



MoGua

imToken 2.14.1.APK 分析报告



APP名称:

imToken

包名:	im.token10.app10
域名线索:	50条
URL线索:	51条
邮箱线索:	2条
分析日期:	2024年10月16日
分析平台:	摸瓜APK反编译平台

文件名: imToken-intl-v2.apk
文件大小: 64.36MB
MD5值: 016fc36ac004e1b91095cda08a970872
SHA1值: efaa83d119fec324b23dc944a229785f4c2f9f40
SHA256值: f2be6aa93b956264d520dff6829b64ea0b4b73dd4a6c2ba396201c773b361d57

i APP 信息

App名称: imToken
包名: im.token10.app10
主活动Activity: org.consenlabs.imtoken.MainActivity
安卓版本名称: 2.14.1
安卓版本: 4651

🔍 域名线索

域名	服务器信息
chatapi.helpscout.net	IP: 54.161.56.162 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
www.tensorflow.org	IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
dns.google	IP: 8.8.4.4 所属国家: United States of America 地区: California

	城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.javadoc.io	IP: 104.21.234.11 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
cipa.jp	IP: 118.82.81.189 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
codepush.appcenter.ms	IP: 20.84.22.134 所属国家: United States of America 地区: Virginia 城市: Washington 纬度: 38.713848 经度: -78.159439
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
docs.helpscout.net	IP: 54.173.152.10 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806

www.aiim.org	IP: 199.60.103.31 所属国家: United States of America 地区: Massachusetts 城市: Cambridge 纬度: 42.370129 经度: -71.086304
iptc.org	IP: 3.64.29.21 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
realm.mongodb.com	IP: 18.138.56.176 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
bbc.co.uk	IP: 157.240.13.8 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
beaconapi.helpscout.net	IP: 34.225.42.149 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
imkeyserver.com	IP: 52.80.70.16 所属国家: China 地区: Beijing 城市: Beijing

	纬度: 39.907501 经度: 116.397102
d33v4339j4l8k0.cloudfront.net	没有服务器地理信息.
doh.pub	IP: 120.53.53.53 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
1.1.1.1	IP: 1.1.1.1 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
helpscout.com	IP: 3.164.110.100 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
plus.google.com	IP: 103.97.3.19 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
ns.adobe.com	没有服务器地理信息.
play.google.com	IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam

	纬度: 37.420624 经度: 127.126717
wiki.torproject.org	IP: 31.13.71.19 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.713192 经度: -74.006065
d33v4339jhl8k0.cloudfront.net	IP: 65.9.37.42 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
pinterest.com	IP: 128.242.245.244 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
dns.alidns.com	IP: 223.6.6.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.slf4j.org	IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge 纬度: 46.180931 经度: 6.138709
	IP: 172.67.183.61 所属国家: United States of America

www.npes.org	地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
javax.xml.xmlconstants	没有服务器地理信息.
cookie-compliance-url.com	没有服务器地理信息.
imtoken-33f29.firebaseio.com	IP: 35.201.97.85 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
raw.githubusercontent.com	IP: 185.199.108.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
cloudflare-dns.com	IP: 104.16.249.249 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
	IP: 52.217.92.6 所属国家: United States of America

s3.amazonaws.com	地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
crashpad.chromium.org	IP: 142.251.33.115 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660 经度: -79.382927
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
search.maven.org	IP: 34.199.162.181 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
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
d3hb14vkzrxvla.cloudfront.net	IP: 13.35.70.219 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322

ns.useplus.org	IP: 54.83.4.77 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
1.gravatar.com	IP: 208.77.47.172 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.323776 经度: -121.914719
docs.brightwurks.com	IP: 3.166.216.48 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
httpseed.bitcoin.schildbach.de	没有服务器地理信息.
xerces.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
drewnoakes.com	IP: 34.229.76.186 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
	IP: 104.244.42.1 所属国家: United States of America

twitter.com	地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
imkey.online	IP: 54.222.175.235 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
purl.org	IP: 207.241.239.241 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.781734 经度: -122.459435
docs.rs	IP: 3.166.228.39 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
www.facebook.com	IP: 157.240.12.5 所属国家: Brazil 地区: Sao Paulo 城市: Sao Paulo 纬度: -23.547121 经度: -46.637184

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/lptc4xmpCore/1.0/xmlns/	com/adobe/internal/xmp/XMPConst.java
http://iptc.org/std/lptc4xmpExt/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
\n">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://d33v4339jh8k0.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://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://github.com/mockito/mockito/issues/new	org/mockito/internal/invocation/TypeSafeMatching.java
https://search.maven.org/artifact/org.mockito/mockito-android	org/mockito/internal/util/Platform.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://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://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://docs.rs/getrandom	lib/armeabi-v7a/libtcx.so

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

手机线索

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=USA, ST=BOSTON, L=OKEX, O=BTC, OU=US, CN=ConsoleLab
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-05 14:11:24+00:00
有效期至: 2298-07-21 14:11:24+00:00
发行人: C=USA, ST=BOSTON, L=OKEX, O=BTC, OU=US, CN=ConsoleLab
序列号: 0xb5cfc310ca84219e
哈希算法: sha256
md5值: 094cd7d2d9efe1d02e4c4bfa554d3010
sha1值: 864ae1ee06c3bf989bb4c1dde0d89c0388f876f7
sha256值: d1836c9cd9ca020decf963401dfb8a0ec7337525fa375783284d3768413fb319
sha512值: ac86ea90eeab9b77bc7ac88e3ec64c47eaf375643940bf74256162ff1c1cc1cd140837e225e99b3212d6f121edd9135945be9bb0efc1b5d1cc5d863993776a94
公钥算法: rsa
密钥长度: 2048
指纹: 80c49bf83b99787a3a847763fe5d99de86d1a61e9955152dcbeebec9aef7c2e6

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" : "AlzaSyC9_xzm_kakdrERhoxCqIQO9dFUwDbo2o8"
"google_crash_reporting_api_key" : "AlzaSyC9_xzm_kakdrERhoxCqIQO9dFUwDbo2o8"

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.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。

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](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。