MoGua

PornHub 1.6.6.APK 分析报告

APP名称: PornHub

包名:	com.android.pstation.d1731094233685033033
域名线索:	13条
URL线索:	15条
邮箱线索:	1条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: pstation_1.6.6_94337998.apk
文件大小: 24.86MB
MD5值: 77d2e1b96ef7537d6fc07c2aa7c4ebf5
SHA1值: 63ff04a4b9a1937e4e71b83ce017616b705a8ced
SHA256值: df0f3923a16b167b6ac528729f6cda0c7795df54be47e7414816694c7b846ce7

APP 信息

App名称: PornHub
包名: com.android.pstation.d1731094233685033033
主活动Activity: com.grass.cstore.ui.SplashActivity
安卓版本名称: 1.6.6
安卓版本: 166

域名线索

域名	服务器信息
playready.directtaps.net	**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
schemas.microsoft.com	**IP**: 13.107.253.39 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
clsp.fun	**IP**: 127.0.0.1 **所属国家**: - **地区**: -

	城市: - **纬度**: 0.000000 **经度**: 0.000000
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
pz.jeyi6u.xyz	**IP**: 103.224.182.214 **所属国家**: Australia **地区**: Victoria **城市**: Beaumaris **纬度**: -37.982201 **经度**: 145.038940
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
data.flurry.com	没有服务器地理信息.
pz.k0cy4s.xyz	**IP**: 69.16.230.165 **所属国家**: United States of America **地区**: Michigan **城市**: Lansing **纬度**: 42.733280 **经度**: -84.637764
dashif.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

pz.jfklm0.xyz	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
exoplayer.dev	**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
d2pecyfr9ihskt.cloudfront.net	**IP**: 13.35.33.148 **所属国家**: Taiwan (Province of China) **地区**: Taipei **城市**: Taipei **纬度**: 25.038172 **经度**: 121.563599

URL线索

URL信息	Url所在文件
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java

https://pz.jeyi6u.xyz	com/grass/cstore/ui/SplashActivity.java
https://pz.jfklm0.xyz	com/grass/cstore/ui/SplashActivity.java
https://pz.k0cy4s.xyz	com/grass/cstore/ui/SplashActivity.java
https://d2pecyfr9ihskt.cloudfront.net/pz.json	com/grass/cstore/ui/SplashActivity.java
https://clsp.fun	com/grass/cstore/databinding/ActivityShareLayoutBindingImpl.java
https://data.flurry.com/aap.do	e/h/b/s0.java
https://data.flurry.com/v1/flr.do	e/h/b/t0.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	e/i/a/a/t0.java
http://dashif.org/guidelines/last-segment-number	e/i/a/a/h1/j0/j/c.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/SlidingTabLayout.java

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.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=23, ST=23, L=23, O=23, OU=23, CN=23
签名算法: rsassa_pkcs1v15
有效期自: 2022-01-28 09:02:56+00:00
有效期至: 2047-01-22 09:02:56+00:00
发行人: C=23, ST=23, L=23, O=23, OU=23, CN=23
序列号: 0x5ae9264d
哈希算法: sha256
md5值: 391ca6996cc15baf54996949e22415a0
sha1值: f648ba26df7715e43eaf59c01e480c70227e3125
sha256值: baf385b1ad7232db7eaa4e25402468468266877bb48ea0488a3cceec59ed58da
sha512值: 7d0f12360c14312552d3ede6487f6d466d0f42e9aef4dbdd6ec7df09fad87ee960c4ab720128d8a05ecd3c387c44ea021c34cff76f1c091d48286eaa50229f11
公钥算法: rsa

密钥长度: 2048
指纹: 6fbd3a2774d5f581003e47904158138701c16c487c7b0f52b76d8aa160e0730b

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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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_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.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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统

应用内通信