



MoGua

Gem 1.3.2.APK 分析报告



APP名称:

Gem

包名:

com.gemwallet.android

域名线索:

20条

URL线索:

22条

邮箱线索:

0条

分析日期:2025年6月26日

分析平台:[摸瓜APK反编译平台](#)

文件信息

文件名: gem_wallet_latest.apk
文件大小: 55.02MB
MD5值: 1e8ecba6012be529ab3d00ccba3e7cf2
SHA1值: e4f6b9d580294de6e0532356ce2f8d7bf703a1fc
SHA256值: e3571d4071fd3d1ae55a9118b4c9b0e7de6173d74551c35b4922bdc03c2db75b

APP 信息

App名称: Gem
包名: com.gemwallet.android
主活动Activity: com.gemwallet.android.MainActivity
安卓版本名称: 1.3.2
安卓版本: 594

域名线索

域名	服务器信息

raw.githubusercontent.com	IP: 185.199.109.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
assets.gemwallet.com	IP: 104.26.1.14 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
rpc.walletconnect.com	IP: 103.252.115.53 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
echo.walletconnect.org	IP: 3.125.168.233 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
appkit-lab.reown.com	IP: 66.33.60.193 所属国家: Canada 地区: Ontario 城市: Etobicoke 纬度: 43.623768 经度: -79.559723
gemwallet.com	IP: 104.26.1.14 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.
	IP: 98.159.108.58 所属国家: United States of America

walletconnect.com	地区: California 城市: Los Angeles 纬度: 34.052986 经度: -118.263687
api.web3modal.com	IP: 104.18.28.72 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
keys.walletconnect.org	IP: 3.73.104.2 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
apk.gemwallet.com	IP: 104.26.0.14 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
registry.walletconnect.org	IP: 172.67.21.108 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
verify.walletconnect.org	IP: 172.67.21.108 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

pulse.walletconnect.org	IP: 172.67.21.108 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
ktor.io	IP: 54.230.175.113 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
api.gemwallet.com	IP: 104.26.0.14 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
xmlpull.org	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

 URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	coil3/decode/ImageSourceKt.java
http://xml.org/sax/features/external-general-entities	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/features/external-parameter-entities	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/properties/lexical-handler	com/caverock/androidsvg/SVGParser.java
http://xmlpull.org/v1/doc/features.html	com/caverock/androidsvg/SVGParser.java
https://apk.gemwallet.com/gem_wallet_latest.apk	com/gemwallet/android/BuildConfig.java
https://gemwallet.com	com/gemwallet/android/App.java

https://gemwallet.com/images/gem-logo-256x256.png	com/gemwallet/android/App.java
https://assets.gemwallet.com/blockchains/	com/gemwallet/android/ui/components/image/IconUrlGenerationKt.java
https://api.gemwallet.com	com/gemwallet/android/data/services/gemapi/di/ClientsModule.java
https://assets.gemwallet.com	com/gemwallet/android/data/services/gemapi/di/ClientsModule.java
https://assets.gemwallet.com/blockchains/	com/gemwallet/android/features/stake/components/DelegationItemKt.java
https://assets.gemwallet.com/blockchains/	com/gemwallet/android/features/stake/model/ValidatorExtKt.java
https://apk.gemwallet.com/gem_wallet_universal_v	com/gemwallet/android/features/update_app/viewmodels/InAppUpdateViewModels.java
https://walletconnect.com	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://raw.githubusercontent.com/WalletConnect/WalletConnectKotlinV2/develop/sample/wallet/src/main/res/drawable-xxxhdpi/wc_icon.png	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://appkit-lab.reown.com/wallet_debug	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://appkit-lab.reown.com/wallet_internal	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://appkit-lab.reown.com/wallet_release	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://appkit-lab.reown.com/rn_walletkit_internal	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://appkit-lab.reown.com/rn_walletkit	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://appkit-lab.reown.com/flutter_walletkit	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://appkit-lab.reown.com/flutter_walletkit_internal	com/reown/android/internal/common/modal/domain/usecase/GetSamplesWalletsUseCaseInterfaceKt.java
https://echo.walletconnect.org/	com/reown/android/internal/common/di/PushModuleKt\$pushModule\$1.java
https://registry.walletconnect.org/	com/reown/android/internal/common/di/ExplorerModuleKt\$explorerModule\$1.java
https://verify.walletconnect.org/	com/reown/android/internal/common/di/VerifyModuleKt\$verifyModule\$1.java
https://keys.walletconnect.org	com/reown/android/internal/common/di/KeyServerModuleKt.java
https://api.web3modal.com/	com/reown/android/internal/common/di/AppKitModuleKt\$appKitModule\$1.java
https://pulse.walletconnect.org	com/reown/android/internal/common/di/PulseModuleKt\$pulseModule\$1.java
https://rpc.walletconnect.com/v1/?chainId=eip155:1&projectId=	com/reown/android/internal/common/signing/eip1271/EIP1271Verifier.java

https://ktor.io/docs/faq.html	io/ktor/client/call/NoTransformationFoundException.java
https://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java

✉ 邮箱线索

📱 手机线索

手机号	所在文件
17179869184	com/caverock/androidsvg/SVGAndroidRenderer.java
17179869184	com/caverock/androidsvg/SVGParser.java
17726896976	com/gemwallet/android/ui/components/ComposableSingletons\$TransactionItemKt\$lambda\$962126172\$1.java

🌸 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=EA, ST=Metaverse, L=Cryptoverse, O=Wallet Labs LLC, OU=Gem Wallet, CN=Gem Wallet
签名算法: rsassa_pkcs1v15
有效期自: 2023-05-02 16:34:01+00:00
有效期至: 2050-09-17 16:34:01+00:00
发行人: C=EA, ST=Metaverse, L=Cryptoverse, O=Wallet Labs LLC, OU=Gem Wallet, CN=Gem Wallet
序列号: 0xd43d061265ced0ff
哈希算法: sha384
md5值: 05c790486026130f86906392608a942f
sha1值: 061d80a774ed0a3562b6d184c50d2efd09420d9d
sha256值: b57d7024a923b36a3538e19ed2199ec1e2003b73601e9b0fd7d2affaafa1717b
sha512值: 6474bb4ac3884f394ff99f4b41f6076815da55fcb81a6496666c4a497d4637e2fe8b5ed4253a12caed3ed94c6716a513f0417b44ea2f08ab66a287ee515043a
公钥算法: rsa
密钥长度: 3072
指纹: 39239f3e70194c8878caab2b24d2deba6ff15eced821a845f52f8d078bb5bdf4

🔑 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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.POST_NOTIFICATIONS	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.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云ToDevice消息传递的权限
com.gemwallet.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

--	--

活动(ACTIVITY)	通信(INTENT)
com.gemwallet.android.MainActivity	Schemes: com.android.ApplicationName://, 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。