MoGua

汤不热视频 10.0.APK 分析报告

TBR02.COM

APP名称:	汤不热视频

包名:	com.soft.play.t2
域名线索:	5条
URL线索:	4条
邮箱线索:	1条
分析日期:	2024年9月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app.apk
文件大小: 26.8MB
MD5值: 49d8b8f8d683bdabfa01710889067d3b
SHA1值: bad8e9c391f21414d83a42cc7fef0e43a2720e60
SHA256值: 07de91639a58313d291b1b610c23cb0ade4e471b97f2e0159d199de05e2de62f

APP 信息

App名称: 汤不热视频
包名: com.soft.play.t2
主活动Activity: com.soft.play.activity.LauncherActivity
安卓版本名称: 10.0
安卓版本: 100

域名线索

域名	服务器信息
www.videolan.org	**IP**: 213.36.253.2 **所属国家**: France **地区**: Ile-de-France **城市**: Paris **纬度**: 48.853409 **经度**: 2.348800
www.openssl.org	**IP**: 23.194.230.23 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
www.ffmpeg.org	**IP**: 79.124.17.100 **所属国家**: Bulgaria **地区**: Sofia (stolitsa)

	城市: Sofia **纬度**: 42.697510 **经度**: 23.324150
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
lame.sf.net	**IP**: 204.68.111.100 **所属国家**: United States of America **地区**: California **城市**: San Diego **纬度**: 32.799797 **经度**: -117.137047

URL线索

URL信息	Url所在文件
http://lame.sf.net	lib/armeabi-v7a/libmp3lame.so
http://lame.sf.net	lib/armeabi-v7a/libffmpeg.so
http://www.videolan.org/x264.html	lib/armeabi-v7a/libffmpeg.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libcrypto.so
http://www.w3.org/2001/XMLSchema-instance'	lib/armeabi-v7a/libmedia-handle.so
http://www.ffmpeg.org/schema/ffprobe'	lib/armeabi-v7a/libmedia-handle.so

http://www.ffmpeg.org/schema/ffprobe	lib/armeabi-v7a/libmedia-handle.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libmedia-handle.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=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2021-07-27 06:42:30+00:00
有效期至: 2046-07-21 06:42:30+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x2d1eaa05
哈希算法: sha256
md5值: 68812afc1821d2514767c1f8c4e113cf
sha1值: 427eaf53dfd476c400525cb3f3ba9a4ee599cf60
sha256值: efa5f895461c32d1e50d822dc68eaf8e93f624f3264f470d20d3f6b14c1f52c7
sha512值: b9a6f696a70058f74c07c42ac2bec4e40e56c3d9295062908aa66cae3c0f6ceaa5d43d2f9e0410da1c276811569a674bd69d7626085685103af60b09ccb32e16
公钥算法: rsa
密钥长度: 2048
指纹: abdd478d19d4bfc0877bf03f71f64ba3b1dc26bcc1a3e73e6d9db9b6123c73e2

硬编码敏感信息

可能的敏感信息
"share_username" : "老汤站长"

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.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.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
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.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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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

应用内通信