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

**Fox VPN（ 1.0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 | Fox VPN |
| 版本 | 1.0 |
| 包名 | FoxVPN\_v1.0 b3速度1M.apk |
| 域名线索 | 79条 |
| URL线索 | 71条 |
| APP图标 |  |
| 分析日期 | 2025年7月6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 | FoxVPN\_v1.0 b3速度1M.apk |
| 文件大小 | 37.36MB |
| MD5值 | 3bd1bc6bb37da9b5fe1b22268be108c0 |
| SHA1值 | 51bc076986d778c1d0cb5b09c593a5ae0c2b63e6 |
| SHA256值 | 389dd524eb707b9d452c42a4dff08c711afaa3b071557eaa2b0ee442fb3a9ba4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Fox VPN |
| 包名 | FoxVPN\_v1.0 b3速度1M.apk |
| 主活动Activity | [] |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 3 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api-s.northghost.com | IP: 173.255.209.47 所属国家: United States of America 地区: California 城市: Fremont  |
| 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  |
| openvpn.net | IP: 49.2.123.56 所属国家: Australia 地区: New South Wales 城市: Macquarie Park  |
| appshost.us | IP: 198.187.31.167 所属国家: United States of America 地区: Georgia 城市: Atlanta  |
| maps.google.com | IP: 172.217.163.46 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.  |
| hooks.stripe.com | IP: 13.115.27.220 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| dash.applovin.com | IP: 34.111.30.212 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| ns.adobe.com | 没有服务器地理信息.  |
| baidu.com | IP: 110.242.68.66 所属国家: China 地区: Hebei 城市: Baoding  |
| exoplayer.dev | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| twitter.com | IP: 31.13.75.12 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| outlook.live.com | IP: 52.98.40.34 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ms.applvn.com | IP: 104.16.165.233 所属国家: United States of America 地区: California 城市: San Francisco  |
| bing.com | IP: 204.79.197.200 所属国家: United States of America 地区: Washington 城市: Redmond  |
| file-examples-com.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| corp.aarki.com | IP: 204.130.244.41 所属国家: United States of America 地区: California 城市: Sunnyvale  |
| assets.applovin.com | IP: 34.120.175.182 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| outcome-arm-ext-med-ext.sonic-us.supersonicads.com | IP: 13.35.121.44 所属国家: United States of America 地区: California 城市: San Francisco  |
| a.applvn.com | IP: 104.16.165.233 所属国家: United States of America 地区: California 城市: San Francisco  |
| dashboard.stripe.com | IP: 54.64.207.232 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| instagram.com | IP: 157.240.10.41 所属国家: United States of America 地区: California 城市: Menlo Park  |
| outcome-ssp.supersonicads.com | IP: 204.246.191.56 所属国家: United States of America 地区: Oregon 城市: Hillsboro  |
| d1pijg9qb98hxx.cloudfront.net | IP: 13.32.50.55 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| errors.stripe.com | IP: 176.34.8.232 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| init.supersonicads.com | IP: 13.35.121.8 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.microsoft.com | IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| api.stripe.com | IP: 13.230.90.110 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| developer.android.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| gist.github.com | IP: 59.24.3.173 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam  |
| www.applovin.com | IP: 141.193.213.21 所属国家: United States of America 地区: Texas 城市: Austin  |
| ip-api.com | IP: 208.95.112.1 所属国家: United States of America 地区: North Carolina 城市: Skyland  |
| microsoft.com | IP: 20.70.246.20 所属国家: Australia 地区: New South Wales 城市: Sydney  |
| www.moloco.com | IP: 52.199.221.217 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| prod-a.applovin.comhttps | 没有服务器地理信息.  |
| yahoo.com | IP: 74.6.143.25 所属国家: United States of America 地区: New York 城市: New York City  |
| developer.apple.com | IP: 17.253.85.201 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| goo.gl | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| amazon.com | IP: 54.239.28.85 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| office.com | IP: 13.107.6.156 所属国家: United States of America 地区: Washington 城市: Redmond  |
| d.applvn.com | IP: 104.16.164.233 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.speedtest.net | IP: 104.18.238.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| m.stripe.com | IP: 44.235.129.191 所属国家: United States of America 地区: Oregon 城市: Portland  |
| api64.ipify.org | IP: 64.185.227.155 所属国家: United States of America 地区: Utah 城市: Ogden  |
| connect.stripe.com | IP: 3.115.110.210 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| www.google.com | IP: 202.160.128.16 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| aomedia.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| support.stripe.com | IP: 54.150.186.249 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| apple.com | IP: 17.253.144.10 所属国家: United States of America 地区: California 城市: Cupertino  |
| android.stable-vpn.com | IP: 143.204.86.102 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| api.taboola.com | IP: 146.75.113.44 所属国家: Sweden 地区: Vastra Gotalands lan 城市: Goeteborg  |
| outcome-crash-report.supersonicads.com | IP: 13.32.50.54 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| wikipedia.org | IP: 108.160.167.167 所属国家: United States of America 地区: California 城市: San Francisco  |
| rt.applvn.com | IP: 104.16.164.233 所属国家: United States of America 地区: California 城市: San Francisco  |
| connectivitycheck.gstatic.com | IP: 203.208.39.226 所属国家: China 地区: Beijing 城市: Beijing  |
| www.privacypolicygenerator.info | IP: 104.21.59.178 所属国家: United States of America 地区: California 城市: San Francisco  |
| gstatic.com | IP: 142.251.43.3 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.adjust.com | IP: 185.151.204.101 所属国家: Germany 地区: Berlin 城市: Berlin  |
| vid.applovin.com | IP: 34.160.64.118 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| stripe.com | IP: 54.187.119.242 所属国家: United States of America 地区: Oregon 城市: Portland  |
| api.pango-paas.co | IP: 35.82.227.202 所属国家: United States of America 地区: Oregon 城市: Portland  |
| d.applovin.com | IP: 34.110.179.88 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| a.applovin.com | IP: 34.117.147.68 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| files.stripe.com | IP: 3.114.158.108 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| play.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| clients3.google.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| schemas.applovin.com | 没有服务器地理信息.  |
| rt.applovin.com | IP: 34.117.147.68 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| ms.applovin.com | IP: 34.102.162.219 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| monetization-support.applovin.com | IP: 34.110.151.135 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| api.ipify.org | IP: 104.237.62.211 所属国家: United States of America 地区: Utah 城市: Ogden  |
| linkedin.com | IP: 52.130.75.155 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.openssl.org | IP: 2.17.62.8 所属国家: France 地区: Ile-de-France 城市: Paris  |
| ebay.com | IP: 66.211.162.136 所属国家: United States of America 地区: California 城市: San Jose  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| awebhtpo3u8g5t.ecoweb-network.com | IP: 13.35.121.101 所属国家: United States of America 地区: California 城市: San Francisco  |
| q.stripe.com | IP: 54.187.119.242 所属国家: United States of America 地区: Oregon 城市: Portland  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://t.me/fun\_apk  | BotX/mod/p/View$OnClickListenerC0000.java  |
| https://emv3ds/challenge  | a/a/a/a/h/u.java  |
| https://emv3ds/challenge  | a/a/a/a/h/a0.java  |
| https://errors.stripe.com/api/  | a/a/a/a/a/b.java  |
| https://awebhtpo3u8g5t.ecoweb-network.com  | com/foxvpn/superfastservers/BuildConfig.java  |
| https://www.speedtest.net/speedtest-config.php  | com/foxvpn/superfastservers/utils/GetSpeedTestHostsHandler.java  |
| https://www.speedtest.net/speedtest-servers-static.php  | com/foxvpn/superfastservers/utils/GetSpeedTestHostsHandler.java  |
| https://play.google.com/store/apps/details?id=  | com/foxvpn/superfastservers/activity/HomeActivity.java  |
| https://play.google.com/store/apps/details?id=  | com/foxvpn/superfastservers/activity/SplashActivity.java  |
| http://ip-api.com/  | com/foxvpn/superfastservers/api/RetrofitBuilder.java  |
| http://ip-api.com/  | com/foxvpn/superfastservers/api/GioRetrofitClient.java  |
| http://schemas.applovin.com/android/1.0  | com/applovin/adview/AppLovinAdView.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | com/applovin/exoplayer2/aw.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | com/applovin/exoplayer2/d/p.java  |
| https://x</LA\_URL>  | com/applovin/exoplayer2/d/o.java  |
| https://x  | com/applovin/exoplayer2/d/o.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | com/applovin/exoplayer2/k/t.java  |
| http://www.w3.org/ns/ttml  | com/applovin/exoplayer2/i/g/c.java  |
| https://aomedia.org/emsg/ID3  | com/applovin/exoplayer2/g/b/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | com/applovin/exoplayer2/g/b/a.java  |
| http://ns.adobe.com/xap/1.0/  | com/applovin/exoplayer2/e/d/a.java  |
| https://ms.applovin.com/1.0/sdk/error  | com/applovin/impl/sdk/t.java  |
| http://developer.android.com/google/play-services/setup.html.  | com/applovin/impl/sdk/utils/d.java  |
| https://ms.applovin.com/  | com/applovin/impl/sdk/c/a.java  |
| https://ms.applvn.com/  | com/applovin/impl/sdk/c/a.java  |
| https://assets.applovin.com/gdpr/flow\_v1/gdpr-flow-1.html  | com/applovin/impl/sdk/c/b.java  |
| https://vid.applovin.com/,https://stage-vid.applovin.com/,https://pdn.applovin.com/,https://stage-pdn.applovin.com/,https://img.applovin.com/,https://stage-img.applovin.com/,https://d.applovin.com/,https://assets.applovin.com/,https://stage-assets.applovin.com/,https://cdnjs.cloudflare.com/,http://vid.applovin.com/,http://stage-vid.applovin.com/,http://pdn.applovin.com/,http://stage-pdn.applovin.com/,http://img.applovin.com/,http://stage-img.applovin.com/,http://d.applovin.com/,http://assets.applovin.com/,http://stage-assets.applovin.com/,http://cdnjs.cloudflare.com/,http://u.appl.vn/,https://u.appl.vn/,https://res.applovin.com/,https://res1.applovin.com/,https://res2.applovin.com/,https://res3.applovin.com/,http://res.applovin.com/,http://res1.applovin.com/,http://res2.applovin.com/,http://res3.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://prod-a.applovin.com,https://rt.applovin.com/4.0/pix,  | com/applovin/impl/sdk/c/b.java  |
| https://rt.applvn.com/4.0/pix,https://ms.applovin.com/,https://ms.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://ms.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://ms.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://a.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://a.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://d.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://d.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://rt.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://rt.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://ms.applovin.com/1.0/sdk/error  | com/applovin/impl/sdk/c/b.java  |
| https://dash.applovin.com/documentation/mediation/android/getting-started/integration  | com/applovin/impl/sdk/c/b.java  |
| https://dash.applovin.com/documentation/mediation/unity/getting-started/integration  | com/applovin/impl/sdk/c/b.java  |
| https://corp.aarki.com/privacy,https://www.adcolony.com/consumer-privacy/,https://www.adikteev.com/privacy-policy-eng,https://advertising.amazon.com/resources/ad-policy/eu-data-protection-and-privacy,https://www.appier.com/privacy-policy/,https://www.appnexus.com/en/company/privacy-policy,https://www.beeswax.com/privacy.html,https://bidease.com/privacy-policy,https://www.bigabid.com/Legal/,https://www.pangleglobal.com/privacy,https://answers.chartboost.com/en-us/articles/200780269,https://clearpier.com/privacy-policy/,https://www.criteo.com/privacy/,https://www.criteo.com/privacy/,https://dataseat.com/privacy-policy,https://nend.net/privacy/sdkpolicy,https://www.fyber.com/services-privacy-statement/,https://privacy-policy.cyberagent.ai/,https://policies.google.com/privacy,https://www.inmobi.com/privacy-policy/,https://www.is.com/privacy-policy/,https://www.jampp.com/privacy-policy-terms-and-conditions,https://www.lifestreet.com/privacy/,https://liftoff.io/privacy-policy/,https://terms2.line.me/creators\_privacy\_policy,https://www.linkedin.com/legal/privacy-policy?src=or-search&veh=www.google.comLiqui,https://loopme.com/end-user-privacy-policy/,https://mediasmart.io/privacy-policy/,https://www.facebook.com/privacy/explanation/,https://www.mintegral.com/en/privacy/  | com/applovin/impl/sdk/c/b.java  |
| https://www.moloco.com/privacy-policy,https://www.motiv-i.com/en/privacy/,https://ogury.com/privacy-policy/,https://persona.ly/privacy\_dsp,https://www.opera.com/privacy,https://pubmatic.com/legal/privacy/,https://kayzen.io/data-privacy-policy,https://www.remerge.io/privacy-policy.html,https://revx.io/privacy-policy,https://www.rtbhouse.com/privacy-center/services-privacy-policy/,https://simpli.fi/simpli-fi-services-privacy-policy/,https://www.smaato.com/privacy/,https://smadex.com/end-user-privacy-policy,https://snap.com/en-US/privacy/privacy-policy,https://www.stackadapt.com/privacy,https://www.start.io/policy/privacy-policy-site/,https://www.tapjoy.com/legal/general/privacy-policy/,https://taurusx.com/privacy-policy.html,https://rubiconproject.com/privacy-policy/,https://www.thetradedesk.com/general/privacy-policy,https://appreciate.mobi/page.html  | com/applovin/impl/sdk/c/b.java  |
| https://twitter.com/privacy,https://uni-corn.net/privacy.html,https://unity3d.com/legal/privacy-policy,https://www.valassis.com/legal/privacy-policy/,https://pubnative.net/privacy-notice/,https://vungle.com/privacy/,https://wildlifestudios.com/policy-center/privacy-policy/wildlife-studios-privacy-policy/,https://www.groundtruth.com/privacy-policy/,https://legal.yahoo.com/us/en/yahoo/privacy/index.html,https://yandex.com/legal/confidential/,https://www.youappi.com/privacy-policy  | com/applovin/impl/sdk/c/b.java  |
| https://www.adjust.com/terms/privacy-policy/,https://www.appsflyer.com/legal/privacy-policy/,https://branch.io/policies/privacy-policy/  | com/applovin/impl/sdk/c/b.java  |
| https://www.applovin.com/privacy/  | com/applovin/impl/sdk/nativeAd/AppLovinNativeAdImpl.java  |
| https://monetization-support.applovin.com/hc/en-us/articles/236114328-How-can-I-expose-verbose-logging-for-the-SDK>  | com/applovin/impl/sdk/e/n.java  |
| https://play.google.com/store/apps/details?id=  | com/applovin/impl/mediation/debugger/c/b.java  |
| https://dash.applovin.com/documentation/mediation/android/getting-started/integration  | com/applovin/impl/mediation/debugger/ui/c/b.java  |
| https://dash.applovin.com/documentation/mediation/android/getting-started/integration  | com/applovin/impl/mediation/debugger/ui/b/b.java  |
| https://developer.android.com/training/articles/security-config  | com/applovin/impl/mediation/debugger/b/c/c.java  |
| https://api.taboola.com/  | com/applovin/impl/mediation/b/b/a.java  |
| http://schemas.android.com/apk/res/android  | com/applovin/mediation/ads/MaxAdView.java  |
| http://whatwg.org/html/common-microsyntaxes.html  | com/mbridge/msdk/c/b/b.java  |
| http://whatwg.org/html/webappapis.html  | com/mbridge/msdk/c/b/b.java  |
| https://gist.github.com/atk/1020396\n  | com/mbridge/msdk/c/b/b.java  |
| http://whatwg.org/C  | com/mbridge/msdk/c/b/b.java  |
| https://play.google.com/  | com/mbridge/msdk/click/a.java  |
| http://www.w3.org/ns/ttml  | com/mbridge/msdk/playercommon/exoplayer2/text/ttml/TtmlDecoder.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/tools/ac.java  |
| https://play.google.com/  | com/mbridge/msdk/foundation/tools/ac.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/webview/a.java  |
| https://play.google.com  | com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java  |
| https://api64.ipify.org/?format=json  | com/anchorfree/sdk/IpInfoFetcher.java  |
| https://file-examples-com.github.io/uploads/2017/02/file\_example\_JSON\_1kb.json  | com/anchorfree/sdk/SdkConnectionProbe.java  |
| https://api-%s.northghost.com/storage/project/%s/files/%s/%s  | com/anchorfree/sdk/RemoteFileHandler.java  |
| https://api.ipify.org  | com/anchorfree/sdk/utils/AndroidUtils.java  |
| https://api.pango-paas.co  | com/anchorfree/vpnsdk/UrlRotatorImpl.java  |
| https://android.stable-vpn.com  | com/anchorfree/vpnsdk/UrlRotatorImpl.java  |
| https://d1pijg9qb98hxx.cloudfront.net  | com/anchorfree/vpnsdk/UrlRotatorImpl.java  |
| https://connectivitycheck.gstatic.com/generate\_204  | com/anchorfree/vpnsdk/vpnservice/credentials/DefaultCaptivePortalChecker.java  |
| http://connectivitycheck.gstatic.com/generate\_204  | com/anchorfree/vpnsdk/vpnservice/credentials/DefaultCaptivePortalChecker.java  |
| https://google.com/generate\_204  | com/anchorfree/vpnsdk/network/probe/CaptivePortalProbe.java  |
| https://gstatic.com/generate\_204  | com/anchorfree/vpnsdk/network/probe/CaptivePortalProbe.java  |
| https://maps.google.com/generate\_204  | com/anchorfree/vpnsdk/network/probe/CaptivePortalProbe.java  |
| https://www.google.com/generate\_204  | com/anchorfree/vpnsdk/network/probe/CaptivePortalProbe.java  |
| https://clients3.google.com/generate\_204  | com/anchorfree/vpnsdk/network/probe/CaptivePortalProbe.java  |
| https://google.com/  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://apple.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://microsoft.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://yahoo.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://baidu.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://amazon.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://instagram.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://linkedin.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://ebay.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://bing.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://goo.gl  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://outlook.live.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://wikipedia.org  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://office.com  | com/anchorfree/vpnsdk/network/probe/CertificateNetworkProbe.java  |
| https://connect.stripe.com  | com/stripe/Stripe.java  |
| https://api.stripe.com  | com/stripe/Stripe.java  |
| https://files.stripe.com  | com/stripe/Stripe.java  |
| https://files.stripe.com/v1/files  | com/stripe/android/FileUploadRequest.java  |
| https://api.stripe.com/v1/  | com/stripe/android/StripeApiRepository.java  |
| https://api.stripe.com/edge-internal/  | com/stripe/android/StripeApiRepository.java  |
| https://q.stripe.com  | com/stripe/android/AnalyticsRequest.java  |
| https://api.stripe.com  | com/stripe/android/ApiRequest.java  |
| https://stripe.com/docs/keys  | com/stripe/android/ApiKeyValidator.java  |
| https://stripe.com/docs/mobile/android/basic  | com/stripe/android/EphemeralKeyManager.java  |
| https://m.stripe.com/6  | com/stripe/android/FingerprintRequest.java  |
| https://twitter.com/stripestatus,  | com/stripe/android/exception/APIConnectionException.java  |
| https://hooks.stripe.com/three\_d\_secure/authenticate  | com/stripe/android/view/PaymentAuthWebView.java  |
| https://hooks.stripe.com/redirect/complete/src\_  | com/stripe/android/view/PaymentAuthWebView.java  |
| https://hooks.stripe.com/3d\_secure/complete/tdsrc\_  | com/stripe/android/view/PaymentAuthWebView.java  |
| https://twitter.com/stripestatus,  | com/stripe/net/StripeRequest.java  |
| https://stripe.com/docs/api/authentication  | com/stripe/net/StripeRequest.java  |
| https://support.stripe.com/email  | com/stripe/net/StripeRequest.java  |
| https://dashboard.stripe.com/account/applications/settings,  | com/stripe/net/OAuth.java  |
| https://stripe.com/docs/connect/standard-accounts  | com/stripe/net/OAuth.java  |
| https://twitter.com/stripestatus,  | com/stripe/net/HttpURLConnectionClient.java  |
| https://outcome-crash-report.supersonicads.com/reporter  | com/ironsource/environment/e.java  |
| https://outcome-ssp.supersonicads.com/mediation?adUnit=3  | com/ironsource/mediationsdk/utils/i.java  |
| https://outcome-ssp.supersonicads.com/mediation?adUnit=3  | com/ironsource/mediationsdk/utils/k.java  |
| https://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemData  | com/ironsource/mediationsdk/utils/k.java  |
| https://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemData  | com/ironsource/mediationsdk/utils/b.java  |
| https://init.supersonicads.com/sdk/v  | com/ironsource/mediationsdk/server/ServerURL.java  |
| https://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemData  | com/ironsource/mediationsdk/impressionData/a.java  |
| https://outcome-ssp.supersonicads.com/mediation?adUnit=3  | com/ironsource/mediationsdk/events/g.java  |
| https://outcome-ssp.supersonicads.com/mediation?adUnit=2  | com/ironsource/mediationsdk/events/f.java  |
| https://stripe.com/au-becs-dd-service-agreement/legal>Direct  | Mogua Engine V1  |
| https://appshost.us/ubddss/foxvpn.json  | Mogua Engine V1  |
| https://www.privacypolicygenerator.info/live.php?token=JSBXc85VOmBykJpDKEzyEXvl5M5mA0AO  | Mogua Engine V1  |
| http://openvpn.net/howto.html  | lib/x86/libopenvpn.so  |
| https://www.openssl.org/docs/faq.html  | lib/x86/libhydra.so  |
| http://openvpn.net/howto.html  | lib/arm64-v8a/libopenvpn.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| support@stripe.com  | com/stripe/android/StripeRequest.java  |
| support@stripe.com  | com/stripe/android/exception/APIConnectionException.java  |
| support@stripe.com  | com/stripe/model/EventDataObjectDeserializer.java  |
| support@stripe.com  | com/stripe/model/ExternalAccountTypeAdapterFactory.java  |
| support@stripe.com  | com/stripe/net/StripeRequest.java  |
| support@stripe.com  | com/stripe/net/ApiResource.java  |
| support@stripe.com  | com/stripe/net/OAuth.java  |
| support@stripe.com  | com/stripe/net/HttpURLConnectionClient.java  |
| support@stripe.com  | com/stripe/net/UntypedMapDeserializer.java  |
| support@stripe.com  | com/stripe/net/ApiRequestParamsConverter.java  |
| sales@openvpn.net  | lib/x86/libopenvpn.so  |
| sales@openvpn.net  | lib/arm64-v8a/libopenvpn.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: True 找到 1 个唯一证书 主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2008-02-29 01:33:46+00:00 有效期至: 2035-07-17 01:33:46+00:00 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0x936eacbe07f201df 哈希算法: sha1 md5值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569 公钥算法: rsa 密钥长度: 2048 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dyStrategy.privateAddress" : "privateAddress"  |
| "is\_key" : "1ad6f0705"  |
| "sdkKey" : "rFibt6NkalDrcQ7r4XaLaXW-l67\_XxiX8pRdTdvRhgaoDE4GksdRBd8usUU9yopJ4V0cHLVDB9wDz0EN9inRgM"  |
| "stripe\_failure\_reason\_authentication" : "We are unable to authenticate your payment method. Please choose a different payment method and try again."  |

## **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 |
| --- | --- | --- | --- |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.applovin.array.apphub.permission.BIND\_APPHUB\_SERVICE | 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 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.google.firebase.auth.internal.GenericIdpActivity | **Schemes**: genericidp://, **Hosts:** firebase.auth, **Paths:** /,  |
| com.google.firebase.auth.internal.RecaptchaActivity | **Schemes**: recaptcha://, **Hosts:** firebase.auth, **Paths:** /,  |

**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。**