MoGua

囧次元 1.0.0.0.APK 分析报告

APP名称:	囧次元

包名:	com.jiongciyuan.tv
域名线索:	11条
URL线索:	14条
邮箱线索:	2条
分析日期:	2025年6月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 囧次元TV_1.0.0.0.apk
文件大小: 16.24MB
MD5值: 88432c2a4a2bc3c17e35ab8369ad2215
SHA1值: 689af3967058c0e682bf60a76d70d22ab86413d0
SHA256值: e217308d53e8d22b88cc90449443d4b71dd62b8e96a900df4459c9c0aaa1363b

APP 信息

App名称: 囧次元
包名: com.jiongciyuan.tv
主活动Activity: com.aihzo.video_tv.activities.LoadingActivity
安卓版本名称: 1.0.0.0
安卓版本: 1

域名线索

域名	服务器信息
vod.api.zshtys888.com	**IP**: 139.159.244.197 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
8.8.8.8	**IP**: 8.8.8.8 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
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
1.1.1.1	**IP**: 1.1.1.1 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.339390 **经度**: -121.894958
xml.org	**IP**: 104.239.142.8 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
1.12.12.12	**IP**: 1.12.12.12 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

223.5.5.5	**IP**: 223.5.5.5 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
lcc.5678.jp	**IP**: 115.163.17.114 **所属国家**: Japan **地区**: Hokkaido **城市**: Sapporo **纬度**: 43.066730 **经度**: 141.350098
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

URL线索

URL信息	Url所在文件
http://)?([\\w-]+\\.)+[\\w-]+(:\\d+)*(/[\\w-	cn/hutool/core/lang/PatternPool.java
http://xml.apache.org/xslt	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/disallow-doctype-decl	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-general-entities	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-parameter-entities	cn/hutool/core/util/XmlUtil.java

http://apache.org/xml/features/nonvalidating/load-external-dtd	cn/hutool/core/util/XmlUtil.java
https://8.8.8.8/resolve	com/aihzo/video_tv/utils/HostsHelper.java
https://223.5.5.5/resolve	com/aihzo/video_tv/utils/HostsHelper.java
https://1.12.12.12/dns-query	com/aihzo/video_tv/utils/HostsHelper.java
https://1.1.1.1/dns-query	com/aihzo/video_tv/utils/HostsHelper.java
http://lcc.5678.jp:30088/upload	com/aihzo/video_tv/utils/AppExceptionUploader.java
http://vod.api.zshtys888.com	com/aihzo/video_tv/global/GlobalService.java
https://github.com/L-JINBIN/ApkSignatureKillerEx	bin/mt/signature/KillerApplication684.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

邮箱线索

邮箱地址	所在文件
auth-agent@openssh.com	cn/hutool/extra/ssh/ChannelType.java
gyteky@mailto.plus	com/aihzo/video_tv/activities/LoginActivity.java

手机线索

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=CN
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-07 15:07:19+00:00
有效期至: 2050-01-01 15:07:19+00:00
发行人: C=CN
序列号: 0x4acc3ad2
哈希算法: sha256
md5值: a3dd276849218fa8ee61eb324fd644d2
sha1值: 371091ea1a92f85634adfeac24f35114f5b2af56
sha256值: 8ab9451b4a280b8baa7bf77a74f9e06da64a14b76fc0ed73795f01e02b818184
sha512值: 78190fe51a20f00e19d5affa86ffd3280bd0f851ce23b9698b6a7c9360ffb2b6611d4ce27e85b9623c2a53834067ebcbcb6c7c8a9b1a5d26bceba01fc26ecf84
公钥算法: rsa
密钥长度: 2048
指纹: 1701e1dc173ffef392657020419bb2719e170b1f5486405a4121ac5c276cf628

硬编码敏感信息

可能的敏感信息

"please_input_password" : "请输入密码"
"please_input_username" : "请输入用户名"

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.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_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.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.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。
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
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
com.jiongciyuan.tv.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信