MoGua

acfan 1.0.2.APK 分析报告

APP名称:	acfan

包名:	com.androidjks.acfan.d1682156448763174048
域名线索:	10条
URL线索:	20条
邮箱线索:	2条
分析日期:	2024年10月17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: acfan.apk
文件大小: 13.28MB
MD5值: d5deb54fb442eca6aab25e1a2e0bdf7a
SHA1值: c978f6832fd231769a91397cb6bc2358a4e436a6
SHA256值: e7d2560e94e374eae103203b090bfdfbe63addcf738b9003e01ce8a710525415

APP 信息

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

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 **纬度**: 39.099731 **经度**: -94.578568
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 **纬度**: 37.775700 **经度**: -122.395203

d2yvno3b6unw4p.cloudfront.net	**IP**: 13.33.211.196 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
www.openssl.org	**IP**: 104.71.138.221 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
schemas.microsoft.com	**IP**: 13.107.238.49 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
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 **纬度**: 47.682899 **经度**: -122.120903
playready.directtaps.net	**IP**: 40.70.71.156 **所属国家**: United States of America **地区**: Virginia **城市**: Boydton **纬度**: 36.667641 **经度**: -78.387497
	IP: 69.147.80.15 **所属国家**: United States of America **地区**: New York

data.flurry.com	**城市**: New York City **纬度**: 40.731323 **经度**: -73.990089

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

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

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=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

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