 城市: Mountain View  |
| alogus.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| firebase-settings.crashlytics.com | IP: 114.250.70.34 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umengcloud.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| cnlogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ulogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| developer.apple.com | IP: 17.253.87.204 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| schemas.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| aomedia.org | IP: 108.160.166.61 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://youtrack.jetbrains.com/issue/KT-55980  | aj/y.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | a3/w0.java  |
| https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings  | bd/g.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://www.tinsyexyz.com/  | com/player/liveww/MyApplication.java  |
| https://en.wikipedia.org/wiki/Blend\_modes\n//  | com/tencent/ugc/videoprocessor/transitions/StereoViewerFilter.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/l.java  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | com/umeng/analytics/pro/aq.java  |
| https://cnlogs.umeng.com/ext\_event  | com/umeng/analytics/pro/aq.java  |
| https://resolve.umeng.com/resolve  | com/umeng/analytics/pro/bt.java  |
| https://ucc.umeng.com/v2/inn/fetch  | com/umeng/analytics/pro/ar.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://developer.umeng.com/docs/119267/detail/118637  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://utoken.umeng.com  | com/umeng/umzid/ZIDManager.java  |
| https://cell.hx-jt.cn/index.php  | com/tinstall/tinstall/TInstall.java  |
| https://bei.hx-jt.cn  | com/tinstall/tinstall/TInstall.java  |
| https://cell.hx-jt.cn  | com/tinstall/tinstall/TInstall.java  |
| https://doll.hx-jt.cn  | com/tinstall/tinstall/TInstall.java  |
| https://e.hx-jt.cn  | com/tinstall/tinstall/TInstall.java  |
| https://full.hx-jt.cn  | com/tinstall/tinstall/TInstall.java  |
| https://game.hx-jt.cn  | com/tinstall/tinstall/TInstall.java  |
| http://www.baidu.com/  | com/tinstall/tinstall/TInstall.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | g2/a.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | g6/q.java  |
| https://issuetracker.google.com/issues/new?component=618491&template=1257717  | g0/g.java  |
| https://github.com/flutter/flutter/issues/165510  | io/flutter/view/f.java  |
| https://developer.android.com/reference/android/view/View  | io/flutter/view/f.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/g.java  |
| https://feedback.rong-edge.com  | io/rong/common/rlog/RLogConfig.java  |
| https://feedback.rong-edge.com  | io/rong/common/dlog/LogEntity.java  |
| http://%s/  | io/rong/imlib/cloudcontroller/CloudController.java  |
| http://cloudcontrol.rongcloud.net/v1/config  | io/rong/imlib/cloudcontroller/CloudUpdater.java  |
| http://s3.amazonaws.com/doc/2006-03-01/  | io/rong/imlib/filetransfer/MinioSliceCompleteRequest.java  |
| http://s3.amazonaws.com/doc/2006-03-01/  | io/rong/imlib/filetransfer/StcSliceCompleteRequest.java  |
| http://xml.org/sax/features/external-general-entities  | io/rong/imlib/common/ParserFactory.java  |
| http://xml.org/sax/features/external-parameter-entities  | io/rong/imlib/common/ParserFactory.java  |
| http://%s  | io/rong/imlib/httpdns/HttpDnsClient.java  |
| https://test-bootstrapprofile-c-1.oss-cn-beijing.aliyuncs.com/  | io/rong/imlib/url/StaticConfigManager.java  |
| https://test-bootstrapprofile-b-2.s3.ap-southeast-1.amazonaws.com/  | io/rong/imlib/url/StaticConfigManager.java  |
| http://%s/  | io/rong/rtlog/upload/RtLogTimingUploadConfig.java  |
| http://%s/  | io/rong/rtlog/upload/RtLogUploadManager.java  |
| https://stats.cn.ronghub.com  | io/rong/libcore/BuildConfig.java  |
| http://%s/  | io/rong/rtslog/RtsConfigEnv.java  |
| http://schemas.android.com/apk/res/android  | e1/l.java  |
| http://dashif.org/guidelines/last-segment-number  | e3/d.java  |
| http://dashif.org/guidelines/trickmode  | e3/d.java  |
| http://dashif.org/thumbnail\_tile  | e3/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | e3/d.java  |
| https://x</LA\_URL>  | f3/l0.java  |
| https://default.url  | f3/l0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | f3/m0.java  |
| https://docs.flutter.dev/deployment/android  | kh/d.java  |
| https://firebase.google.com/support/privacy/init-options.  | md/g.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | mk/m.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | p9/u0.java  |
| https://firebase.google.com/docs/crashlytics/get-started?platform=android  | tc/d0.java  |
| https://issuetracker.google.com/issues/new?component=907884&template=1466542  | x1/j.java  |
| https://issuetracker.google.com/issues/241760537  | x1/a0.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | y2/q.java  |
| http://g.co/dev/packagevisibility.  | y2/w.java  |
| https://aomedia.org/emsg/ID3  | ga/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | ga/a.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | nk/o.java  |
| http://ns.adobe.com/xap/1.0/  | g4/b.java  |
| https://aomedia.org/emsg/ID3  | j4/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | j4/a.java  |
| https://doll.hx-jt.cn/  | 摸瓜V2引擎  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/arm64-v8a/libbarhopper\_v3.so  |
| http://http  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/arm64-v8a/libbarhopper\_v3.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided  | com/tencent/liteav/base/PiiElider.java  |
| u0013android@android.com0 u0013android@android.com  | eb/q.java  |
| z@r1762.tmp z@r120a.tmp z@r1751.tmp  | 摸瓜V2引擎  |
| appro@openssl.org  | lib/arm64-v8a/libRongIMLib.so  |
| android-sdk-releaser@oouc14.prod  | lib/arm64-v8a/libbarhopper\_v3.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14159265358  | com/tencent/ugc/videoprocessor/transitions/BounceFilter.java  |
| 17179869184  | com/faceunity/wrapper/faceunity.java  |
| 17512775099  | gc/a.java  |
| 18222222222  | q4/e.java  |
| 19222222222  | q4/e.java  |

## **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=ch, ST=ch, L=cc, O=aa, OU=dd, CN=ff 签名算法: rsassa\_pkcs1v15 有效期自: 2025-01-08 03:44:37+00:00 有效期至: 2025-04-08 03:44:37+00:00 发行人: C=ch, ST=ch, L=cc, O=aa, OU=dd, CN=ff 序列号: 0x540902a9 哈希算法: sha256 md5值: 94ce3f4eae92347cffd993d1fb52bc24 sha1值: 9bcdcf9cf477e2d8c66a64a9fe6d978ca0a803f5 sha256值: 651e0927cf2d55a4334ce7d1d7079ce505a7f204c6a5763add029f554c704495 sha512值: 4c3d7b5dbff4342059fadd2e8284b40b5ef071a30b55dde43520d9ad2df4d179b75c3ae62d4dfe786f6e801d465453eace2124620247c13ead28b0778c4b92ff 公钥算法: rsa 密钥长度: 2048 指纹: 1bdda66912d1d367a7f5627e0f0f584ee37bfa42fd6d200d6d9401038293c713**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "com.google.firebase.crashlytics.mapping\_file\_id" : "7f31fe3ff3734261a60ebab895cb69c3"  |
| "facebook\_client\_token" : "42f1cd02420c6f6422f7b0de268590ad"  |

## **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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_SPECIAL\_USE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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.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.VIDEO\_CAPTURE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.AUDIO\_CAPTURE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.GET\_PACKAGE\_SIZE | 正常 | 测量应用程序存储空间 | 允许应用程序找出任何包使用的空间 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| com.player.liveww.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| com.player.liveww.permission.RONG\_ACCESS\_RECEIVER | 未知 | Unknown permission | Unknown permission from android reference |
| com.player.liveww.permission.RONG\_BRIDGE\_ACTIVITY | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PROJECTION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.player.liveww.MainActivity | **Schemes**: um.683fe3d6bc47b67d837bbdca://,  |

**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。**