



MoGua

家庭影院 7.0.APK 分析报告



APP名称:

家庭影院

包名:	com.jt.yy
域名线索:	33条
URL线索:	21条
邮箱线索:	2条
分析日期:	2025年6月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 家庭影院_7.0.apk

文件大小: 15.69MB
MD5值: 6f7605e9399f2cd56421f84f1e84d0a6
SHA1值: 28ff47086cb4a7f0e1f0144ae12d43f3636c8b4a
SHA256值: e85048f4056abf10e701b5d24465ee6334f6303062daa3d7ea07143cbd9214ab

i APP 信息

App名称: 家庭影院
包名: com.jt.yy
主活动Activity: com.shenma.tvlauncher.SplashActivity
安卓版本名称: 7.0
安卓版本: 117

🔍 域名线索

域名	服务器信息
www.oasis-open.org	IP: 172.99.100.168 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
www.inkscape.org	IP: 140.211.9.79 所属国家: United States of America 地区: Oregon 城市: Eugene 纬度: 44.036083 经度: -123.052429
profandesign.se	IP: 194.68.84.237 所属国家: Sweden 地区: Stockholms lan 城市: Stockholm

	纬度: 59.332748 经度: 18.064840
www.opensource.org	IP: 104.22.64.197 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.smtvzm.com	IP: 172.233.219.49 所属国家: United States of America 地区: Illinois 城市: Chicago 纬度: 41.875771 经度: -87.620605
schemas.xmlsoap.org	IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
swfupload.googlecode.com	IP: 142.250.107.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
10.0.2.15	IP: 10.0.2.15 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 194.117.171.80 所属国家: Sweden

www.vinterwebb.se	地区: Norrbottens lan 城市: Lulea 纬度: 65.584198 经度: 22.155371
log.umsns.com	IP: 59.82.31.160 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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
purl.oclc.org	IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.781734 经度: -122.459435
www.ascc.net	IP: 140.109.4.18 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei 纬度: 25.038172 经度: 121.563599
code.google.com	IP: 142.250.73.110 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

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
www.cybergarage.org	IP: 104.21.39.67 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
sodipodi.sourceforge.net	IP: 104.18.13.149 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
aps.lsott.com	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
alog.umeng.co	没有服务器地理信息.
live.lsott.com	IP: 221.229.166.85 所属国家: China 地区: Jiangsu 城市: Xuzhou 纬度: 34.266666 经度: 117.166664

alog.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
purl.org	IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.781734 经度: -122.459435
oc.umeng.co	没有服务器地理信息.
oc.umeng.com	IP: 59.82.23.79 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
wenku.baidu.com	IP: 111.206.210.110 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
wephd.live.cctv1949.com	没有服务器地理信息.
www.swfupload.org	IP: 172.67.187.227 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: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
diy.vbohd.com	没有服务器地理信息.
drm.media.baidubce.com	IP: 111.206.208.5 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
relaxng.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
cybertran.baidu.com	IP: 110.242.69.43 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280

 URL线索

URL信息	Url所在文件
http://cybertran.baidu.com/video?ak=	com/baidu/cyberplayer/core/CyberPlayer.java

https://drm.media.baidubce.com	com/baidu/cyberplayer/core/BVideoView.java
http://127.0.0.1:	com/baidu/cyberplayer/core/CyberPlayerCore.java
http://cybertran.baidu.com/mediasdk/video?method=sdkupdate	com/baidu/cyberplayer/utils/VersionManager.java
http://purl.org/dc/elements/1.1/	com/baidu/cyberplayer/utils/C0106bq.java
http://schemas.xmlsoap.org/soap/envelope/	com/baidu/cyberplayer/utils/R.java
http://schemas.xmlsoap.org/soap/encoding/	com/baidu/cyberplayer/utils/R.java
http://cybertran.baidu.com	com/baidu/cyberplayer/utils/C0124k.java
http://www.cybergarage.org</manufacturerURL>\n	com/baidu/cyberplayer/utils/C0097bh.java
http://www.cybergarage.org</modelURL>\n	com/baidu/cyberplayer/utils/C0097bh.java
http://diy.vbohd.com/user_list_xml.php?user_id=10086	com/shenma/tvlauncher/tvlive/TVLivePlayer.java
http://wephd.live.cctv1949.com/api_new/wephd.xml	com/shenma/tvlauncher/tvlive/TVLivePlayer.java
http://aps.lsott.com/egp/	com/shenma/tvlauncher/tvlive/TVLivePlayer.java
http://www.smtvzm.com/index.php/user/getmychannel.xml?loginname=	com/shenma/tvlauncher/tvlive/TVLivePlayer.java
http://www.smtvzm.com/xmlfile/	com/shenma/tvlauncher/tvlive/TVLivePlayer.java
http://live.lsott.com/wepower/wephd_v3.xml	com/shenma/tvlauncher/tvlive/TVLivePlayer.java
http://live.lsott.com/wepower/wephd_test.xml	com/shenma/tvlauncher/tvlive/TVLivePlayer.java
http://live.lsott.com/wepower/plugs.xml	com/shenma/tvlauncher/tvlive/IL1Iii/Ooo.java
http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd'	com/shenma/tvlauncher/view/shapeimageview/p03408oO8o8/p03508oO8o8/oO.java

http://www.inkscape.org/namespaces/inkscape'	com/shenma/tvlauncher/view/shapeimageview/p03408o08o8/p03508o08o8/oO.java
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umeng.co/app_logs	com/umeng/analytics/a.java
http://oc.umeng.com/check_config_update	com/umeng/analytics/a.java
http://oc.umeng.co/check_config_update	com/umeng/analytics/a.java
http://log.umsns.com/	com/umeng/analytics/social/e.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/f.java
http://xmlpull.org/v1/doc/features.html	org/IL1l1i/p03908o08o8/Ooo.java
http://xmlpull.org/v1/doc/	org/p04008o08o8/p04108o08o8/O8o08o8.java
http://xmlpull.org/v1/doc/features.html	org/p04008o08o8/p04108o08o8/O8o08o8.java
http://10.0.2.15:10101	摸瓜V1引擎
http://code.google.com/p/swfobject/>	摸瓜V2引擎
http://www.opensource.org/licenses/mit-license.php>	摸瓜V2引擎
http://www.swfupload.org,	摸瓜V2引擎
http://swfupload.googlecode.com	摸瓜V2引擎
http://profandesign.se/swfupload/,	摸瓜V2引擎

http://www.vinterwebb.se/	摸瓜V2引擎
http://www.opensource.org/licenses/mit-license.php	摸瓜V2引擎
http://%s:%d%s	lib/armeabi-v7a/liblivcffmpegpeg.so
http://%s%s	lib/armeabi-v7a/liblivcffmpegpeg.so
http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd	lib/armeabi-v7a/liblivcffmpegpeg.so
http://relaxng.org/ns/structure/1.0	lib/armeabi-v7a/liblivcffmpegpeg.so
http://purl.oclc.org/dsdl/schematron	lib/armeabi-v7a/liblivcffmpegpeg.so
http://www.ascc.net/xml/schematron	lib/armeabi-v7a/liblivcffmpegpeg.so
https://wenku.baidu.com	lib/armeabi-v7a/libijkffmpegpeg.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpegpeg.so
https://vod.	lib/armeabi-v7a/libsaasCorePlayer.so
https://mts.	lib/armeabi-v7a/libsaasCorePlayer.so
https://live.	lib/armeabi-v7a/libsaasCorePlayer.so
http://xxx	lib/armeabi-v7a/libsaasCorePlayer.so

 邮箱线索

邮箱地址	所在文件
fto@example.com	lib/armeabi-v7a/liblivcffmpegpeg.so

ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so
-------------------------	---------------------------------

☰ 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=273300, ST=山东省, L=临沂市, O=个人, OU=个人, CN=zsqorcs.keystore
签名算法: rsassa_pkcs1v15
有效期自: 2024-01-31 02:05:34+00:00
有效期至: 2048-09-21 02:05:34+00:00
发行人: C=273300, ST=山东省, L=临沂市, O=个人, OU=个人, CN=zsqorcs.keystore
序列号: 0x9b4902db438e4da5
哈希算法: sha256
md5值: a5f3728dc63aa55b6cfd5d1ff914751
sha1值: 67eea6c90202f2337e2f7e7fa6d9c69dccf2b70a
sha256值: b69793df825042aed41ee025c35da17b7f413ad7f63e574949b3c9b8f69f4d50
sha512值: ef4bb913c35f14af799ac54505a3a333e871e37b97330c58cae749128a6e3a9ff58cadfb96a1e0bf28021f585b7fbcac9c19a357b70de65516915440ce8fdc24
公钥算法: rsa
密钥长度: 1024
指纹: 8a4c3ddce5d479abf811791459301a8cc9eab909f03dc1a695b7d958b3428132

🔑 硬编码敏感信息

可能的敏感信息
"Input_authorization": "输入授权码"
"authorization_codes": "授权码: "
"forget_password": "找回密码"
"illegal_password": "密码不合标准，要求8位以上数字或英文"
"input_password": "请输入密码"
"input_pwd": "请输入类目密码"
"input_username": "请输入账户"
"none_password": "请输入密码"
"please_input_password": "请输入密码"
"user": "用户"
"wifiap_pwd_notice": "请输入正确的密码6位以上数字或字母"

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_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_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
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_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.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.KILL_BACKGROUND_PROCESSES	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

应用内通信

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。