MoGua

护线通 2.0.6.APK 分析报告

APP名称:	护线通

包名:	com.csg.szdwgd.hxt
域名线索:	22条
URL线索:	7条
邮箱线索:	0条
分析日期:	2025年5月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: hxt206.apk
文件大小: 58.6MB
MD5值: 2f6b67784ce4fc6a971c53fd618253db
SHA1值: fbeb2b69f64b592d07bd6ae7101772c797439e2b
SHA256值: e626934c1da7f16af92915615abef1f1138ef67d86443d2b6134b1d93efa31e2

APP 信息

App名称: 护线通
包名: com.csg.szdwgd.hxt
主活动Activity: com.comtop.map.poros.MainActivity
安卓版本名称: 2.0.6
安卓版本: 206

域名线索

域名	服务器信息
store-at-dre.hispace.dbankcloud.com	没有服务器地理信息.
data-dra.push.dbankcloud.com	**IP**: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
store2.hispace.hicloud.com	**IP**: 18.65.168.75 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

store3.hispace.hicloud.com	**IP**: 96.17.70.43 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
grs.dbankcloud.cn	**IP**: 121.36.116.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.dbankcloud.asia	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
store1.hispace.hicloud.com	**IP**: 123.249.62.130 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
play.google.com	**IP**: 142.251.42.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
store-drru.hispace.hicloud.com	**IP**: 159.138.202.186 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498

	经度: 60.612499
grs.dbankcloud.com	**IP**: 113.201.107.54 **所属国家**: China **地区**: Shaanxi **城市**: Baoji **纬度**: 34.353611 **经度**: 107.375275
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
grs.dbankcloud.eu	没有服务器地理信息.
store.hispace.hicloud.com	**IP**: 123.249.62.130 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics.dt.dbankcloud.ru	**IP**: 159.138.204.140 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
data-drcn.push.dbankcloud.com	**IP**: 118.194.33.160 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948

appgallery.cloud.huawei.com	**IP**: 49.4.35.16 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics2.data.hicloud.com	**IP**: 80.158.2.190 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
metrics1.data.hicloud.com	**IP**: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
metrics-dra.dt.hicloud.com	**IP**: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.platform.dbankcloud.ru	没有服务器地理信息.
data-drru.push.dbankcloud.com	**IP**: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
	IP: 159.138.203.215 **所属国家**: Russian Federation

metrics5.data.hicloud.com	**地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499

URL线索

URL信息	Url所在文件
https://play.google.com/store/apps/details?id=	Mogua Engine V1
https://appgallery.cloud.huawei.com	Mogua Engine V1
https://store.hispace.hicloud.com/hwmarket/api/	Mogua Engine V1
https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/	Mogua Engine V2
https://metrics1.data.hicloud.com:6447	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2
https://metrics5.data.hicloud.com:6447	Mogua Engine V2
https://metrics.dt.dbankcloud.ru	Mogua Engine V2
https://data-drcn.push.dbankcloud.com	Mogua Engine V2
https://data-dra.push.dbankcloud.com	Mogua Engine V2
https://data-dre.push.dbankcloud.com	Mogua Engine V2
https://data-drru.push.dbankcloud.com	Mogua Engine V2

https://metrics1.data.hicloud.com:6447	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2
https://metrics2.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.data.hicloud.com:6447	Mogua Engine V2
https://store1.hispace.hicloud.com/hwmarket/api/	Mogua Engine V2
https://store2.hispace.hicloud.com/hwmarket/api/	Mogua Engine V2
https://store3.hispace.hicloud.com/hwmarket/api/	Mogua Engine V2
https://store-drru.hispace.hicloud.com/hwmarket/api/	Mogua Engine V2
https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2
https://grs.platform.dbankcloud.ru	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2

邮箱线索

手机线索

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=CN, O=yourcomname, OU=IT, CN=yourcomname
签名算法: rsassa_pkcs1v15
有效期自: 2022-10-27 08:19:21+00:00
有效期至: 2122-10-03 08:19:21+00:00
发行人: C=CN, O=yourcomname, OU=IT, CN=yourcomname
序列号: 0x1e7208bd
哈希算法: sha256
md5值: 95b20d530e73b7a9a51971b895b1a828
sha1值: 3cc707871d210e4cd00c37e86f59eeaa3f4cca60
sha256值: dd46604d8921dbc36364f9dc8f0411c6a89af605656237caa985ceb6b43b72ce
sha512值: 765ecf1a4cc2d05140cca363c4b9942f567c8782408e13489bc969c9056d1faf19f6672c85cd63131c1bb6230c5859496387eb40a95d34e09b0cfbc5f1950f0e
公钥算法: rsa
密钥长度: 2048
指纹: 294912d9df8665e8dc1dae318916841a8f5a6f0811a2f17baf9c8a8979e21348

🔑 硬编码敏感信息

可能的敏感信息
"jiguang_privates_channel_high" : "HIGH"
"jiguang_privates_channel_low" : "LOW"
"jiguang_privates_channel_normal" : "NORMAL"
"jssdk_input_login_safety_pwd" : "请输入登录密码"
"jssdk_input_pwd" : "请输入密码"
"jssdk_input_safety_pwd" : "请输入安全密码"
"[illegible]" : "重置"

"jiguang_privates_channel_high" : "重要"
"jiguang_privates_channel_low" : "不重要"
"jiguang_privates_channel_normal" : "普通"

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_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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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
ohos.permission.DISTRIBUTED_DATASYNC	未知	Unknown permission	Unknown permission from android reference
ohos.permission.GET_DISTRIBUTED_DEVICE_INFO	未知	Unknown permission	Unknown permission from android reference
ohos.permission.GET_BUNDLE_INFO	未知	Unknown permission	Unknown permission from android reference
ohos.permission.SYSTEM_FLOAT_WINDOW	未知	Unknown permission	Unknown permission from android reference
ohos.permission.DISTRIBUTED_DEVICE_STATE_CHANGE	未知	Unknown permission	Unknown permission from android reference
	未	Unknown	

ohos.permission.DISTRIBUTED_SCHEDULER_REMOTE_SERVICE	知	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.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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
com.comtop.store.app.permission.RECEIVE_SSO_TOKEN	未知	Unknown permission	Unknown permission from android reference
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.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
android.permission.NFC_TRANSACTION_EVENT	正常		允许应用程序接收 NFC 交易事件
	危	后台访问位	

android.permission.ACCESS_BACKGROUND_LOCATION	险	置	允许应用程序在后台访问位置
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
com.csg.szdwgd.hxt.permission.XPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.csg.szdwgd.hxt.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.csg.szdwgd.hxt.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知	在 htc 手机的应用程序启动图标上显示通知计数或徽章。

		计数	
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
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.huawei.android.launcher.permission.READ_SETTINGS	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.huawei.android.launcher.permission.WRITE_SETTINGS	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
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章

com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
com.csg.szdwgd.hxt.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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。
com.vivo.notification.permission.BADGE_ICON	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.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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.push.permission.UPSTAGESERVICE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
com.csg.szdwgd.hxt.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.comtop.map.porosandroidlib.poros.AcceptThirdAppDataActivity	Schemes: poros://, Hosts: com.csg.szdwgd.hxt,

---