MoGua

重口社 1.7.9.APK 分析报告

APP名称:	重口社

包名:	com.androidjks.kstv.d1742968297958135137
域名线索:	15条
URL线索:	20条
邮箱线索:	3条
分析日期:	2025年4月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 91pron_1.7.9_68387321.apk
文件大小: 26.13MB
MD5值: f8d077166a020e04d708dbc7bb7763c0
SHA1值: 2ce0885caf1b3877dd9c6f8c8fadfa03cf6c642e
SHA256值: 9084e95a3b8917b69f3b6e747d3b5c55b8dc477e1bdcef301276b525c689decf

APP 信息

App名称: 重口社
包名: com.androidjks.kstv.d1742968297958135137
主活动Activity: com.grass.mh.SplashActivity
安卓版本名称: 1.7.9
安卓版本: 179

域名线索

域名	服务器信息
ks.oxfodc.xyz	没有服务器地理信息.
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
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

ns.adobe.com	没有服务器地理信息.
ks.ymqykz.xyz	没有服务器地理信息.
d2kawsyia2dh8i.cloudfront.net	**IP**: 3.164.148.21 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
clsp.fun	**IP**: 143.92.53.201 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
dashif.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
schemas.android.com	没有服务器地理信息.
d2pugxkmpwkrrb.cloudfront.net	**IP**: 18.154.149.230 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
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
drikj7343ari7.cloudfront.net	**IP**: 3.163.128.49 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
data.flurry.com	没有服务器地理信息.
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.microsoft.com	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

URL线索

URL**信息**	Url**所在文件**
http://schemas.android.com/apk/res/android	c/j/b/b/e.java
http://ns.adobe.com/xap/1.0/\u0000	c/n/a/a.java
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://ks.oxfodc.xyz	com/grass/mh/SplashActivity.java
https://ks.ymqykz.xyz	com/grass/mh/SplashActivity.java
https://drikj7343ari7.cloudfront.net/ks_ldy.json	com/grass/mh/SplashActivity.java
https://d2pugxkmpwkrrb.cloudfront.net/ks.json	com/grass/mh/SplashActivity.java
https://d2kawsyia2dh8i.cloudfront.net/ks.json	com/grass/mh/SplashActivity.java
https://clsp.fun	com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java
https://data.flurry.com/aap.do	e/e/b/s0.java
https://data.flurry.com/v1/flr.do	e/e/b/t0.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	e/f/a/a/t0.java
http://dashif.org/guidelines/last-segment-number	e/f/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://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/SlidingTabLayout.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	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	n/a/a/f.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

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java
zimuquan01@gmail.com	e/g/a/b0.java
zimuquan01@gmail.com	摸瓜V1引擎

手机线索

手机号	所在文件
	tv/danmaku/ijk/media/player/IjkMediaMeta.java

17179869184	

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=24, ST=24, L=24, O=24, OU=24, CN=24
签名算法: rsassa_pkcs1v15
有效期自: 2023-05-20 04:30:49+00:00
有效期至: 2048-05-13 04:30:49+00:00
发行人: C=24, ST=24, L=24, O=24, OU=24, CN=24
序列号: 0x32fb0dde
哈希算法: sha256
md5值: 981d4e370caa310e449070ce49a8c0ba
sha1值: a1dfb5f19a586534bc15a340a2738d4b1277744e
sha256值: a2bf8011f52ba69f99422acbf0fd2465f03db4cd4498c439b4064699dabf1904
sha512值: 2d5c1775b32648466a3ae999f1c9ffcb7db786aa7b7cd23f848327ed2143a81a62c9b9fb4fc5feb1355c7fe97cc15fe48ca9360471ac1797ebd01dd784d3a98b
公钥算法: rsa
密钥长度: 2048
指纹: 9b1c03f92f3eab79b40cfd21e4d221967faf26ca7f0eb1297d42ce5b6400e247

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.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.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.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
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

应用内通信
