MoGua

TVBox 20221018-1518.APK 分析报告

APP名称: TVBox

包名:	com.github.tvbox.osc
域名线索:	29条
URL线索:	20条
邮箱线索:	4条
分析日期:	2024年9月24日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: TVbox最新版.apk
文件大小: 13.12MB
MD5值: ec1519aa5742dafefd2c679a7a2df206
SHA1值: 264cd9694755967af424228d2a76dbec127c927d
SHA256值: f6585661746d3e2898f4466b5332c8244fd919de285add796f950fb1e37810c0

APP 信息

App名称: TVBox
包名: com.github.tvbox.osc
主活动Activity: com.github.tvbox.osc.ui.activity.HomeActivity
安卓版本名称: 20221018-1518
安卓版本: 1

域名线索

域名	服务器信息
api.pullword.com	**IP**: 47.56.210.205 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
suggest.video.iqiyi.com	**IP**: 116.211.198.189 **所属国家**: China **地区**: Hubei **城市**: Wuhan **纬度**: 30.583330 **经度**: 114.266853
schemas.android.com	没有服务器地理信息.
	IP: 202.160.130.145

www.btspread.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
com.thoughtworks.xstream	没有服务器地理信息.
ipip-darwin.xycdn.com	**IP**: 121.228.176.25 **所属国家**: China **地区**: Jiangsu **城市**: Suzhou **纬度**: 31.311365 **经度**: 120.617691
seeds-darwin.xycdn.com	**IP**: 140.249.254.142 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
www.ibm.com	**IP**: 104.101.129.116 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
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
seeds1-darwin.xycdn.com	**IP**: 121.228.176.151 **所属国家**: China **地区**: Jiangsu

	城市: Suzhou **纬度**: 31.311365 **经度**: 120.617691
cache.tkys.tv	没有服务器地理信息.
xmlpull.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
underscorejs.org	**IP**: 172.67.134.18 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
schemas.xmlsoap.org	**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
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
www.openssl.org	**IP**: 23.52.189.201 **所属国家**: Colombia **地区**: Distrito Capital de Bogota **城市**: Bogota **纬度**: 4.609710 **经度**: -74.081749

sdk1xyajs.data.p2cdn.com	没有服务器地理信息.
seeds3-darwin.xycdn.com	**IP**: 140.249.254.142 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
xml.org	**IP**: 104.239.240.11 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
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
xmlconf.rcv.sandai.net	**IP**: 101.133.169.157 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
seeds2-darwin.xycdn.com	**IP**: 140.249.254.142 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
	IP: 222.209.245.177

epg.51zmt.top	**所属国家**: China **地区**: Sichuan **城市**: Chengdu **纬度**: 30.666670 **经度**: 104.066269
fcrc.video.p2cdn.com	没有服务器地理信息.
d1.lengziyuan.com	没有服务器地理信息.
node.video.qq.com	**IP**: 109.244.244.237 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
conf-darwin.xycdn.com	**IP**: 140.249.63.92 **所属国家**: China **地区**: Shandong **城市**: Linyi **纬度**: 35.063061 **经度**: 118.342781
torcache.net	**IP**: 185.53.177.11 **所属国家**: Germany **地区**: Bayern **城市**: Munich **纬度**: 48.137428 **经度**: 11.575490
crosswalk-project.org	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html	org/xmlpull/v1/XmlPullParser.java
http://schemas.android.com/apk/res-auto	org/xwalk/core/XWalkView.java
https://suggest.video.iqiyi.com/	com/github/tvbox/osc/ui/activity/SearchActivity.java
https://node.video.qq.com/x/api/hot_search	com/github/tvbox/osc/ui/activity/SearchActivity.java
http://api.pullword.com/get.php?source=	com/github/tvbox/osc/ui/activity/FastSearchActivity.java
http://127.0.0.1	com/github/tvbox/osc/ui/activity/PlayActivity.java
http://epg.51zmt.top:8000/api/diyp/	com/github/tvbox/osc/ui/activity/LivePlayActivity.java
http://127.0.0.1	com/github/tvbox/osc/ui/activity/LivePlayActivity.java
http://apache.org/xml/features/disallow-doctype-decl	com/thoughtworks/xstream/io/xml/JDomDriver.java
http://apache.org/xml/features/disallow-doctype-decl	com/thoughtworks/xstream/io/xml/Dom4JDriver.java
http://com.thoughtworks.xstream/XStreamSource/feature	com/thoughtworks/xstream/io/xml/TraxSource.java
http://apache.org/xml/features/disallow-doctype-decl	com/thoughtworks/xstream/io/xml/DomDriver.java
http://apache.org/xml/features/disallow-doctype-decl	com/thoughtworks/xstream/io/xml/JDom2Driver.java
http://com.thoughtworks.xstream/sax/property/configured-xstream	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://com.thoughtworks.xstream/sax/property/source-object-list	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://xml.org/sax/features/namespaces	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://xml.org/sax/features/namespace-prefixes	com/thoughtworks/xstream/io/xml/SaxWriter.java

http://com.thoughtworks.xstream/sax/property/configured-xstream\	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://com.thoughtworks.xstream/sax/property/source-object-list\	com/thoughtworks/xstream/io/xml/SaxWriter.java
https://cache.tkys.tv/m3u8/dsj/guochan/mp1/1.m3u8	tv/danmaku/ijk/media/player/demo/IjkDemoActivity.java
https://crosswalk-project.org/).	Mogua Engine V1
http://'+r+'	Mogua Engine V2
http://www.w3.org/1999/xhtml	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/XML/1998/namespace	Mogua Engine V2
http://www.w3.org/2000/xmlns/	Mogua Engine V2
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	Mogua Engine V2
https://underscorejs.org	Mogua Engine V2
http://xmlconf.rcv.sandai.net/?appid=	lib/armeabi-v7a/libxl_stat.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libconceal.so
https://torcache.net/	lib/armeabi-v7a/libxl_thunder_sdk.so
http://www.btspread.com/	lib/armeabi-v7a/libxl_thunder_sdk.so

http://www.btspread.com/	lib/armeabi-v7a/libxl_thunder_sdk.so
http://d1.lengziyuan.com/?infohash=	lib/armeabi-v7a/libxl_thunder_sdk.so
http://i	lib/armeabi-v7a/libxl_thunder_sdk.so
http://127.0.0.1:%d/%s	lib/armeabi-v7a/libxl_thunder_sdk.so
http://127.0.0.1:%d/%s%s	lib/armeabi-v7a/libxl_thunder_sdk.so
http://conf-darwin.xycdn.com/psdk_param?version=	lib/armeabi-v7a/libxl_thunder_sdk.so
http://ipip-darwin.xycdn.com/dnsQuery?domain=	lib/armeabi-v7a/libxl_thunder_sdk.so
http://seeds-darwin.xycdn.com/psdk/getseeds	lib/armeabi-v7a/libxl_thunder_sdk.so
http://sdk1xyajs.data.p2cdn.com/o_live_p2p_mobilesdk	lib/armeabi-v7a/libxl_thunder_sdk.so
http://seeds1-darwin.xycdn.com/psdk/getseeds	lib/armeabi-v7a/libxl_thunder_sdk.so
http://seeds2-darwin.xycdn.com/psdk/getseeds	lib/armeabi-v7a/libxl_thunder_sdk.so
http://seeds3-darwin.xycdn.com/psdk/getseeds	lib/armeabi-v7a/libxl_thunder_sdk.so
http://%s]	lib/armeabi-v7a/libxl_thunder_sdk.so
http://%s],	lib/armeabi-v7a/libxl_thunder_sdk.so
http://%s].	lib/armeabi-v7a/libxl_thunder_sdk.so
http://fcrc.video.p2cdn.com/flashp2p_chat_demo/flashp2pchatdemo.swf	lib/armeabi-v7a/libxl_thunder_sdk.so
http://fcrc.video.p2cdn.com/flashp2p_chat_demo/	lib/armeabi-v7a/libxl_thunder_sdk.so
http://[fe80:	lib/armeabi-v7a/libxl_thunder_sdk.so

http://schemas.xmlsoap.org/soap/envelope/	lib/armeabi-v7a/libxl_thunder_sdk.so
http://schemas.xmlsoap.org/soap/encoding/	lib/armeabi-v7a/libxl_thunder_sdk.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libxl_thunder_sdk.so

邮箱线索

邮箱地址	所在文件
null@null.xml	com/thoughtworks/xstream/persistence/FilePersistenceStrategy.java
jhruby.web@gmail.com	Mogua Engine V2
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libplayer.so
download@qq.com	lib/armeabi-v7a/libxl_thunder_sdk.so

手机线索

手机号	所在文件
13923744320	com/xunlei/downloadlib/XLAppKeyChecker.java
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=TVBoxOSC, ST=TVBoxOSC, L=TVBoxOSC, O=TVBoxOSC, OU=TVBoxOSC, CN=TVBoxOSC
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-24 03:53:08+00:00
有效期至: 2032-06-21 03:53:08+00:00
发行人: C=TVBoxOSC, ST=TVBoxOSC, L=TVBoxOSC, O=TVBoxOSC, OU=TVBoxOSC, CN=TVBoxOSC
序列号: 0x4d304996
哈希算法: sha256
md5值: 1c3a6151c2760010bd0e969b857ea43e
sha1值: 926f6f00d5013972c8567f6d382ebd52c40329d3
sha256值: 4b9421de6d46778f6280b180179413fa6973845f0a0132c00f6800c06464e051
sha512值: 72ae5900eb168961537179fea8230970f3b7951586e03dd396655676006fc2d15c01c51178bf6f3aaf5b76fdd89a45182c93a188413a8348a7c6f7612b10ad6b
公钥算法: rsa
密钥长度: 2048
指纹: cb71940cb11c6e2a3465eb5784fdca872c44890f9bb96e5a2ccb45a87d9efce3

硬编码敏感信息

可能的敏感信息
"http_auth_log_in" : "Log In"
"http_auth_password" : "Password"
"http_auth_title" : "Authentication Required"
"http_auth_user_name" : "Username"

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.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.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
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.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
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.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.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.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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息

应用内通信