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

**撸包小能手（ 2.9.0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 | 撸包小能手 |
| 版本 | 2.9.0 |
| 包名 | com.xhxy.hid |
| 域名线索 | 15条 |
| URL线索 | 21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 | base(1).apk |
| 文件大小 | 96.25MB |
| MD5值 | 307282bf320dc8155d28d403740cf725 |
| SHA1值 | d46390c70c19d5735b67200776d891bff8a22be0 |
| SHA256值 | c849fc361bfb4127e8e839b8f31d75bb86bf4998244aae1f5425e94f93b03c55 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 撸包小能手 |
| 包名 | com.xhxy.hid |
| 主活动Activity | com.main.app.SplashActivity |
| 安卓版本名称 | 2.9.0 |
| 安卓版本 | 290 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| aip.baidubce.com | IP: 111.206.210.12  所属国家: China  地区: Beijing  城市: Beijing |
| tbs.imtt.qq.com | IP: 61.54.94.120  所属国家: China  地区: Henan  城市: Luoyang |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| cfg.imtt.qq.com | IP: 60.28.172.238  所属国家: China  地区: Tianjin  城市: Tianjin |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| ieeexplore.ieee.org | IP: 108.139.10.8  所属国家: United States of America  地区: California  城市: San Francisco |
| bugs.llvm.org | IP: 54.67.122.174  所属国家: United States of America  地区: California  城市: San Jose |
| pms.mb.qq.com | IP: 60.28.172.238  所属国家: China  地区: Tianjin  城市: Tianjin |
| schemas.android.com | 没有服务器地理信息. |
| openmp.llvm.org | IP: 54.67.122.174  所属国家: United States of America  地区: California  城市: San Jose |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| log.tbs.qq.com | IP: 124.95.224.248  所属国家: China  地区: Liaoning  城市: Shenyang |
| www.slf4j.org | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| mdc.html5.qq.com | IP: 116.130.223.178  所属国家: China  地区: Beijing  城市: Beijing |
| www.openssl.org | IP: 34.49.79.89  所属国家: United States of America  地区: California  城市: Mountain View |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| https://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/k.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079 | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/o.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/o.java |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs | com/tencent/smtt/utils/d.java |
| http://schemas.android.com/apk/res/android | ILil/p020IiL/p027lLi1LL/I1I/IiL.java |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection | p043lLi1LL/I1I/IL1Iii.java |
| http://www.slf4j.org/codes.html | p043lLi1LL/p052IL/I1I.java |
| http://aip.baidubce.com/oauth/2.0/token?grant\_type=client\_credentials&client\_id= | lib/arm64-v8a/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/general\_basic?access\_token= | lib/arm64-v8a/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate?access\_token= | lib/arm64-v8a/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate\_basic?access\_token= | lib/arm64-v8a/libengine.so |
| https://www.openssl.org/docs/faq.html | lib/arm64-v8a/libengine.so |
| http://openmp.llvm.org/ | lib/arm64-v8a/libncnn.so |
| https://bugs.llvm.org/. | lib/arm64-v8a/libncnn.so |
| https://ieeexplore.ieee.org/document/1163711 | lib/arm64-v8a/libonnxruntime.so |
| https://github.com/opencv/opencv/issues/16739 | lib/arm64-v8a/libopencv\_java4.so |
| https://github.com/opencv/opencv/issues/5412. | lib/arm64-v8a/libopencv\_java4.so |
| https://github.com/opencv/opencv/issues/19634 | lib/arm64-v8a/libopencv\_java4.so |
| http://aip.baidubce.com/oauth/2.0/token?grant\_type=client\_credentials&client\_id= | lib/armeabi-v7a/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/general\_basic?access\_token= | lib/armeabi-v7a/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate?access\_token= | lib/armeabi-v7a/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate\_basic?access\_token= | lib/armeabi-v7a/libengine.so |
| https://www.openssl.org/docs/faq.html | lib/armeabi-v7a/libengine.so |
| http://openmp.llvm.org/ | lib/armeabi-v7a/libncnn.so |
| https://bugs.llvm.org/. | lib/armeabi-v7a/libncnn.so |
| https://ieeexplore.ieee.org/document/1163711 | lib/armeabi-v7a/libonnxruntime.so |
| https://github.com/opencv/opencv/issues/16739 | lib/armeabi-v7a/libopencv\_java4.so |
| https://github.com/opencv/opencv/issues/5412. | lib/armeabi-v7a/libopencv\_java4.so |
| https://github.com/opencv/opencv/issues/19634 | lib/armeabi-v7a/libopencv\_java4.so |
| http://aip.baidubce.com/oauth/2.0/token?grant\_type=client\_credentials&client\_id= | lib/x86/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/general\_basic?access\_token= | lib/x86/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate?access\_token= | lib/x86/libengine.so |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate\_basic?access\_token= | lib/x86/libengine.so |
| https://www.openssl.org/docs/faq.html | lib/x86/libengine.so |
| http://openmp.llvm.org/ | lib/x86/libncnn.so |
| https://bugs.llvm.org/. | lib/x86/libncnn.so |
| https://ieeexplore.ieee.org/document/1163711 | lib/x86/libonnxruntime.so |
| https://github.com/opencv/opencv/issues/16739 | lib/x86/libopencv\_java4.so |
| https://github.com/opencv/opencv/issues/5412. | lib/x86/libopencv\_java4.so |
| https://github.com/opencv/opencv/issues/19634 | lib/x86/libopencv\_java4.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| javamail@sun.com | com/sun/mail/imap/IMAPFolder.java |
| x5tbs@tencent.com | com/tencent/smtt/sdk/X5Downloader.java |
| ftp@example.com | lib/arm64-v8a/libengine.so |
| yay@y.u5vcghyy  6h@fo.lwft  w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh | lib/arm64-v8a/libocrapi.so |
| yay@y.u5vcghyy  6h@fo.lwft  w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh | lib/arm64-v8a/libtscolor.so |
| ftp@example.com | lib/armeabi-v7a/libengine.so |
| yay@y.u5vcghyy  6h@fo.lwft  w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh | lib/armeabi-v7a/libocrapi.so |
| yay@y.u5vcghyy  6h@fo.lwft  w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh | lib/armeabi-v7a/libtscolor.so |
| ftp@example.com | lib/x86/libengine.so |
| yay@y.u5vcghyy  6h@fo.lwft  w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh | lib/x86/libocrapi.so |
| yay@y.u5vcghyy  6h@fo.lwft  w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh | lib/x86/libtscolor.so |

### **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=lrzs, ST=lrzs, L=lrzs, O=lrzs, OU=lrzs, CN=lrzs 签名算法: rsassa\_pkcs1v15 有效期自: 2020-06-22 13:26:11+00:00 有效期至: 2045-06-16 13:26:11+00:00 发行人: C=lrzs, ST=lrzs, L=lrzs, O=lrzs, OU=lrzs, CN=lrzs 序列号: 0x49bc92d8 哈希算法: sha256 md5值: dc24d846f032dd4047be3c280cf50c5b sha1值: 5f93b225b66b775a13aa44afb93e94586b1ed310 sha256值: 9fb2fd402397312752fee5f7c08b5d65c7bbad437287a3e8236bd83c06ed2ecc sha512值: c746a52cc9aaecf0ac0ca4d0ec68335abda81ae33afb3cb2eee2a012b130a0d3625e5bc45376eaf576243cb56864c1399863369ab29937df417300252d57df41 公钥算法: rsa 密钥长度: 2048 指纹: 612558d92f6a6cf766c013f3ad0a5510988d9c65d9707c7d9e105c622fcc78f8**

## **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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 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.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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 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.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.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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收 | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| android.permission.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.SEND\_SMS | 危险 | 发送短信 | 允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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\_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.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\_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.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\_UPDATES | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.WRITE\_INTERNAL\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_INTERNAL\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_USER\_DICTIONARY | 危险 | 读取用户定义词典 | 允许应用程序读取用户可能存储在用户字典中的任何私人单词,名称和短语 |
| android.permission.ACCESS\_MTK\_MMHW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SAMSUNG\_TUNTAP | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.ACCESS\_SUPERUSER | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 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。**