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

**Ant Messenger（ 2.0.40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 | Ant Messenger |
| 版本 | 2.0.40 |
| 包名 | com.yxim.ant |
| 域名线索 | 85条 |
| URL线索 | 51条 |
| APP图标 |  |
| 分析日期 | 2025年5月23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 | Ant Messenger\_092838.apk |
| 文件大小 | 132.29MB |
| MD5值 | 9a43dcc9626a570329e11243ee8285f7 |
| SHA1值 | e3b276046860986fb6b81908530ffcac9502babe |
| SHA256值 | fd74cd72a41d829196a12f2e9577d4cc39bd4dc586ab28bf6750358ede003a2f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Ant Messenger |
| 包名 | com.yxim.ant |
| 主活动Activity | org.thoughtcrime.securesms.ant\_main.AntSplashActivity |
| 安卓版本名称 | 2.0.40 |
| 安卓版本 | 1040 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.backup.signal.org | IP: 162.125.1.8  所属国家: United States of America  地区: California  城市: San Francisco |
| support.ant.org | 没有服务器地理信息. |
| rttgpsreport.map.qq.com | IP: 60.28.215.105  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.google.com.qa | IP: 31.13.94.37  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| signal.art | IP: 104.21.91.110  所属国家: United States of America  地区: California  城市: San Francisco |
| maps.googleapis.com | IP: 142.251.215.234  所属国家: United States of America  地区: California  城市: Mountain View |
| config.mapbox.com | IP: 34.254.129.133  所属国家: Ireland  地区: Dublin  城市: Dublin |
| ant.org | IP: 31.222.223.91  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Farnborough |
| signalcaptchas.org | IP: 104.18.25.215  所属国家: United States of America  地区: California  城市: San Francisco |
| api.mapbox.com | IP: 3.165.11.27  所属国家: United States of America  地区: Washington  城市: Seattle |
| 34.150.36.70 | IP: 34.150.36.70  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| mkkcff.xyz | 没有服务器地理信息. |
| cdn.sstatic.net | IP: 104.18.40.222  所属国家: United States of America  地区: California  城市: San Francisco |
| www.google.com | IP: 31.13.94.49  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 13.212.123.138 | IP: 13.212.123.138  所属国家: Singapore  地区: Singapore  城市: Singapore |
| sfu.staging.voip.signal.org | IP: 4.78.139.50  所属国家: United States of America  地区: New Jersey  城市: Newark |
| xmlpull.org | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| 34.96.135.36 | IP: 34.96.135.36  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| magic.google.com | 没有服务器地理信息. |
| maps.google.com | IP: 142.250.217.78  所属国家: United States of America  地区: California  城市: Mountain View |
| open.scdn.co | 没有服务器地理信息. |
| cloudfront-staging.tilestream.net | IP: 3.164.110.121  所属国家: United States of America  地区: Washington  城市: Seattle |
| signal.org | IP: 104.244.46.57  所属国家: United States of America  地区: California  城市: San Francisco |
| antchat.com | IP: 43.134.117.145  所属国家: Singapore  地区: Singapore  城市: Singapore |
| sfu.test.voip.signal.org | IP: 74.86.142.55  所属国家: United States of America  地区: Texas  城市: Dallas |
| android.clients.google.com | IP: 142.251.33.78  所属国家: Canada  地区: Ontario  城市: Toronto |
| othstr.beacon.qq.com | IP: 140.206.162.29  所属国家: China  地区: Shanghai  城市: Shanghai |
| apps.mapbox.com | IP: 3.166.205.110  所属国家: United States of America  地区: Washington  城市: Seattle |
| cs.map.qq.com | IP: 125.36.181.143  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.mapbox.com | IP: 146.75.40.143  所属国家: Sweden  地区: Vastra Gotalands lan  城市: Goeteborg |
| cdn2.signal.org | IP: 199.59.150.40  所属国家: United States of America  地区: California  城市: San Francisco |
| events.mapbox.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| clients3.google.com | IP: 142.251.33.110  所属国家: Canada  地区: Ontario  城市: Toronto |
| api.stripe.com | IP: 52.196.95.231  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.google.com.ua | IP: 157.240.20.18  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| debuglogs.org | IP: 107.20.183.188  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| 2tndo.xyz | 没有服务器地理信息. |
| cdsi.staging.signal.org | IP: 104.244.46.21  所属国家: United States of America  地区: California  城市: San Francisco |
| otheve.beacon.qq.com | IP: 113.56.189.242  所属国家: China  地区: Hubei  城市: Huangshi |
| api.zebhkws.info | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| inbox.google.com | IP: 142.251.33.101  所属国家: Canada  地区: Ontario  城市: Toronto |
| global-at.oss-accelerate.aliyuncs.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| play.google.com | IP: 142.251.211.238  所属国家: United States of America  地区: California  城市: Mountain View |
| storage.signal.org | IP: 50.23.209.199  所属国家: United States of America  地区: California  城市: San Jose |
| h.trace.qq.com | IP: 113.56.189.162  所属国家: China  地区: Hubei  城市: Huangshi |
| antchats.app | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| lbs-trpc.map.qq.com | IP: 116.130.224.82  所属国家: China  地区: Beijing  城市: Beijing |
| confinfo.map.qq.com | IP: 116.130.223.83  所属国家: China  地区: Beijing  城市: Beijing |
| corssdk.map.qq.com | IP: 116.130.220.65  所属国家: China  地区: Beijing  城市: Beijing |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| clients4.google.com | IP: 142.251.33.110  所属国家: Canada  地区: Ontario  城市: Toronto |
| www.mobilecoin.com | IP: 4.174.241.162  所属国家: Canada  地区: Ontario  城市: Toronto |
| api-events-staging.tilestream.net | IP: 44.224.1.201  所属国家: United States of America  地区: Oregon  城市: Boardman |
| mt.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| cdn.signal.org | IP: 108.160.162.115  所属国家: United States of America  地区: California  城市: San Francisco |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| apis.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| api.antkyol.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| api.giphy.com | IP: 108.160.166.148  所属国家: United States of America  地区: California  城市: San Francisco |
| sfu.voip.signal.org | IP: 157.240.2.50  所属国家: United States of America  地区: California  城市: Menlo Park |
| lbs6.map.qq.com | IP: 125.36.181.163  所属国家: China  地区: Tianjin  城市: Tianjin |
| lstest.map.qq.com | IP: 116.130.223.83  所属国家: China  地区: Beijing  城市: Beijing |
| api.lqosgc.xyz | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| www.google.com.eg | IP: 162.125.32.6  所属国家: United States of America  地区: California  城市: San Francisco |
| www.slf4j.org | IP: 159.100.250.151  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| testdatalbs.sparta.html5.qq.com | IP: 157.255.4.30  所属国家: China  地区: Guangdong  城市: Guangzhou |
| api-events-config-staging.tilestream.net | IP: 98.82.225.215  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| nlp.map.qq.com | IP: 116.130.220.102  所属国家: China  地区: Beijing  城市: Beijing |
| docs.mapbox.com | IP: 3.171.198.76  所属国家: United States of America  地区: Washington  城市: Seattle |
| pinterest.com | IP: 202.160.130.52  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.google.ae | IP: 199.59.148.106  所属国家: United States of America  地区: California  城市: San Francisco |
| api.directory.signal.org | IP: 103.252.115.169  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.google.co.uz | IP: 192.133.77.197  所属国家: United States of America  地区: California  城市: San Francisco |
| pay.google.com | IP: 142.250.107.92  所属国家: United States of America  地区: California  城市: Mountain View |
| analytics.map.qq.com | IP: 125.36.181.142  所属国家: China  地区: Tianjin  城市: Tianjin |
| updates2.signal.org | IP: 88.191.249.182  所属国家: France  地区: Ile-de-France  城市: Paris |
| www.redditstatic.com | IP: 151.101.89.140  所属国家: United States of America  地区: California  城市: San Francisco |
| 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.google.com.om | IP: 108.160.169.186  所属国家: United States of America  地区: California  城市: San Francisco |
| signal.tube | IP: 104.18.19.175  所属国家: United States of America  地区: California  城市: San Francisco |
| github.githubassets.com | IP: 185.199.108.154  所属国家: United States of America  地区: Pennsylvania  城市: California |
| signal.group | IP: 104.18.26.114  所属国家: United States of America  地区: California  城市: San Francisco |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://rttgpsreport.map.qq.com/report | c/t/m/g/g3.java |
| https://cs.map.qq.com/key | c/t/m/g/g3.java |
| https://analytics.map.qq.com/ | c/t/m/g/g3.java |
| https://analytics.map.qq.com/tr | c/t/m/g/g3.java |
| https://nlp.map.qq.com/ | c/t/m/g/g3.java |
| https://lbs6.map.qq.com/k | c/t/m/g/g3.java |
| https://lbs6.map.qq.com/loc | c/t/m/g/g3.java |
| https://lbs-trpc.map.qq.com/k | c/t/m/g/g3.java |
| https://mt.map.qq.com/key | c/t/m/g/g3.java |
| https://corssdk.map.qq.com/key | c/t/m/g/g3.java |
| https://lstest.map.qq.com/nlpdr?sf | c/t/m/g/l.java |
| https://testdatalbs.sparta.html5.qq.com/tr?sf | c/t/m/g/l.java |
| https://testdatalbs.sparta.html5.qq.com/tr?wf4 | c/t/m/g/j.java |
| https://testdatalbs.sparta.html5.qq.com/tr?utr | c/t/m/g/i.java |
| https://apis.map.qq.com/ws/geocoder/v1/?location= | c/t/m/g/i5.java |
| http://xmlpull.org/v1/doc/features.html | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/features/external-general-entities | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/features/external-parameter-entities | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/properties/lexical-handler | com/caverock/androidsvg/SVGParser.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| https://docs.mapbox.com/android/maps/guides/user-location/ | com/mapbox/common/location/IncompatibleGooglePlayServicesLocationVersion.java |
| https://docs.mapbox.com/android/maps/guides/user-location/ | com/mapbox/common/location/IncompatibleGooglePlayServicesActivityRecognitionVersion.java |
| https://api.mapbox.com/sdk-sessions/v1 | com/mapbox/common/module/okhttp/MapboxOkHttpService.java |
| https://events.mapbox.com | com/mapbox/common/module/okhttp/MapboxOkHttpService.java |
| https://config.mapbox.com | com/mapbox/common/module/okhttp/MapboxOkHttpService.java |
| https://api-events-staging.tilestream.net | com/mapbox/common/module/okhttp/MapboxOkHttpService.java |
| https://api-events-config-staging.tilestream.net | com/mapbox/common/module/okhttp/MapboxOkHttpService.java |
| https://cloudfront-staging.tilestream.net | com/mapbox/common/module/okhttp/MapboxOkHttpService.java |
| https://www.mapbox.com/help/create-api-access-token/ | com/mapbox/maps/MapboxConfigurationException.java |
| https://www.mapbox.com/help/first-steps-android-sdk/ | com/mapbox/maps/MapboxConfigurationException.java |
| https://apps.mapbox.com/feedback | com/mapbox/maps/plugin/MapAttributionDelegateImpl.java |
| https://www.mapbox.com/about/maps/ | com/mapbox/maps/plugin/attribution/Attribution.java |
| https://www.mapbox.com/telemetry/ | com/mapbox/maps/plugin/attribution/Attribution.java |
| https://www.mapbox.com/legal/privacy | com/mapbox/maps/plugin/attribution/Attribution.java |
| https://www.mapbox.com/feedback/ | com/mapbox/maps/attribution/AttributionParser.java |
| https://www.mapbox.com/map-feedback/ | com/mapbox/maps/attribution/AttributionParser.java |
| https://apps.mapbox.com/feedback/ | com/mapbox/maps/attribution/AttributionParser.java |
| https://api.mapbox.com | com/mapbox/search/SearchEngineSettings.java |
| https://confinfo.map.qq.com/confinfo? | com/tencent/mapsdk/internal/rm.java |
| https://apis.map.qq.com/ws/ | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/distance/v1/matrix | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/district/v1/getchildren | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/district/v1/list | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/district/v1/search | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/place/v1/explore | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/customapi/mobike/geocoder | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/geocoder/v1 | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/streetview/v1/getpano | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/direction/v1/bicycling | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/direction/v1/driving | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/direction/v1/transit | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/direction/v1/trucking | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/direction/v1/walking | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/place/v1/detail | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/place/v1/search | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/place/v1/suggestion | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://apis.map.qq.com/ws/coord/v1/translate | com/tencent/lbssearch/httpresponse/UrlConstant.java |
| https://h.trace.qq.com/kv | com/tencent/tmsbeacon/a/b/d.java |
| https://otheve.beacon.qq.com/analytics/v2\_upload | com/tencent/tmsbeacon/base/net/b/b.java |
| https://othstr.beacon.qq.com/analytics/v2\_upload | com/tencent/tmsbeacon/base/net/b/b.java |
| http://apache.org/xml/features/disallow-doctype-decl | ezvcard/util/XmlUtils.java |
| http://xml.org/sax/features/external-general-entities | ezvcard/util/XmlUtils.java |
| http://xml.org/sax/features/external-parameter-entities | ezvcard/util/XmlUtils.java |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | ezvcard/util/XmlUtils.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/rxjava3/exceptions/UndeliverableException.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Maybe.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Flowable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Observable.java |
| https://api.stripe.com/v1 | org/signal/donations/StripeApi$Configuration.java |
| https://updates2.signal.org/static/badges/ | org/thoughtcrime/securesms/BuildConfig.java |
| https://signalcaptchas.org/challenge/generate.html | org/thoughtcrime/securesms/BuildConfig.java |
| https://signalcaptchas.org/registration/generate.html | org/thoughtcrime/securesms/BuildConfig.java |
| https://cdn2.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| https://cdn.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| https://cdsi.staging.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| https://api.directory.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| https://api.backup.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| https://sfu.voip.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| http://13.212.123.138:18090 | org/thoughtcrime/securesms/BuildConfig.java |
| https://storage.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| https://sfu.test.voip.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| https://sfu.staging.voip.signal.org | org/thoughtcrime/securesms/BuildConfig.java |
| http://antchat.com/migrate/msgRecord? | org/thoughtcrime/securesms/ant\_setting/ant\_migration\_record/AntMigrationRecordDeviceQRCode.java |
| https://signal.org | org/thoughtcrime/securesms/components/qr/QrView.java |
| https://maps.google.com/maps | org/thoughtcrime/securesms/components/location/SignalPlace.java |
| http://xmlpull.org/v1/doc/features.html | org/thoughtcrime/securesms/database/XmlBackup.java |
| https://signal.group/ | org/thoughtcrime/securesms/groups/v2/GroupInviteLinkUrl.java |
| https://debuglogs.org | org/thoughtcrime/securesms/logsubmit/SubmitDebugLogRepository.java |
| https://debuglogs.org/ | org/thoughtcrime/securesms/logsubmit/SubmitDebugLogRepository.java |
| http://www.google.com/oha/rdf/ua-profile-kila.xml | org/thoughtcrime/securesms/mms/LegacyMmsConnection.java |
| http://magic.google.com | org/thoughtcrime/securesms/mms/LegacyMmsConnection.java |
| https://signal\\.art/addstickers/ | org/thoughtcrime/securesms/stickers/StickerUrl.java |
| https://signal.art/addstickers/ | org/thoughtcrime/securesms/stickers/StickerUrl.java |
| https://play.google.com/store/apps/details?id= | org/thoughtcrime/securesms/util/PlayStoreUtil.java |
| https://antchats.app | org/thoughtcrime/securesms/util/AntCheckAddressTool.java |
| https://mkkcff.xyz | org/thoughtcrime/securesms/util/AntCheckAddressTool.java |
| https://signal.tube/ | org/thoughtcrime/securesms/util/SignalProxyUtil.java |
| https://api.giphy.com/v1/gifs/ | org/thoughtcrime/securesms/giph/mp4/GiphyMp4PagedDataSource.java |
| http://maps.googleapis.com/maps/api/staticmap? | org/thoughtcrime/securesms/ant\_photo\_album/GetStaticMapHelper.java |
| https://apis.map.qq.com/ws/staticmap/v2/? | org/thoughtcrime/securesms/ant\_photo\_album/GetStaticMapHelper.java |
| https://api.mapbox.com/styles/v1/mapbox/streets-v12/static/ | org/thoughtcrime/securesms/ant\_photo\_album/GetStaticMapHelper.java |
| https://maps.googleapis.com/maps/api/place/nearbysearch/json?location=%s,%s&radius=1000&key=%s&language=%s&keyword=%s | org/thoughtcrime/securesms/ant\_photo\_album/PhotoAlbumFragment.java |
| https://maps.googleapis.com/maps/api/place/nearbysearch/json?location=%s,%s&radius=1000&key=%s&language=%s | org/thoughtcrime/securesms/ant\_photo\_album/AntPlacePickerFragment.java |
| https://api.zebhkws.info | org/thoughtcrime/securesms/ant\_api/HttpHelperRetrofitImpl.java |
| https://api.antkyol.com | org/thoughtcrime/securesms/ant\_api/HttpHelperRetrofitImpl.java |
| https://api.lqosgc.xyz | org/thoughtcrime/securesms/ant\_api/HttpHelperRetrofitImpl.java |
| https://global-at.oss-accelerate.aliyuncs.com/sealing1.txt | org/thoughtcrime/securesms/ant\_api/HttpHelperRetrofitImpl.java |
| http://34.96.135.36:8080 | org/thoughtcrime/securesms/ant\_api/HttpHelperRetrofitImpl.java |
| https://2tndo.xyz | org/thoughtcrime/securesms/ant\_api/HttpHelperRetrofitImpl.java |
| http://34.150.36.70:9000/firewall/sealing1.txt | org/thoughtcrime/securesms/ant\_api/HttpHelperRetrofitImpl.java |
| https://www.google.com | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://android.clients.google.com | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://clients3.google.com | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://clients4.google.com | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://inbox.google.com | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://cdn.sstatic.net | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://github.githubassets.com | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://pinterest.com | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://open.scdn.co | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://www.redditstatic.com | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://www.google.com.eg | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://www.google.ae | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://www.google.com.om | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://www.google.com.qa | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://www.google.co.uz | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://www.google.com.ua | org/thoughtcrime/securesms/push/SignalServiceNetworkAccess.java |
| https://t.me/ | org/thoughtcrime/securesms/ant\_constant/AntConstants.java |
| https://updates2.signal.org | org/thoughtcrime/securesms/s3/S3.java |
| http://www.slf4j.org/codes.html | org/slf4j/LoggerFactory.java |
| https://support.ant.org/hc/articles/360007059792 | 摸瓜V1引擎 |
| https://ant.org/blog/sealed-sender | 摸瓜V1引擎 |
| https://support.ant.org/hc/articles/360057625692 | 摸瓜V1引擎 |
| https://support.ant.org/hc/articles/360007459591 | 摸瓜V1引擎 |
| https://support.ant.org/hc/articles/360007318591 | 摸瓜V1引擎 |
| https://support.ant.org | 摸瓜V1引擎 |
| https://www.mobilecoin.com/terms-of-use.html | 摸瓜V1引擎 |
| https://support.ant.org/hc/articles/360007059752 | 摸瓜V1引擎 |
| https://ant.org/donate | 摸瓜V1引擎 |
| https://support.ant.org/hc/articles/4408365318426 | 摸瓜V1引擎 |
| https://pay.google.com | 摸瓜V1引擎 |
| https://ant.org/install | 摸瓜V1引擎 |
| https://github.com/vinc3m1 | 摸瓜V1引擎 |
| https://github.com/vinc3m1/RoundedImageView | 摸瓜V1引擎 |
| https://github.com/vinc3m1/RoundedImageView.git | 摸瓜V1引擎 |
| https://www.mapbox.com/telemetry/ | 摸瓜V1引擎 |
| https://docs.mapbox.com/help/getting-started/attribution/ | 摸瓜V1引擎 |
| https://www.mapbox.com/legal/tos | 摸瓜V1引擎 |
| https://support.ant.org/hc/articles/360055276112 | 摸瓜V1引擎 |
| https://support.ant.org/ | 摸瓜V1引擎 |
| https://ant.org/legal | 摸瓜V1引擎 |
| https://ant.org/redirect/safety-numbers>Learn | 摸瓜V1引擎 |
| https://ant.org/redirect/safety-numbers> | 摸瓜V1引擎 |
| https://( | 摸瓜V1引擎 |
| https://api.mapbox.com | lib/arm64-v8a/libSearchCore.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| poi\_icon@2x.png  poi\_icon\_indoor\_ex@2x.png  icon\_indoor\_ex\_night@2x.png | com/tencent/mapsdk/internal/er.java |
| icon\_head\_logo@3x.png | org/thoughtcrime/securesms/components/AntAvatarImageView.java |
| support@signal.org | org/thoughtcrime/securesms/logsubmit/SubmitDebugLogActivity.java |
| icon\_head\_logo@3x.png | org/thoughtcrime/securesms/notifications/v2/NotificationExtensionsKt.java |
| zant94725@gmail.com | org/thoughtcrime/securesms/ant\_constant/AntConstants.java |
| support@ant.org | 摸瓜V1引擎 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | com/caverock/androidsvg/SVGParser.java |
| 17179869184 | com/caverock/androidsvg/SVGAndroidRenderer.java |
| 15552000000 | org/thoughtcrime/securesms/ant\_setting/ant\_privacy\_security/AntPrivacySecurityActivity.java |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=aaa, ST=aaa, L=aaa, O=aaa, OU=aaa, CN=aaa 签名算法: rsassa\_pkcs1v15 有效期自: 2018-10-12 09:20:27+00:00 有效期至: 2043-10-06 09:20:27+00:00 发行人: C=aaa, ST=aaa, L=aaa, O=aaa, OU=aaa, CN=aaa 序列号: 0x11fbb8ce 哈希算法: sha256 md5值: 3998613f312f5d49971a507743ddccb9 sha1值: 0d7e2addc5f0d0b737acc96276092ba28e1e3186 sha256值: 479c8e4b145862b4816153c30df699c32355ac98e1f440450da893da22f77e45 sha512值: 3eaff5618a52bd46dd1d15846e2de0c228955791f5c62c06da906a50db3b325471c5129d84a34a9ac963f7d192ec5b65750371e45b658c67999129171ec6b707 公钥算法: rsa 密钥长度: 2048 指纹: 80c81a7690353d02efc58a60aa273b33edbbda16c7e158e77208dbdcfe87cf24**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "ContactSelectionListFragment\_s\_is\_not\_a\_signal\_user" : "%1$s is not a Ant user. Please check the username and try again." |
| "DecryptionFailedDialog\_chat\_session\_refreshed" : "Chat session refreshed" |
| "EditPrivateStoryNameFragment\_\_edit\_story\_name" : "Edit story name" |
| "EditPrivateStoryNameFragment\_\_save" : "Save" |
| "EditPrivateStoryNameFragment\_\_story\_name" : "Story name" |
| "GroupManagement\_invite\_single\_user" : "“%1$s” can’t be automatically added to this group by you. They’ve been invited to join, and won’t see any group messages until they accept." |
| "MAPS\_QQ\_API\_KEY" : "NI5BZ-QXEEA-ASCKU-CIX3C-PV4ME-6UBFV" |
| "ManageProfileFragment\_username" : "Username" |
| "ManageProfileFragment\_your\_username" : "Your username" |
| "PrivateStorySettingsFragment\_\_add\_viewer" : "Add viewer" |
| "PrivateStorySettingsFragment\_\_are\_you\_sure" : "Are you sure?" |
| "PrivateStorySettingsFragment\_\_delete\_private\_story" : "Delete private story" |
| "PrivateStorySettingsFragment\_\_remove" : "Remove" |
| "PrivateStorySettingsFragment\_\_remove\_s" : "Remove %1$s?" |
| "StoryGroupReplyItem\_\_private\_reply" : "Private Reply" |
| "StoryReplyComposer\_\_replying\_privately\_to\_s" : "Replying privately to %1$s" |
| "StorySettingsFragment\_\_private\_stories" : "Private stories" |
| "StorySettingsFragment\_\_private\_stories\_can\_only\_be\_viewed" : "Private stories can only be viewed by the people you add to them. Only you can see the story name." |
| "ThreadRecord\_chat\_session\_refreshed" : "Chat session refreshed" |
| "ThreadRecord\_secure\_session\_reset" : "Secure session reset." |
| "UsernameEditFragment\_successfully\_removed\_username" : "Successfully removed username." |
| "UsernameEditFragment\_successfully\_set\_username" : "Successfully set username." |
| "UsernameEditFragment\_username" : "Username" |
| "ant\_GenerateIentityKey" : "Generate idk error" |
| "ant\_HW\_ACCOUNT\_AUTH\_NOT\_FOUND" : "Account not found" |
| "ant\_HW\_ACCOUNT\_DEVICE\_AUTH\_FAILD" : "Permission authentication failed" |
| "ant\_HW\_ACCOUNT\_DEVICE\_AUTH\_NOT\_FOUND" : "Device not found" |
| "ant\_authorization" : "Authorization" |
| "ant\_authorize" : "Settings" |
| "ant\_authorized\_login" : "Authorized login" |
| "ant\_authorized\_login\_fail" : "Authorized login failed" |
| "ant\_authorized\_login\_successfully" : "Authorized login successfully" |
| "ant\_copy\_username" : "Copy username" |
| "ant\_debug\_remove\_prekey" : "Remove local prekey" |
| "ant\_details\_security\_key" : "Security key" |
| "ant\_double\_ratchet\_dynamic\_key" : "double ratchet dynamic key" |
| "ant\_download\_setting\_media\_type\_details\_private\_chat" : "Private chat" |
| "ant\_group\_add\_user" : "Add user" |
| "ant\_group\_search\_for\_a\_contact\_or\_username" : "Search for a contact or username" |
| "ant\_lock\_screen\_password" : "Lock screen password" |
| "ant\_lock\_unlock\_password" : "%s unlock password" |
| "ant\_proxy\_auth\_label" : "Authentication information (optional)" |
| "ant\_proxy\_auth\_password" : "password" |
| "ant\_proxy\_auth\_username" : "username" |
| "ant\_recent\_online\_add\_user" : "Add user" |
| "ant\_reset\_password" : "Reset password" |
| "ant\_setting\_add\_user" : "Add account" |
| "ant\_setting\_copy\_user\_name" : "Copy user name" |
| "ant\_setting\_manage\_profile\_check\_user\_name" : "Checking username" |
| "ant\_setting\_manage\_profile\_user\_name" : "Your username" |
| "ant\_setting\_user\_name" : "Username" |
| "conversation\_secure\_verified\_\_menu\_reset\_secure\_session" : "Reset secure session" |
| "google\_api\_key" : "AIzaSyAAQ8SwvozItBvBFP0Uv47TgzwlwYimlYs" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAAQ8SwvozItBvBFP0Uv47TgzwlwYimlYs" |
| "library\_roundedimageview\_author" : "Vince Mi" |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1" |
| "mapbox\_access\_token" : "pk.eyJ1IjoiZ2diYW5kcGlnMSIsImEiOiJjbG95MGIxbmUxY2s3Mmpwa29lYWc5azU3In0.j4DqwpUqaqNfU0cRhXC9Gg" |
| "preferences\_\_internal\_delete\_session" : "Delete Session" |
| "preferences\_\_internal\_rotate\_profile\_key" : "Rotate profile key" |
| "preferences\_\_internal\_sender\_key" : "Sender Key" |
| "preferences\_\_mmsc\_password" : "MMSC Password" |
| "preferences\_\_mmsc\_username" : "MMSC Username" |
| "preferences\_setup\_a\_username" : "Setup a username" |
| "ContactSelectionListFragment\_s\_is\_not\_a\_signal\_user" : ""%1$s"不是 Ant 使用者。請檢查使用者名稱並再試一次。" |
| "DecryptionFailedDialog\_chat\_session\_refreshed" : "聊天會話已刷新" |
| "EditPrivateStoryNameFragment\_\_edit\_story\_name" : "編輯限時動態名稱" |
| "EditPrivateStoryNameFragment\_\_save" : "儲存" |
| "EditPrivateStoryNameFragment\_\_story\_name" : "限時動態名稱" |
| "GroupManagement\_invite\_single\_user" : "「%1$s」不能由你自動新增到此群組中。 他們已獲邀請加入，並且在他們接受之前不會看到任何群組訊息。" |
| "ManageProfileFragment\_username" : "使用者名稱" |
| "ManageProfileFragment\_your\_username" : "你的使用者名稱" |
| "PrivateStorySettingsFragment\_\_add\_viewer" : "新增觀看者" |
| "PrivateStorySettingsFragment\_\_are\_you\_sure" : "你確定嗎？" |
| "PrivateStorySettingsFragment\_\_delete\_private\_story" : "刪除個人限時動態" |
| "PrivateStorySettingsFragment\_\_remove" : "移除" |
| "PrivateStorySettingsFragment\_\_remove\_s" : "要移除 %1$s嗎？" |
| "StoryGroupReplyItem\_\_private\_reply" : "私下回覆" |
| "StoryReplyComposer\_\_replying\_privately\_to\_s" : "正在私下回覆 %1$s" |
| "StorySettingsFragment\_\_private\_stories" : "個人限時動態" |
| "StorySettingsFragment\_\_private\_stories\_can\_only\_be\_viewed" : "私人限時動態只能由你加入的人能看。 只有你可以看到限時動態名稱。" |
| "ThreadRecord\_chat\_session\_refreshed" : "聊天會話已刷新" |
| "ThreadRecord\_secure\_session\_reset" : "安全對話已重設" |
| "UsernameEditFragment\_successfully\_removed\_username" : "成功移除使用者名稱。" |
| "UsernameEditFragment\_successfully\_set\_username" : "成功設定使用者名稱。" |
| "UsernameEditFragment\_username" : "使用者名稱" |
| "ant\_GenerateIentityKey" : "產生idk錯誤" |
| "ant\_HW\_ACCOUNT\_AUTH\_NOT\_FOUND" : "找不到賬戶" |
| "ant\_HW\_ACCOUNT\_DEVICE\_AUTH\_FAILD" : "權限鑑定失敗" |
| "ant\_HW\_ACCOUNT\_DEVICE\_AUTH\_NOT\_FOUND" : "找不到設備" |
| "ant\_authorization" : "授權" |
| "ant\_authorize" : "設置" |
| "ant\_authorized\_login" : "授權登錄" |
| "ant\_authorized\_login\_fail" : "授權登錄失敗" |
| "ant\_authorized\_login\_successfully" : "授權登錄成功" |
| "ant\_copy\_username" : "複製用戶名" |
| "ant\_debug\_remove\_prekey" : "移除本地端的prekey" |
| "ant\_details\_security\_key" : "安全密匙" |
| "ant\_double\_ratchet\_dynamic\_key" : "雙棘輪動態密匙" |
| "ant\_download\_setting\_media\_type\_details\_private\_chat" : "私聊" |
| "ant\_group\_add\_user" : "新增用戶" |
| "ant\_group\_search\_for\_a\_contact\_or\_username" : "搜尋聯絡人或使用者名稱" |
| "ant\_lock\_screen\_password" : "鎖屏密碼" |
| "ant\_lock\_unlock\_password" : "%s位解鎖密碼" |
| "ant\_proxy\_auth\_label" : "認證資訊（可選）" |
| "ant\_proxy\_auth\_password" : "密碼" |
| "ant\_proxy\_auth\_username" : "使用者名稱" |
| "ant\_recent\_online\_add\_user" : "添加用戶" |
| "ant\_reset\_password" : "重置密碼" |
| "ant\_setting\_add\_user" : "添加賬戶" |
| "ant\_setting\_copy\_user\_name" : "複製用戶名" |
| "ant\_setting\_manage\_profile\_check\_user\_name" : "正在檢查用戶名" |
| "ant\_setting\_manage\_profile\_user\_name" : "您的用戶名" |
| "ant\_setting\_user\_name" : "用戶名" |
| "conversation\_secure\_verified\_\_menu\_reset\_secure\_session" : "重設安全對話" |
| "preferences\_\_mmsc\_password" : "MMSC 密碼" |
| "preferences\_\_mmsc\_username" : "MMSC 使用者名稱" |
| "preferences\_setup\_a\_username" : "設定使用者名稱" |
| "ContactSelectionListFragment\_s\_is\_not\_a\_signal\_user" : "'%1$s' 님은 Ant 사용자가 아니니 사용자명 확인후 다시 시도하시기 바랍니다." |
| "DecryptionFailedDialog\_chat\_session\_refreshed" : "채팅기록이 새로고침됨" |
| "EditPrivateStoryNameFragment\_\_save" : "저장" |
| "GroupManagement\_invite\_single\_user" : "“%1$s”님은 회원님의 요청에 의해 바로 그룹에 가입할수 없습니다. 상대방은 이미 그룹 요청을 접수했으나 동의하기 전까지 그룹내 정보를 확인할수 없습니다." |
| "ManageProfileFragment\_username" : "사용자명" |
| "ManageProfileFragment\_your\_username" : "회원님의 사용자명" |
| "PrivateStorySettingsFragment\_\_remove" : "제거" |
| "StorySettingsFragment\_\_private\_stories\_can\_only\_be\_viewed" : "비공개 스토리는 회원님께서 선택한 사용자만 볼 수 있으며 회원님만 스토리 명칭을 볼 수 있습니다." |
| "ThreadRecord\_chat\_session\_refreshed" : "대화 세션 새로 고침 완료" |
| "ThreadRecord\_secure\_session\_reset" : "보안 세션이 초기화되었습니다." |
| "UsernameEditFragment\_successfully\_removed\_username" : "아이디를 성공적으로 삭제했습니다。" |
| "UsernameEditFragment\_successfully\_set\_username" : "아이디 설정 완료" |
| "UsernameEditFragment\_username" : "아이디" |
| "ant\_GenerateIentityKey" : "IDK 생성 오류" |
| "ant\_HW\_ACCOUNT\_AUTH\_NOT\_FOUND" : "계정을 찾을 수 없음" |
| "ant\_HW\_ACCOUNT\_DEVICE\_AUTH\_FAILD" : "권한 검증 실패" |
| "ant\_HW\_ACCOUNT\_DEVICE\_AUTH\_NOT\_FOUND" : "기기를 찾을수 없음" |
| "ant\_authorization" : "권한 부여" |
| "ant\_authorize" : "설정" |
| "ant\_authorized\_login" : "로그인 권한 부여" |
| "ant\_authorized\_login\_fail" : "로그인 인증 실패" |
| "ant\_authorized\_login\_successfully" : "로그인 인증 성공" |
| "ant\_copy\_username" : "사용자명 복사" |
| "ant\_debug\_remove\_prekey" : "로컬 prekey 제거" |
| "ant\_details\_security\_key" : "보안키" |
| "ant\_double\_ratchet\_dynamic\_key" : "더블 래칫 다이내믹 키" |
| "ant\_download\_setting\_media\_type\_details\_private\_chat" : "개인 채팅" |
| "ant\_group\_add\_user" : "사용자 추가" |
| "ant\_group\_search\_for\_a\_contact\_or\_username" : "연락처 혹은 사용자명 검색" |
| "ant\_lock\_screen\_password" : "화면 잠금 암호" |
| "ant\_lock\_unlock\_password" : "%s자리 잠금해제 비밀번호" |
| "ant\_proxy\_auth\_label" : "인증 정보(옵션)" |
| "ant\_proxy\_auth\_password" : "비밀번호" |
| "ant\_proxy\_auth\_username" : "사용자명" |
| "ant\_recent\_online\_add\_user" : "사용자 추가" |
| "ant\_reset\_password" : "비밀번호 재설정" |
| "ant\_setting\_add\_user" : "계정 추가" |
| "ant\_setting\_copy\_user\_name" : "사용자명 복사" |
| "ant\_setting\_manage\_profile\_check\_user\_name" : "사용자명 점검중" |
| "ant\_setting\_manage\_profile\_user\_name" : "귀하의 사용자명" |
| "ant\_setting\_user\_name" : "사용자명" |
| "conversation\_secure\_verified\_\_menu\_reset\_secure\_session" : "보안 세션 초기화" |
| "preferences\_\_mmsc\_password" : "MMSC 암호" |
| "preferences\_\_mmsc\_username" : "MMSC 사용자명" |
| "preferences\_setup\_a\_username" : "사용자명 설정" |
| "ContactSelectionListFragment\_s\_is\_not\_a\_signal\_user" : "“%1$s”不是 Ant 用户，请检查用户名并重试。" |
| "DecryptionFailedDialog\_chat\_session\_refreshed" : "聊天会话已刷新" |
| "EditPrivateStoryNameFragment\_\_save" : "保存" |
| "GroupManagement\_invite\_single\_user" : "“%1$s”不能直接被您邀请入群。 对方已收到入群邀请，但在他同意入群前他将无法看到群消息。" |
| "ManageProfileFragment\_username" : "用户名" |
| "ManageProfileFragment\_your\_username" : "你的用户名" |
| "PrivateStorySettingsFragment\_\_remove" : "移除" |
| "StorySettingsFragment\_\_private\_stories\_can\_only\_be\_viewed" : "私密动态仅对您选中的用户可见。只有您能看见动态名称。" |
| "ThreadRecord\_chat\_session\_refreshed" : "聊天会话已刷新" |
| "ThreadRecord\_secure\_session\_reset" : "安全会话已重置。" |
| "UsernameEditFragment\_successfully\_removed\_username" : "成功移除用户名。" |
| "UsernameEditFragment\_successfully\_set\_username" : "成功设置用户名。" |
| "UsernameEditFragment\_username" : "用户名" |
| "ant\_GenerateIentityKey" : "生成idk错误" |
| "ant\_HW\_ACCOUNT\_AUTH\_NOT\_FOUND" : "找不到账户" |
| "ant\_HW\_ACCOUNT\_DEVICE\_AUTH\_FAILD" : "权限鉴定失败" |
| "ant\_HW\_ACCOUNT\_DEVICE\_AUTH\_NOT\_FOUND" : "找不到设备" |
| "ant\_authorization" : "授权" |
| "ant\_authorize" : "设置" |
| "ant\_authorized\_login" : "授权登录" |
| "ant\_authorized\_login\_fail" : "授权登录失败" |
| "ant\_authorized\_login\_successfully" : "授权登录成功" |
| "ant\_copy\_username" : "复制用户名" |
| "ant\_debug\_remove\_prekey" : "移除本地的prekey" |
| "ant\_details\_security\_key" : "安全密匙" |
| "ant\_double\_ratchet\_dynamic\_key" : "双棘轮动态密匙" |
| "ant\_download\_setting\_media\_type\_details\_private\_chat" : "私聊" |
| "ant\_group\_add\_user" : "添加用户" |
| "ant\_group\_search\_for\_a\_contact\_or\_username" : "搜索联系人或用户名" |
| "ant\_lock\_screen\_password" : "锁屏密码" |
| "ant\_lock\_unlock\_password" : "%s位解锁密码" |
| "ant\_proxy\_auth\_label" : "认证信息（可选）" |
| "ant\_proxy\_auth\_password" : "密码" |
| "ant\_proxy\_auth\_username" : "用户名" |
| "ant\_recent\_online\_add\_user" : "添加用户" |
| "ant\_reset\_password" : "重置密码" |
| "ant\_setting\_add\_user" : "添加账户" |
| "ant\_setting\_copy\_user\_name" : "复制用户名" |
| "ant\_setting\_manage\_profile\_check\_user\_name" : "正在检查用户名" |
| "ant\_setting\_manage\_profile\_user\_name" : "您的用户名" |
| "ant\_setting\_user\_name" : "用户名" |
| "conversation\_secure\_verified\_\_menu\_reset\_secure\_session" : "重置安全会话" |
| "preferences\_\_mmsc\_password" : "MMSC 密码" |
| "preferences\_\_mmsc\_username" : "MMSC 用户名" |
| "preferences\_setup\_a\_username" : "设置用户名" |

## **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**

## **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。**