



MoGua

Nomad VPN 4.0.8 (426).APK 分析报告



APP名称:

Nomad VPN

包名:	com.rg.nomadvpn
域名线索:	55条
URL线索:	24条
邮箱线索:	5条
分析日期:	2025年6月5日
分析平台:	摸瓜APK反编译平台

文件名: Nomad VPN Pro v4.0.8.apk
文件大小: 11.92MB
MD5值: cdb43dae190a717806b663abb0266fcd
SHA1值: bf419a825b6a1187a3808946ad2dd0ab7167a7b3
SHA256值: 71f01e5fca58a192adae714f34b82d314b13d2c968c2a3dd6d4336aee50695b2

i APP 信息

App名称: Nomad VPN
包名: com.rg.nomadvpn
主活动Activity: com.rg.nomadvpn.MainActivity
安卓版本名称: 4.0.8 (426)
安卓版本: 426

🔍 域名线索

域名	服务器信息
openvpn.net	IP: 197.4.4.12 所属国家: Tunisia 地区: Jendouba 城市: Tabarka 纬度: 36.954418 经度: 8.758010
ns.adobe.com	没有服务器地理信息.
play.google.com	IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe 纬度: 32.548328 经度: -92.045235
	IP: 95.164.118.41

estonia2.nomad.twc1.net	所属国家: United States of America 地区: New Jersey 城市: Hackensack 纬度: 40.887573 经度: -74.049881
germany2.nomad.twc1.net	IP: 5.182.87.46 所属国家: Russian Federation 地区: Moskovskaya oblast' 城市: Dmitrov 纬度: 56.349998 经度: 37.516670
hongkong2.nomad.twc1.net	IP: 213.159.70.33 所属国家: Russian Federation 地区: Sankt-Peterburg 城市: Saint Petersburg 纬度: 59.894440 经度: 30.264200
canada2.nomad.twc1.net	没有服务器地理信息.
usa2.nomad.twc1.net	IP: 138.124.60.58 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
goo.gl	IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
moldova2.nomad.twc1.net	没有服务器地理信息.
	IP: 77.239.101.184

austria2.nomad.twc1.net	所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Telford 纬度: 52.676590 经度: -2.449260
leakcheck.io	IP: 104.26.15.183 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
lithuania2.nomad.twc1.net	IP: 45.12.136.178 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
nomadvpn.ru	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
finland2.nomad.twc1.net	IP: 91.184.243.35 所属国家: Poland 地区: - 城市: - 纬度: 52.229771 经度: 21.011780
greece2.nomad.twc1.net	没有服务器地理信息.
community.openvpn.net	IP: 49.2.123.56 所属国家: Australia 地区: New South Wales 城市: Macquarie Park

	纬度: -33.781216 经度: 151.127838
poland2.nomad.twc1.net	IP: 94.131.96.210 所属国家: Poland 地区: Mazowieckie 城市: Warsaw 纬度: 52.229771 经度: 21.011780
sweden2.nomad.twc1.net	IP: 77.239.120.24 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Telford 纬度: 52.676590 经度: -2.449260
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
10.0.2.2	IP: 10.0.2.2 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
belgium2.nomad.twc1.net	IP: 95.164.62.169 所属国家: Belgium 地区: Brussels Hoofdstedelijk Gewest 城市: Brussels 纬度: 50.850849 经度: 4.348780
	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland

t.me	地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
schemas.android.com	没有服务器地理信息.
issuetracker.google.com	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
japan2.nomad.twc1.net	IP: 45.12.134.63 所属国家: United States of America 地区: Colorado 城市: Denver 纬度: 39.739361 经度: -104.983597
italy2.nomad.twc1.net	没有服务器地理信息.
schemas.microsoft.com	IP: 13.107.253.49 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
xposed.info	IP: 45.55.233.97 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
kazakhstan2.nomad.twc1.net	没有服务器地理信息.

denmark2.nomad.twc1.net	IP: 95.164.85.46 所属国家: Denmark 地区: Hovedstaden 城市: Copenhagen 纬度: 55.675941 经度: 12.565530
france2.nomad.twc1.net	IP: 46.226.166.105 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
mobile.yandexadexchange.net	IP: 213.180.193.198 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
exoplayer.dev	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
spain2.nomad.twc1.net	IP: 176.120.74.137 所属国家: Russian Federation 地区: Permskiy kray 城市: Vavilova 纬度: 58.716671 经度: 55.599998
czechia2.nomad.twc1.net	IP: 45.12.109.76 所属国家: United States of America 地区: California 城市: Los Angeles

	纬度: 34.052570 经度: -118.243904
romania2.nomad.twc1.net	没有服务器地理信息.
armenia2.nomad.twc1.net	IP: 91.132.132.31 所属国家: Greece 地区: Attiki 城市: Athens 纬度: 37.979450 经度: 23.716246
latvia2.nomad.twc1.net	IP: 45.142.213.224 所属国家: Latvia 地区: Riga 城市: Riga 纬度: 56.945999 经度: 24.105890
turkey2.nomad.twc1.net	IP: 45.89.52.95 所属国家: Turkey 地区: Izmir 城市: Izmir 纬度: 38.412731 经度: 27.138380
balancer.nomad.twc1.net	IP: 188.225.79.143 所属国家: Russian Federation 地区: Sankt-Peterburg 城市: Saint Petersburg 纬度: 59.894440 经度: 30.264200
appmetrica.io	IP: 213.180.204.242 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471

android.googlesource.com	IP: 142.251.188.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
greatbritain2.nomad.twc1.net	没有服务器地理信息.
brazil2.nomad.twc1.net	IP: 45.82.245.62 所属国家: United States of America 地区: Ohio 城市: Delaware 纬度: 40.298775 经度: -83.067764
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
hungary2.nomad.twc1.net	没有服务器地理信息.
switzerland2.nomad.twc1.net	没有服务器地理信息.
netherlands2.nomad.twc1.net	IP: 176.124.203.13 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
	IP: 104.18.23.19 所属国家: United States of America 地区: California

www.w3.org	城市: San Francisco 纬度: 37.775700 经度: -122.395203
repo.xposed.info	IP: 45.55.233.97 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
crowdin.net	IP: 44.215.191.137 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
yandex.ru	IP: 5.255.255.77 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
norway2.nomad.twc1.net	IP: 77.239.113.40 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Brierley Hill 纬度: 52.481731 经度: -2.121390
xmlpull.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724

URL线索

URL信息	Url所在文件
http://xml.org/sax/features/external-general-entities	M1/N0.java
http://xml.org/sax/features/external-parameter-entities	M1/N0.java
http://xml.org/sax/properties/lexical-handler	M1/N0.java
http://xmllpull.org/v1/doc/features.html	M1/N0.java
http://schemas.android.com/apk/res/android	G5/u.java
http://schemas.android.com/apk/res/android	R0/o.java
http://schemas.android.com/apk/res/android	J/b.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	Y/o.java
https://play.google.com/store/apps/details?id=com.rg.nomadvpn	com/rg/nomadvpn/ui/rating/RatingFragment.java
http://10.0.2.2:8081/api/anr?token=	com/rg/nomadvpn/ui/leak/LeakFragment.java
https://leakcheck.io/api/v2/query/	com/rg/nomadvpn/ui/leak/LeakFragment.java
https://play.google.com/store/apps/details?id=com.rg.nomadvpn	com/rg/nomadvpn/ui/share/ShareFragment.java
https://t.me/nomadvpn	com/rg/nomadvpn/ui/telegram/TelegramFragment.java
https://balancer.nomad.twc1.net/api/bandwidth?token=	com/rg/nomadvpn/service/StatsRunnable.java
https://exoplayer.dev/issues/cleartext-not-permitted	com/yandex/mobile/ads/impl/qh0.java

http://xmlpull.org/v1/doc/features.html	com/yandex/mobile/ads/impl/ua2.java
http://xmlpull.org/v1/doc/features.html	com/yandex/mobile/ads/impl/mi2.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	com/yandex/mobile/ads/impl/zh0.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	com/yandex/mobile/ads/impl/r60.java
https://x</LA_URL>	com/yandex/mobile/ads/impl/sc0.java
https://x	com/yandex/mobile/ads/impl/sc0.java
http://ns.adobe.com/xap/1.0/	com/yandex/mobile/ads/impl/sq0.java
https://appmetrica.io/docs/mobile-sdk-dg/android/about/android-initialize.html	io/appmetrica/analytics/impl/C3029b0.java
http://ns.adobe.com/xap/1.0/\u0000	f0/g.java
https://goo.gl/J1sWQy	n2/r.java
https://nomadvpn.ru/nomadvpn/privacy/privacy_policy.html>read. 	摸瓜V1引擎
https://github.com/schwabe/ics-openvpn/issues/18>Issue	摸瓜V1引擎
https://github.com/schwabe/ics-openvpn/issues/29>Issue	摸瓜V1引擎
http://xposed.info/	摸瓜V1引擎
http://repo.xposed.info/module/de.blinkt.vpndialogxposed	摸瓜V1引擎
https://github.com/schwabe/ics-openvpn/issues/34	摸瓜V1引擎
https://github.com/schwabe/ics-openvpn/issues/185	摸瓜V1引擎

https://crowdin.net/project/ics-openvpn/invite	摸瓜V1引擎
https://community.openvpn.net/	摸瓜V1引擎
https://nomadvpn.ru/nomadvpn/privacy/policy.html >	摸瓜V1引擎
http://schemas.android.com/apk/res/androidkkm0	摸瓜V3引擎
estonia2.nomad.twc1.net	摸瓜V3引擎
germany2.nomad.twc1.net	摸瓜V3引擎
hongkong2.nomad.twc1.net	摸瓜V3引擎
canada2.nomad.twc1.net	摸瓜V3引擎
usa2.nomad.twc1.net	摸瓜V3引擎
moldova2.nomad.twc1.net	摸瓜V3引擎
austria2.nomad.twc1.net	摸瓜V3引擎
lithuania2.nomad.twc1.net	摸瓜V3引擎
finland2.nomad.twc1.net	摸瓜V3引擎
greece2.nomad.twc1.net	摸瓜V3引擎
null	摸瓜V3引擎
poland2.nomad.twc1.net	摸瓜V3引擎
sweden2.nomad.twc1.net	摸瓜V3引擎

belgium2.nomad.twc1.net	摸瓜V3引擎
japan2.nomad.twc1.net	摸瓜V3引擎
italy2.nomad.twc1.net	摸瓜V3引擎
kazakhstan2.nomad.twc1.net	摸瓜V3引擎
denmark2.nomad.twc1.net	摸瓜V3引擎
france2.nomad.twc1.net	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
mobile.yandexadexchange.net	摸瓜V3引擎
spain2.nomad.twc1.net	摸瓜V3引擎
czechia2.nomad.twc1.net	摸瓜V3引擎
romania2.nomad.twc1.net	摸瓜V3引擎
armenia2.nomad.twc1.net	摸瓜V3引擎
latvia2.nomad.twc1.net	摸瓜V3引擎
turkey2.nomad.twc1.net	摸瓜V3引擎
balancer.nomad.twc1.net	摸瓜V3引擎
greatbritain2.nomad.twc1.net	摸瓜V3引擎
brazil2.nomad.twc1.net	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎

hungary2.nomad.twc1.net	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
switzerland2.nomad.twc1.net	摸瓜V3引擎
netherlands2.nomad.twc1.net	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
yandex.ru	摸瓜V3引擎
norway2.nomad.twc1.net	摸瓜V3引擎
http://openvpn.net/howto.html	lib/arm64-v8a/libopenvpn.so
http://openvpn.net/howto.html	lib/armeabi-v7a/libopenvpn.so

 邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	T1/k.java
ram219219@gmail.com	com/rg/nomadvpn/ui/leak/LeakFragment.java
android.studio@android.com	摸瓜V1引擎
sales@openvpn.net	lib/arm64-v8a/libopenvpn.so
sales@openvpn.net	lib/armeabi-v7a/libopenvpn.so

手机线索

手机号	所在文件
17179869184	M1/N0.java
17179869184	M1/D0.java

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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfce6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

硬编码敏感信息

可能的敏感信息
"age_restricted_user" : "Age Restricted User"
"auth_username" : "Username"
"client_no_certificate" : "No Certificate"
"country_turkey" : "Turkey"
"external_authenticator" : "External Authenticator"
"faq_remote_api" : "OpenVPN for Android supports two remote APIs, a sophisticated API using AIDL (remoteEXample in the git repository) and a simple one using Intents. <p>Examples using adb shell and the intents. Replace profilname with your profile name<p><p> adb shell am start-activity -a android.intent.action.MAIN de.blinkt.openvpn/.api.i.DisconnectVPN<p> adb shell am start-activity -a android.intent.action.MAIN -e de.blinkt.openvpn.api.profileName Blinkt de.blinkt.openvpn/.api.ConnectVPN"
"filter_user" : "User"
"google_api_key" : "AlzaSyB_DhiaPLSmrRqqRH9r3FKTNVbl82EH8vl"
"google_crash_reporting_api_key" : "AlzaSyB_DhiaPLSmrRqqRH9r3FKTNVbl82EH8vl"
"missing_ca_certificate" : "Missing CA certificate"
"no_certificate" : "You must select a certificate"
"packet_auth" : "Packet authentication"
"password" : "Password"
"pkcs12_file_encryption_key" : "PKCS12 File Encryption Key"
"private_key_password" : "Private Key Password"
"save_password" : "Save Password"

"session_ipv4string" : "%1\$s - %2\$s"
"session_ipv6string" : "%1\$s - %3\$s, %2\$s"
"settings_auth" : "Authentication/Encryption"
"show_password" : "Show password"
"state_auth" : "Authenticating"
"state_auth_failed" : "Authentication failed"
"state_auth_pending" : "Authentication pending"
"state_user_vpn_password" : "Waiting for user VPN password"
"yandex_mobileads_age_restricted_user" : "com.yandex.mobile.ads.AGE_RESTRICTED_USER"
"age_restricted_user" : "Age Restricted User"
"country_turkey" : "Турция"
"filter_user" : "Пользовательские"

 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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FOREGROUND_SERVICE_DATA_SYNC	未知	Unknown permission	Unknown permission from android reference
			允许应用程序在后台运行并接收数据，即使设备处于睡眠状态。

android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
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
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
com.rg.nomadvpn.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.rg.nomadvpn.MainActivity	Schemes: nomadvpn://, Hosts: nomadvpn.com,