MoGua

硬汉视频 2.6.2.APK 分析报告

APP名称:	硬汉视频

包名:	tv.i999.inhand
域名线索:	5条
URL线索:	11条
邮箱线索:	3条
分析日期:	2025年5月22日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 2_6_2_inhand.apk
文件大小: 17.37MB
MD5值: 0016bd848204ab2cdf0ca56f53a5edd2
SHA1值: 357e60805f994f2073c461233f450b5a7c84b77a
SHA256值: 4feb0015746e8ea07e50f1a4d6c47b3f7c342604d33f61a447519003687bbdd5

APP 信息

App名称: 硬汉视频
包名: tv.i999.inhand
主活动Activity: tv.i999.inhand.MVVM.Activity.SuperLandingActivity.SuperLandingActivity
安卓版本名称: 2.6.2
安卓版本: 55

域名线索

域名	服务器信息
app-inhand-f221d.firebaseio.com	**IP**: 34.120.160.131 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
proton.flurry.com	没有服务器地理信息.
crashpad.chromium.org	**IP**: 142.251.42.243 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

data.flurry.com	**IP**: 69.147.80.12 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
github.com	**IP**: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

URL线索

URL信息	Url所在文件
http://%s:%d/%s	com/danikula/videocache/k.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/k.java
http://%s:%d/%s	com/danikula/videocache/g.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/i.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/i.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/i.java
https://data.flurry.com/aap.do	com/flurry/sdk/K.java
http://data.flurry.com/aap.do	com/flurry/sdk/K.java

https://data.flurry.com/pcr.do	com/flurry/sdk/A.java
https://proton.flurry.com/sdk/v1/config	com/flurry/sdk/C0555s.java
https://app-inhand-f221d.firebaseio.com	Mogua Engine V1
https://crashpad.chromium.org/bug/new	lib/armeabi-v7a/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/armeabi-v7a/libcrashlytics-common.so
https://crashpad.chromium.org/bug/new	lib/x86_64/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/x86_64/libcrashlytics-common.so
https://crashpad.chromium.org/bug/new	lib/x86/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/x86/libcrashlytics-common.so
https://crashpad.chromium.org/bug/new	lib/arm64-v8a/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/arm64-v8a/libcrashlytics-common.so

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/i.java
o@netstream.failed	lib/x86_64/librtmp-jni.so
o@netstream.failed	lib/x86/librtmp-jni.so

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: O=AvNight, OU=IT, CN=Eric Lin
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-05-06 02:54:23+00:00
Valid To: 2041-04-30 02:54:23+00:00
Issuer: O=AvNight, OU=IT, CN=Eric Lin
Serial Number: 0x633954be
Hash Algorithm: sha256
md5: ae49c75d9549826f5b7adfb259649fcb
sha1: 7302bcc88f1adb1b280497f8b83627f720c59474
sha256: 4d16c34c491c9e6ca60524f7c139f74127d9cc8b70258380a40f274ea562ea78
sha512: 15d82146fc34a20ef65ef43518807548f188cf55defe2932f0e684cc74abd258098c7008f923ff548fb1da2f6f529b1317982d3fcf4b6828c2444527f828b811
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f8128e85d6b21bfbdbbcb784f3d7be801f82df0129d340ff82e93a317cbed2ea

硬编码敏感信息

可能的敏感信息
"account_forget_password" : "忘记密码"
"do_you_forget_password" : "忘记密码了？"
"fileProvider_authorities" : "inhand_number_one"

"firebase_database_url" : "https://app-inhand-f221d.firebaseio.com"
"forget_password" : "忘记密码"
"go_to_forget_password" : "去找回密码"
"google_api_key" : "AIzaSyBoRcTuC9zYXJgBqOmYxd61FmpwRHjNsUc"
"google_crash_reporting_api_key" : "AIzaSyBoRcTuC9zYXJgBqOmYxd61FmpwRHjNsUc"
"key_in_email" : "输入邮箱"
"key_in_password" : "输入密码"
"password" : "密码"
"privatePhotos" : "情欲私照"

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_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.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
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_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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.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.CHANGE_WIFI_STATE	正	更改Wi-Fi状	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

	常	态	改
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_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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
getui.permission.GetuiService.tv.i999.inhand	未知	Unknown permission	Unknown permission from android reference
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

com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
tv.i999.inhand.MVVM.Activity.SuperLandingActivity.SuperLandingActivity	Schemes: bg8://, http://, https://, Hosts: bg8,

---