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

**Meta Seal（ 1.0.3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 | Meta Seal |
| 版本 | 1.0.3 |
| 包名 | com.startower.chian |
| 域名线索 | 49条 |
| URL线索 | 36条 |
| APP图标 |  |
| 分析日期 | 2025年7月5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 | 2hVTBWuYzANcY6m6.apk |
| 文件大小 | 96.6MB |
| MD5值 | 7716f0ae93579db169be880b766910bb |
| SHA1值 | 5d9a7820c12ae93a3aff2b784e1b199a2f06f87c |
| SHA256值 | 7f1ca8ff3f332482ecc4ba108b4f1c0b7edcdbc7ebec4b6fb9e8233ec2c323f9 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| api-ropsten.etherscan.io | IP: 31.13.86.21 所属国家: Italy 地区: Lombardia 城市: Milan  |
| paulbakaus.com | IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| 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  |
| journeyapps.com | IP: 18.65.168.90 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| registry.npmjs.org | IP: 104.16.26.34 所属国家: United States of America 地区: California 城市: San Francisco  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| example.com | IP: 96.7.128.175 所属国家: United States of America 地区: California 城市: El Segundo  |
| dev.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-rinkeby.etherscan.io | IP: 202.160.129.6 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api.trongrid.io | IP: 54.254.86.84 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| www.tronlink.org | IP: 162.125.32.6 所属国家: United States of America 地区: California 城市: San Francisco  |
| 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  |
| a.app.qq.com | IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 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  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| links.ethers.org | IP: 3.164.143.58 所属国家: United States of America 地区: Washington 城市: Seattle  |
| stats.cn.ronghub.com | IP: 47.94.172.98 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| stackoverflow.com | IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| 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  |
| app.mi.com | IP: 123.125.102.202 所属国家: China 地区: Beijing 城市: Beijing  |
| sun.tronex.io | IP: 52.15.86.168 所属国家: United States of America 地区: Ohio 城市: Columbus  |
| www.example.com | IP: 173.222.248.144 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| api.etherscan.io | IP: 173.236.182.137 所属国家: United States of America 地区: California 城市: Brea  |
| api.devnet.solana.com | IP: 162.125.2.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| s3.amazonaws.com | IP: 16.15.177.108 所属国家: United States of America 地区: Washington 城市: Seattle  |
| feedback.rong-edge.com | IP: 47.93.244.185 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| infura.io | IP: 13.35.202.118 所属国家: India 地区: Telangana 城市: Hyderabad  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| list.tronlink.org | IP: 162.125.7.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.google.com | IP: 31.13.106.4 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| 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  |
| dartbug.com | IP: 216.239.38.21 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| api-goerli.etherscan.io | IP: 118.184.78.78 所属国家: China 地区: Shanghai 城市: Shanghai  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| api.testnet.solana.com | IP: 31.13.70.33 所属国家: United States of America 地区: California 城市: Los Angeles  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api-kovan.etherscan.io | IP: 199.59.150.40 所属国家: United States of America 地区: California 城市: San Francisco  |
| 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  |
| cloudcontrol.rongcloud.net | IP: 47.94.224.40 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| 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://paulbakaus.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  |

### **4.3 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  |

### **4.4 手机号线索**

| 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  |

## **5. 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**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |

## **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 |
| --- | --- | --- | --- |
| 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 permission | Unknown permission from android reference |

## **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。**