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

**狂神无双（ 24031816(841275.841413)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 | 狂神无双 |
| 版本 | 24031816(841275.841413) |
| 包名 | com.kswsfl.xianyu1 |
| 域名线索 | 34条 |
| URL线索 | 27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 | 狂神无双.apk |
| 文件大小 | 264.04MB |
| MD5值 | a4e10d6b6839760a14f366d402b6f748 |
| SHA1值 | b5288af59fb67bcc9cde67bb552a800a11786afe |
| SHA256值 | 7d6edb64c0287ba2cc41a639e8983c87fd16ed637847f58add6565e93466d9ac |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 狂神无双 |
| 包名 | com.kswsfl.xianyu1 |
| 主活动Activity | com.jhtools.sdk.JHToolsSplashActivity |
| 安卓版本名称 | 24031816(841275.841413) |
| 安卓版本 | 118768 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| mobilegw.aaa.alipay.net | 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  |
| m.alipay.com | IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mcgw.alipay.com | IP: 116.142.245.206 所属国家: China 地区: Beijing 城市: Beijing  |
| www.51wansy.sdkv3.com | 没有服务器地理信息.  |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mobilegw.alipay.com | IP: 203.209.250.8 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mta.oa.com | IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| wap.cmpassport.com | IP: 120.232.169.168 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| opencloud.wostore.cn | IP: 116.128.209.136 所属国家: China 地区: Beijing 城市: Beijing  |
| com.51wansy.cn | 没有服务器地理信息.  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |
| wappaygw.alipay.com | IP: 116.142.245.205 所属国家: China 地区: Beijing 城市: Beijing  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| nvs.im.tencent.cn | IP: 61.149.23.56 所属国家: China 地区: Beijing 城市: Beijing  |
| mclient.alipay.com | IP: 116.142.235.204 所属国家: China 地区: Beijing 城市: Beijing  |
| www.7749g.com | IP: 120.26.41.26 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.weixin.qq.com | IP: 140.207.191.167 所属国家: China 地区: Shanghai 城市: Shanghai  |
| 182.254.179.21 | IP: 182.254.179.21 所属国家: China 地区: Beijing 城市: Beijing  |
| wpd.b.qq.com | IP: 116.130.229.17 所属国家: China 地区: Beijing 城市: Beijing  |
| d.alipay.com | IP: 116.142.245.206 所属国家: China 地区: Beijing 城市: Beijing  |
| mobile.unionpay.com | 没有服务器地理信息.  |
| h5.m.taobao.com | IP: 221.194.162.215 所属国家: China 地区: Hebei 城市: Langfang  |
| mta.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| e.189.cn | IP: 42.123.76.65 所属国家: China 地区: Beijing 城市: Beijing  |
| oauth.baina.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| centermhtx.ios.shyouai.com | IP: 111.231.114.233 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  |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息.  |
| www.baidu.com | IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding  |
| pingma.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/sdk/cons/a.java  |
| https://mcgw.alipay.com/sdklog.do  | com/alipay/sdk/packet/impl/d.java  |
| https://h5.m.taobao.com/mlapp/olist.html  | com/alipay/sdk/data/a.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://wap.cmpassport.com/resources/html/contract.html  | com/cmic/sso/sdk/view/LoginAuthActivity.java  |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true  | com/cmic/sso/sdk/view/LoginAuthActivity.java  |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true  | com/cmic/sso/sdk/view/LoginAuthActivity.java  |
| https://github.com/mcxiaoke/packer-ng-plugin  | com/gzpublic/app/sdk/framework/PackerNg.java  |
| https://d.alipay.com  | com/gzpublic/app/sdk/framework/h5/PoolH5WebView.java  |
| https://www.7749g.com  | com/hn669/sysdk/ui/model/ActivityPageInfo.java  |
| https://www.baidu.com  | com/hn669/sysdk/ui/view/ExitAppDialog.java  |
| https://www.baidu.com  | com/hn669/sysdk/ui/fragment/ExitAppDialogFragment.java  |
| https://www.baidu.com  | com/hn669/sysdk/ui/fragment/AccountLoginFragment.java  |
| https://www.baidu.com  | com/hn669/sysdk/ui/fragment/PhoneLoginFragment.java  |
| https://www.baidu.com  | com/hn669/sysdk/ui/fragment/RegisterDialogFragment.java  |
| http://com.51wansy.cn/?tag=  | com/hn669/sysdk/ui/activity/WXH5PayActivity.java  |
| http://wpd.b.qq.com/page/webchat.html  | com/hn669/sysdk/ui/activity/FloatExtensionBarActivity.java  |
| http://www.51wansy.sdkv3.com/  | com/hn669/sysdk/ui/activity/FloatExtensionBarActivity.java  |
| https://oauth.baina.com/richinfo\_oauth\_interface/sdkInterface/v2/verifyMobile  | com/rich/oauth/core/RichAuth.java  |
| https://nvs.im.tencent.cn/v5/rapidauth/initialize?sdkappid=  | com/rich/oauth/core/RichAuth.java  |
| http://xml.apache.org/xslt  | com/rich/oauth/util/RichLogUtil.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://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://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  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.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://centermhtx.ios.shyouai.com:8004/log/change\_channel\_key  | com/xingchen/sdk/guangka/GuangKaSDK.java  |
| http://182.254.179.21:8001/certification/account\_info  | com/xingchen/sdk/guangka/GuangKaSDK.java  |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\  | com/unionpay/UPPayAssistEx.java  |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\  | com/unionpay/mobile/android/utils/c.java  |
| https://nvs.im.tencent.cn/v5/rapidauth/querytoken?sdkappid=  | rich/w0.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 3@9il2cpp.usym  | lib/arm64-v8a/libil2cpp.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13800138000  | com/rich/oauth/util/MD5Utils.java  |
| 15060355040  | com/unionpay/UPPayAssistEx.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=中国/China, ST=湖南省, L=长沙市, O=手游开发部, OU=湖南六六九互动娱乐有限公司, CN=Jenkins 签名算法: rsassa\_pkcs1v15 有效期自: 2017-07-26 03:59:53+00:00 有效期至: 2117-07-02 03:59:53+00:00 发行人: C=中国/China, ST=湖南省, L=长沙市, O=手游开发部, OU=湖南六六九互动娱乐有限公司, CN=Jenkins 序列号: 0x1da30c5e 哈希算法: sha256 md5值: 4af7a258e7078d53ddcb7f0094bba030 sha1值: 0f86b05d249d2adaf455009c368608b767121f1b sha256值: e70768bc92d44caa04a6a11ba94a5c67510b3e1a1564bfd7a81464406a77b289 sha512值: 09c4d358308dca8c8d60d1d5576619f977850595cbb0a9ffc94496ac977681babba22336138b226c1bd47985de181a8eb96151c57e43812453f1f860c529b534 公钥算法: rsa 密钥长度: 2048 指纹: 60d1636d767a4ff0c122cf0b3aab6fceb9927f501030c802934552bf2224e9ea**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "cucc\_oauth\_login" : "一键登录"  |
| "cucc\_oauth\_title" : "免密登录"  |
| "hnssn\_bind\_realname\_authentication" : "实名认证"  |
| "oauth" : "认证"  |
| "oauth\_login" : "一键登录"  |
| "oauth\_title" : "免密登录"  |
| "umcsdk\_oauth\_version\_name" : "v1.4.1"  |

## **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\_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 |
| 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.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.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.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.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.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.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.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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.ACCESS\_DOWNLOAD\_MANAGER | 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.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**