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

**松鼠加速器（ 1.4.31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 | 松鼠加速器 |
| 版本 | 1.4.31 |
| 包名 | com.sg.netProxy |
| 域名线索 | 45条 |
| URL线索 | 38条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | com.sg.netProxy.apk |
| 文件大小 | 48.43MB |
| MD5值 | 63d9184c01b844e418e4c7f30b183584 |
| SHA1值 | caee01936cee8968190c090591e256d4368ef680 |
| SHA256值 | d3a6a793352b2e5b716c6dd174c000aef416be06fcceab9eeda635342fd3e0b6 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 松鼠加速器 |
| 包名 | com.sg.netProxy |
| 主活动Activity | com.sg.netProxy.MainActivity |
| 安卓版本名称 | 1.4.31 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.ip.sgxz.cn | IP: 61.48.83.227 所属国家: China 地区: Beijing 城市: Beijing  |
| apis.map.qq.com | IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing  |
| 47.96.175.103 | IP: 47.96.175.103 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| quilljs.com | IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.ys.sgxz.cn | 没有服务器地理信息.  |
| qm.qq.com | IP: 125.39.104.69 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ys.sgxz.cn | 没有服务器地理信息.  |
| uniapp.dcloud.net.cn | IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin  |
| eco.taobao.com | IP: 59.82.120.12 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 192.168.10.66 | IP: 192.168.10.66 所属国家: - 地区: - 城市: -  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| itunes.apple.com | IP: 116.179.52.16 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| accel.sgxz.cn | IP: 111.202.5.198 所属国家: China 地区: Beijing 城市: Beijing  |
| verify.cmpassport.com | IP: 112.33.110.6 所属国家: China 地区: Anhui 城市: Hefei  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| api-e189.21cn.com | IP: 222.93.106.185 所属国家: China 地区: Jiangsu 城市: Suzhou  |
| 10.0.0.21 | IP: 10.0.0.21 所属国家: - 地区: - 城市: -  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| api.next.bspapp.com | IP: 203.107.60.33 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 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  |
| ask.dcloud.net.cn | IP: 124.163.195.89 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| opencloud.wostore.cn | IP: 116.128.209.136 所属国家: China 地区: Beijing 城市: Beijing  |
| nisportal.10010.com | IP: 124.64.196.20 所属国家: China 地区: Beijing 城市: Beijing  |
| service.dcloud.net.cn | IP: 110.40.181.119 所属国家: China 地区: Beijing 城市: Beijing  |
| id6.me | IP: 42.123.76.150 所属国家: China 地区: Beijing 城市: Beijing  |
| e.189.cn | IP: 42.123.76.65 所属国家: China 地区: Beijing 城市: Beijing  |
| msv6.wosms.cn | IP: 124.64.196.35 所属国家: China 地区: Beijing 城市: Beijing  |
| www.google.com | IP: 199.59.148.20 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| 96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com | 没有服务器地理信息.  |
| open.weixin.qq.com | IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai  |
| h.trace.qq.com | IP: 113.56.189.162 所属国家: China 地区: Hubei 城市: Huangshi  |
| tongji.dcloud.io | IP: 124.221.250.97 所属国家: China 地区: Beijing 城市: Beijing  |
| m3w.cn | IP: 123.6.25.115 所属国家: China 地区: Henan 城市: Zhengzhou  |
| wap.cmpassport.com | IP: 120.232.169.168 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| api.bspapp.com | IP: 39.96.249.142 所属国家: China 地区: Beijing 城市: Beijing  |
| android.bugly.qq.com | IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang  |
| dypnsapi.aliyuncs.com | IP: 106.11.45.35 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| stream.dcloud.net.cn | IP: 115.159.41.92 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.android.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  |
| stream.mobihtml5.com | 没有服务器地理信息.  |
| ip.sgxz.cn | IP: 61.48.83.230 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://wap.cmpassport.com/resources/html/contract.html  | com/cmic/sso/sdk/view/LoginAuthActivity.java  |
| https://eco.taobao.com/router/rest  | com/mobile/auth/BuildConfig.java  |
| https://wap.cmpassport.com/resources/html/contract.html  | com/mobile/auth/gatewayauth/Constant.java  |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true  | com/mobile/auth/gatewayauth/Constant.java  |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true  | com/mobile/auth/gatewayauth/Constant.java  |
| https://msv6.wosms.cn/html/oauth/protocol2.html  | com/mobile/auth/gatewayauth/Constant.java  |
| https://dypnsapi.aliyuncs.com/?  | com/mobile/auth/gatewayauth/detectnet/e.java  |
| https://dypnsapi.aliyuncs.com/?  | com/mobile/auth/gatewayauth/network/TopRequestUtils.java  |
| https://dypnsapi.aliyuncs.com/?  | com/mobile/auth/gatewayauth/network/RequestUtil.java  |
| https://id6.me/auth/preauth.do  | com/mobile/auth/d/a.java  |
| https://api-e189.21cn.com/gw/client/accountMsg.do  | com/mobile/auth/c/d.java  |
| https://verify.cmpassport.com/h5/getMobile  | com/nirvana/tools/logger/UaidTracker.java  |
| https://nisportal.10010.com:9001/api  | com/nirvana/tools/logger/UaidTracker.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/ad.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/proguard/ac.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  |
| http://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://stream.mobihtml5.com/  | io/dcloud/common/constant/StringConst.java  |
| https://stream.dcloud.net.cn/  | io/dcloud/common/constant/StringConst.java  |
| http://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| http://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://ask.dcloud.net.cn/article/35627  | io/dcloud/f/b/a.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/f/b/a.java  |
| https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=  | io/dcloud/f/c/h/b.java  |
| http://ask.dcloud.net.cn/article/283  | io/dcloud/h/b.java  |
| http://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  |
| 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  |
| https://qm.qq.com/cgi-bin/qm/qr?k=  | 摸瓜V2引擎  |
| https://tongji.dcloud.io/uni/stat  | 摸瓜V2引擎  |
| https://tongji.dcloud.io/uni/stat.gif?  | 摸瓜V2引擎  |
| https://itunes.apple.com/lookup?bundleId=com.sg.netProxy  | 摸瓜V2引擎  |
| https://ip.sgxz.cn/doc/law.html  | 摸瓜V2引擎  |
| https://ip.sgxz.cn/doc/web.html  | 摸瓜V2引擎  |
| http://10.0.0.21:8090/\_\_UNI\_\_6D45942.wgt  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://feross.org/opensource>  | 摸瓜V2引擎  |
| https://ys.sgxz.cn/android/  | 摸瓜V2引擎  |
| https://api.ys.sgxz.cn:90  | 摸瓜V2引擎  |
| http://192.168.10.66:8086  | 摸瓜V2引擎  |
| http://47.96.175.103:8081  | 摸瓜V2引擎  |
| https://api.ip.sgxz.cn  | 摸瓜V2引擎  |
| https://ip.sgxz.cn/  | 摸瓜V2引擎  |
| https://api.next.bspapp.com  | 摸瓜V2引擎  |
| https://api.bspapp.com  | 摸瓜V2引擎  |
| https://uniapp.dcloud.net.cn/uniCloud/secure-network.html  | 摸瓜V2引擎  |
| https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| https://ip.sgxz.cn  | 摸瓜V2引擎  |
| https://accel.sgxz.cn  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| oadsdyoavxtqibmkfw@hh5begljvj\_.nk0rsx2t7f jhruby.web@gmail.com  | 摸瓜V2引擎  |

### **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: False 找到 1 个唯一证书 主题: CN=sg 签名算法: rsassa\_pkcs1v15 有效期自: 2023-11-22 06:08:05+00:00 有效期至: 2048-11-15 06:08:05+00:00 发行人: CN=sg 序列号: 0x81afc3 哈希算法: sha256 md5值: 78f0f1b125efa75f19412a6c023d9a9c sha1值: b7c777ab04f1f2c113c1e87c6a0f7e4b90280017 sha256值: ea78d20643541819237d5f659cbd22e3d68e202f5abce8b61a6cfc1357b1e74f sha512值: fb33d1148c23e1e7ca18e7dfaabb7cc1b8f6c67f100f124cc4197ac80c452a289fa6daa220651ef73b736bbfa2a1a6f0ffe93496c0cb587dbe300834e5ab9f0b 公钥算法: rsa 密钥长度: 2048 指纹: 13634ed191f8602ad6829295401297916b85f04ea32449e61b0523b825849b82**

## **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\_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"  |

## **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.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.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\_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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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 |
| getui.permission.GetuiService.com.sg.netProxy | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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 |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntryActivity | **Schemes**: ://,  |

**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。**