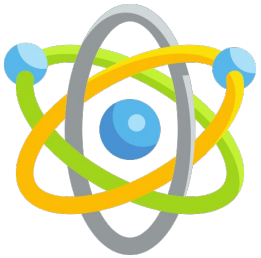
MoGua

Atom VPN 3.0.APK 分析报告



APP名称: Atom VPN

包名:	net.lab.flying
域名线索:	14条
URL线索:	14条
邮箱线索:	3条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 原子加速器.apk
文件大小: 14.53MB
MD5值: 5582c5dfedca0ff0a54a8547c0ef14a7
SHA1值: 5dd285799147afd3512658a86e06e692176f5ecc
SHA256值: 4c3981a37a7d120a8d8902c66cbdcf4872abb83933be769b3a7081ed7423ddb7

APP 信息

App名称: Atom VPN
包名: net.lab.flying
主活动Activity: io.github.trojan_gfw.igniter.MainActivity
安卓版本名称: 3.0
安卓版本: 3000

域名线索

域名	服务器信息
www.google.com	**IP**: 157.240.17.35 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790
schemas.android.com	没有服务器地理信息.
pagead2.googlesyndication.com	**IP**: 114.250.70.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

svc955.github.io	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
plus.google.com	IP: 142.250.217.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.gstatic.com	IP: 203.208.50.98 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
play.google.com	IP: 59.24.3.174 **所属国家**: Korea (Republic of) **地区**: Gyeonggi-do **城市**: Seongnam **纬度**: 37.420624 **经度**: 127.126717
imasdk.googleapis.com	IP: 114.250.67.33 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
atomdata.azurewebsites.net	没有服务器地理信息.
	IP: 142.250.217.110 **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
www.example.com	IP: 23.193.186.12 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
googleads.g.doubleclick.net	IP: 114.250.69.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.tensorflow.org	IP: 142.251.33.78 **所属国家**: Canada **地区**: Ontario **城市**: Toronto **纬度**: 43.653660 **经度**: -79.382927
csi.gstatic.com	IP: 114.250.70.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL**信息**	Url**所在文件**

https://atomdata.azurewebsites.net/api/main	io/github/trojan_gfw/igniter/MainActivity.java
https://www.google.com	io/github/trojan_gfw/igniter/MainActivity.java
https://plus.google.com/	o3/a1.java
http://www.example.com	w3/yf.java
https://support.google.com/dfp_premium/answer/7160685	w3/c9.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40.html	w3/f20.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js	w3/f20.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_banner.js	w3/f20.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_expanded_banner.js	w3/f20.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_interstitial.js	w3/f20.java
https://csi.gstatic.com/csi	w3/f20.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html	w3/f20.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/native_ads.js	w3/f20.java
https://imasdk.googleapis.com/admob/sdkloader/native_video.html	w3/f20.java
https://www.google.com/dfp/linkDevice	w3/f20.java
https://www.google.com/dfp/inAppPreview	w3/f20.java
https://www.google.com/dfp/debugSignals	w3/f20.java

https://www.google.com/dfp/sendDebugData	w3/f20.java
http://www.example.com	w3/d30.java
https://pagead2.googlesyndication.com/pagead/gen_204	w3/u3.java
http://www.google.com	w3/y3.java
https://atomdata.azurewebsites.net/api/main	j7/d.java
http://schemas.android.com/apk/res/android	z0/k.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	z2/b.java
https://play.google.com/store/apps/details?id=net.lab.flying,	摸瓜V1引擎
https://svc955.github.io	摸瓜V1引擎
www.gstatic.com	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

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	l3/r.java

android-sdk-releaser@lmbz11.prod	lib/arm64-v8a/libbarhopper_v3.so
go-tun2socks@v1.16	lib/arm64-v8a/libgojni.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: 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。

应用内通信
