MoGua

EhViewer 1.13.1.APK 分析报告

No icon

APP名称: EhViewer

包名:	moe.tarsin.ehviewer
域名线索:	19条
URL线索:	49条
邮箱线索:	0条
分析日期:	2025年1月9日
分析平台:	摸瓜APK反编译平台

📦 文件信息

文件名: EhViewer_1.13.1.apk
文件大小: 8.54MB
MD5值: 07d6026dfacacf2a5bc765b23371cbaa
SHA1值: 573ceec600187ea9ffa675fd5eabbd245d3211de
SHA256值: 1262234550491f451d01cb5789e344e33201eea9ee48f2d303b0998941c1e5b8

ⓘ APP 信息

App名称: EhViewer
包名: moe.tarsin.ehviewer
主活动Activity: com.hippo.ehviewer.ui.MainActivity
安卓版本名称: 1.13.1
安卓版本: 180062

ⓠ 域名线索

域名	服务器信息
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
schemas.android.com	没有服务器地理信息.
goo.gle	**IP**: 67.199.248.13 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.750134 **经度**: -73.997009

forums.e-hentai.org	**IP:** 108.160.169.179 **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
s.exhentai.org	**IP:** 184.173.136.86 **所属国家:** United States of America **地区:** California **城市:** San Jose **纬度:** 37.339390 **经度:** -121.894958
developer.android.com	**IP:** 142.251.33.78 **所属国家:** Canada **地区:** Ontario **城市:** Toronto **纬度:** 43.653660 **经度:** -79.382927
youtrack.jetbrains.com	**IP:** 63.33.88.220 **所属国家:** Ireland **地区:** Dublin **城市:** Dublin **纬度:** 53.344151 **经度:** -6.267249
api.e-hentai.org	**IP:** 23.234.30.58 **所属国家:** United States of America **地区:** Delaware **城市:** Newark

	纬度: 39.707489 **经度**: -75.734329
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
ehwiki.org	**IP**: 178.162.151.58 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.378502 **经度**: 4.899980
ktor.io	**IP**: 18.64.123.19 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
ehgt.org	**IP**: 62.112.8.21 **所属国家**: Netherlands **地区**: Zuid-Holland **城市**: Naaldwijk **纬度**: 51.994064 **经度**: 4.209895
e-hentai.org	**IP**: 157.240.10.41 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604
ns.adobe.com	没有服务器地理信息.

issuetracker.google.com	IP: 142.250.217.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
exhentai.org	IP: 199.96.58.105 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
api.github.com	IP: 20.205.243.168 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
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

🌐 URL线索

URL信息	Url所在文件
https://youtrack.jetbrains.com/issue/KT-55980	defpackage/AbstractC0236Da1.java
https://www.slf4j.org/codes.html	defpackage/AbstractC3611hI0.java

https://raw.githubusercontent.com/anansi-project/comicinfo/main/schema/v2.0/ComicInfo.xsd	defpackage/C1148Ot.java
https://goo.gle/compose-feedback	defpackage/AbstractC5092oy.java
https://ehgt.org/	defpackage/FT0.java
https://s.exhentai.org/t/	defpackage/FT0.java
https://exhentai.org/t/	defpackage/FT0.java
https://developer.android.com/training/articles/direct-boot	defpackage/RunnableC4442lb0.java
http://ns.adobe.com/xap/1.0/\u0000	defpackage/Z20.java
http://wrapperns\	defpackage/AbstractC5982tX1.java
https://s.exhentai.org/	defpackage/XE0.java
https://forums.e-hentai.org/	defpackage/C6270v2.java
https://e-hentai.org	defpackage/SR.java
https://exhentai.org	defpackage/SR.java
https://exhentai.org/	defpackage/C1274Qj.java
https://github.com/saket/telephoto/issues/41?\n	defpackage/C5034oe1.java
https://api.github.com/repos/FooIbar/EhViewer	defpackage/C6386vd.java
https://api.github.com/repos/FooIbar/EhViewer/actions/workflows/ci.yml/runs?branch=	defpackage/C6386vd.java
https://api.github.com/repos/FooIbar/EhViewer/releases/latest	defpackage/C6386vd.java
https://api.github.com/repos/FooIbar/EhViewer/compare/	defpackage/C6386vd.java

https://issuetracker.google.com/issues/new?component=907884&template=1466542	defpackage/C6974yg.java
https://e-hentai.org/	defpackage/C4303kt1.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	defpackage/FG.java
https://e-hentai.org/	defpackage/C2429bB1.java
https://e-hentai.org	defpackage/C2429bB1.java
https://exhentai.org	defpackage/C2429bB1.java
https://github.com/saket/telephoto/issues?	defpackage/C6540wQ.java
https://github.com/saket/telephoto/issues	defpackage/C6540wQ.java
https://e-hentai.org/popular	defpackage/C6897yG0.java
https://exhentai.org/popular	defpackage/C6897yG0.java
https://e-hentai.org	defpackage/WA1.java
https://exhentai.org	defpackage/WA1.java
https://issuetracker.google.com/issues/new?component=413106	defpackage/G01.java
https://e-hentai.org	defpackage/C3561h3.java
https://exhentai.org	defpackage/C3561h3.java
https://e-hentai.org/home.php	defpackage/C3561h3.java
https://forums.e-hentai.org/index.php?act=Login&CODE=01	defpackage/C3561h3.java

https://forums.e-hentai.org/index.php?act=Login&CODE=00	defpackage/C3561h3.java
https://forums.e-hentai.org	defpackage/C3561h3.java
https://api.e-hentai.org/api.php	defpackage/C3561h3.java
https://s.exhentai.org/api.php	defpackage/C3561h3.java
https://forums.e-hentai.org/	defpackage/C3561h3.java
https://e-hentai.org/	defpackage/C3561h3.java
https://exhentai.org/uconfig.php	defpackage/C3561h3.java
https://e-hentai.org/exchange.php?t=gp	defpackage/C3561h3.java
https://forums.e-hentai.org/index.php?act=Login	defpackage/AbstractC3851iX1.java
https://e-hentai.org/	defpackage/HZ.java
https://exhentai.org/	defpackage/HZ.java
https://ktor.io/docs/http-client-engines.html	defpackage/AbstractC2738co0.java
http://schemas.android.com/apk/res/android	defpackage/AbstractC2402b32.java
http://wrapperns	defpackage/C3762i42.java
https://forums.e-hentai.org/index.php?act=Reg&CODE=00	defpackage/AbstractC6330vK0.java
https://ehgt.org/	defpackage/HX.java
https://s.exhentai.org/t/	defpackage/HX.java
https://s.exhentai.org/	defpackage/HX.java

https://e-hentai.org/uconfig.php	defpackage/AbstractC4651mg0.java
https://exhentai.org/uconfig.php	defpackage/AbstractC4651mg0.java
https://ktor.io/docs/faq.html	defpackage/IT0.java
https://raw.githubusercontent.com/anansi-project/comicinfo/main/schema/v2.0/ComicInfo.xsd	defpackage/C1304Qt.java
https://ehwiki.org/wiki/	defpackage/C0247De0.java
https://api.e-hentai.org/api.php	defpackage/C6177uY.java
https://s.exhentai.org/api.php	defpackage/C6177uY.java
https://e-hentai.org	defpackage/C6177uY.java
https://exhentai.org	defpackage/C6177uY.java
https://e-hentai.org/mytags	defpackage/AbstractC0097Bg0.java
https://exhentai.org/mytags	defpackage/AbstractC0097Bg0.java
https://e-hentai.org/news.php	defpackage/AbstractC2420b81.java
https://e-hentai.org	defpackage/AbstractC2420b81.java
https://e-hentai.org/news.php	defpackage/V71.java
https://e-hentai.org	defpackage/V71.java
https://exhentai.org/uconfig.php	defpackage/V71.java
https://e-hentai.org/	defpackage/W02.java

https://issuetracker.google.com/issues/241760537	defpackage/C6173uW1.java
https://e-hentai.org/home.php	defpackage/JY.java
https://e-hentai.org/exchange.php?t=gp	defpackage/KY.java
https://e-hentai.org/uconfig.php	defpackage/U71.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	defpackage/C4960oG.java
https://e-hentai.org/uconfig.php	defpackage/C5273pt1.java
https://exhentai.org/uconfig.php	defpackage/C5273pt1.java
https://e-hentai.org	defpackage/C4260kf0.java
https://exhentai.org	defpackage/C4260kf0.java
https://e-hentai.org	defpackage/QR.java
https://exhentai.org	defpackage/QR.java
https://github.com/FooIbar/EhViewer/releases	defpackage/C4904o.java
https://github.com/FooIbar/EhViewer	defpackage/C4904o.java

✉ 邮箱线索

🗄 手机线索

手机号	所在文件

19222222222	defpackage/WA1.java

🏵 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: ST=Unknown, L=Unknown, O=Person, CN=tarsin
签名算法: rsassa_pkcs1v15
有效期自: 2022-05-20 13:59:06+00:00
有效期至: 2047-05-14 13:59:06+00:00
发行人: ST=Unknown, L=Unknown, O=Person, CN=tarsin
序列号: 0x6d2c0ffe
哈希算法: sha256
md5值: 4599da2d5f1a184c6c72803f75269ca4
sha1值: a026976f97a478bb1e83ee43c431e8afc68836a1
sha256值: 5d91dff13b6489a9cfadbb197b3e795eefc8c39f849c4543f32c160720fb40a6
sha512值: b75a9ecff3fc9b58cf80d6bf4a5ec5a59168d81f64921709b8bbde539bfc93b47b692dd667ee40c7ceb39a7c6681ce785fd3966312db5eab6316d99636050a25
公钥算法: rsa
密钥长度: 2048
指纹: 26234b85348c964e30353b4572dc4c181bd92ebbbf0f13ec5dc523a9d61faa62

🔑 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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE_DATA_SYNC	未知	Unknown permission	Unknown permission from android reference
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.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
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.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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
moe.tarsin.ehviewer.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.hippo.ehviewer.ui.MainActivity	Schemes: http://, https://, file://, content://, Hosts: exhentai.org, e-hentai.org, *, Mime Types: application/octet-stream, application/zip, application/x-7z-compressed, application/x-tar, application/x-xz, application/gzip, application/vnd.rar, application/vnd.comicbook+zip, application/vnd.comicbook-rar, application/7z, application/rar, application/x-cbz, application/x-cbr, application/x-cbt, application/x-cb7, application/x-zip-compressed, application/x-rar-compressed, application/x-compressed-tar, application/x-bzip-compressed-tar, application/x-lzma-compressed-tar, application/x-xz-compressed-tar, text/plain, image/*,