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

**万利汇（ 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 | 万利汇 |
| 版本 | 1.0.0 |
| 包名 | wanlh.caht.com |
| 域名线索 | 40条 |
| URL线索 | 45条 |
| APP图标 |  |
| 分析日期 | 2025年6月30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 | 万利汇高电商.apk |
| 文件大小 | 34.69MB |
| MD5值 | 38b4c59739d9cf0e1f928d500fd4ac7c |
| SHA1值 | 2b78976fc145dfcfcd36d120a6f4bbb01832cb93 |
| SHA256值 | b2b3429d7531d282e069118d11898087695f8998f62d28302af3150f9fc30f23 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 万利汇 |
| 包名 | wanlh.caht.com |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| wappaygw.alipay.com | IP: 111.202.5.210  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| adiu.amap.com | IP: 110.253.189.146  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| schemas.android.com | 没有服务器地理信息. |
| loggw-exsdk.alipay.com | IP: 119.42.231.4  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| open.weixin.qq.com | IP: 140.207.176.25  所属国家: China  地区: Shanghai  城市: Shanghai |
| restapi.amap.com | IP: 203.119.169.174  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| m3w.cn | IP: 116.196.150.249  所属国家: China  地区: Zhejiang  城市: Jinhua |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| ask.dcloud.net.cn | IP: 220.194.123.111  所属国家: China  地区: Tianjin  城市: Tianjin |
| next.vuex.vuejs.org | IP: 15.197.167.90  所属国家: United States of America  地区: Washington  城市: Seattle |
| render.alipay.com | IP: 124.95.153.222  所属国家: China  地区: Liaoning  城市: Shenyang |
| mclient.alipay.com | IP: 116.142.235.203  所属国家: China  地区: Beijing  城市: Beijing |
| mths.be | IP: 83.137.145.144  所属国家: Netherlands  地区: Groningen  城市: Groningen |
| apis.map.qq.com | IP: 116.130.223.114  所属国家: China  地区: Beijing  城市: Beijing |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| qiniu.syoupin.com | IP: 222.134.1.30  所属国家: China  地区: Shandong  城市: Binzhou |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| restsdk.amap.com | IP: 106.11.43.113  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 |
| quilljs.com | IP: 172.66.43.93  所属国家: United States of America  地区: California  城市: San Francisco |
| cgicol.amap.com | IP: 110.253.189.211  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| h5.m.taobao.com | IP: 125.39.155.171  所属国家: China  地区: Tianjin  城市: Tianjin |
| er.dcloud.io | 没有服务器地理信息. |
| hyg.lplive.cn | IP: 47.93.2.56  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mobilegw.alipay.com | IP: 203.209.243.27  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| service.dcloud.net.cn | IP: 110.40.181.119  所属国家: China  地区: Beijing  城市: Beijing |
| lbs.amap.com | IP: 110.253.189.212  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| dualstack-a.apilocate.amap.com | IP: 106.11.43.81  所属国家: China  地区: Beijing  城市: Beijing |
| system.wanlh.com | IP: 110.42.43.192  所属国家: China  地区: Zhejiang  城市: Ningbo |
| mobilegwpre.alipay.com | IP: 110.75.138.35  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| at.alicdn.com | IP: 119.249.53.239  所属国家: China  地区: Hebei  城市: Baoding |
| www.google.com | IP: 199.16.158.8  所属国家: United States of America  地区: California  城市: San Francisco |
| vuejs.org | IP: 15.197.167.90  所属国家: United States of America  地区: Washington  城市: Seattle |
| er.dcloud.net.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| apilocate.amap.com | IP: 106.11.43.81  所属国家: China  地区: Beijing  城市: Beijing |
| ns.adobe.com | 没有服务器地理信息. |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| mcgw.alipay.com | IP: 111.202.5.210  所属国家: China  地区: Beijing  城市: Beijing |
| dualstack-arestapi.amap.com | IP: 203.119.169.174  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://mobilegwpre.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/m/l/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | com/alipay/sdk/m/l/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | com/alipay/sdk/m/m/a.java |
| https://render.alipay.com/p/s/i?scheme=%s | com/alipay/sdk/app/OpenAuthTask.java |
| https://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/ | com/amap/api/location/AMapLocation.java |
| https://adiu.amap.com/ws/device/adius | com/loc/bo.java |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74& | com/loc/df.java |
| http://apilocate.amap.com/mobile/binary | com/loc/fv.java |
| http://dualstack-a.apilocate.amap.com/mobile/binary | com/loc/fv.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fv.java |
| https://restsdk.amap.com/sdk/compliance/params | com/loc/ay.java |
| http://restsdk.amap.com/sdk/compliance/params | com/loc/ay.java |
| http://restsdk.amap.com | com/loc/w.java |
| http://restsdk.amap.com/v3/place/text? | com/loc/a.java |
| http://restsdk.amap.com/v3/config/district? | com/loc/a.java |
| http://restsdk.amap.com/v3/place/around? | com/loc/a.java |
| https://restapi.amap.com/rest/aaid/get | com/loc/ag.java |
| http://restapi.amap.com/rest/aaid/get | com/loc/ag.java |
| https://restsdk.amap.com/v3/iasdkauth | com/loc/n.java |
| https://dualstack-arestapi.amap.com/v3/iasdkauth | com/loc/n.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/gb.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fo.java |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo | com/loc/fq.java |
| http://restsdk.amap.com/v3/geocode/regeo | com/loc/fq.java |
| http://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/c.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/b.java |
| http://ns.adobe.com/xap/1.0/\u0000 | io/dcloud/common/util/ExifInterface.java |
| https://m3w.cn/s/ | io/dcloud/common/util/ShortCutUtil.java |
| https://ask.dcloud.net.cn/article/282 | io/dcloud/common/constant/DOMException.java |
| https://ask.dcloud.net.cn/article/35058 | io/dcloud/feature/audio/AudioRecorderMgr.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/feature/utsplugin/ProxyModule.java |
| https://er.dcloud.io/sc | io/dcloud/feature/gg/dcloud/ADHandler.java |
| https://er.dcloud.net.cn/sc | io/dcloud/feature/gg/dcloud/ADHandler.java |
| https://ask.dcloud.net.cn/article/35627 | io/dcloud/e/b/a.java |
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/e/b/a.java |
| https://er.dcloud.io/rv | io/dcloud/e/c/h/c.java |
| https://er.dcloud.net.cn/rv | io/dcloud/e/c/h/c.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/g/b.java |
| https://ask.dcloud.net.cn/article/287 | io/dcloud/share/IFShareApi.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifViewUtils.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextureView.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextView.java |
| https://ask.dcloud.net.cn/article/36199 | 摸瓜V1引擎 |
| http://system.wanlh.com/service.html\ | 摸瓜V2引擎 |
| http://system.wanlh.com/privacy.html\ | 摸瓜V2引擎 |
| http://system.wanlh.com | 摸瓜V2引擎 |
| https://at.alicdn.com/t/c/font\_4197023\_t7j01i1rx6j.ttf?t=1699249073419 | 摸瓜V2引擎 |
| http://qiniu.syoupin.com/svideo/ | 摸瓜V2引擎 |
| http://hyg.lplive.cn/image/image/canbk.png | 摸瓜V2引擎 |
| http://hyg.lplive.cn/image/image/pm.png | 摸瓜V2引擎 |
| https://github.com/ecomfe/zrender/blob/master/LICENSE.txt | 摸瓜V2引擎 |
| https://next.vuex.vuejs.org/ | 摸瓜V2引擎 |
| https://vuejs.org/images/icons/favicon-96x96.png | 摸瓜V2引擎 |
| https://mths.be/base64 | 摸瓜V2引擎 |
| https://vuejs.org/error-reference/ | 摸瓜V2引擎 |
| https://service.dcloud.net.cn/uniapp/feedback.html | 摸瓜V2引擎 |
| https://github.com/uuidjs/uuid | 摸瓜V2引擎 |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=$ | 摸瓜V2引擎 |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to= | 摸瓜V2引擎 |
| https://www.google.com/maps/?daddr= | 摸瓜V2引擎 |
| https://www.google.com/maps/ | 摸瓜V2引擎 |
| https://quilljs.com/ | 摸瓜V2引擎 |
| https://quilljs.com | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| https://github.com/ecomfe/zrender/blob/master/LICENSE.txt | 摸瓜V2引擎 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14222222222 | com/loc/n.java |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |
| 13012345666 | 摸瓜V2引擎 |

## **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=ZH, ST=CDS, L=CD, O=JSB, OU=WLH, CN=WL 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-10 07:53:34+00:00 有效期至: 2125-04-16 07:53:34+00:00 发行人: C=ZH, ST=CDS, L=CD, O=JSB, OU=WLH, CN=WL 序列号: 0x340d75bc 哈希算法: sha256 md5值: afdb576d3b5649d7912ab6d3c1dbdaba sha1值: 50a7974d8c08d5630dcf81b7eee2c04d7430c635 sha256值: 7d4ff8784ec773af2eedfc322ede047150f5d377a043ba4ee82eaad79e9fec76 sha512值: 8ce30898fcc8214878c6420579cce9b1ff47289f914fd426b4f0bcbdcc8429414b23fab9957289c56ed0f2d0e74a186fb56b80bd43648ed051835114a325bbc1 公钥算法: rsa 密钥长度: 2048 指纹: 52e4c57630d53d3429639c00335f23eefae084079c6b0e6855bad57b6363c026**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API" |
| "dcloud\_io\_without\_authorization" : "not authorized" |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service" |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed" |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out" |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained" |
| "dcloud\_oauth\_token\_failed" : "failed to get token" |
| "dcloud\_permissions\_reauthorization" : "reauthorize" |
| "dcloud\_tips\_certificate" : "certificate" |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问" |
| "dcloud\_io\_without\_authorization" : "没有获得授权" |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败" |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败" |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销" |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权" |
| "dcloud\_oauth\_token\_failed" : "获取token失败" |
| "dcloud\_permissions\_reauthorization" : "重新授权" |
| "dcloud\_tips\_certificate" : "证书" |

## **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.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\_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\_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.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\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_DOWNLOAD\_MANAGER | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_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 |

## **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。**