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

**acfan（ 1.0.2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 | acfan |
| 版本 | 1.0.2 |
| 包名 | com.androidjks.acfan.d1682156448763174048 |
| 域名线索 | 10条 |
| URL线索 | 20条 |
| APP图标 |  |
| 分析日期 | 2024年10月17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 | acfan.apk |
| 文件大小 | 13.28MB |
| MD5值 | d5deb54fb442eca6aab25e1a2e0bdf7a |
| SHA1值 | c978f6832fd231769a91397cb6bc2358a4e436a6 |
| SHA256值 | e7d2560e94e374eae103203b090bfdfbe63addcf738b9003e01ce8a710525415 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | acfan |
| 包名 | com.androidjks.acfan.d1682156448763174048 |
| 主活动Activity | com.grass.mh.ui.SplashActivity |
| 安卓版本名称 | 1.0.2 |
| 安卓版本 | 102 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| clsp.fun | IP: 35.244.166.146  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| schemas.android.com | 没有服务器地理信息. |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| d2yvno3b6unw4p.cloudfront.net | IP: 13.33.211.196  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.openssl.org | IP: 104.71.138.221  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| schemas.microsoft.com | IP: 13.107.238.49  所属国家: United States of America  地区: Washington  城市: Redmond |
| ns.adobe.com | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| playready.directtaps.net | IP: 40.70.71.156  所属国家: United States of America  地区: Virginia  城市: Boydton |
| data.flurry.com | IP: 69.147.80.15  所属国家: United States of America  地区: New York  城市: New York City |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.w3.org/ns/ttml | d/h/a/a/k0/l/c.java |
| https://data.flurry.com/v1/flr.do | d/f/b/t0.java |
| https://data.flurry.com/aap.do | d/f/b/s0.java |
| http://schemas.android.com/apk/res/android | org/dsq/library/widget/tablayout/SlidingTabLayout.java |
| http://schemas.android.com/apk/res/android | org/dsq/library/widget/tablayout/CommonTabLayout.java |
| http://schemas.android.com/apk/res/android | org/dsq/library/widget/tablayout/SegmentTabLayout.java |
| http://schemas.android.com/apk/res/android | l/a/a/f.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/exceptions/UndeliverableException.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/exceptions/OnErrorNotImplementedException.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextView.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextureView.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/danikula/videocache/HttpUrlSource.java |
| http://%s:%d/%s | com/danikula/videocache/Pinger.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/Pinger.java |
| http://%s:%d/%s | com/danikula/videocache/HttpProxyCacheServer.java |
| https://d2yvno3b6unw4p.cloudfront.net/json/acfan.json | com/grass/mh/ui/SplashActivity.java |
| https://clsp.fun | com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java |
| http://ns.adobe.com/xap/1.0/\u0000 | b/n/a/a.java |
| http://schemas.android.com/apk/res/android | b/j/b/b/e.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 |
| http://www.openssl.org/support/faq.html | lib/armeabi-v7a/libijkffmpeg.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | com/danikula/videocache/HttpUrlSource.java |
| ffmpeg-devel@ffmpeg.org | lib/armeabi-v7a/libijkplayer.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: C=24, ST=24, L=24, O=24, OU=24, CN=24 签名算法: rsassa\_pkcs1v15 有效期自: 2023-04-11 08:13:34+00:00 有效期至: 2048-04-04 08:13:34+00:00 发行人: C=24, ST=24, L=24, O=24, OU=24, CN=24 序列号: 0x5b314548 哈希算法: sha256 md5值: 59dce2df07bc49e3af085610344fcf0c sha1值: 2eb5ddc7b1d78f582ca80f645059c9e541ad1088 sha256值: f4b7c9635aed1c7497ee326b87c7582f056828b3a5aadef7f1cf3d6d7cff18ab sha512值: 28e56e5a5d79319d8662fb3c9515aa23e7ebcbf3439bd55539a9be0d160408cfc81f098ba114e7b88134ed8ea766fc90c45a164152764472bce088778f1f64b0 公钥算法: rsa 密钥长度: 2048 指纹: caf802b26b74d9cdeb6c2cea46100e9deebe50e76f7d4f863eaf36e0da92f991**

## **6. 硬编码敏感信息**

## **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.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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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 |
| 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 |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**