Evaluation Warning: The document was created with Spire.Doc for Python.

**硬汉视频（ 2.7.4版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 硬汉视频 |
| 版本 | 2.7.4 |
| 包名 | tv.i999.inhand |
| 域名线索 | 48条 |
| URL线索 | 21条 |
| APP图标 |  |
| 分析日期 | 2025年6月1日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | side\_image\_floating\_left\_inhand.apk |
| 文件大小 | 20.1MB |
| MD5值 | 5f4e7c9a941a0ede1d8d3040e9d7c1bc |
| SHA1值 | c925dad4d74fe078923c5610f8d79c6461fb0f67 |
| SHA256值 | e5b62698d0747819798be293fa028cf9650b5ebb88febf6f390766f56c55328d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 | 2.7.4 |
| 安卓版本 | 69 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| sdk.open.amp.igexin.com | IP: 124.160.124.197  所属国家: China  地区: Zhejiang  城市: Wenzhou |
| d1vcfwitp2um8b.cloudfront.net | IP: 13.225.0.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| exoplayer.dev | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| sdk.open.talk.gepush.com | IP: 124.160.124.209  所属国家: China  地区: Zhejiang  城市: Wenzhou |
| inin-1304042779.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.149  所属国家: China  地区: Fujian  城市: Fuzhou |
| sdk.open.phone.igexin.com | IP: 124.160.155.42  所属国家: China  地区: Zhejiang  城市: Jiaxing |
| sdk.open.inc2.igexin.com | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| schemas.microsoft.com | IP: 13.107.253.39  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| hcdnw102.gslb.c.cdnhwc2.com | IP: 123.125.16.229  所属国家: China  地区: Beijing  城市: Beijing |
| cdn-sdk-opt.getui.com.e590cf8e.cdnhwc8.cn | IP: 123.125.16.230  所属国家: China  地区: Beijing  城市: Beijing |
| sdk.conf.getui.com | IP: 123.125.16.229  所属国家: China  地区: Beijing  城市: Beijing |
| s-gt.getui.com | IP: 124.160.155.55  所属国家: China  地区: Zhejiang  城市: Jiaxing |
| data.flurry.com | IP: 98.136.147.18  所属国家: United States of America  地区: New York  城市: New York City |
| psbiv4-6.cname.getui.com | IP: 101.68.218.177  所属国家: China  地区: Zhejiang  城市: Jiaxing |
| app-inhand-f221d.firebaseio.com | IP: 35.201.97.85  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| lh5.googleusercontent.com | IP: 172.217.160.97  所属国家: United States of America  地区: California  城市: Mountain View |
| sdk-open-phone.getui.com | IP: 101.68.218.171  所属国家: China  地区: Zhejiang  城市: Jiaxing |
| sdk.open.talk.getui.com | IP: 124.160.124.209  所属国家: China  地区: Zhejiang  城市: Wenzhou |
| cm-10-139.getui.com | IP: 183.134.98.109  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| inin-1305277877.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.150  所属国家: China  地区: Fujian  城市: Fuzhou |
| app-measurement.com | IP: 114.250.66.33  所属国家: China  地区: Beijing  城市: Beijing |
| android.googlesource.com | IP: 173.194.174.82  所属国家: United States of America  地区: California  城市: Mountain View |
| api2.i9999.pw | IP: 199.59.243.226  所属国家: United States of America  地区: Florida  城市: Tampa |
| sdk.open.talk.igexin.com | IP: 124.160.124.209  所属国家: China  地区: Zhejiang  城市: Wenzhou |
| schemas.android.com | 没有服务器地理信息. |
| playready.directtaps.net | IP: 104.45.231.79  所属国家: United States of America  地区: California  城市: San Francisco |
| d.gt.igexin.com | 没有服务器地理信息. |
| encrypted-tbn0.gstatic.com | IP: 172.217.163.46  所属国家: United States of America  地区: California  城市: Mountain View |
| i.imgur.com | IP: 151.101.40.193  所属国家: United States of America  地区: California  城市: San Francisco |
| sdk.open.talk.getui.net | IP: 124.160.124.209  所属国家: China  地区: Zhejiang  城市: Wenzhou |
| firebase-settings.crashlytics.com | IP: 114.250.69.34  所属国家: China  地区: Beijing  城市: Beijing |
| googlehosted.l.googleusercontent.com | IP: 172.217.160.97  所属国家: United States of America  地区: California  城市: Mountain View |
| hcdnw101.gslb.v6.c.cdnhwc2.com | IP: 116.130.221.33  所属国家: China  地区: Beijing  城市: Beijing |
| api.api98.xyz | 没有服务器地理信息. |
| sdk.open.lbs.igexin.com | IP: 121.52.255.89  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| storage.googleapis.com | IP: 142.251.43.27  所属国家: United States of America  地区: California  城市: Mountain View |
| crashpad.chromium.org | IP: 172.217.163.51  所属国家: United States of America  地区: California  城市: Mountain View |
| sdk.conf.getui.com.e590cf8e.cdnhwc8.cn | IP: 116.130.221.32  所属国家: China  地区: Beijing  城市: Beijing |
| aomedia.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| bitdash-a.akamaihd.net | IP: 23.62.226.196  所属国家: Australia  地区: New South Wales  城市: Sydney |
| proton.flurry.com | 没有服务器地理信息. |
| c-hzgt2.getui.com | IP: 124.160.155.57  所属国家: China  地区: Zhejiang  城市: Jiaxing |
| ps.cname2.getui.com | IP: 124.160.155.59  所属国家: China  地区: Zhejiang  城市: Jiaxing |
| sd.cname3.getui.com | IP: 124.160.124.209  所属国家: China  地区: Zhejiang  城市: Wenzhou |
| goo.gl | IP: 142.251.43.14  所属国家: United States of America  地区: California  城市: Mountain View |
| cdn-sdk-opt.getui.com | IP: 123.125.16.232  所属国家: China  地区: Beijing  城市: Beijing |
| dashif.org | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |

### **4.2 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 |
| 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 |
| http://%s:%d/%s | com/danikula/videocache/g.java |
| https://data.flurry.com/pcr.do | com/flurry/sdk/A.java |
| https://proton.flurry.com/sdk/v1/config | com/flurry/sdk/C0465s.java |
| https://data.flurry.com/aap.do | com/flurry/sdk/K.java |
| http://data.flurry.com/aap.do | com/flurry/sdk/K.java |
| http://sdk.open.amp.igexin.com/api.htm | com/igexin/push/config/SDKUrlConfig.java |
| http://sdk.open.phone.igexin.com/api.php | com/igexin/push/config/SDKUrlConfig.java |
| http://c-hzgt2.getui.com/api.php | com/igexin/push/config/SDKUrlConfig.java |
| http://sdk.open.inc2.igexin.com/api.php | com/igexin/push/config/SDKUrlConfig.java |
| http://sdk.open.lbs.igexin.com/api.htm | com/igexin/push/config/SDKUrlConfig.java |
| http://d.gt.igexin.com/api.htm | com/igexin/push/config/SDKUrlConfig.java |
| http://s-gt.getui.com/api.php | com/igexin/push/config/SDKUrlConfig.java |
| http://bi. | com/igexin/push/config/p.java |
| http://config. | com/igexin/push/config/p.java |
| http://stat. | com/igexin/push/config/p.java |
| http://log. | com/igexin/push/config/p.java |
| http://amp. | com/igexin/push/config/p.java |
| http://lbs. | com/igexin/push/config/p.java |
| http://inc. | com/igexin/push/config/p.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | f/a/f.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/exceptions/UndeliverableException.java |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java |
| https://api.api98.xyz/s1/ | tv/i999/inhand/Core/BG8Application.java |
| https://bitdash-a.akamaihd.net/content/sintel/hls/video/ | tv/i999/inhand/Download/k.java |
| https://storage.googleapis.com/ihih/inhand.jsonb | tv/i999/inhand/MVVM/API/ApiServiceManager.java |
| https://inin-1304042779.cos.ap-guangzhou.myqcloud.com/inhand.jsonb | tv/i999/inhand/MVVM/API/ApiServiceManager.java |
| https://inin-1305277877.cos.ap-guangzhou.myqcloud.com/inhand.jsonb | tv/i999/inhand/MVVM/API/ApiServiceManager.java |
| https://d1vcfwitp2um8b.cloudfront.net/api/inhand.jsonb | tv/i999/inhand/MVVM/API/ApiServiceManager.java |
| https://api2.i9999.pw/s1/share/ | tv/i999/inhand/MVVM/API/ApiServiceManager.java |
| https://api.api98.xyz/s1/ | tv/i999/inhand/MVVM/API/ApiServiceManager.java |
| https://i.imgur.com/XIKVZ49.png | tv/i999/inhand/MVVM/Bean/AvVideoBean.java |
| https://i.imgur.com/18NJJa4.jpeg | tv/i999/inhand/MVVM/Bean/OnlyFans/FakeOnlyFansActorData.java |
| https://i.imgur.com/d9vJpeL.jpeg | tv/i999/inhand/MVVM/Bean/OnlyFans/IOnlyFansPhotoData$Companion$getFakeData$1$data$1.java |
| https://i.imgur.com/d9vJpeL.jpeg | tv/i999/inhand/MVVM/Bean/OnlyFans/IOnlyFansVideoData$Companion$getFakeData$1$data$1.java |
| https://app-inhand-f221d.firebaseio.com | Mogua Engine V1 |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | Mogua Engine V3 |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread | Mogua Engine V3 |
| https://inin-1304042779.cos.ap-guangzhou.myqcloud.com/inhand.jsonb | Mogua Engine V3 |
| sdk.open.talk.gepush.com | Mogua Engine V3 |
| https://d1vcfwitp2um8b.cloudfront.net/api/inhand.jsonb | Mogua Engine V3 |
| sdk.open.phone.igexin.com | Mogua Engine V3 |
| http://sdk.open.inc2.igexin.com/api.php | Mogua Engine V3 |
| https://github.com/ReactiveX/RxJava/wiki/What | Mogua Engine V3 |
| https://github.com/danikula/AndroidVideoCache/issues/43. | Mogua Engine V3 |
| https://aomedia.org/emsg/ID3 | Mogua Engine V3 |
| hcdnw102.gslb.c.cdnhwc2.com | Mogua Engine V3 |
| cdn-sdk-opt.getui.com.e590cf8e.cdnhwc8.cn | Mogua Engine V3 |
| https://goo.gl/NAOOOI. | Mogua Engine V3 |
| sdk.conf.getui.com | Mogua Engine V3 |
| psbiv4-6.cname.getui.com | Mogua Engine V3 |
| https://app-measurement.com/a | Mogua Engine V3 |
| https://data.flurry.com/pcr.do | Mogua Engine V3 |
| http://sdk.open.lbs.igexin.com/api.htm | Mogua Engine V3 |
| lh5.googleusercontent.com | Mogua Engine V3 |
| sdk-open-phone.getui.com | Mogua Engine V3 |
| cm-10-139.getui.com | Mogua Engine V3 |
| sdk.open.talk.getui.com | Mogua Engine V3 |
| https://i.imgur.com/18NJJa4.jpeg | Mogua Engine V3 |
| http://c-hzgt2.getui.com/api.php | Mogua Engine V3 |
| https://crashpad.chromium.org/bug/new | Mogua Engine V3 |
| https://goo.gl/NAOOOI | Mogua Engine V3 |
| http://schemas.android.com/apk/res/android)i | Mogua Engine V3 |
| http://sdk.open.phone.igexin.com/api.php | Mogua Engine V3 |
| https://proton.flurry.com/sdk/v1/config | Mogua Engine V3 |
| http://dashif.org/guidelines/trickmode | Mogua Engine V3 |
| http://goo.gl/naFqQk | Mogua Engine V3 |
| http://goo.gl/8Rd3yj | Mogua Engine V3 |
| sdk.open.talk.igexin.com | Mogua Engine V3 |
| http://sdk.open.amp.igexin.com/api.htm | Mogua Engine V3 |
| https://data.flurry.com/aap.do | Mogua Engine V3 |
| encrypted-tbn0.gstatic.com | Mogua Engine V3 |
| sdk.open.talk.getui.net | Mogua Engine V3 |
| firebase-settings.crashlytics.com | Mogua Engine V3 |
| https://inin-1305277877.cos.ap-guangzhou.myqcloud.com/inhand.jsonb | Mogua Engine V3 |
| http://s-gt.getui.com/api.php | Mogua Engine V3 |
| hcdnw101.gslb.v6.c.cdnhwc2.com | Mogua Engine V3 |
| googlehosted.l.googleusercontent.com | Mogua Engine V3 |
| http://data.flurry.com/aap.do | Mogua Engine V3 |
| https://github.com/danikula/AndroidVideoCache/issues/88. | Mogua Engine V3 |
| https://crashpad.chromium.org/bug/newhttps://crashpad.chromium.org/%s: | Mogua Engine V3 |
| http://schemas.android.com/apk/res-auto | Mogua Engine V3 |
| https://i.imgur.com/XIKVZ49.png | Mogua Engine V3 |
| http://schemas.android.com/apk/res/android | Mogua Engine V3 |
| http://dashif.org/guidelines/last-segment-number | Mogua Engine V3 |
| https://crashpad.chromium.org/ | Mogua Engine V3 |
| http://d.gt.igexin.com/api.htm | Mogua Engine V3 |
| https://android.googlesource.com/toolchain/llvm-project | Mogua Engine V3 |
| https://github.com/danikula/AndroidVideoCache/issues/134. | Mogua Engine V3 |
| https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings | Mogua Engine V3 |
| sdk.conf.getui.com.e590cf8e.cdnhwc8.cn | Mogua Engine V3 |
| https://goo.gl/J1sWQy | Mogua Engine V3 |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx | Mogua Engine V3 |
| c-hzgt2.getui.com | Mogua Engine V3 |
| https://github.com/danikula/AndroidVideoCache/issues. | Mogua Engine V3 |
| ps.cname2.getui.com | Mogua Engine V3 |
| sd.cname3.getui.com | Mogua Engine V3 |
| https://api.api98.xyz/s1/ | Mogua Engine V3 |
| cdn-sdk-opt.getui.com | Mogua Engine V3 |
| https://i.imgur.com/d9vJpeL.jpeg | Mogua Engine V3 |
| https://crashpad.chromium.org/bug/new | lib/x86\_64/libcrashlytics-common.so |
| https://crashpad.chromium.org/ | lib/x86\_64/libcrashlytics-common.so |

### **4.3 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 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **5. 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: O=AvNight, OU=IT, CN=Eric Lin 签名算法: rsassa\_pkcs1v15 有效期自: 2016-05-06 02:54:23+00:00 有效期至: 2041-04-30 02:54:23+00:00 发行人: O=AvNight, OU=IT, CN=Eric Lin 序列号: 0x633954be 哈希算法: sha256 md5值: ae49c75d9549826f5b7adfb259649fcb sha1值: 7302bcc88f1adb1b280497f8b83627f720c59474 sha256值: 4d16c34c491c9e6ca60524f7c139f74127d9cc8b70258380a40f274ea562ea78 sha512值: 15d82146fc34a20ef65ef43518807548f188cf55defe2932f0e684cc74abd258098c7008f923ff548fb1da2f6f529b1317982d3fcf4b6828c2444527f828b811 公钥算法: rsa 密钥长度: 2048 指纹: f8128e85d6b21bfbdbbcb784f3d7be801f82df0129d340ff82e93a317cbed2ea**

## **6. 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\_password" : "输入密码" |
| "password" : "密码" |
| "privatePhotos" : "情欲私照" |
| "retryApi" : "刷新重试" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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.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\_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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

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

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**