MoGua

MetaMask 7.10.0.APK 分析报告

APP名称:	MetaMask
包名:	io.festival1.app227

域名线索:	35条
URL线索:	36条
邮箱线索:	2条
分析日期:	2025年1月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: MetaMask.apk
文件大小: 31.93MB
MD5值: 2433e49bd0a0748d2f657fcc68c296ea
SHA1值: f550e2639bef58dbcade0ca9d6224e2f8b91dc73
SHA256值: b57993f00420d98be5606cb7cfadd6a8f355cbd8fcb85b1b233b69c0fea3e866

APP 信息

App名称: MetaMask
包名: io.festival1.app227
主活动Activity: io.metamask.SplashActivity
安卓版本名称: 7.10.0
安卓版本: 1187

域名线索

域名	服务器信息
medium.com	**IP**: 202.160.128.210 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
cdn.foxabc.cc	**IP**: 143.92.61.80 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
bnc.lt	**IP**: 108.157.254.104 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.604309 **经度**: -122.329842
aomedia.org	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647

	经度: -79.891724
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
schemas.microsoft.com	IP: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
api.mixpanel.com	IP: 107.178.240.159 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
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
www.facebook.com	IP: 157.240.0.35 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604
developer.apple.com	IP: 17.253.85.203 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

www.npes.org	**IP**: 172.67.183.61 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
schemas.android.com	没有服务器地理信息.
exoplayer.dev	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
docs.rs	**IP**: 13.33.88.49 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
twitter.com	**IP**: 104.244.42.129 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
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 **纬度**: 42.370129 **经度**: -71.086304
	IP: 52.84.229.121 **所属国家**: Singapore

cdn.branch.io	**地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
metamask-sdk-socket.metafi.codefi.network	IP: 199.59.149.238 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
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
plus.google.com	IP: 199.59.149.244 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
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
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
	IP: 142.251.42.238 **所属国家**: United States of America **地区**: California

play.google.com	**城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
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
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
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
dashif.org	IP: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
api2.branch.io	IP: 108.156.133.117 **所属国家**: United States of America **地区**: Washington

	城市: Seattle **纬度**: 47.604309 **经度**: -122.329842
developer.android.com	**IP**: 142.251.42.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
pinterest.com	**IP**: 173.252.248.244 **所属国家**: United States of America **地区**: California **城市**: Santa Clara **纬度**: 37.347729 **经度**: -121.984909
eips.ethereum.org	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
docs.metamask.io	**IP**: 199.96.62.21 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
ns.adobe.com	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**
https://api.mixpanel.com	com/mixpanel/android/mpmetrics/l.java

https://github.com/mixpanel/mixpanel-android/issues/567)	com/mixpanel/android/mpmetrics/a.java
https://twitter.com/i/wallet/verify	com/reactnativecommunity/webview/RNCWebViewManager.java
https://).	com/reactnativecommunity/cookies/CookieManagerModule.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/n.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/q.java
https://exoplayer.dev/issues/cleartext-not-permitted	ca/w.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	e8/w1.java
https://metamask-sdk-socket.metafi.codefi.network/debug	io/metamask/nativesdk/a.java
https://x</LA_URL>	j8/g0.java
https://x	j8/g0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	j8/h0.java
https://cdn.branch.io/	lg/d0.java
https://api2.branch.io/	lg/d0.java
https://bnc.lt/a/	lg/g0.java
https://cdn.foxabc.cc/wallet/wallet.php	org/inject/Task.java
http://dashif.org/guidelines/last-segment-number	l9/c.java
http://dashif.org/guidelines/trickmode	l9/c.java
https://developer.android.com/reference/com/google/android/play/core/assetpacks/model/AssetPackErrorCode.html	sc/a.java
https://plus.google.com/	pa/l1.java

http://schemas.android.com/apk/res/android	u/j.java
http://ns.adobe.com/xap/1.0/	j1/p.java
http://purl.org/dc/elements/1.1/	j1/p.java
http://ns.adobe.com/xap/1.0/rights/	j1/p.java
http://ns.adobe.com/pdf/1.3/	j1/p.java
http://ns.adobe.com/photoshop/1.0/	j1/p.java
http://ns.adobe.com/tiff/1.0/	j1/p.java
http://ns.adobe.com/png/1.0/	j1/p.java
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	j1/p.java
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	j1/p.java
http://ns.adobe.com/DICOM/	j1/p.java
http://ns.useplus.org/ldf/xmp/1.0/	j1/p.java
http://ns.adobe.com/iX/1.0/	j1/p.java
http://ns.adobe.com/xap/1.0/mm/	j1/p.java
http://ns.adobe.com/xap/1.0/bj/	j1/p.java
http://ns.adobe.com/xmp/note/	j1/p.java
http://ns.adobe.com/pdfx/1.3/	j1/p.java
http://www.npes.org/pdfx/ns/id/	j1/p.java
http://www.aiim.org/pdfa/ns/schema	j1/p.java

http://www.aiim.org/pdfa/ns/property	j1/p.java
http://www.aiim.org/pdfa/ns/type	j1/p.java
http://www.aiim.org/pdfa/ns/field	j1/p.java
http://www.aiim.org/pdfa/ns/id/	j1/p.java
http://www.aiim.org/pdfa/ns/extension/	j1/p.java
http://ns.adobe.com/album/1.0/	j1/p.java
http://ns.adobe.com/exif/1.0/	j1/p.java
http://cipa.jp/exif/1.0/	j1/p.java
http://ns.adobe.com/exif/1.0/aux/	j1/p.java
http://ns.adobe.com/jpeg/1.0/	j1/p.java
http://ns.adobe.com/jp2k/1.0/	j1/p.java
http://ns.adobe.com/camera-raw-settings/1.0/	j1/p.java
http://ns.adobe.com/StockPhoto/1.0/	j1/p.java
http://ns.adobe.com/creatorAtom/1.0/	j1/p.java
http://ns.adobe.com/asf/1.0/	j1/p.java
http://ns.adobe.com/xmp/wav/1.0/	j1/p.java
http://ns.adobe.com/bwf/bext/1.0/	j1/p.java
http://ns.adobe.com/riff/info/	j1/p.java

http://ns.adobe.com/xmp/1.0/Script/	j1/p.java
http://ns.adobe.com/TransformXMP/	j1/p.java
http://ns.adobe.com/swf/1.0/	j1/p.java
http://ns.adobe.com/xmp/1.0/DynamicMedia/	j1/p.java
http://ns.adobe.com/xmp/transient/1.0/	j1/p.java
http://ns.adobe.com/xap/1.0/t/	j1/p.java
http://ns.adobe.com/xap/1.0/t/pg/	j1/p.java
http://ns.adobe.com/xap/1.0/g/	j1/p.java
http://ns.adobe.com/xap/1.0/g/img/	j1/p.java
http://ns.adobe.com/xap/1.0/sType/Font	j1/p.java
http://ns.adobe.com/xap/1.0/sType/Dimensions	j1/p.java
http://ns.adobe.com/xap/1.0/sType/ResourceEvent	j1/p.java
http://ns.adobe.com/xap/1.0/sType/ResourceRef	j1/p.java
http://ns.adobe.com/xap/1.0/sType/Version	j1/p.java
http://ns.adobe.com/xap/1.0/sType/Job	j1/p.java
http://ns.adobe.com/xap/1.0/sType/ManifestItem	j1/p.java
http://ns.adobe.com/xmp/Identifier/qual/1.0/	j1/p.java
http://purl.org/dc/1.1/	j1/f.java
http://purl.org/dc/elements/1.1/	j1/f.java

http://purl.org/dc/elements/1.1/	j1/o.java
http://ns.adobe.com/exif/1.0/	j1/o.java
http://ns.adobe.com/xmp/1.0/DynamicMedia/	j1/o.java
http://ns.adobe.com/xap/1.0/rights/	j1/o.java
http://ns.adobe.com/xap/1.0/mm/	j1/o.java
http://javax.xml.XMLConstants/feature/secure-processing	j1/l.java
http://apache.org/xml/features/disallow-doctype-decl	j1/l.java
http://xml.org/sax/features/external-general-entities	j1/l.java
http://xerces.apache.org/xerces2-j/features.html	j1/l.java
http://xml.org/sax/features/external-parameter-entities	j1/l.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	j1/l.java
http://ns.adobe.com/xap/1.0/\u0000	o0/a.java
https://aomedia.org/emsg/ID3	a9/a.java
https://developer.apple.com/streaming/emsg-id3	a9/a.java
http://ns.adobe.com/xap/1.0/	p8/a.java
https://www.facebook.com/sharer/sharer.php?u=	e1/c.java
https://www.facebook.com/sharer/sharer.php?u=	e1/b.java
https://plus.google.com/share?url=	e1/f.java
https://pinterest.com/pin/create/button/?url=	e1/k.java

https://twitter.com/intent/tweet?text=	e1/r.java
https://play.google.com/store/apps/details?id=com.instagram.android	e1/g.java
https://play.google.com/store/apps/details?id=com.instagram.android	e1/h.java
http://ns.adobe.com/xmp/note/	b4/c.java
http://ns.adobe.com/xap/1.0/\u0000	b4/c.java
http://ns.adobe.com/xmp/extension/\u0000	b4/c.java
https://eips.ethereum.org/EIPS/eip-6963	摸瓜V2引擎
https://github.com/MetaMask/metamask-improvement-proposals/discussions/23	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1102	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1193	摸瓜V2引擎
https://medium.com/metamask/metamask-api-method-deprecation-2b0564a84686	摸瓜V2引擎
https://github.com/MetaMask/metamask-improvement-proposals/blob/main/MIPs/mip-1.md	摸瓜V2引擎
https://github.com/MetaMask/metamask-improvement-proposals/blob/main/PROCESS-GUIDE.md	摸瓜V2引擎
https://docs.metamask.io/guide/provider-migration.html	摸瓜V2引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://docs.rs/getrandom	lib/arm64-v8a/libecies.so

邮箱线索

邮箱地址	所在文件

u0013android@android.com0 u0013android@android.com	la/r.java
superstruct@0.11 webextension@metamask.io webextension-beta@metamask.io webextension-flask@metamask.io	摸瓜V2引擎

手机线索

手机号	所在文件
18222222222	q8/e.java

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 17:10:52+00:00
有效期至: 2079-05-17 17:10:52+00:00
发行人: C=CN, ST=ST, L=L, O=O, OU=OU, CN=CN
序列号: 0x5378eebc0d04c8d
哈希算法: sha256
md5值: 76ce991e68f933ba5595855fd9996e69
sha1值: 1849940bf97cd2208eef06ef10629aba58db85f9
sha256值: cf611bd9bed1f139891cc160c6028c59591578d4189de32edf2255e48bbdce8f
sha512值: 2e057497d202ba2a44e9aeafc2c205eb0d1c5555a6b398a6e1ab1ebe215c2ce50584e1f421cfff3c0cbe99399f08c595758abb328b460b8b4050aeb2aa409a36
公钥算法: rsa
密钥长度: 2048
指纹: 2984e9df49351274f42dff90fdd24ef7b26704912fcf27d5fc405e1cc4636700

硬编码敏感信息

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.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.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.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.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.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.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.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
com.android.vending.CHECK_LICENSE	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
android.permission.POST_NOTIFICATIONS	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。
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	在索尼手机的应用程序启动图标上显示通知计数或徽章。

		计数	
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.metamask.MainActivity	Schemes: https://, metamask://, ethereum://, dapp://, wc://, http://, Hosts: metamask.app.link, metamask-alternate.app.link, metamask.test-app.link, metamask-alternate.test-app.link,