MoGua

松鼠加速器 1.4.31.APK 分析报告

APP名称:	松鼠加速器

包名:	com.sg.netProxy
域名线索:	45条
URL线索:	38条
邮箱线索:	1条
分析日期:	2025年7月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.sg.netProxy.apk
文件大小: 48.43MB
MD5值: 63d9184c01b844e418e4c7f30b183584
SHA1值: caee01936cee8968190c090591e256d4368ef680
SHA256值: d3a6a793352b2e5b716c6dd174c000aef416be06fcceab9eeda635342fd3e0b6

APP 信息

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

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 **纬度**: 39.907501 **经度**: 116.397102
apis.map.qq.com	**IP**: 116.130.224.140 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 47.96.175.103 **所属国家**: China **地区**: Zhejiang

47.96.175.103	**城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
quilljs.com	**IP**: 172.66.40.163 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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 **纬度**: 39.142181 **经度**: 117.176102
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 **纬度**: 39.142181 **经度**: 117.176102
eco.taobao.com	**IP**: 59.82.120.12 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 192.168.10.66 **所属国家**: -

192.168.10.66	**地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
itunes.apple.com	**IP**: 116.179.52.16 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
accel.sgxz.cn	**IP**: 111.202.5.198 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
verify.cmpassport.com	**IP**: 112.33.110.6 **所属国家**: China **地区**: Anhui **城市**: Hefei **纬度**: 31.863815 **经度**: 117.280830
feross.org	**IP**: 50.116.11.184 **所属国家**: United States of America **地区**: California **城市**: Fremont **纬度**: 37.548271 **经度**: -121.988571

api-e189.21cn.com	**IP**: 222.93.106.185 **所属国家**: China **地区**: Jiangsu **城市**: Suzhou **纬度**: 31.311365 **经度**: 120.617691
10.0.0.21	**IP**: 10.0.0.21 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
long.open.weixin.qq.com	**IP**: 112.65.193.150 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
api.next.bspapp.com	**IP**: 203.107.60.33 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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 **纬度**: 37.775700 **经度**: -122.395203
	IP: 124.163.195.89

ask.dcloud.net.cn	**所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
opencloud.wostore.cn	**IP**: 116.128.209.136 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
nisportal.10010.com	**IP**: 124.64.196.20 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
service.dcloud.net.cn	**IP**: 110.40.181.119 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
id6.me	**IP**: 42.123.76.150 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
e.189.cn	**IP**: 42.123.76.65 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

msv6.wosms.cn	**IP**: 124.64.196.35 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.google.com	**IP**: 199.59.148.20 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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 **纬度**: 31.224333 **经度**: 121.468948
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
	IP: 124.221.250.97

tongji.dcloud.io	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
m3w.cn	**IP**: 123.6.25.115 **所属国家**: China **地区**: Henan **城市**: Zhengzhou **纬度**: 34.757778 **经度**: 113.648613
wap.cmpassport.com	**IP**: 120.232.169.168 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
api.bspapp.com	**IP**: 39.96.249.142 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
android.bugly.qq.com	**IP**: 124.95.225.146 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
dypnsapi.aliyuncs.com	**IP**: 106.11.45.35 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

astat.bugly.qcloud.com	**IP**: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
stream.dcloud.net.cn	**IP**: 115.159.41.92 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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 **纬度**: 37.774929 **经度**: -122.419418
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 **纬度**: 39.907501 **经度**: 116.397102

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

邮箱线索

邮箱地址	所在文件
oadsdyoavxtqibmkfw@hh5begljvj_.nk0rsx2t7f jhruby.web@gmail.com	摸瓜V2引擎

手机线索

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

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"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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
		精细定位	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

android.permission.ACCESS_FINE_LOCATION	危险	（GPS）	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

应用内通信

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