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

**00TV（ 2.1.0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 | 00TV |
| 版本 | 2.1.0 |
| 包名 | com.o00.android.movie |
| 域名线索 | 78条 |
| URL线索 | 58条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | kb000.apk |
| 文件大小 | 15.41MB |
| MD5值 | 437771960eb38240d63190a7f5d3c9d1 |
| SHA1值 | 821a7d538db498afac024c5784e0b32d88bb856e |
| SHA256值 | 365d81a6315d137da4bdfaf6a5acefd5c7d02a02fb65bc1a44dc1ec563a96931 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 00TV |
| 包名 | com.o00.android.movie |
| 主活动Activity | com.fongmi.android.tv.ui.activity.MainActivity |
| 安卓版本名称 | 2.1.0 |
| 安卓版本 | 210 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developers.cloudflare.com | IP: 104.16.5.189  所属国家: United States of America  地区: California  城市: San Francisco |
| openrcv.baidu.com | IP: 111.206.209.112  所属国家: China  地区: Beijing  城市: Beijing |
| www.sec.co.kr | IP: 112.106.187.200  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| dashif.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| www.ibm.com | IP: 23.13.189.250  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| schemas.android.com | 没有服务器地理信息. |
| o00tv.com | IP: 192.69.90.129  所属国家: United States of America  地区: California  城市: Los Angeles |
| dns.sb | IP: 185.222.222.222  所属国家: Belgium  地区: Brussels Hoofdstedelijk Gewest  城市: Brussels |
| www.jiesuomi.com | IP: 140.238.36.223  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| dns10.quad9.net | IP: 149.112.112.10  所属国家: United States of America  地区: California  城市: San Francisco |
| www.slf4j.org | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| dns.quad9.net | IP: 149.112.112.112  所属国家: United States of America  地区: California  城市: San Francisco |
| doh-02.spectrum.com | IP: 24.240.146.8  所属国家: United States of America  地区: Minnesota  城市: Saint Cloud |
| www.quad9.net | IP: 216.21.3.77  所属国家: United States of America  地区: California  城市: Berkeley |
| dns64.dns.google | 没有服务器地理信息. |
| wpa.qq.com | IP: 125.39.104.95  所属国家: China  地区: Tianjin  城市: Tianjin |
| doh.xfinity.com | IP: 75.75.77.99  所属国家: United States of America  地区: Massachusetts  城市: Chelmsford |
| doh.cleanbrowsing.org | IP: 185.228.168.168  所属国家: United States of America  地区: California  城市: Temecula |
| public.dns.iij.jp | IP: 103.2.57.5  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| xml.org | IP: 104.239.240.11  所属国家: United States of America  地区: Texas  城市: Windcrest |
| doh.dns.sb | IP: 103.121.210.210  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| u.o00tv.top | IP: 132.226.7.246  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| chromium.dns.nextdns.io | IP: 45.11.104.186  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| chrome.cloudflare-dns.com | IP: 162.159.61.3  所属国家: United States of America  地区: California  城市: San Francisco |
| purl.org | IP: 207.241.239.242  所属国家: United States of America  地区: California  城市: San Francisco |
| npms.io | IP: 172.67.152.251  所属国家: United States of America  地区: California  城市: San Francisco |
| xmlpull.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| odvr.nic.cz | IP: 185.43.135.1  所属国家: Czechia  地区: Praha, Hlavni mesto  城市: Prague |
| hmma.baidu.com | IP: 110.242.68.196  所属国家: China  地区: Hebei  城市: Baoding |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| www.oracle.com | IP: 184.50.92.108  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| schemas.microsoft.com | IP: 13.107.213.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| youtubei.googleapis.com | IP: 172.217.163.42  所属国家: United States of America  地区: California  城市: Mountain View |
| dns11.quad9.net | IP: 9.9.9.11  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| ns.adobe.com | 没有服务器地理信息. |
| o00tv.link | IP: 192.69.90.129  所属国家: United States of America  地区: California  城市: Los Angeles |
| developer.android.com | IP: 172.217.163.46  所属国家: United States of America  地区: California  城市: Mountain View |
| ghproxy.net | IP: 51.195.241.253  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: London |
| www.cisco.com | IP: 184.50.93.5  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| aomedia.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| api.live.bilibili.com | IP: 221.204.56.92  所属国家: China  地区: Shanxi  城市: Taiyuan |
| www.youtube.com | IP: 128.242.240.59  所属国家: United States of America  地区: Washington  城市: Redmond |
| doh.quickline.ch | IP: 212.60.61.246  所属国家: Switzerland  地区: Bern  城市: Biel |
| dns.google | IP: 8.8.8.8  所属国家: United States of America  地区: California  城市: Mountain View |
| nextdns.io | IP: 172.67.75.111  所属国家: United States of America  地区: California  城市: San Francisco |
| raw.githubusercontent.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| api.web.360kan.com | IP: 101.199.255.49  所属国家: China  地区: Beijing  城市: Beijing |
| datax.baidu.com | 没有服务器地理信息. |
| developers.google.com | IP: 172.217.163.46  所属国家: United States of America  地区: California  城市: Mountain View |
| suggest.video.iqiyi.com | IP: 123.126.131.94  所属国家: China  地区: Beijing  城市: Beijing |
| dxp.baidu.com | IP: 110.242.68.94  所属国家: China  地区: Hebei  城市: Baoding |
| alekberg.net | 没有服务器地理信息. |
| journeyapps.com | IP: 18.155.68.69  所属国家: Singapore  地区: Singapore  城市: Singapore |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| dnsnl.alekberg.net | IP: 89.38.131.38  所属国家: Netherlands  地区: Flevoland  城市: Dronten |
| www.4thline.org | IP: 51.15.52.165  所属国家: Netherlands  地区: Noord-Holland  城市: Haarlem |
| u.o00tv.com | IP: 132.226.7.246  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| cleanbrowsing.org | IP: 45.77.168.207  所属国家: Singapore  地区: Singapore  城市: Singapore |
| developer.apple.com | IP: 17.253.87.204  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.360kan.com | IP: 110.242.21.33  所属国家: China  地区: Hebei  城市: Baoding |
| schemas.xmlsoap.org | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| doh.opendns.com | IP: 146.112.41.2  所属国家: United States of America  地区: Washington  城市: Vancouver |
| t.me | IP: 149.154.167.99  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Warrington |
| u.o00tv.link | 没有服务器地理信息. |
| doh.cox.net | IP: 68.105.28.11  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| default.url | 没有服务器地理信息. |
| www.nic.cz | IP: 217.31.205.50  所属国家: Czechia  地区: Praha, Hlavni mesto  城市: Prague |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| o00tv.top | IP: 192.69.90.129  所属国家: United States of America  地区: California  城市: Los Angeles |
| javax.xml.xmlconstants | 没有服务器地理信息. |
| doh.familyshield.opendns.com | IP: 146.112.41.3  所属国家: United States of America  地区: Washington  城市: Vancouver |
| m.kb000.xyz | IP: 216.24.184.197  所属国家: United States of America  地区: California  城市: Los Angeles |
| dns.switch.ch | IP: 130.59.31.251  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| mozilla.github.io | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| doh-01.spectrum.com | IP: 24.240.146.7  所属国家: United States of America  地区: Minnesota  城市: Saint Cloud |
| pic.rmb.bdstatic.com | IP: 123.130.123.35  所属国家: China  地区: Shandong  城市: Yantai |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android | b0/k.java |
| https://o00tv.top/json/00tv.json | c6/v.java |
| https://hmma.baidu.com/auto.gif | com/baidu/mobstat/Config.java |
| http://hmma.baidu.com/app.gif | com/baidu/mobstat/Config.java |
| https://hmma.baidu.com/app.gif | com/baidu/mobstat/Config.java |
| https://openrcv.baidu.com/1010/bplus.gif | com/baidu/mobstat/r.java |
| https://datax.baidu.com/xs.gif | com/baidu/mobstat/y.java |
| https://dxp.baidu.com/upgrade | com/baidu/mobstat/y.java |
| https://suggest.video.iqiyi.com/?if=mobile&key= | com/fongmi/android/tv/ui/activity/CollectActivity.java |
| http://127.0.0.1: | com/fongmi/quickjs/method/Global.java |
| https://www.youtube.com/embed/ | ec/b.java |
| https://www.youtube.com | ec/b.java |
| https://www.youtube.com/s/player/%s/player\_ias.vflset/en\_US/base.js | ec/b.java |
| https://www.youtube.com/iframe\_api | ec/b.java |
| https://www.youtube.com/youtubei/v1/guide?key=AIzaSyAO\_FJ2SlqU8Q4STEHLGCilw\_Y9\_11qcW8&prettyPrint=false | ec/h.java |
| https://www.youtube.com/watch?v= | ec/h.java |
| https://www.youtube.com/results?search\_query=&ucbcb=1 | ec/h.java |
| https://www.youtube.com/sw.js | ec/h.java |
| https://www.youtube.com/youtubei/v1/ | ec/h.java |
| https://youtubei.googleapis.com/youtubei/v1/ | ec/h.java |
| https://www.youtube.com | ec/h.java |
| https://www.youtube.com | gc/b.java |
| https://www.youtube.com/watch?v= | gc/b.java |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted | h1/o.java |
| https://www.jiesuomi.com | h6/c.java |
| http://wpa.qq.com | h6/d.java |
| https://t.me | h6/d.java |
| https://o00tv.com/ | h6/i.java |
| http://m.kb000.xyz/opt/index | h6/k.java |
| https://api.web.360kan.com/v1/rank?cat=1 | h6/u.java |
| https://www.360kan.com/rank/general | h6/u.java |
| http://www.w3.org/ns/ttml | i3/c.java |
| http://purl.org/dc/elements/1.1/\ | j4/d.java |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread | m1/b0.java |
| https://o00tv.com/ | n3/e.java |
| https://o00tv.com/ | n5/c.java |
| http://ns.adobe.com/xap/1.0/ | o2/a.java |
| http://www.sec.co.kr/dlna | org/fourthline/cling/binding/xml/Descriptor.java |
| http://schemas.xmlsoap.org/soap/envelope/ | org/fourthline/cling/model/Constants.java |
| http://schemas.xmlsoap.org/soap/encoding/ | org/fourthline/cling/model/Constants.java |
| http://www.w3.org/2000/xmlns/ | org/fourthline/cling/support/contentdirectory/DIDLParser.java |
| http://purl.org/dc/elements/1.1/ | org/fourthline/cling/support/model/DIDLObject.java |
| http://www.sec.co.kr/ | org/fourthline/cling/support/model/DIDLObject.java |
| http://www.4thline.org/projects/mailinglists-cling.html\n\n | org/fourthline/cling/support/shared/Main.java |
| http://127.0.0.1 | org/mozilla/javascript/tools/debugger/Dim.java |
| http://javax.xml.XMLConstants/feature/secure-processing | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://apache.org/xml/features/disallow-doctype-decl | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://javax.xml.XMLConstants/property/accessExternalDTD | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://javax.xml.XMLConstants/property/accessExternalStylesheet | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://www.w3.org/2000/xmlns/ | org/mozilla/javascript/xmlimpl/XmlNode.java |
| http://www.w3.org/2001/xml.xsd | org/seamless/xml/b.java |
| http://www.w3.org/2001/xml.xsd | org/seamless/xml/g.java |
| http://www.w3.org/2001/XMLSchema | org/seamless/xml/g.java |
| http://apache.org/xml/features/xinclude/fixup-base-uris | org/seamless/xml/d.java |
| http://apache.org/xml/features/xinclude/fixup-language | org/seamless/xml/d.java |
| http://www.oracle.com/xml/is-standalone | org/seamless/xml/d.java |
| http://xml.apache.org/xslt | org/seamless/xml/d.java |
| http://www.w3.org/2001/XMLSchema | org/seamless/xml/d.java |
| http://www.w3.org/TR/html4/loose.dtd | org/seamless/xml/d.java |
| http://www.w3.org/1999/xhtml\ | org/seamless/xml/d.java |
| http://xmlpull.org/v1/doc/features.html | org/xmlpull/v1/XmlPullParser.java |
| http://xmlpull.org/v1/doc/properties.html | org/xmlpull/v1/builder/impl/XmlPullBuilderImpl.java |
| http://apache.org/xml/features/validation/dynamic | org/xmlpull/v1/sax2/Driver.java |
| http://apache.org/xml/features/validation/schema | org/xmlpull/v1/sax2/Driver.java |
| http://xml.org/sax/properties/declaration-handler | org/xmlpull/v1/sax2/Driver.java |
| http://xml.org/sax/properties/lexical-handler | org/xmlpull/v1/sax2/Driver.java |
| http://xml.org/sax/features/namespaces | org/xmlpull/v1/sax2/Driver.java |
| http://xml.org/sax/features/namespace-prefixes | org/xmlpull/v1/sax2/Driver.java |
| http://xml.org/sax/features/validation | org/xmlpull/v1/sax2/Driver.java |
| http://www.w3.org/2001/XMLSchema-instance | org/xmlpull/v1/wrapper/XmlPullParserWrapper.java |
| http://www.w3.org/2001/XMLSchema-instance | org/xmlpull/v1/wrapper/XmlSerializerWrapper.java |
| http://www.w3.org/2001/XMLSchema-instance | org/xmlpull/v1/wrapper/classic/StaticXmlPullParserWrapper.java |
| http://xmlpull.org/v1/doc/features.html | org/xmlpull/v1/wrapper/classic/StaticXmlSerializerWrapper.java |
| http://www.w3.org/2001/XMLSchema-instance | org/xmlpull/v1/wrapper/classic/StaticXmlSerializerWrapper.java |
| http://www.w3.org/2001/XMLSchema-instance | org/xmlpull/v1/util/XmlPullUtil.java |
| https://pic.rmb.bdstatic.com/bjh/1d0b02d0f57f0a42201f92caba5107ed.jpeg | p5/w.java |
| http://dashif.org/thumbnail\_tile | q1/d.java |
| http://dashif.org/guidelines/thumbnail\_tile | q1/d.java |
| http://dashif.org/guidelines/trickmode | q1/d.java |
| http://dashif.org/guidelines/last-segment-number | q1/d.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | r1/s.java |
| https://x</LA\_URL> | r1/r.java |
| https://default.url | r1/r.java |
| https://aomedia.org/emsg/ID3 | r2/a.java |
| https://developer.apple.com/streaming/emsg-id3 | r2/a.java |
| http://www.slf4j.org/codes.html | rc/c.java |
| https://u.o00tv.top/ | v6/a.java |
| https://u.o00tv.com/ | v6/a.java |
| https://u.o00tv.link/ | v6/a.java |
| https://raw.githubusercontent.com/ | v6/a.java |
| https://ghproxy.net/ | v6/a.java |
| http://ns.adobe.com/xap/1.0/\u0000 | w0/a.java |
| https://api.live.bilibili.com/room/v1/Room/playUrl?cid=%s&qn=20000&platform=h5 | y5/a.java |
| http://127.0.0.1: | y5/b.java |
| http://127.0.0.1: | y5/c.java |
| http://127.0.0.1:6677/stream/live?uuid= | y5/h.java |
| http://127.0.0.1:6677/stream/open?uuid= | y5/h.java |
| https://www.youtube.com/playlist?list= | yb/d.java |
| https://journeyapps.com/ | Mogua Engine V1 |
| https://github.com/journeyapps/zxing-android-embedded | Mogua Engine V1 |
| https://o00tv.link/ | Mogua Engine V1 |
| 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 |
| http://'+n+' | Mogua Engine V2 |
| http://mozilla.github.io/nunjucks/api.html | Mogua Engine V2 |
| https://npms.io/search?q=ponyfill. | Mogua Engine V2 |
| 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://dnsnl.alekberg.net/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.xfinity.com/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.opendns.com/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.familyshield.opendns.com/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh-02.spectrum.com/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh-01.spectrum.com/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.quickline.ch/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://dns.google/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://dns64.dns.google/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.dns.sb/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.cleanbrowsing.org/doh/security-filter | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.cleanbrowsing.org/doh/family-filter | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.cleanbrowsing.org/doh/adult-filter | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://doh.cox.net/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://dns.quad9.net/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://dns11.quad9.net/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://dns10.quad9.net/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://public.dns.iij.jp/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://chrome.cloudflare-dns.com/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://dns.switch.ch/dns-query | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://alekberg.net/privacy | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://developers.google.com/speed/public-dns/privacy | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://nextdns.io/privacy | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://cleanbrowsing.org/privacy | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://chromium.dns.nextdns.io | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://www.cisco.com/c/en/us/about/legal/privacy-full.html | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://odvr.nic.cz/doh | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://www.quad9.net/home/privacy/ | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://dns.sb/privacy/ | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://www.nic.cz/odvr/ | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://developers.cloudflare.com/1.1.1.1/privacy/public-dns-resolver/ | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| https://public.dns.iij.jp/ | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| http://s | lib/arm64-v8a/libcronet.101.0.4951.41.so |
| http://wpad/wpad.dat | lib/arm64-v8a/libcronet.101.0.4951.41.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| jhruby.web@gmail.com | Mogua Engine V2 |
| appro@openssl.org | lib/arm64-v8a/libcronet.101.0.4951.41.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099 | m8/a.java |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |
| 14222222222 | y2/d.java |
| 17678684267 | Mogua Engine V2 |
| 15401904755 | Mogua Engine V2 |
| 15161718191 | Mogua Engine V2 |

## **5. 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: CN=SMmovie, OU=SMmovie, O=SMmovie, L=SMmovie, ST=SMmovie, C=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2023-04-27 08:26:20+00:00 有效期至: 2048-04-20 08:26:20+00:00 发行人: CN=SMmovie, OU=SMmovie, O=SMmovie, L=SMmovie, ST=SMmovie, C=CN 序列号: 0x1 哈希算法: sha256 md5值: 1c233f7859aac5d58cd2781a104dc1ac sha1值: e816f0e937658d51a7685e4aee52c27e6e00a072 sha256值: b129ee1b9d25d8e758fbd3cbc71d13d46dd0f8c8a72bbb5e0e114f11195686bc sha512值: ee1a18251503aec2ac168cbc75515143b4459d5390e1f467326d3eac57640f9bcebfc1434a19b040779ccd14b4c0cd27a49aed95b83ee0c86fa94625e1c72280 公钥算法: rsa 密钥长度: 2048 指纹: 524ff5d41a61946f3b0d2c9e319ca266bbadb5c037b244ba9887f92f33b55e82**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps" |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/" |

## **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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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\_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.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| 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.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 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| 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.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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.o00.android.movie.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.fongmi.android.tv.ui.activity.MainActivity | **Schemes**: content://, file://, smb://, http://, https://, ftp://, ed2k://, magnet://, thunder://, mitv://, jianpian://,  **Mime Types:** text/plain, video/\*, audio/\*, |
| com.fongmi.android.tv.ui.activity.ImportUrlActivity | **Schemes**: o00tv://,  **Hosts:** import,  **Ports:** 8888,  **Paths:** /configurl, |

**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。**