Evaluation Warning: The document was created with Spire.Doc for Python.

**TVBox（ 20221018-1518版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | TVBox |
| 版本 | 20221018-1518 |
| 包名 | com.github.tvbox.osc |
| 域名线索 | 29条 |
| URL线索 | 20条 |
| APP图标 |  |
| 分析日期 | 2024年11月22日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | TVbox最新版.apk |
| 文件大小 | 13.12MB |
| MD5值 | ec1519aa5742dafefd2c679a7a2df206 |
| SHA1值 | 264cd9694755967af424228d2a76dbec127c927d |
| SHA256值 | f6585661746d3e2898f4466b5332c8244fd919de285add796f950fb1e37810c0 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| suggest.video.iqiyi.com | IP: 116.211.198.189 所属国家: China 地区: Hubei 城市: Wuhan  |
| schemas.android.com | 没有服务器地理信息.  |
| www.btspread.com | IP: 202.160.130.145 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 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  |
| seeds-darwin.xycdn.com | IP: 140.249.254.142 所属国家: China 地区: Shandong 城市: Qingdao  |
| www.ibm.com | IP: 104.101.129.116 所属国家: United States of America 地区: California 城市: Los Angeles  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| seeds1-darwin.xycdn.com | IP: 121.228.176.151 所属国家: China 地区: Jiangsu 城市: Suzhou  |
| 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  |
| underscorejs.org | IP: 172.67.134.18 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.xmlsoap.org | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.openssl.org | IP: 23.52.189.201 所属国家: Colombia 地区: Distrito Capital de Bogota 城市: Bogota  |
| 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  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| xmlconf.rcv.sandai.net | IP: 101.133.169.157 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| seeds2-darwin.xycdn.com | IP: 140.249.254.142 所属国家: China 地区: Shandong 城市: Qingdao  |
| epg.51zmt.top | IP: 222.209.245.177 所属国家: China 地区: Sichuan 城市: Chengdu  |
| 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  |
| conf-darwin.xycdn.com | IP: 140.249.63.92 所属国家: China 地区: Shandong 城市: Linyi  |
| torcache.net | IP: 185.53.177.11 所属国家: Germany 地区: Bayern 城市: Munich  |
| crosswalk-project.org | 没有服务器地理信息.  |

### **4.2 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://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  |

### **4.3 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  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13923744320  | com/xunlei/downloadlib/XLAppKeyChecker.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 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**

## **6. 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"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**