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

**Atom VPN（ 3.2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 | Atom VPN |
| 版本 | 3.2 |
| 包名 | base.apk |
| 域名线索 | 19条 |
| URL线索 | 26条 |
| APP图标 |  |
| 分析日期 | 2024年10月22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 | base.apk |
| 文件大小 | 22.1MB |
| MD5值 | a533687c276d1297d9c06e0db4003d92 |
| SHA1值 | 5f04898974cefbca6c7b11e54f9c12b845b472a6 |
| SHA256值 | a2546d8f930274a7ac477f3fc5e04865d3b412f8d559b48bbff2613898646e81 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Atom VPN |
| 包名 | base.apk |
| 主活动Activity | [] |
| 安卓版本名称 | 3.2 |
| 安卓版本 | 3200 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.tensorflow.org | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| schemas.android.com | 没有服务器地理信息.  |
| csi.gstatic.com | IP: 220.181.174.102 所属国家: China 地区: Beijing 城市: Beijing  |
| www.example.com | IP: 93.184.216.34 所属国家: United States of America 地区: California 城市: Los Angeles  |
| imasdk.googleapis.com | IP: 220.181.174.97 所属国家: China 地区: Beijing 城市: Beijing  |
| admob-gmats.uc.r.appspot.com | IP: 31.13.95.169 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| googleads.g.doubleclick.net | IP: 220.181.174.38 所属国家: China 地区: Beijing 城市: Beijing  |
| www.google.com | IP: 199.59.149.238 所属国家: United States of America 地区: California 城市: San Francisco  |
| goo.gl | IP: 172.217.160.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| ns.adobe.com | 没有服务器地理信息.  |
| plus.google.com | IP: 128.242.245.29 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| developers.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| pagead2.googlesyndication.com | IP: 203.208.50.70 所属国家: China 地区: Beijing 城市: Beijing  |
| googlemobileadssdk.page.link | IP: 172.217.163.33 所属国家: United States of America 地区: California 城市: Mountain View  |
| play.google.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| support.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| svc955.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| exoplayer.dev | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mainamapi.azurewebsites.net | IP: 20.43.132.134 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | a1/l.java  |
| https://goo.gl/J1sWQy  | y4/n0.java  |
| https://mainamapi.azurewebsites.net/api/main  | io/github/trojan\_gfw/igniter/MainActivity.java  |
| https://www.google.com  | io/github/trojan\_gfw/igniter/MainActivity.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | p3/b.java  |
| https://mainamapi.azurewebsites.net/api/main  | h8/d.java  |
| https://googlemobileadssdk.page.link/admob-android-update-manifest  | s3/p2.java  |
| https://googlemobileadssdk.page.link/ad-manager-android-update-manifest.  | s3/p2.java  |
| https://plus.google.com/  | l4/a1.java  |
| http://www.google.com  | u3/w0.java  |
| http://www.example.com  | u3/w0.java  |
| https://support.google.com/dfp\_premium/answer/7160685  | u3/t.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | t4/tu1.java  |
| https://csi.gstatic.com/csi  | t4/rs.java  |
| https://googlemobileadssdk.page.link/admob-interstitial-policies  | t4/zt0.java  |
| http://ns.adobe.com/xap/1.0/  | t4/o0.java  |
| https://googlemobileadssdk.page.link/admob-interstitial-policies  | t4/xz0.java  |
| http://www.google.com  | t4/x50.java  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html  | t4/gt.java  |
| https://developers.google.com/admob/android/test-ads  | t4/n31.java  |
| https://developers.google.com/admob/android/test-ads  | t4/jo1.java  |
| https://googlemobileadssdk.page.link/admob-interstitial-policies  | t4/bl0.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | t4/fl2.java  |
| http://www.example.com  | t4/hs.java  |
| https://googleads.g.doubleclick.net  | t4/lr.java  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native\_ads.html  | t4/lr.java  |
| https://imasdk.googleapis.com/admob/sdkloader/native\_video.html  | t4/lr.java  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid\_app\_banner.js  | t4/lr.java  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid\_app\_expanded\_banner.js  | t4/lr.java  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid\_app\_interstitial.js  | t4/lr.java  |
| https://pagead2.googlesyndication.com/pagead/ping?e=2&f=1  | t4/lr.java  |
| https://admob-gmats.uc.r.appspot.com/  | t4/lr.java  |
| https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html  | t4/lr.java  |
| https://www.google.com/dfp/linkDevice  | t4/lr.java  |
| https://www.google.com/dfp/inAppPreview  | t4/lr.java  |
| https://www.google.com/dfp/debugSignals  | t4/lr.java  |
| https://www.google.com/dfp/sendDebugData  | t4/lr.java  |
| http://www.example.com  | t4/rr.java  |
| https://play.google.com/store/apps/details?id=net.lab.flying,  | Mogua Engine V1  |
| https://svc955.github.io  | Mogua Engine V1  |
| 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.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  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | i4/r.java  |
| android-sdk-releaser@lmbz11.prod  | lib/arm64-v8a/libbarhopper\_v3.so  |
| go-tun2socks@v1.16  | lib/arm64-v8a/libgojni.so  |
| android-sdk-releaser@lmbz11.prod  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| go-tun2socks@v1.16  | lib/armeabi-v7a/libgojni.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13222222222  | t4/bq2.java  |
| 16222222222  | t4/s2.java  |

## **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: C=US, ST=WA, L=USA, O=UK, OU=US, CN=Tom 签名算法: rsassa\_pkcs1v15 有效期自: 2021-04-09 12:55:48+00:00 有效期至: 2046-04-03 12:55:48+00:00 发行人: C=US, ST=WA, L=USA, O=UK, OU=US, CN=Tom 序列号: 0x29364a3c 哈希算法: sha256 md5值: 04228e2e53792a12aa4eef80b0119115 sha1值: f537c6411f7054d347740108254d5131470cd8d7 sha256值: ff58ee16fb10f2070728012d116fd3e267c0bb6f3a0f60803e6043e841c9db05 sha512值: 120057b01d2a24b74602da002d47626481c8fd5baf41e7c0fcd716ecefbc7d5183d8fbc68f8fa77d677212826e2521df697ff766e0bbc81cbdf1e98625a67395 公钥算法: rsa 密钥长度: 2048 指纹: 51e604575a4d62a2d2a6391ef1d2cdebbdeb08b3a86fb564d21e0494e0ca1e42**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "password" : "Password"  |
| "verify\_certificate" : "Verify Certificate"  |
| "password" : "密码"  |
| "verify\_certificate" : "验证证书"  |

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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。 |
| com.google.android.gms.permission.AD\_ID | 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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |

## **10. 应用内通信**

**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。**