



MoGua

Meta Seal 1.0.3.APK 分析报告



APP名称:

Meta Seal

包名:	com.startower.chian
域名线索:	49条
URL线索:	36条
邮箱线索:	6条
分析日期:	2025年7月5日
分析平台:	摸瓜APK反编译平台

文件名: 2hVTBWuYzANcY6m6.apk
文件大小: 96.6MB
MD5值: 7716f0ae93579db169be880b766910bb
SHA1值: 5d9a7820c12ae93a3aff2b784e1b199a2f06f87c
SHA256值: 7f1ca8ff3f332482ecc4ba108b4f1c0b7edcdcb7ebec4b6fb9e8233ec2c323f9

i APP 信息

App名称: Meta Seal
包名: com.startower.chian
主活动Activity: com.hdwallet.app.MainActivity
安卓版本名称: 1.0.3
安卓版本: 5

🔍 域名线索

域名	服务器信息
grs.dbankcloud.asia	IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api-ropsten.etherscan.io	IP: 31.13.86.21 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
	IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey

paulbakaus.com	城市: Clifton 纬度: 40.858585 经度: -74.163605
test-bootstrapprofile-c-1.oss-cn-beijing.aliyuncs.com	IP: 123.125.18.57 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
journeyapps.com	IP: 18.65.168.90 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
registry.npmjs.org	IP: 104.16.26.34 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
example.com	IP: 96.7.128.175 所属国家: United States of America 地区: California 城市: El Segundo 纬度: 33.919201 经度: -118.416580

dev.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api-rinkeby.etherscan.io	IP: 202.160.129.6 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
grs.dbankcloud.com	IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
api.trongrid.io	IP: 54.254.86.84 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271

	经度: -121.988571
play.google.com	IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig 纬度: 52.266121 经度: 10.526730
www.tronlink.org	IP: 162.125.32.6 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
grs.dbankcloud.eu	没有服务器地理信息.
www.gnu.org	IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville 纬度: 42.387600 经度: -71.099503
a.app.qq.com	IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
manger.tronlending.org	没有服务器地理信息.
developer.android.com	IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991

	经度: -122.078514
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
links.ethers.org	IP: 3.164.143.58 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
stats.cn.ronghub.com	IP: 47.94.172.98 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
stackoverflow.com	IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
test-bootstrapprofile-b-2.s3.ap-southeast-1.amazonaws.com	IP: 3.5.148.68 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
	IP: 123.125.102.202 所属国家: China

app.mi.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
sun.tronex.io	IP: 52.15.86.168 所属国家: United States of America 地区: Ohio 城市: Columbus 纬度: 39.961380 经度: -82.997749
www.example.com	IP: 173.222.248.144 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
api.etherscan.io	IP: 173.236.182.137 所属国家: United States of America 地区: California 城市: Brea 纬度: 33.930222 经度: -117.888420
api.devnet.solana.com	IP: 162.125.2.3 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

www.unicode.org	IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204
s3.amazonaws.com	IP: 16.15.177.108 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
feedback.rong-edge.com	IP: 47.93.244.185 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
infura.io	IP: 13.35.202.118 所属国家: India 地区: Telangana 城市: Hyderabad 纬度: 17.375290 经度: 78.474388
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
list.tronlink.org	IP: 162.125.7.1 所属国家: United States of America 地区: California 城市: San Francisco

	纬度: 37.775700 经度: -122.395203
www.google.com	IP: 31.13.106.4 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
api.mainnet-beta.solana.com	IP: 31.13.94.37 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
dartbug.com	IP: 216.239.38.21 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
api-goerli.etherscan.io	IP: 118.184.78.78 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
docs.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
	IP: 31.13.70.33 所属国家: United States of America

api.testnet.solana.com	地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
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
api-kovan.etherscan.io	IP: 199.59.150.40 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
web3.gastracker.io	没有服务器地理信息.
grs.dbankcloud.cn	IP: 124.70.116.153 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
cloudcontrol.rongcloud.net	IP: 47.94.224.40 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

URL信息	Url所在文件
https://github.com/Baseflow/flutter-permission-handler/issues	com/baseflow/permissionhandler/PermissionManager.java
https://a.app.qq.com/o/simple.jsp?pkgname=	com/example/r_upgrade/common/tasks/CheckTencentStoreVersionTask.java
https://app.mi.com/details?id=	com/example/r_upgrade/common/tasks/CheckXiaoMiStoreVersionTask.java
https://app.mi.com	com/example/r_upgrade/common/tasks/CheckXiaoMiStoreVersionTask.java
https://play.google.com/store/apps/details?id=	com/example/r_upgrade/common/tasks/CheckGooglePlayVersionTask.java
http://www.google.com	com/example/r_upgrade/common/tasks/CheckGooglePlayVersionTask.java
http://www.example.com	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java
https://)([\\s\\S]+)	com/huawei/hms/scankit/p/C0093bd.java
https://docs.flutter.dev/deployment/android	io/flutter/embedding/engine/loader/FlutterLoader.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/videoplayer/VideoPlayerPlugin.java
https://feedback.rong-edge.com	io/rong/common/dlog/LogEntity.java
https://feedback.rong-edge.com	io/rong/common/rlog/RLogConfig.java
http://s3.amazonaws.com/doc/2006-03-01/	io/rong/imlib/filetransfer/MinioSliceCompleteRequest.java
http://s3.amazonaws.com/doc/2006-03-01/	io/rong/imlib/filetransfer/StcSliceCompleteRequest.java
http://%s/	io/rong/imlib/cloudcontroller/CloudController.java

http://cloudcontrol.rongcloud.net/v1/config	io/rong/imlib/cloudcontroller/CloudUpdater.java
http://%s	io/rong/imlib/httpdns/HttpDnsClient.java
http://xml.org/sax/features/external-general-entities	io/rong/imlib/common/ParserFactory.java
http://xml.org/sax/features/external-parameter-entities	io/rong/imlib/common/ParserFactory.java
https://test-bootstrapprofile-c-1.oss-cn-beijing.aliyuncs.com/	io/rong/imlib/url/StaticConfigManager.java
https://test-bootstrapprofile-b-2.s3.ap-southeast-1.amazonaws.com/	io/rong/imlib/url/StaticConfigManager.java
http://%s/	io/rong/rtslog/RtsConfigEnv.java
http://%s/	io/rong/rtlog/upload/RtLogTimingUploadConfig.java
http://%s/	io/rong/rtlog/upload/RtLogUploadManager.java
https://stats.cn.ronghub.com	io/rong/libcore/BuildConfig.java
http://undefined/	org/jsoup/helper/HttpConnection.java
https://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://github.com/nodeca/pica	摸瓜V2引擎

http://paulbikaus.com/tutorials/html5/web-audio-on-ios/	摸瓜V2引擎
http://stackoverflow.com/questions/24119684	摸瓜V2引擎
.">https://www.gnu.org/licenses/>.	摸瓜V2引擎
.">https://www.gnu.org/licenses/>.	摸瓜V2引擎
.">https://www.gnu.org/licenses/>.	摸瓜V2引擎
http://api.devnet.solana.com	摸瓜V2引擎
http://api.testnet.solana.com	摸瓜V2引擎
http://api.mainnet-beta.solana.com/	摸瓜V2引擎
https://api.devnet.solana.com	摸瓜V2引擎
https://api.testnet.solana.com	摸瓜V2引擎
https://api.mainnet-beta.solana.com/	摸瓜V2引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://links.ethers.org/v5-errors-	摸瓜V2引擎
https://github.com/indutny/elliptic/issues	摸瓜V2引擎
https://github.com/indutny/elliptic	摸瓜V2引擎
">http://feross.org>	摸瓜V2引擎
https://api.etherscan.io	摸瓜V2引擎

https://api-ropsten.etherscan.io	摸瓜V2引擎
https://api-rinkeby.etherscan.io	摸瓜V2引擎
https://api-kovan.etherscan.io	摸瓜V2引擎
https://api-goerli.etherscan.io	摸瓜V2引擎
https://infura.io)	摸瓜V2引擎
https://web3.gastracker.io	摸瓜V2引擎
https://web3.gastracker.io/morden	摸瓜V2引擎
https://www.tronlink.org/phishing.html?href=	摸瓜V2引擎
https://github.com/indutny/elliptic/issues	摸瓜V2引擎
https://github.com/indutny/elliptic	摸瓜V2引擎
https://feross.org >	摸瓜V2引擎
https://manger.tronlending.org	摸瓜V2引擎
https://github.com/crypto-browserify/crypto-browserify	摸瓜V2引擎
https://github.com/emn178/js-sha3	摸瓜V2引擎
https://api.trongrid.io	摸瓜V2引擎
https://sun.tronex.io	摸瓜V2引擎
https://list.tronlink.org	摸瓜V2引擎
http://127.0.0.1	摸瓜V2引擎

https://github.com/crypto-browserify/crypto-browserify	摸瓜V2引擎
https://registry.npmjs.org/elliptic/-/elliptic-6.5.4.tgz	摸瓜V2引擎
https://github.com/indutny/elliptic/issues	摸瓜V2引擎
https://github.com/indutny/elliptic	摸瓜V2引擎
https://example.com	摸瓜V2引擎
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	摸瓜V2引擎
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so
http://www.unicode.org/copyright.html	lib/arm64-v8a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121	lib/arm64-v8a/libflutter.so

 邮箱线索

邮箱地址	所在文件
red_bag_bg_take@3x.png	摸瓜V2引擎

superstruct@0.11 git@github.com fedor@indutny.com	摸瓜V2引擎
feross@feross.org git@github.com fedor@indutny.com me@ricmoo.com emn178@gmail.com	摸瓜V2引擎
fedor@indutny.com git@github.com	摸瓜V2引擎
appro@openssl.org	lib/arm64-v8a/libRongIMLib.so
appro@openssl.org	lib/arm64-v8a/libflutter.so

手机线索

手机号	所在文件
19919152923	摸瓜V2引擎
19919152923	摸瓜V2引擎
19919152923	摸瓜V2引擎

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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2024-04-10 03:45:46+00:00
有效期至: 2051-08-27 03:45:46+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x299e07e346a3433e
哈希算法: sha256
md5值: 9a593b02890b1dc439e1b5610fdf47af
sha1值: 7e4cf2e6d22c967011800fe3268d5e043216ff95
sha256值: 0b3e33ff9484b6c2e7002122f26d5742d174215e03825f02f1ed487b1b430a48
sha512值: 1b004e6a6759b46a8605d5cf9072b499a8188e76d8d106aa70acb73b21e5909ac39404a4f99b6678e28ee644619fbf172be9b87857d64462bc21bb74f3afc431
公钥算法: rsa
密钥长度: 2048
指纹: 8538e7f2d3967565db19dfdd246dcbb50c3e87aa79c0c13ed1ba1fc0de0389b0

 硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

 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.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.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.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.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.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.startower.chian.permission.RONG_ACCESS_RECEIVER	未知	Unknown permission	Unknown permission from android reference
com.startower.chian.permission.RONG_BRIDGE_ACTIVITY	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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
com.startower.chian.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown	Unknown permission from android reference

		permission	
--	--	------------	--

应用内通信

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。