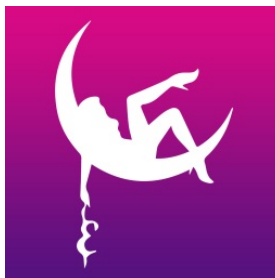




MoGua

..午夜影院.. 48246046 1.2.3.APK 分析报告



APP名称:

..午夜影院.. 48246046

包名:	com.asf.dvo.klhzy
域名线索:	17条
URL线索:	23条
邮箱线索:	1条
分析日期:	2025年8月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 1730191693.apk

文件大小: 25.78MB
MD5值: a86b1f4015940d5c87393f2cb4be74e1
SHA1值: c14bb6cb691b2b954c70473dd1fff7d3984b4baf
SHA256值: dd6b6a1ecd39064cfa56058dadfa845c1a1a4d6c4ca93620f81c81321eb61d82

i APP 信息

App名称: ..午夜影院.. 48246046
包名: com.asf.dvo.klhzy
主活动Activity: net.aiyida.coco.ui.loading.LoadingActivity
安卓版本名称: 1.2.3
安卓版本: 33

🔍 域名线索

域名	服务器信息
xml.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
api.fidn3.com	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
lucaapap.dyami.top	IP: 125.39.165.87 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102

api.wuc0jp1e.com	没有服务器地理信息.
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
vfx.mtime.cn	IP: 121.29.38.198 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
gitlab.com	IP: 172.65.251.78 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.khlapi2.com	IP: 45.207.12.21 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.baidu.com	IP: 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
download.wuc0jp1e.com	没有服务器地理信息.

api.canary.shdewqknc.com	IP: 154.86.23.52 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
cms-bucket.nosdn.127.net	IP: 60.222.200.223 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
api.canary.tianyapro.top	没有服务器地理信息.
api.khlapi1.com	IP: 45.207.12.21 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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
github.net.aiyida.coco	没有服务器地理信息.

 URL线索

URL信息	Url所在文件

http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://github.net.aiyida.coco/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.net.aiyida.coco/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.net.aiyida.coco/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
https://github.net.aiyida.coco/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
https://api.wuc0jp1e.com/	com/example/mvvmlibrary/net/ApiService.java
https://api.canary.shdewqknc.com	com/example/mvvmlibrary/net/ApiService.java
https://gitlab.com/yes6677/sdfafdfdf/raw/main/ssdfdsdf	com/example/mvvmlibrary/net/ApiService.java
https://gitlab.com/yes6677/sdfafdfdf/raw/main/test	com/example/mvvmlibrary/net/ApiService.java
http://api.fidn3.com/	com/example/mvvmlibrary/net/DownloadService.java
https://api.wuc0jp1e.com/	com/example/mvvmlibrary/net/ApiServiceByServerConfig.java
https://api.canary.tianyapro.top	com/example/mvvmlibrary/net/ApiServiceByServerConfig.java
https://gitlab.com/yes6677/sdfafdfdf/raw/main/ssdfdsdf	com/example/mvvmlibrary/net/ApiServiceByServerConfig.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java

https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.java
https://api.khlapi1.com	net/aiyida/coco/BuildConfig.java
https://api.khlapi2.com	net/aiyida/coco/BuildConfig.java
https://lucaapap.dyami.top	net/aiyida/coco/BuildConfig.java
http://vfx.mtime.cn/Video/2019/03/14/mp4/190314223540373995.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
https://cms-bucket.nosdn.127.net/eb411c2810f04ffa8aaafc42052b233820180418095416.jpeg	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/02/04/mp4/190204084208765161.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
https://cms-bucket.nosdn.127.net/cb37178af1584c1588f4a01e5ecf323120180418133127.jpeg	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/21/mp4/190321153853126488.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/19/mp4/19031922227698228.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/19/mp4/190319212559089721.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/18/mp4/190318231014076505.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/18/mp4/190318214226685784.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java

http://vfx.mtime.cn/Video/2019/03/19/mp4/190319104618910544.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/19/mp4/190319125415785691.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/17/mp4/190317150237409904.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/14/mp4/190314102306987969.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/13/mp4/190313094901111138.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/12/mp4/190312143927981075.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://vfx.mtime.cn/Video/2019/03/12/mp4/190312083533415853.mp4	net/aiyida/coco/shortVideo/util/DataUtil.java
http://127.0.0.1:%d%s	net/aiyida/coco/shortVideo/util/m3u8downloader/M3U8DownloadTask.java
http://127.0.0.1:	net/aiyida/coco/shortVideo/util/m3u8downloader/server/M3U8HttpServer.java
http://127.0.0.1:%d%s	net/aiyida/coco/shortVideo/util/m3u8downloader/server/M3U8HttpServer.java
http://www.baidu.com	net/aiyida/coco/ui/main/fragment/model/GamePageModel\$getUrl\$1.java
https://download.wuc0jp1e.com/d/v3/image/dl?id=file%3A%2F%2F%2F5577cbdf8d29687f0e6c82d4c801730.jpg	net/aiyida/coco/ui/post/BloggerActivity.java
https://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎

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: True
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-29 08:47:34+00:00
有效期至: 2052-03-16 08:47:34+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x884173355a7a4edb
哈希算法: sha256
md5值: 78bbea7911495eca495147ae81816679
sha1值: 4b26bb9627342c84a6bb2a600898484c5f6171d1
sha256值: 637e1392ad5c705e00c8f4b2fcd73dc5ccc619c92a31ca43e12728b903e9a6c6
sha512值: 8d179d09c17452f894f4a31cbdcecb4d5af32ace215ac100fd9c899047434a4a13067a16c95b78fc6a5922aaf4d1c52ddc2b51ef41a8087bcda89a1ccf343c30
公钥算法: rsa
密钥长度: 2048
指纹: 524af2b512d7aff4c777ca05ada8e4dbaf2d9c7d7e022268c6de490f576863a0

硬编码敏感信息

可能的敏感信息
"check_password" : "确认密码"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"password" : "请输入密码"
"user_name" : "请输入用户名"
"check_password" : "确认密码"
"password" : "请输入密码"
"user_name" : "请输入用户名"
"check_password" : "check password"
"password" : "password"
"user_name" : "phone"

加壳分析

加壳类型	所属文件
盛旺集团网站门户	

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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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.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。
	正常	获取网络、	允许应用程序创建网络套接字

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.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_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
com.android.providers.media.MediaProvider	未知	Unknown permission	Unknown permission from android reference
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_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.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

应用内通信

活动(ACTIVITY)	通信(INTENT)
net.aiyida.coco.ui.loading.LoadingActivity	Schemes: ae03se://,
net.aiyida.coco.ui.loading.TianqiLoadingActivity	Schemes: ae03se://,
net.aiyida.coco.ui.loading.AnquanLoadingActivity	Schemes: ae03se://,
net.aiyida.coco.ui.loading.QingliLoadingActivity	Schemes: ae03se://,

net.aiyida.coco.ui.loading.WenjianjiaLoadingActivity	Schemes: ae03se://,
--	---------------------

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。