



MoGua

Ultimate VPN 1.4.5.APK 分析报告



APP名称:

Ultimate VPN

包名: com.open.hotspot.vpn.free

域名线索: 19条

URL线索: 16条

邮箱线索: 4条

分析日期: 2025年7月17日

分析平台: [摸瓜APK反编译平台](#)

文件名: ultimate-vpn-1-4-5.apk
文件大小: 8.38MB
MD5值: 545e84316c6a242113bff6d25227dd81
SHA1值: 1fa7c9c1c8eff0a25d91725026ea4b457183d1bd
SHA256值: acc559035d505793827b7531b45a169cf4c0f05698101179cd033e4ab64fd6ec

i APP 信息

App名称: Ultimate VPN
包名: com.open.hotspot.vpn.free
主活动Activity: com.open.hotspot.vpn.free.ui.activity.LauncherActivity
安卓版本名称: 1.4.5
安卓版本: 161

🔍 域名线索

域名	服务器信息
www.openssl.org	IP: 34.36.58.177 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
premiumvpnlist.com	IP: 18.195.8.75 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
schemas.android.com	没有服务器地理信息.
e.crashlytics.com	没有服务器地理信息.

openvpn.net	IP: 188.5.4.96 所属国家: Belgium 地区: Vlaams-Brabant 城市: Zaventem 纬度: 50.883690 经度: 4.473398
vpntest.speedtestcustom.com	IP: 151.101.110.219 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.ipgeolocation.io	IP: 172.67.18.64 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.google.com	IP: 122.10.85.4 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
vpn1-5c924.firebaseio.com	IP: 35.201.97.85 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
sgindex.biz	IP: 54.255.102.70 所属国家: Singapore 地区: Singapore 城市: Singapore

	纬度: 1.289987 经度: 103.850281
13.58.7.163	IP: 13.58.7.163 所属国家: United States of America 地区: Ohio 城市: Columbus 纬度: 39.961380 经度: -82.997749
deindex.biz	IP: 18.193.171.158 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
www.dappium.co	IP: 103.224.182.251 所属国家: Australia 地区: Victoria 城市: Beaumaris 纬度: -37.982201 经度: 145.038940
settings.crashlytics.com	没有服务器地理信息.
fastvpnlist.com	IP: 3.0.233.32 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
supervpnlist.com	IP: 3.13.118.143 所属国家: United States of America 地区: Ohio 城市: Columbus 纬度: 39.961380 经度: -82.997749

www.freevpn.company	IP: 91.195.240.123 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Koeln 纬度: 50.933346 经度: 6.949720
usindex.biz	IP: 18.190.40.225 所属国家: United States of America 地区: Ohio 城市: Columbus 纬度: 39.961380 经度: -82.997749
play.google.com	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

 URL线索

URL信息	Url所在文件
https://e.crashlytics.com/spi/v2/events	b/a/a/a/a/g/k.java
https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings	b/a/a/a/a/g/q.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
https://api.ipgeolocation.io/getip	com/open/hotspot/vpn/free/api/b.java
https://api.ipgeolocation.io/ipgeo	com/open/hotspot/vpn/free/api/b.java

http://vpntest.speedtestcustom.com	com/open/hotspot/vpn/free/ui/activity/SpeedTestActivity.java
http://vpntest.speedtestcustom.com	com/open/hotspot/vpn/free/ui/activity/ToolsActivity.java
http://www.dappium.co/policy/privacyPolicy.html	com/open/hotspot/vpn/free/ui/activity/WelcomeActivity.java
https://play.google.com/store/apps/details?id=com.open.hotspot.vpn.free	com/open/hotspot/vpn/free/ui/activity/BaseActivity.java
http://www.freevpn.company/	com/open/hotspot/vpn/free/ui/activity/HomeActivity.java
http://13.58.7.163/newannouncement.txt	com/open/hotspot/vpn/free/ui/activity/HomeActivity.java
http://www.freevpn.company/	com/open/hotspot/vpn/free/ui/activity/MyIPActivity.java
https://www.google.com/search?q=my+ip	com/open/hotspot/vpn/free/ui/activity/MyIPActivity.java
http://www.freevpn.company/	com/open/hotspot/vpn/free/ui/activity/LoaderActivity.java
http://fastvpnlist.com	com/open/hotspot/vpn/free/util/g.java
http://sgindex.biz	com/open/hotspot/vpn/free/util/g.java
http://supervpnlist.com	com/open/hotspot/vpn/free/util/g.java
http://usindex.biz	com/open/hotspot/vpn/free/util/g.java
http://premiumvpnlist.com	com/open/hotspot/vpn/free/util/g.java
http://deindex.biz	com/open/hotspot/vpn/free/util/g.java
https://vpn1-5c924.firebaseio.com	Mogua Engine V1
https://play.google.com/store/apps/details?id=com.open.hotspot.vpn.free	Mogua Engine V1

http://openvpn.net/howto.html	lib/armeabi-v7a/libopenvpn.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libopenvpn.so

 邮箱线索

邮箱地址	所在文件
ultimum.vpn@gmail.com	com/open/hotspot/vpn/free/ui/activity/SendSuggestActivity.java
ultimum.vpn@gmail.com	com/open/hotspot/vpn/free/ui/activity/BaseActivity.java
freeinternnet@gmail.com	Mogua Engine V1
sales@openvpn.net	lib/armeabi-v7a/libopenvpn.so

 手机线索

手机号	所在文件
15552000000	b/a/a/a/a/e/h.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=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2018-08-10 16:51:30+00:00
有效期至: 2048-08-10 16:51:30+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xf3f058c28070fc6a18a0f1e2c1ecee0d42f392bd
哈希算法: sha256
md5值: ff23b31dfa2b9dccf3cbb1d0f9cfab13
sha1值: 6fb2b866121c36d636e58d80faac231b3b587393
sha256值: c3e6eeacd54b01ff5d4a3056627acd2591961b4fba6593ea73284302253cf180
sha512值: 84050fccdb0f37cc69a5884974a3bc777fd43ca9b42b26748352b8767b7587a79559a89cc8a5438340b8139d0f4f18093b4839a7cd186bccb73ff79e5810973c
公钥算法: rsa
密钥长度: 4096
指纹: f933a30f2d1a7da88aa0cfdcd6a6f6ed4b740a7991d62123be134dbf20041009

硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://vpn1-5c924.firebaseio.com"
"google_api_key" : "AlzaSyCTfX0DL11UVDhiyue1WYgFXfahrHnH6Tc"
"google_crash_reporting_api_key" : "AlzaSyCTfX0DL11UVDhiyue1WYgFXfahrHnH6Tc"
"google_maps_key" : "AlzaSyC5X-t4qFbPsyGeiRM1lfdCoPBTTtR7IIA"
"missing_ca_certificate" : "Missing CA certificate"
"password" : "Password"
"pkcs12_file_encryption_key" : "PKCS12 File Encryption Key"
"private_key_password" : "Private Key Password"

"session_ipv4string": "%1\$s - %2\$s"
"session_ipv6string": "%1\$s - %3\$s, %2\$s"
"state_auth": "Authenticating"
"state_auth_failed": "Authentication failed"

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	类型	详细情况

	险		
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
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
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.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.REAL_GET_TASKS	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。
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。