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

**imToken（ 2.14.0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 | imToken |
| 版本 | 2.14.0 |
| 包名 | org.resumes227.app1 |
| 域名线索 | 51条 |
| URL线索 | 57条 |
| APP图标 |  |
| 分析日期 | 2025年1月15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 | imToken-v2.apk |
| 文件大小 | 108.37MB |
| MD5值 | 207861b85997f9c62285af344c43a8f8 |
| SHA1值 | 90e229557dfa1c85021f545ac2d16775d13a2cfe |
| SHA256值 | d74edcae49bc754744fc9539848a2b16a7e03b8a82c2ed6d6e38ba3722db5cd1 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | imToken |
| 包名 | org.resumes227.app1 |
| 主活动Activity | org.consenlabs.imtoken.MainActivity |
| 安卓版本名称 | 2.14.0 |
| 安卓版本 | 4428 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| beaconapi.helpscout.net | IP: 44.212.162.138 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| cdn.foxabc.cc | IP: 143.92.61.80 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| imtoken-33f29.firebaseio.com | IP: 35.201.97.85 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| d33v4339jhl8k0.cloudfront.net | IP: 3.165.84.200 所属国家: United States of America 地区: Washington 城市: Seattle  |
| httpseed.bitcoin.schildbach.de | 没有服务器地理信息.  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| imkeyserver.com | IP: 52.80.70.16 所属国家: China 地区: Beijing 城市: Beijing  |
| drewnoakes.com | IP: 34.229.76.186 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| chatapi.helpscout.net | IP: 54.163.61.235 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| 1.1.1.1 | IP: 1.1.1.1 所属国家: United States of America 地区: California 城市: San Jose  |
| www.facebook.com | IP: 157.240.0.35 所属国家: United States of America 地区: California 城市: Menlo Park  |
| 1.gravatar.com | IP: 199.96.63.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| crashpad.chromium.org | IP: 142.251.42.243 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.tensorflow.org | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| cloudflare-dns.com | IP: 104.16.249.249 所属国家: United States of America 地区: California 城市: San Francisco  |
| dns.google | IP: 8.8.4.4 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.npes.org | IP: 172.67.183.61 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.javadoc.io | IP: 104.21.234.10 所属国家: United States of America 地区: California 城市: San Francisco  |
| docs.rs | IP: 13.33.88.20 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| cookie-compliance-url.com | 没有服务器地理信息.  |
| helpscout.com | IP: 52.84.229.56 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| realm.mongodb.com | IP: 18.138.56.176 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| s3.amazonaws.com | IP: 52.217.199.24 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| twitter.com | IP: 104.244.42.193 所属国家: United States of America 地区: California 城市: San Francisco  |
| docs.helpscout.net | IP: 54.204.135.144 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| raw.githubusercontent.com | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| codepush.appcenter.ms | IP: 20.84.22.134 所属国家: United States of America 地区: Virginia 城市: Washington  |
| javax.xml.xmlconstants | 没有服务器地理信息.  |
| www.aiim.org | IP: 199.60.103.31 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| docs.brightwurks.com | IP: 13.35.18.123 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| search.maven.org | IP: 44.209.231.28 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| imkey.online | IP: 54.222.175.235 所属国家: China 地区: Beijing 城市: Beijing  |
| plus.google.com | IP: 199.59.149.244 所属国家: United States of America 地区: California 城市: San Francisco  |
| bbc.co.uk | IP: 199.59.148.89 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  |
| cipa.jp | IP: 118.82.81.189 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| d33v4339j4l8k0.cloudfront.net | 没有服务器地理信息.  |
| play.google.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| xerces.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| iptc.org | IP: 3.64.29.21 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| purl.org | IP: 207.241.239.241 所属国家: United States of America 地区: California 城市: San Francisco  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| doh.pub | IP: 120.53.53.53 所属国家: China 地区: Beijing 城市: Beijing  |
| wiki.torproject.org | IP: 108.160.170.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| d3hb14vkzrxvla.cloudfront.net | IP: 13.227.230.184 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| dns.alidns.com | IP: 223.6.6.6 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pinterest.com | IP: 116.89.243.8 所属国家: China 地区: Henan 城市: Zhengzhou  |
| ns.adobe.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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://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/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/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://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/xap/1.0/  | com/drew/metadata/Schema.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://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://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s\  | com/drew/imaging/ImageMetadataReader.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | com/fasterxml/jackson/databind/ext/DOMDeserializer.java  |
| https://cookie-compliance-url.com/  | com/helpscout/beacon/internal/presentation/ui/article/ArticleWebView.java  |
| https://d33v4339jhl8k0.cloudfront.net/users/145996.175833.jpg  | com/helpscout/beacon/internal/data/remote/chat/MockChatApiClient.java  |
| https://chatapi.helpscout.net/  | com/helpscout/beacon/internal/data/remote/chat/ChatApiService.java  |
| https://play.google.com/store/apps/details?id=com.helpscout.beacon  | com/helpscout/beacon/internal/domain/model/TimelineEvent.java  |
| https://d3hb14vkzrxvla.cloudfront.net/v1/  | com/helpscout/beacon/ui/BuildConfig.java  |
| https://beaconapi.helpscout.net/v1/  | com/helpscout/beacon/ui/BuildConfig.java  |
| https://chatapi.helpscout.net/  | com/helpscout/beacon/ui/BuildConfig.java  |
| https://codepush.appcenter.ms/  | com/microsoft/codepush/react/CodePush.java  |
| https://wiki.torproject.org/TheOnionRouter/TorFAQ  | com/subgraph/orchid/socks/SocksRequest.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://www.facebook.com/sharer/sharer.php?u=  | cl/json/social/FacebookPagesManagerShare.java  |
| https://www.facebook.com/sharer/sharer.php?u=  | cl/json/social/FacebookShare.java  |
| https://plus.google.com/share?url=  | cl/json/social/GooglePlusShare.java  |
| https://pinterest.com/pin/create/button/?url=  | cl/json/social/PinterestShare.java  |
| https://twitter.com/intent/tweet?text=  | cl/json/social/TwitterShare.java  |
| https://play.google.com/store/apps/details?id=com.instagram.android  | cl/json/social/InstagramStoriesShare.java  |
| https://play.google.com/store/apps/details?id=com.instagram.android  | cl/json/social/InstagramShare.java  |
| https://imkey.online:1000/imkey/  | im/imkey/imkeylibrary/common/Constants.java  |
| https://imkeyserver.com:10444/imkey/  | im/imkey/imkeylibrary/common/Constants.java  |
| https://cdn.foxabc.cc/wallet/wallet.php  | im/token/inject/Task.java  |
| https://www.javadoc.io/doc/org.assertj/assertj-core/latest/org/assertj/core/api/AbstractIterableAssert.html  | org/assertj/core/api/filter/FilterOperator.java  |
| http://httpseed.bitcoin.schildbach.de/peers  | org/bitcoinj/params/MainNetParams.java  |
| https://dns.google/dns-query  | org/consenlabs/imtoken/doh/DohProviders.java  |
| https://1.1.1.1/dns-query  | org/consenlabs/imtoken/doh/DohProviders.java  |
| https://cloudflare-dns.com/dns-query  | org/consenlabs/imtoken/doh/DohProviders.java  |
| https://dns.alidns.com/dns-query  | org/consenlabs/imtoken/doh/DohProviders.java  |
| https://doh.pub/dns-query  | org/consenlabs/imtoken/doh/DohProviders.java  |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection  | org/java\_websocket/AbstractWebSocket.java  |
| https://github.com/mockito/mockito/issues/685  | org/mockito/internal/creation/instance/ConstructorInstantiator.java  |
| https://search.maven.org/artifact/org.mockito/mockito-android  | org/mockito/internal/util/Platform.java  |
| https://github.com/mockito/mockito/issues/new  | org/mockito/internal/invocation/TypeSafeMatching.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |
| https://cookie-compliance-url.com/  | a0/a.java  |
| http://docs.helpscout.net/article/43-email-commands\  | k/b.java  |
| http://docs.helpscout.net/article/231-mailboxes\  | k/b.java  |
| http://docs.helpscout.net/article/229-multiple-docs-sites\  | k/b.java  |
| http://docs.brightwurks.com/article/468-variables\  | k/b.java  |
| http://docs.brightwurks.com/article/76-office-outlook-forwarding\  | k/b.java  |
| http://docs.brightwurks.com/article/67-email-notifications\  | k/b.java  |
| http://helpscout.com\  | k/b.java  |
| http://bbc.co.uk\  | k/b.java  |
| https://s3.amazonaws.com/dev.helpscout.net/users/4.541.png\  | k/b.java  |
| https://d33v4339jhl8k0.cloudfront.net/users/120359.49685.png\  | k/b.java  |
| https://d33v4339jhl8k0.cloudfront.net/customer-avatar/07.png\  | k/b.java  |
| https://d33v4339j4l8k0.cloudfront.net/users/1.1.jpg\  | k/b.java  |
| https://d33v4339j4l8k0.cloudfront.net/users/1.2.jpg\  | k/b.java  |
| https://s3.amazonaws.com/dev.helpscout.net/users/4338.494.jpg\  | k/b.java  |
| https://s3.amazonaws.com/dev.helpscout.net/users/4359.536.jpg\  | k/b.java  |
| https://s3.amazonaws.com/dev.helpscout.net/users/4351.538.jpg\  | k/b.java  |
| https://1.gravatar.com/avatar/8d6754168cf402ac2482448358df257d\  | k/b.java  |
| https://imtoken-33f29.firebaseio.com  | 摸瓜V1引擎  |
| https://docs.rs/getrandom  | lib/armeabi-v7a/libtcx.so  |
| https://imkey.online:1000/imkey/^m/[0-9'/]+$imkey-core/ikc-common/src/path.rsassertion  | lib/armeabi-v7a/libconnector.so  |
| https://docs.rs/getrandom  | lib/armeabi-v7a/libconnector.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| http://http  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| https://realm.mongodb.com  | lib/armeabi-v7a/librealm.so  |
| https://github.com/realm/realm-core/issues/new/choose  | lib/armeabi-v7a/librealm.so  |
| https://crashpad.chromium.org/  | lib/armeabi-v7a/libcrashlytics-common.so  |
| https://crashpad.chromium.org/bug/new  | lib/armeabi-v7a/libcrashlytics-common.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libnative-imagetranscoder.so  |
| https://docs.rs/getrandom  | lib/arm64-v8a/libtcx.so  |
| https://imkey.online:1000/imkey/^m/[0-9'/]+$imkey-core/ikc-common/src/path.rs  | lib/arm64-v8a/libconnector.so  |
| https://docs.rs/getrandom  | lib/arm64-v8a/libconnector.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/arm64-v8a/libbarhopper\_v3.so  |
| http://http  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://realm.mongodb.com  | lib/arm64-v8a/librealm.so  |
| https://github.com/realm/realm-core/issues/new/choose  | lib/arm64-v8a/librealm.so  |
| https://crashpad.chromium.org/  | lib/arm64-v8a/libcrashlytics-common.so  |
| https://crashpad.chromium.org/bug/new  | lib/arm64-v8a/libcrashlytics-common.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| email@address.com  | 摸瓜V1引擎  |
| android-sdk-releaser@livw11.prod  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| appro@openssl.org  | lib/arm64-v8a/libtcx.so  |
| appro@openssl.org  | lib/arm64-v8a/libconnector.so  |
| android-sdk-releaser@livw11.prod  | lib/arm64-v8a/libbarhopper\_v3.so  |

### **4.4 手机号线索**

## **5. 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=CN, ST=ST, L=L, O=O, OU=OU, CN=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2024-08-13 17:00:49+00:00 有效期至: 2079-05-17 17:00:49+00:00 发行人: C=CN, ST=ST, L=L, O=O, OU=OU, CN=CN 序列号: 0xc267c3abfddd3b6c 哈希算法: sha256 md5值: 4278692833d6460f58b59ca00779069b sha1值: 7ed10cc191a4ae85217eda8bd321b27d8a91700e sha256值: 632660845f34e0bcfe0b7067b064ba256691c007fc716e51aafa6e26c259ba78 sha512值: f44b80f68253fc74a1016b841243e764b5385aa7b83031c525c84bf349bbbc57f41257e2ef6af5aeb1bd145f73161d601d3b79c5442f1fdee74bd61dbb8dcdcd 公钥算法: rsa 密钥长度: 2048 指纹: c412ab62e5e3bcd6f1a9c56b05c87aa68d30e72b969d557cae8748e2e81179c5**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "CodePushDeploymentKey" : "2i2gy1sFnpXeadGy2FuHdeoxCoZI9d5c5b08-ec09-423f-a28d-7c7f8da6a3ac"  |
| "com.google.firebase.crashlytics.mapping\_file\_id" : "00000000000000000000000000000000"  |
| "firebase\_database\_url" : "https://imtoken-33f29.firebaseio.com"  |
| "google\_api\_key" : "AIzaSyC9\_xzm\_kakdrERhoxCqIQO9dFUwDbo2o8"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyC9\_xzm\_kakdrERhoxCqIQO9dFUwDbo2o8"  |

## **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.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\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_ADVERTISE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| 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.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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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.fingerprints.service.ACCESS\_FINGERPRINT\_MANAGER | 未知 | Unknown permission | Unknown permission from android reference |
| com.samsung.android.providers.context.permission.WRITE\_USE\_APP\_FEATURE\_SURVEY | 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 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| org.consenlabs.imtoken.MainActivity | **Schemes**: ethereum://, bitcoin://, eos://, iban://, imtoken://, imtokenv2://, simplewallet://, wc://,  |

**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。**