MoGua

爸爸上我 7.0.0.APK 分析报告

APP名称:	爸爸上我

包名:	com.androidjks.dsx.d1739872337200175217
域名线索:	16条
URL线索:	20条
邮箱线索:	3条
分析日期:	2025年10月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: shishidh_7.0.0_72436403.apk
文件大小: 28.15MB
MD5值: 04898e6a9f31242a71a123971d3d460f
SHA1值: c61f7041b3eb778690f3b4d9aa99823008999c5d
SHA256值: e4c86fb7e137858b265376d13ae793c4a03145f8837ed7c72e0dbada7851497a

APP 信息

App名称: 爸爸上我
包名: com.androidjks.dsx.d1739872337200175217
主活动Activity: com.grass.mh.SplashActivity
安卓版本名称: 7.0.0
安卓版本: 700

域名线索

域名	服务器信息
d12ilce452zs0c.cloudfront.net	**IP**: 13.35.226.188 **所属国家**: India **地区**: Telangana **城市**: Hyderabad **纬度**: 17.375290 **经度**: 78.474388
exoplayer.dev	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
playready.directtaps.net	**IP**: 104.45.231.79 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.774929 **经度**: -122.419418
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
clsp.fun	**IP**: 143.92.53.216 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
d3q94thu3glhi5.cloudfront.net	**IP**: 13.35.212.19 **所属国家**: India **地区**: Telangana **城市**: Hyderabad **纬度**: 17.375290 **经度**: 78.474388
ds.ozra0j.xyz	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
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 **纬度**: 40.731323 **经度**: -73.990089
schemas.android.com	没有服务器地理信息.
	IP: 185.199.111.153

dashif.org	**所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
d1r1vv8zvbqvut.cloudfront.net	IP: 143.204.102.61 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
ds.ok2a84.xyz	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 **纬度**: 1.289987 **经度**: 103.850281
ds.o5h7ek.xyz	IP: 103.224.212.213 **所属国家**: Australia **地区**: Victoria **城市**: Beaumaris **纬度**: -37.982201 **经度**: 145.038940
schemas.microsoft.com	IP: 13.107.246.74 **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://schemas.android.com/apk/res/android	c/j/b/b/e.java
http://ns.adobe.com/xap/1.0/\u0000	c/n/a/a.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	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://ds.o5h7ek.xyz	com/grass/mh/SplashActivity.java
https://ds.ok2a84.xyz	com/grass/mh/SplashActivity.java
https://ds.ozra0j.xyz	com/grass/mh/SplashActivity.java
https://d12ilce452zs0c.cloudfront.net/zy_ldy.json	com/grass/mh/SplashActivity.java
https://d1r1vv8zvbqvut.cloudfront.net/zy.json	com/grass/mh/SplashActivity.java
https://d3q94thu3glhi5.cloudfront.net/zy.json	com/grass/mh/SplashActivity.java
https://clsp.fun	com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java
https://data.flurry.com/aap.do	e/f/b/s0.java

https://data.flurry.com/v1/flr.do	e/f/b/t0.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	e/g/a/a/t0.java
http://dashif.org/guidelines/last-segment-number	e/g/a/a/h1/j0/j/c.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
http://schemas.android.com/apk/res/android	n/a/a/f.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/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	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
aw666me01@gmail.com	e/h/a/d0.java

aw666me01@gmail.com	摸瓜V1引擎

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=cn, ST=dd, L=ss, O=ee, OU=ff, CN=dd
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-13 04:09:34+00:00
有效期至: 2048-11-06 04:09:34+00:00
发行人: C=cn, ST=dd, L=ss, O=ee, OU=ff, CN=dd
序列号: 0x743b01c
哈希算法: sha256
md5值: 0fbe5383c8188c582e547bde875098e3
sha1值: f978cf6b8366b6fd7713288782ce2e5a39eb2d80
sha256值: 51d8a5b8de8643f770b91beadd5349a62006edd59aa3b4c3aae9fb3bbd6a432d
sha512值: 81fe1ae3c05bc8b40d4775f34f9179bd6d3e6b5bce30082333fccff039daf51794f5d0348151f56314e329844d8e7d86520a283a9d22be9ad46ed9dfec3f99ef
公钥算法: rsa
密钥长度: 2048
指纹: 2c1178775019873bd5ff023747db0cfd8700b725966dc65554cdb354a40a214d

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.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.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.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