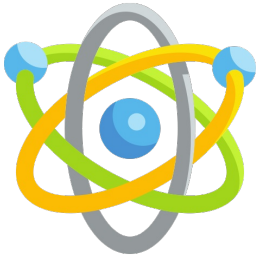
MoGua

Atom VPN 3.2.APK 分析报告



APP名称:	Atom VPN

包名:	base.apk
域名线索:	19条
URL线索:	26条
邮箱线索:	5条
分析日期:	2024年10月22日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk

文件大小: 22.1MB
MD5值: a533687c276d1297d9c06e0db4003d92
SHA1值: 5f04898974cefbca6c7b11e54f9c12b845b472a6
SHA256值: a2546d8f930274a7ac477f3fc5e04865d3b412f8d559b48bbff2613898646e81

APP 信息

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

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 **纬度**: 37.405991 **经度**: -122.078514
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 **纬度**: 39.907501 **经度**: 116.397102
	IP: 93.184.216.34

www.example.com	**所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
imasdk.googleapis.com	IP: 220.181.174.97 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
admob-gmats.uc.r.appspot.com	IP: 31.13.95.169 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
googleads.g.doubleclick.net	IP: 220.181.174.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.google.com	IP: 199.59.149.238 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
goo.gl	IP: 172.217.160.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

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 **纬度**: 35.689499 **经度**: 139.692322
developers.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
pagead2.googlesyndication.com	**IP**: 203.208.50.70 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
googlemobileadssdk.page.link	**IP**: 172.217.163.33 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
play.google.com	**IP**: 142.251.42.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
	IP: 142.251.43.14 **所属国家**: United States of America

support.google.com	**地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
svc955.github.io	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
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
mainamapi.azurewebsites.net	**IP**: 20.43.132.134 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

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

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

手机线索

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

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

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"

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.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

应用内通信