Evaluation Warning: The document was created with Spire.Doc for Python.

**MahsaNG（ 7.0版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | MahsaNG |
| 版本 | 7.0 |
| 包名 | com.MahsaNet.MahsaNG |
| 域名线索 | 13条 |
| URL线索 | 22条 |
| APP图标 |  |
| 分析日期 | 2025年9月5日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | MahsaNG\_7.0\_generic.apk |
| 文件大小 | 61.46MB |
| MD5值 | a8a62d9a550a363cca888823666dabfc |
| SHA1值 | 29545f4de0841cf2a0b73bfbf4b7628fad1d26c1 |
| SHA256值 | f8e8b73dc42ae3566515633b8a6563f614571e1077b4a687495ab6ed8544d35a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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 |
| www.tensorflow.org | IP: 142.250.217.110  所属国家: United States of America  地区: California  城市: Mountain View |
| android.googlesource.com | IP: 142.250.99.82  所属国家: United States of America  地区: California  城市: Mountain View |
| www.google.com | IP: 31.13.94.10  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| cloudflare-dns.com | IP: 104.16.248.249  所属国家: United States of America  地区: California  城市: San Francisco |
| 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 |
| api.bigdatacloud.net | IP: 13.248.207.97  所属国家: United States of America  地区: Washington  城市: Seattle |
| 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 |
| www.mahsaserver.com | IP: 104.21.19.181  所属国家: United States of America  地区: California  城市: San Francisco |
| ip-api.com | IP: 208.95.112.1  所属国家: United States of America  地区: North Carolina  城市: Skyland |
| api.ipify.org | IP: 104.26.12.205  所属国家: United States of America  地区: California  城市: San Francisco |
| raw.githubusercontent.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |

### **4.2 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 |

### **4.3 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 |

### **4.4 手机号线索**

## **5. 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**

## **6. 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" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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 |

## **10. 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, |

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