MoGua

MahsaNG 7.0.APK 分析报告

APP名称:	MahsaNG

包名:	com.MahsaNet.MahsaNG
域名线索:	13条
URL线索:	22条
邮箱线索:	11条
分析日期:	2025年9月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: MahsaNG_7.0_generic.apk
文件大小: 61.46MB
MD5值: a8a62d9a550a363cca888823666dabfc
SHA1值: 29545f4de0841cf2a0b73bfbf4b7628fad1d26c1
SHA256值: f8e8b73dc42ae3566515633b8a6563f614571e1077b4a687495ab6ed8544d35a

APP 信息

App名称: MahsaNG
包名: com.MahsaNet.MahsaNG
主活动Activity: com.v2ray.ang.ui.MainActivity
安卓版本名称: 7.0
安卓版本: 900

域名线索

域名	服务器信息
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
www.tensorflow.org	**IP**: 142.250.217.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
android.googlesource.com	**IP**: 142.250.99.82 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.google.com	**IP**: 31.13.94.10 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
cloudflare-dns.com	**IP**: 104.16.248.249 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
gfw.mahsa	没有服务器地理信息.
fonts.gstatic.com	**IP**: 203.208.49.130 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.bigdatacloud.net	**IP**: 13.248.207.97 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
t.me	**IP**: 149.154.167.99 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: Warrington **纬度**: 52.184460 **经度**: -0.687590

www.mahsaserver.com	**IP**: 104.21.19.181 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ip-api.com	**IP**: 208.95.112.1 **所属国家**: United States of America **地区**: North Carolina **城市**: Skyland **纬度**: 35.483757 **经度**: -82.521996
api.ipify.org	**IP**: 104.26.12.205 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
raw.githubusercontent.com	**IP**: 0.0.0.0 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

URL线索

URL**信息**	Url**所在文件**
https://raw.githubusercontent.com/2dust/androidpackagenamelist/master/proxy.txt	com/v2ray/ang/AppConfig.java

https://github.com/Loyalsoldier/v2ray-rules-dat/releases/latest/download/	com/v2ray/ang/AppConfig.java
https://raw.githubusercontent.com/2dust/v2rayCustomRoutingList/master/	com/v2ray/ang/AppConfig.java
https://github.com/2dust/v2rayNG/issues	com/v2ray/ang/AppConfig.java
https://raw.githubusercontent.com/2dust/v2rayNG/master/CR.md	com/v2ray/ang/AppConfig.java
https://github.com/2dust/v2rayNG/wiki/Mode	com/v2ray/ang/AppConfig.java
https://t.me/	com/v2ray/ang/util/Utils.java
https://t.me/mahsa_net	com/v2ray/ang/util/Utils.java
https://gfw.mahsa/	com/v2ray/ang/util/MmkvManager.java
https://raw.githubusercontent.com/mahsanet/MahsaFreeConfig/main/app/sub.txt	com/v2ray/ang/ui/MainActivity.java
https://raw.githubusercontent.com/GFW-knocker/MahsaNG/master/remote_config_update_v7.json	com/v2ray/ang/ui/MainActivity.java
https://raw.githubusercontent.com/ircfspace/mahsaNGAd/main/mahsa_accounts_v3.txt	com/v2ray/ang/ui/MainActivity.java
https://t.me/mahsa_net	com/v2ray/ang/ui/MainActivity.java
https://www.mahsaserver.com/donors/	com/v2ray/ang/ui/MainActivity.java
https://raw.githubusercontent.com/mahsanet/MahsaFreeConfig/main/telegram/index.html	com/v2ray/ang/gfwknocker/GFW_tlg_proxy_activity.java
https://www.mahsaserver.com/authorize?token=	com/v2ray/ang/gfwknocker/GFW_donate_config_activity.java
https://www.mahsaserver.com/login/	com/v2ray/ang/gfwknocker/GFW_donate_config_activity.java
https://www.mahsaserver.com/register-donor/	com/v2ray/ang/gfwknocker/GFW_donate_config_activity.java
https://raw.githubusercontent.com/yebekhe/TelegramV2rayCollector/main/json/configs_deduplicate.json	com/v2ray/ang/gfwknocker/GFW_telegram_config_Activity.java

https://raw.githubusercontent.com/mahsanet/MahsaFreeConfig/main/app/sub.txt	com/v2ray/ang/gfwknocker/GFW_github_config_activity.java
https://raw.githubusercontent.com/GFW-knocker/MahsaNG/master/mahsa_EMS_accounts.json	com/v2ray/ang/gfwknocker/GFW_tunnel_config_Activity.java
https://api.ipify.org/	h/c.java
https://api.bigdatacloud.net/data/client-ip	h/c.java
http://ip-api.com/json	h/c.java
https://raw.githubusercontent.com/mahsanet/MahsaFreeConfig/main/app/wireguard.txt	h/l.java
https://raw.githubusercontent.com/ircfspace/mahsaNGAd/main/ads_home.txt	摸瓜V1引擎
https://raw.githubusercontent.com/ircfspace/mahsaNGAd/main/ads.html	摸瓜V1引擎
https://raw.githubusercontent.com/ircfspace/mahsaNGAd/main/ads.txt	摸瓜V1引擎
https://raw.githubusercontent.com/GFW-knocker/MahsaNG/master/web_announcement.html	摸瓜V1引擎
https://raw.githubusercontent.com/GFW-knocker/MahsaNG/master/txt_announcement.txt	摸瓜V1引擎
https://www.mahsaserver.com/terms	摸瓜V1引擎
https://www.mahsaserver.com/privacy	摸瓜V1引擎
https://raw.githubusercontent.com/ircfspace/mahsaNGAd/main/mahsa_accounts.txt	摸瓜V1引擎
https://raw.githubusercontent.com/GFW-knocker/MahsaNG/master/remote_config_update_v7.json	摸瓜V1引擎
https://raw.githubusercontent.com/yebekhe/TelegramV2rayCollector/main/json/configs.json	摸瓜V1引擎
https://cloudflare-dns.com/dns-query	摸瓜V2引擎

https://cloudflare-dns.com/dns-query?name=	摸瓜V2引擎
https://raw.githubusercontent.com/ircfspace/mahsaNGAd/main/mahsa_accounts_v3.txt	摸瓜V3引擎
https://raw.githubusercontent.com/mahsanet/MahsaFreeConfig/main/app/wireguard.txt	摸瓜V3引擎
https://raw.githubusercontent.com/GFW-knocker/MahsaNG/master/remote_config_update_v7.json	摸瓜V3引擎
https://api.ipify.org/	摸瓜V3引擎
https://github.com/2dust/v2rayNG/wiki/Mode	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
https://www.mahsaserver.com/donors/	摸瓜V3引擎
https://t.me/	摸瓜V3引擎
https://www.tensorflow.org/lite/guide/ops_custom	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
https://raw.githubusercontent.com/mahsanet/MahsaFreeConfig/main/app/sub.txt	摸瓜V3引擎
https://raw.githubusercontent.com/mahsanet/MahsaFreeConfig/main/telegram/index.html	摸瓜V3引擎
https://raw.githubusercontent.com/2dust/androidpackagenamelist/master/proxy.txt	摸瓜V3引擎
https://www.mahsaserver.com/login/	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://raw.githubusercontent.com/2dust/v2rayCustomRoutingList/master/	摸瓜V3引擎

https://www.mahsaserver.com/register-donor/	摸瓜V3引擎
https://github.com/Loyalsoldier/v2ray-rules-dat/releases/latest/download/	摸瓜V3引擎
https://api.bigdatacloud.net/data/client-ip	摸瓜V3引擎
https://www.tensorflow.org/lite/guide/ops_select	摸瓜V3引擎
https://www.tensorflow.org/lite/guide/ops_selectInput	摸瓜V3引擎
play.googleapis.com	摸瓜V3引擎
https://raw.githubusercontent.com/GFW-knocker/MahsaNG/master/mahsa_EMS_accounts.json	摸瓜V3引擎
https://gfw.mahsa/	摸瓜V3引擎
https://www.mahsaserver.com/authorize?token=	摸瓜V3引擎
fonts.gstatic.com	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://raw.githubusercontent.com/yebekhe/TelegramV2rayCollector/main/json/configs_deduplicate.json	摸瓜V3引擎
http://ip-api.com/json	摸瓜V3引擎
safebrowsing.googleapis.com	摸瓜V3引擎
https://t.me/mahsa_net	摸瓜V3引擎
https://www.tensorflow.org/lite/guide/ops_select	lib/arm64-v8a/libbarhopper_v3.so
http://http	lib/arm64-v8a/libbarhopper_v3.so

https://www.tensorflow.org/lite/guide/ops_custom	lib/arm64-v8a/libbarhopper_v3.so
https://www.google.com/generate_204PrepareDomain	lib/arm64-v8a/libgojni.so
https://www.tensorflow.org/lite/guide/ops_select	lib/armeabi-v7a/libbarhopper_v3.so
http://http	lib/armeabi-v7a/libbarhopper_v3.so
https://www.tensorflow.org/lite/guide/ops_custom	lib/armeabi-v7a/libbarhopper_v3.so
https://www.google.com/generate_204PrepareDomain	lib/armeabi-v7a/libgojni.so
https://www.tensorflow.org/lite/guide/ops_select	lib/x86/libbarhopper_v3.so
http://http	lib/x86/libbarhopper_v3.so
https://www.tensorflow.org/lite/guide/ops_custom	lib/x86/libbarhopper_v3.so
https://www.google.com/generate_204PrepareDomain	lib/x86/libgojni.so
https://www.tensorflow.org/lite/guide/ops_select	lib/x86_64/libbarhopper_v3.so
http://http	lib/x86_64/libbarhopper_v3.so
https://www.tensorflow.org/lite/guide/ops_custom	lib/x86_64/libbarhopper_v3.so

邮箱线索

邮箱地址	所在文件
android-sdk-releaser@oqdw3.prod	lib/arm64-v8a/libbarhopper_v3.so
jason@zx2c4.comreceive	lib/arm64-v8a/libgojni.so

ambrop7@gmail.com	lib/arm64-v8a/libtun2socks.so
android-sdk-releaser@oqdw3.prod	lib/armeabi-v7a/libbarhopper_v3.so
jason@zx2c4.comreceive	lib/armeabi-v7a/libgojni.so
ambrop7@gmail.com	lib/armeabi-v7a/libtun2socks.so
android-sdk-releaser@oqdw3.prod	lib/x86/libbarhopper_v3.so
jason@zx2c4.comreceive	lib/x86/libgojni.so
ambrop7@gmail.com	lib/x86/libtun2socks.so
android-sdk-releaser@oqdw3.prod	lib/x86_64/libbarhopper_v3.so
ambrop7@gmail.com	lib/x86_64/libtun2socks.so

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=MahsaNG, OU=MahsaNet Dev, O=MahsaNet Inc., L=Dortmund, ST=North Rhine-Westphalia, C=DE
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-31 21:15:22+00:00
有效期至: 2048-08-24 21:15:22+00:00
发行人: CN=MahsaNG, OU=MahsaNet Dev, O=MahsaNet Inc., L=Dortmund, ST=North Rhine-Westphalia, C=DE

序列号: 0x1
哈希算法: sha256
md5值: d63b2eabf70b5fefc6ac38be9923bd1b
sha1值: b492d43be7a93005ad37d769507b1927149838f3
sha256值: e2c23265d7b81c0a331b954902ff6a6c835bf1117ee61292c3b69f4a7c246b73
sha512值: ad2c252cc0bea64367dd8d68371486df6398986cd816cfce9568b99ecd17eac8a2814122dc13e8f991ac8b26617a0a4f0bfaa916ac50d6773c0faf49e4bc5745
公钥算法: rsa
密钥长度: 2048
指纹: 1ae16515c21e92bf408ffe06bdeac201093b46e6c12053eb1899e8a8ec9eb731

硬编码敏感信息

可能的敏感信息
"server_lab_public_key" : "PublicKey"
"server_lab_secret_key" : "Secret or Private Key"
"server_lab_public_key" : "PublicKey"

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.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.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_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.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.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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference

com.MahsaNet.MahsaNG.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.v2ray.ang.ui.UrlSchemeActivity	Schemes: v2rayng://, Hosts: install-config, install-sub, Mime Types: text/plain,

---