



# MoGua

## acfan 1.3.4.APK 分析报告



APP名称:

acfan

包名: com.androidjks.acfan.d1725183295436173455

域名线索: 9条

URL线索: 18条

邮箱线索: 1条

分析日期: 2025年9月8日

分析平台: [摸瓜APK反编译平台](#)

文件名: aayy1\_1.3.4\_83402128.apk  
文件大小: 24.16MB  
MD5值: 6e575a41fbb6d8af893df8ea4ddf051e  
SHA1值: 084532cf37cf3c2442481a83f61eec840fbd01ce  
SHA256值: e8ef27a0eaa0c5419783fe72a06b48a519e4bff3ebf7603f4a2bf6961c3049a0

## i APP 信息

App名称: acfan  
包名: com.androidjks.acfan.d1725183295436173455  
主活动Activity: com.grass.mh.ui.SplashActivity  
安卓版本名称: 1.3.4  
安卓版本: 134

## 🔍 域名线索

| 域名                    | 服务器信息                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------|
| clsp.fun              | 没有服务器地理信息.                                                                                                               |
| ns.adobe.com          | 没有服务器地理信息.                                                                                                               |
| github.com            | IP: 20.205.243.166<br>所属国家: Singapore<br>地区: Singapore<br>城市: Singapore<br>纬度: 1.289987<br>经度: 103.850281                |
| schemas.microsoft.com | IP: 13.107.246.73<br>所属国家: United States of America<br>地区: Washington<br>城市: Redmond<br>纬度: 47.682899<br>经度: -122.120903 |

|                              |                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| data.flurry.com              | IP: 98.136.147.18<br><b>所属国家:</b> United States of America<br><b>地区:</b> New York<br><b>城市:</b> New York City<br><b>纬度:</b> 40.731323<br><b>经度:</b> -73.990089    |
| d2d63bvtwvflg.cloudfront.net | IP: 13.32.54.59<br><b>所属国家:</b> Japan<br><b>地区:</b> Tokyo<br><b>城市:</b> Tokyo<br><b>纬度:</b> 35.689499<br><b>经度:</b> 139.692322                                    |
| playready.directtaps.net     | IP: 104.45.231.79<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Francisco<br><b>纬度:</b> 37.774929<br><b>经度:</b> -122.419418 |
| schemas.android.com          | 没有服务器地理信息.                                                                                                                                                        |
| www.w3.org                   | IP: 104.18.22.19<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Francisco<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203  |

## URL线索

| URL信息 | Url所在文件 |
|-------|---------|
|       |         |

|                                                                                                                                                 |                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                             | b/j/b/b/e.java                                               |
| <a href="http://ns.adobe.com/xap/1.0/\u0000">http://ns.adobe.com/xap/1.0/\u0000</a>                                                             | b/n/a/a.java                                                 |
| <a href="https://github.com/danikula/AndroidVideoCache/issues/88">https://github.com/danikula/AndroidVideoCache/issues/88</a> .                 | com/danikula/videocache/HttpUrlSource.java                   |
| <a href="https://github.com/danikula/AndroidVideoCache/issues/43">https://github.com/danikula/AndroidVideoCache/issues/43</a> .                 | com/danikula/videocache/HttpUrlSource.java                   |
| <a href="https://github.com/danikula/AndroidVideoCache/issues">https://github.com/danikula/AndroidVideoCache/issues</a> .                       | com/danikula/videocache/HttpUrlSource.java                   |
| <a href="http://%s:%d/%s">http://%s:%d/%s</a>                                                                                                   | com/danikula/videocache/Pinger.java                          |
| <a href="https://github.com/danikula/AndroidVideoCache/issues/134">https://github.com/danikula/AndroidVideoCache/issues/134</a> .               | com/danikula/videocache/Pinger.java                          |
| <a href="http://%s:%d/%s">http://%s:%d/%s</a>                                                                                                   | com/danikula/videocache/HttpProxyCacheServer.java            |
| <a href="https://d2d63bvtwvflg.cloudfront.net/acfun.json">https://d2d63bvtwvflg.cloudfront.net/acfun.json</a>                                   | com/grass/mh/ui/SplashActivity.java                          |
| <a href="https://clsp.fun">https://clsp.fun</a>                                                                                                 | com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java |
| <a href="https://data.flurry.com/aap.do">https://data.flurry.com/aap.do</a>                                                                     | d/f/b/s0.java                                                |
| <a href="https://data.flurry.com/v1/flr.do">https://data.flurry.com/v1/flr.do</a>                                                               | d/f/b/t0.java                                                |
| <a href="https://github.com/ReactiveX/RxJava/wiki/Error-Handling">https://github.com/ReactiveX/RxJava/wiki/Error-Handling</a>                   | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| <a href="https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0">https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0</a> | io/reactivex/exceptions/UndeliverableException.java          |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                             | l/a/a/f.java                                                 |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                             | org/dsq/library/widget/tablayout/SlidingTabLayout.java       |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                             | org/dsq/library/widget/tablayout/SegmentTabLayout.java       |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>                                             | org/dsq/library/widget/tablayout/CommonTabLayout.java        |

|                                                                   |                                                                        |
|-------------------------------------------------------------------|------------------------------------------------------------------------|
| http://schemas.android.com/apk/res/android                        | pl/droidsonroids/gif/GifTextureView.java                               |
| http://schemas.android.com/apk/res/android                        | pl/droidsonroids/gif/GifTextView.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 |

## 邮箱线索

| 邮箱地址               | 所在文件                                       |
|--------------------|--------------------------------------------|
| danikula@gmail.com | com/danikula/videocache/HttpUrlSource.java |

## 手机线索

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

## 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=86, ST=Hainan, L=Haikou, O=wujikeji, OU=CHN, CN=ChenXiaopeng

签名算法: rsassa\_pkcs1v15  
 有效期自: 2024-07-08 03:53:48+00:00  
 有效期至: 2049-07-02 03:53:48+00:00  
 发行人: C=86, ST=Hainan, L=Haikou, O=wujikeji, OU=CHN, CN=ChenXiaopeng  
 序列号: 0x1d9272ce  
 哈希算法: sha256  
 md5值: 6611eaf74372fd774c2e0599ebb2c5b3  
 sha1值: a735159e80a7445642fd7f8f506780d21e50f4a4  
 sha256值: ec46082daea84aac1dd4c81bb2b30d5f42bf332edd75bf9a0e577b6371c39363  
 sha512值: d4323dd601f8b2d81906a885b2ea5aa0e8311a90e05426430ceb88b20dd440c979ad5872f742516359e635b2028079748dd697e97865dc3f78517d31520747b5  
 公钥算法: rsa  
 密钥长度: 2048  
 指纹: 9bd3fbcbf530ffe3d8d5456295aa7f20e1535a2e2bc53d729056f38ba85ad51a



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_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                     |

# 应用内通信

---

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