



MoGua

MAX 12.0.0.APK 分析报告



APP名称:

MAX

包名:

com.maicoïn.max

| | |
|--------|----------------------------|
| 域名线索: | 43条 |
| URL线索: | 11条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2025年3月20日 |
| 分析平台: | 摸瓜APK反编译平台 |

文件信息

文件名: MAXExchangeBuyBitcoin.apk

文件大小: 42.48MB

MD5值: 5bfc72e49bb55dab4ac415e03a88ef0d

SHA1值: a1d66345005ac15f5cbaf179d5dc938c9eba1dd7

SHA256值: 5553992d41eb640da4225f547ac926e30715db695a253dc2bf13cf56f80dc9e5

i APP 信息

App名称: MAX

包名: com.maicoi.max

主活动Activity: com.maicoi.max.MainActivity

安卓版本名称: 12.0.0

安卓版本: 23060116

🔍 域名线索

| 域名 | 服务器信息 |
|------------------------------------|--|
| o169335.ingest.sentry.io | IP: 34.120.195.249 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568 |
| max-api.maicoi.com | IP: 108.160.169.179 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| instantmessaging-pa.googleapis.com | IP: 142.251.42.234 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 |
| growth-pa.googleapis.com | IP: 172.217.160.106 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 |

| | |
|----------------------------------|---|
| momentjs.com | IP: 104.16.32.155 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| react-native-vision-camera.com | IP: 76.76.21.164 所属国家: United States of America 地区: California 城市: Walnut 纬度: 34.015400 经度: -117.858223 |
| www.bouncycastle.org | IP: 203.32.61.103 所属国家: Australia 地区: Victoria 城市: Drouin 纬度: -38.136581 经度: 145.858383 |
| reactnavigation.org | IP: 172.67.166.222 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| dogs.are.greaterthanorequaltotal | 没有服务器地理信息. |
| max-stream-global.maicoi.com | IP: 31.13.67.19 所属国家: United States of America 地区: Florida 城市: Miami 纬度: 25.774269 经度: -80.193604 |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 |

| | |
|-------------------------------|---|
| | 经度: -94.578568 |
| be5invis.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724 |
| clientservices.googleapis.com | IP: 114.250.67.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102 |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281 |
| u.expo.dev | IP: 104.18.4.104 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| schemas.android.com | 没有服务器地理信息. |
| www.googleapis.com | IP: 142.251.42.234 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 |
| exp.host | IP: 34.110.201.56 所属国家: United States of America 地区: Missouri 城市: Kansas City |

| | |
|--------------------------------------|---|
| | 纬度: 39.099731 经度: -94.578568 |
| max.maico.in.com | IP: 52.175.9.80 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692 |
| firebaseinstallations.googleapis.com | IP: 172.217.163.42 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 |
| android.googleusercontent.com | IP: 108.177.125.82 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: 203.208.50.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102 |
| gmscompliance-pa.googleapis.com | IP: 172.217.163.42 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 |
| shopify.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 |

| | |
|--------------------------------------|---|
| | 经度: -79.891724 |
| region1.app-measurement.com | IP: 216.239.34.36 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 |
| docs.swmansion.com | IP: 172.67.142.188 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| max-app-ee84d.firebaseio.com | IP: 35.190.39.113 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568 |
| assets.eascdn.net | IP: 104.18.12.23 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| connectivitycheck.gstatic.com | IP: 203.208.50.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102 |
| react-native-async-storage.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 |

| | |
|---------------------------|---|
| classic-assets.eascdn.net | IP: 104.18.0.204 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| stackoverflow.com | IP: 172.64.155.249 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| scripts.sil.org | IP: 172.67.29.248 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| assets.maico.in.com | IP: 104.244.43.234 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446 |
| android.googleapis.com | IP: 142.251.42.234 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 |
| | IP: 185.199.111.153 |

| | |
|----------------------|--|
| xmlpull.org | 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724 |
| app-measurement.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 |
| xrpcharts.ripple.com | IP: 52.39.119.154 所属国家: United States of America 地区: Oregon 城市: Portland 纬度: 45.523460 经度: -122.676468 |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246 |
| bscscan.com | IP: 104.26.12.158 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 |
| invertase.link | IP: 52.21.33.16 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806 |
| | IP: 104.18.22.19 所属国家: United States of America |

www.w3.org

地区: California

城市: San Francisco

纬度: 37.775700

经度: -122.395203

URL线索

| URL信息 | Url所在文件 |
|---|--|
| http://www.w3.org/TR/SVG11/feature | com/caverock/androidsvg/SVGParser.java |
| http://www.w3.org/2000/svg | com/caverock/androidsvg/SVGParser.java |
| http://www.w3.org/1999/xlink | com/caverock/androidsvg/SVGParser.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 |
| https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenableroot | com/swmansion/gesturehandler/react/RNGestureRecognizerEnabledRootView.java |
| https://github.com/software-mansion/react-native-screens/issues/17 | com/swmansion/rnscreens/ScreenStackFragment.java |
| https://github.com/software-mansion/react-native-screens/issues/17 | com/swmansion/rnscreens/ScreenFragment.java |
| https://react-native-vision-camera.com/docs/guides/devices | com/mrousavy/camera/ParallelVideoProcessingNotSupportedError.java |
| https://shopify.github.io/flash-list/docs/usage | com/shopify/reactnative/flash_list/AutoLayoutView.java |
| https://github.com/expo/expo/tree/main/packages/expo-splash-screen | expo/modules/splashscreen/singletons/SplashScreen.java |
| https://exp.host/--/manifest-public-key | expo/modules/updates/loader/LegacySignatureUtilsKt.java |

| | |
|---|---|
| https://classic-assets.eascdn.net/ | expo/modules/updates/manifest/LegacyUpdateManifest.java |
| https://max-app-ee84d.firebaseio.com | 摸瓜V1引擎 |
| o169335.ingest.sentry.io | 摸瓜V3引擎 |
| max-api.maicoi.com | 摸瓜V3引擎 |
| https://shopify.github.io/flash-list/docs/usage#cellrendercomponent | 摸瓜V3引擎 |
| http://schemas.android.com/aapt | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| instantmessaging-pa.googleapis.com | 摸瓜V3引擎 |
| https://developer.mozilla.org/docs/Web/CSS/box-flex-groupsafari-web-extension:UnstakeMaxScreenpm | 摸瓜V3引擎 |
| https://xrpcharts.ripple.com/#/transactions/api/mobile/members/setting/yield_flagsmax_token:aprViewe | 摸瓜V3引擎 |
| growth-pa.googleapis.com | 摸瓜V3引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V3引擎 |
| http://xml.org/sax/features/external-parameter-entities | 摸瓜V3引擎 |
| http://%s/%s.%s?platform=android&dev=%s&minify=%s&app=%s&modulesOnly=%s&runModule=%s%s | 摸瓜V3引擎 |
| https://github.com/software-mansion/react-native-gesture-handler.github:facebook/react-native-gestur | 摸瓜V3引擎 |
| http://be5invis.github.io/losevkaThis | 摸瓜V3引擎 |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | 摸瓜V3引擎 |
| max-stream-global.maicoi.com | 摸瓜V3引擎 |
| http://dogs.are.greaterThanOrEqualTotal | 摸瓜V3引擎 |

| | |
|---|--------|
| http://xml.org/sax/properties/lexical-handler | 摸瓜V3引擎 |
| https://www.bouncycastle.org | 摸瓜V3引擎 |
| clientservices.googleapis.com | 摸瓜V3引擎 |
| http://momentjs.com/guides/#/warnings/add-inverted-param/ | 摸瓜V3引擎 |
| u.expo.dev | 摸瓜V3引擎 |
| http://xml.org/sax/features/external-general-entities | 摸瓜V3引擎 |
| www.googleapis.com | 摸瓜V3引擎 |
| firebaseinstallations.googleapis.com | 摸瓜V3引擎 |
| www.gstatic.com | 摸瓜V3引擎 |
| gmscompliance-pa.googleapis.com | 摸瓜V3引擎 |
| https://developer.mozilla.org/docs/Web/CSS/-ms-ime-alignItems | 摸瓜V3引擎 |
| region1.app-measurement.com | 摸瓜V3引擎 |
| https://github.com/react-native-community/react-native-netinfo | 摸瓜V3引擎 |
| https://developer.mozilla.org/docs/Web/CSS/table-layoutHeight https://developer.mozilla.org/docs/Web/CS | 摸瓜V3引擎 |
| https://developer.mozilla.org/docs/Web/CSS/mask-border-modetectFactoryAndVerify | 摸瓜V3引擎 |
| https://max-app-ee84d.firebaseio.com | 摸瓜V3引擎 |
| https://react-native-vision-camera.com/docs/guides/devices#the-supportsparallelvideoprocessing-prop | 摸瓜V3引擎 |
| https://bscscan.com/tx/api/mobile/max_token/exchange_rate-ios_backgroundColor | 摸瓜V3引擎 |
| https://reactnavigation.org/docs/configuring-links | 摸瓜V3引擎 |
| | |

| | |
|---|--------|
| assets.eascdn.net | 摸瓜V3引擎 |
| connectivitycheck.gstatic.com | 摸瓜V3引擎 |
| https://max.maico.in.com/docs/limits | 摸瓜V3引擎 |
| http://invertase.link/ios | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| https://react-native-async-storage.github.io/async-storage/docs/advanced/jest | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| https://docs.swmansion.com/react-native-gesture-handler/docs/#installationstripTrailingSlashouldCrea | 摸瓜V3引擎 |
| https://stackoverflow.com/q/5189914/28465 | 摸瓜V3引擎 |
| https://developer.mozilla.org/docs/Web/CSS/shape-image-thresholdFreedmanDiaconisAncestorInSet.protot | 摸瓜V3引擎 |
| https://reactnavigation.org/docs/nesting-navigators | 摸瓜V3引擎 |
| assets.maico.in.com | 摸瓜V3引擎 |
| android.googlesource.com | 摸瓜V3引擎 |
| app-measurement.com | 摸瓜V3引擎 |
| https://developer.mozilla.org/docs/Web/CSS/outline-offsetFromStringgetOperatoreplaceExistingNonRootVi | 摸瓜V3引擎 |
| http://scripts.sil.org/OFL | 摸瓜V3引擎 |
| http://xmlpull.org/v1/doc/features.html#process-docdecl | 摸瓜V3引擎 |
| https://github.com/react-native-async-storage/async-storage/issues | 摸瓜V3引擎 |

✉ 邮箱线索

☰ 手机线索

| 手机号 | 所在文件 |
|-------------|---|
| 17179869184 | com/caverock/androidsvg/SVGParser.java |
| 17179869184 | com/caverock/androidsvg/SVG.java |
| 17179869184 | com/caverock/androidsvg/SVGAndroidRenderer.java |
| 13222222222 | expo/modules/updates/UpdatesConfiguration.java |

☀ 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=Google Inc., OU=Android, CN=Android

签名算法: rsassa_pkcs1v15

有效期自: 2018-06-01 10:32:55+00:00

有效期至: 2048-06-01 10:32:55+00:00

发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

序列号: 0xeb0a916a0ab8c55adb28a7de08a3690bb5d4edd

哈希算法: sha256

md5值: 525530ac16213bb5119b2700034e9f78

sha1值: 74c4d03ba238dd67d71965d9b19cfa4edb3c66b4

sha256值: ddd6ffe39c395b89dc1efd0aea35d078ba7d7457900ec09cd4ee631afda279c7

sha512值: 18b2762049d2113519449c38376ca0769ef8c9e4bb79b55ce6f9bb01c54a72dac8016c1dc56fda3c9a7067bf7c75f3543e48bbfd45947a4c2958a3013703f4ea

公钥算法: rsa

密钥长度: 4096

指纹: 1088cd5aa831b322cf88b59de5f2c80ff5b0d18fe566041b70498341aec5cf

硬编码敏感信息

| |
|--|
| 可能的敏感信息 |
| "firebase_database_url" : "https://max-app-ee84d.firebaseio.com" |
| "google_api_key" : "AlzaSyACqu_14RrThzkC-I-To-Op7cBx53s8f2A" |
| "google_crash_reporting_api_key" : "AlzaSyACqu_14RrThzkC-I-To-Op7cBx53s8f2A" |

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

| | 是否危 | 类型 | 详细情况 |
|----------|-----|----|------|
| 向手机申请的权限 | | | |

| | 险 | | |
|---|----|--------------------|---|
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| 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.READ_EXTERNAL_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.READ_INTERNAL_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.SYSTEM_ALERT_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.USE_BIOMETRIC | 正常 | | 允许应用使用设备支持的生物识别模式。 |
| android.permission.USE_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.WRITE_EXTERNAL_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| 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.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 |
| 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.READ_MEDIA_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ_MEDIA_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

| | | | |
|--|----|--------------------|---|
| android.permission.POST_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.google.android.gms.permission.AD_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER_INSERT_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.CHANGE_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.huawei.android.launcher.permission.READ_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |

| | | | |
|---|----|--------------------|---|
| com.huawei.android.launcher.permission.WRITE_SETTINGS | 正常 | 示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| android.permission.READ_APP_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE_COUNT_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE_COUNT_WRITE | 未知 | Unknown permission | Unknown permission from android reference |

应用内通信

| 活动(ACTIVITY) | 通信(INTENT) |
|-----------------------------|---|
| com.maicoi.max.MainActivity | Schemes: max://, com.maicoi.max://, exp+max://, |

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。