MoGua

合家欢影院 3.2.APK 分析报告

APP名称:	合家欢影院

包名:	com.hjhyy.tv
域名线索:	17条
URL线索:	4条
邮箱线索:	1条
分析日期:	2025年7月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 合家欢影院-3.2.apk

文件大小: 15.22MB
MD5值: 2e31a251aae1962055777a9eeba9dcee
SHA1值: 2e29a9fc07438a91867917bfba50a78dd88738b1
SHA256值: 845fd255e5f90e48ba78ecd19c40fcc54897f0564a3ff5bb1e2c9d068b46b975

APP 信息

App名称: 合家欢影院
包名: com.hjhyy.tv
主活动Activity: com.shenma.tvlauncher.SplashActivity
安卓版本名称: 3.2
安卓版本: 126

域名线索

域名	服务器信息
www.swfupload.org	**IP**: 104.21.64.216 **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
www.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.vinterwebb.se	IP: 194.117.171.80 **所属国家**: Sweden **地区**: Norrbottens lan **城市**: Lulea **纬度**: 65.584198 **经度**: 22.155371
swfupload.googlecode.com	IP: 74.125.197.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
foo.com	IP: 50.16.218.27 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
www.opensource.org	IP: 172.67.197.41 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
connectivitycheck.gstatic.com	IP: 203.208.43.98 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 112.86.231.45

sh.file.myqcloud.com	**所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
git.code.oa.com	IP: 141.144.196.217 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.378502 **经度**: 4.899980
www.gstatic.com	IP: 203.208.39.194 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
ns.attribution.com	没有服务器地理信息.
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
	IP: 112.86.231.42 **所属国家**: China **地区**: Jiangsu

lx-1316376600.cos.ap-shanghai.myqcloud.com	**城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
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
code.google.com	**IP**: 142.250.69.206 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

URL线索

URL信息	Url所在文件
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://foo.com	摸瓜V3引擎
http://git.code.oa.com/SecurityResearchProject/ANTI-Reverse.git	摸瓜V3引擎
connectivitycheck.gstatic.com	摸瓜V3引擎
android.googleapis.com	摸瓜V3引擎
growth-pa.googleapis.com	摸瓜V3引擎
sh.file.myqcloud.com	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
www.gstatic.com	摸瓜V3引擎
http://ns.attribution.com/ads/1.0/	摸瓜V3引擎
lx-1316376600.cos.ap-shanghai.myqcloud.com	摸瓜V3引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://wenku.baidu.com	lib/armeabi-v7a/libijkffmpeg.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

硬编码敏感信息

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
