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

**OneKey（ 5.8.0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 | OneKey |
| 版本 | 5.8.0 |
| 包名 | so.onekey.app.wallet |
| 域名线索 | 33条 |
| URL线索 | 68条 |
| APP图标 |  |
| 分析日期 | 2025年8月16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 | OneKey.apk |
| 文件大小 | 65.07MB |
| MD5值 | bba29b169ed8e273ea1c1cdb94bb4578 |
| SHA1值 | 5bee34da4ab8aedf0905d74204afc5b4249bd697 |
| SHA256值 | 0250ca1d4cab08958a2f01b4e0d32e08cfba47505d106dc557f26286c6305993 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | OneKey |
| 包名 | so.onekey.app.wallet |
| 主活动Activity | so.onekey.app.wallet.MainActivity |
| 安卓版本名称 | 5.8.0 |
| 安卓版本 | 2025042141 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| docs.revenuecat.com | IP: 3.165.102.30 所属国家: United States of America 地区: Washington 城市: Seattle  |
| logback.qos.ch | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| play.google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| iptc.org | IP: 3.64.29.21 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| xerces.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| ns.useplus.org | IP: 54.83.4.77 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| raw.githubusercontent.com | IP: 185.199.109.133 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api.revenuecat.com | IP: 54.205.40.174 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| 10.0.2.2 | IP: 10.0.2.2 所属国家: - 地区: - 城市: -  |
| purl.org | IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.apple.com | IP: 104.70.124.203 所属国家: Germany 地区: Hamburg 城市: Hamburg  |
| docs.swmansion.com | IP: 172.67.142.188 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.aiim.org | IP: 199.60.103.225 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| api-paywalls.revenuecat.com | IP: 54.159.155.171 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| api-diagnostics.revenuecat.com | IP: 44.193.104.211 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.slf4j.org | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| cipa.jp | IP: 118.82.81.189 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| ns.adobe.com | 没有服务器地理信息.  |
| schemas.android.com | 没有服务器地理信息.  |
| errors.rev.cat | IP: 67.199.248.13 所属国家: United States of America 地区: New York 城市: New York City  |
| drewnoakes.com | IP: 34.229.76.186 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.npes.org | IP: 104.21.43.185 所属国家: United States of America 地区: California 城市: San Francisco  |
| notifee.app | IP: 13.52.115.166 所属国家: United States of America 地区: California 城市: San Jose  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| expo.dev | IP: 104.18.5.104 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.googleapis.com | IP: 142.251.33.74 所属国家: Canada 地区: Ontario 城市: Toronto  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| rev.cat | IP: 52.72.49.79 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.amazon.com | IP: 3.175.229.98 所属国家: United States of America 地区: Washington 城市: Seattle  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| cs.android.com | IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| shopify.github.io | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://notifee.app/react-native/docs/triggers  | app/notifee/core/b.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/CoreConstants.java  |
| http://logback.qos.ch/manual/  | ch/qos/logback/core/CoreConstants.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/FileAppender.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/OutputStreamAppender.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/joran/action/AppenderRefAction.java  |
| http://xml.org/sax/features/validation  | ch/qos/logback/core/joran/event/SaxEventRecorder.java  |
| http://xml.org/sax/features/namespaces  | ch/qos/logback/core/joran/event/SaxEventRecorder.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/net/SyslogAppenderBase.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/net/AbstractSocketAppender.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/net/SMTPAppenderBase.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/SizeBasedTriggeringPolicy.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/TimeBasedRollingPolicy.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/RollingFileAppender.java  |
| http://logback.qos.ch/manual/appenders.html  | ch/qos/logback/core/rolling/SizeAndTimeBasedFNATP.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/FixedWindowRollingPolicy.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/TimeBasedFileNamingAndTriggeringPolicyBase.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/helper/RenameUtil.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/pattern/parser/Parser.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/sift/SiftingJoranConfiguratorBase.java  |
| http://logback.qos.ch/css/classic.css  | ch/qos/logback/classic/html/UrlCssBuilder.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/classic/net/SocketReceiver.java  |
| http://ns.adobe.com/StockPhoto/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/asf/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/bwf/bext/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/camera-raw-settings/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/ccv/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/creatorAtom/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/internal/xmp/XMPConst.java  |
| http://purl.org/dc/1.1/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/DICOM/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/1.0/DynamicMedia/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/exif/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://cipa.jp/exif/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/exif/1.0/aux/  | com/adobe/internal/xmp/XMPConst.java  |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/  | com/adobe/internal/xmp/XMPConst.java  |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/iX/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/jp2k/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/jpeg/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/pdf/1.3/  | com/adobe/internal/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/extension/  | com/adobe/internal/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/field  | com/adobe/internal/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/id/  | com/adobe/internal/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/property  | com/adobe/internal/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/schema  | com/adobe/internal/xmp/XMPConst.java  |
| http://www.aiim.org/pdfa/ns/type  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/pdfx/1.3/  | com/adobe/internal/xmp/XMPConst.java  |
| http://www.npes.org/pdfx/ns/id/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/photoshop/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.useplus.org/ldf/xmp/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/png/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/album/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/riff/info/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/1.0/Script/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/swf/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/tiff/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/transient/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/TransformXMP/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/wav/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/bj/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/mm/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/note/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/rights/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/Dimensions  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/Font  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/g/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xmp/Identifier/qual/1.0/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/g/img/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/ManifestItem  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/t/pg/  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/ResourceEvent  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/ResourceRef  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/Job  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/sType/Version  | com/adobe/internal/xmp/XMPConst.java  |
| http://ns.adobe.com/xap/1.0/t/  | com/adobe/internal/xmp/XMPConst.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/internal/xmp/impl/Utils.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/internal/xmp/impl/Utils.java  |
| http://ns.adobe.com/tiff/1.0/  | com/adobe/internal/xmp/impl/Utils.java  |
| http://ns.adobe.com/exif/1.0/  | com/adobe/internal/xmp/impl/Utils.java  |
| http://ns.adobe.com/exif/1.0/aux/  | com/adobe/internal/xmp/impl/Utils.java  |
| http://ns.adobe.com/photoshop/1.0/  | com/adobe/internal/xmp/impl/Utils.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/internal/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/internal/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/photoshop/1.0/  | com/adobe/internal/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/exif/1.0/  | com/adobe/internal/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/exif/1.0/aux/  | com/adobe/internal/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/tiff/1.0/  | com/adobe/internal/xmp/impl/XMPSchemaRegistryImpl.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/internal/xmp/impl/XMPUtilsImpl.java  |
| http://ns.adobe.com/photoshop/1.0/  | com/adobe/internal/xmp/impl/XMPUtilsImpl.java  |
| http://ns.adobe.com/xap/1.0/  | com/adobe/internal/xmp/impl/XMPSerializerRDF.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/internal/xmp/impl/ParseRDF.java  |
| http://purl.org/dc/elements/1.1/  | com/adobe/internal/xmp/impl/XMPNormalizer.java  |
| http://ns.adobe.com/exif/1.0/  | com/adobe/internal/xmp/impl/XMPNormalizer.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | com/adobe/internal/xmp/impl/XMPMetaParser.java  |
| http://xml.org/sax/features/external-general-entities  | com/adobe/internal/xmp/impl/XMPMetaParser.java  |
| http://xerces.apache.org/xerces2-j/features.html  | com/adobe/internal/xmp/impl/XMPMetaParser.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/adobe/internal/xmp/impl/XMPMetaParser.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | com/adobe/internal/xmp/impl/XMPMetaParser.java  |
| http://www.amazon.com/gp/mas/get-appstore/android/ref=mas\_mx\_mba\_iap\_dl  | com/amazon/device/iap/internal/a/a.java  |
| http://www.amazon.com/gp/mas/get-appstore/android/ref=mas\_mx\_mba\_iap\_dl  | com/amazon/a/a/i/a.java  |
| https://www.amazon.com/appstore-error-help  | com/amazon/a/a/i/g.java  |
| http://purl.org/dc/elements/1.1/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/exif/1.0/aux/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/exif/1.0/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/tiff/1.0/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/photoshop/1.0/  | com/drew/metadata/Schema.java  |
| http://ns.adobe.com/xap/1.0/  | com/drew/metadata/Schema.java  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd\  | com/drew/metadata/plist/BplistReader.java  |
| http://ns.adobe.com/xmp/note/  | com/drew/metadata/xmp/XmpReader.java  |
| http://ns.adobe.com/xmp/extension/\u0000  | com/drew/metadata/xmp/XmpReader.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | com/drew/metadata/xmp/XmpReader.java  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s\  | com/drew/imaging/ImageMetadataReader.java  |
| https://drewnoakes.com/code/exif/\n  | com/drew/tools/ProcessAllImagesInFolderUtility.java  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s/%s)  | com/drew/tools/ProcessAllImagesInFolderUtility.java  |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s/metadata/%s.txt)\n  | com/drew/tools/ProcessAllImagesInFolderUtility.java  |
| https://github.com/Polidea/RxAndroidBle/tree/master/mockrxandroidble'  | com/polidea/rxandroidble2/RxBleClientImpl.java  |
| https://cs.android.com/android/platform/superproject/+/master:packages/modules/Bluetooth/system/stack/include/gatt\_api.h  | com/polidea/rxandroidble2/exceptions/BleGattException.java  |
| https://docs.revenuecat.com/docs/ios-subscription-offers  | com/revenuecat/purchases/PurchasesErrorCode.java  |
| https://rev.cat/trusted-entitlements  | com/revenuecat/purchases/PurchasesErrorCode.java  |
| https://rev.cat/enter-amazon-sandbox  | com/revenuecat/purchases/amazon/AmazonStrings.java  |
| https://play.google.com/store/account/subscriptions  | com/revenuecat/purchases/common/Constants.java  |
| https://api-diagnostics.revenuecat.com/  | com/revenuecat/purchases/common/AppConfig.java  |
| https://api-paywalls.revenuecat.com/  | com/revenuecat/purchases/common/AppConfig.java  |
| https://api.revenuecat.com/  | com/revenuecat/purchases/common/AppConfig.java  |
| https://errors.rev.cat/configuring-products  | com/revenuecat/purchases/strings/OfferingStrings.java  |
| https://rev.cat/how-to-configure-offerings.\nMore  | com/revenuecat/purchases/strings/OfferingStrings.java  |
| https://rev.cat/why-are-offerings-empty  | com/revenuecat/purchases/strings/OfferingStrings.java  |
| https://rev.cat/google-duplicated-listener-timeouts  | com/revenuecat/purchases/strings/OfferingStrings.java  |
| https://rev.cat/offline-entitlements  | com/revenuecat/purchases/strings/OfflineEntitlementsStrings.java  |
| https://errors.rev.cat/finishTransactions  | com/revenuecat/purchases/strings/PurchaseStrings.java  |
| https://rev.cat/google-duplicated-listener-timeouts  | com/revenuecat/purchases/strings/RestoreStrings.java  |
| https://errors.rev.cat/allowsSharingPlayStoreAccount  | com/revenuecat/purchases/strings/RestoreStrings.java  |
| https://github.com/RevenueCat/purchases-android/issues/381  | com/revenuecat/purchases/strings/BillingStrings.java  |
| https://rev.cat/auth  | com/revenuecat/purchases/strings/ConfigureStrings.java  |
| https://errors.rev.cat/configuring-sdk  | com/revenuecat/purchases/strings/ConfigureStrings.java  |
| https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot  | com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java  |
| https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting  | com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenStackFragment.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://expo.dev  | expo/modules/webbrowser/CustomTabsActivitiesHelperKt.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| http://10.0.2.2:8969/stream  | io/sentry/SpotlightIntegration.java  |
| https://www.googleapis.com/auth/drive.appdata  | org/rncloudfs/RNCloudFsModule.java  |
| https://www.googleapis.com/auth/drive.file  | org/rncloudfs/RNCloudFsModule.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |
| http://logback.qos.ch/codes.html  | org/slf4j/impl/StaticLoggerBinder.java  |
| http://schemas.android.com/apk/res/android  | so/onekey/app/wallet/widget/SlidingTabLayoutBase.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False 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: 2022-01-23 13:06:00+00:00 有效期至: 2052-01-23 13:06:00+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0xea9124c63a795978d6dd6092c58feaee2f607f36 哈希算法: sha256 md5值: 15f88234a07afe8a1f903179ae2c09a9 sha1值: 35756f3db5b5b56ef6af460f5a1008015796bc61 sha256值: 6e3d1b40484a3b0d467466bce96dfc9efab45834fe17b3a447073a0c18b246d4 sha512值: f4d949a1e5c1db9e82ee6cb5517e66dbc48892e805c090adf7c0d7d009a14e1c7676eb29b8808edc05ab2cf1dbb1b3be6da562c2010942af802bd4411a2bfb7b 公钥算法: rsa 密钥长度: 4096 指纹: 70355197e72656fff26cb8a5089461d7909fef929ef3995f8d07e4ea05b77289**

## **6. 硬编码敏感信息**

## **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.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.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.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.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.BILLING | 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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| so.onekey.app.wallet.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| 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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| so.onekey.app.wallet.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| android.permission.BROADCAST\_CLOSE\_SYSTEM\_DIALOGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| 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 | 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 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| so.onekey.app.wallet.MainActivity | **Schemes**: onekey-wallet://, so.onekey.app.wallet://, wc://, ethereum://,  |

**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。**