MoGua

萌萝社 1.4.9.APK 分析报告

APP名称: 萌萝社

包名:	com.android.mh.d1704764048169093408
域名线索:	14条
URL线索:	21条
邮箱线索:	1条
分析日期:	2025年10月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: mls_1.4.9_64252878.apk
文件大小: 24.52MB
MD5值: 7a19ee77086d99c59e317c870102b8b1
SHA1值: 6b17173a8552d42d3ec0e077c97f97fd542fe38e
SHA256值: fe0a08966c1254383b1b259283431418062c6a8a8ebb0e4b707bffbff916634d

APP 信息

App名称: 萌萝社
包名: com.android.mh.d1704764048169093408
主活动Activity: com.grass.mh.ui.SplashActivity
安卓版本名称: 1.4.9
安卓版本: 149

域名线索

域名	服务器信息
data.flurry.com	**IP**: 69.147.88.7 **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
dashif.org	**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
mh.u4tblg.xyz	**IP**: 172.67.158.109 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
schemas.android.com	没有服务器地理信息.
mh.tzgmbg.xyz	**IP**: 172.67.222.48 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ns.adobe.com	没有服务器地理信息.
mh.u68hn2.xyz	**IP**: 104.21.68.13 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.w3.org	**IP**: 104.18.22.19 **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**: 54.230.174.43 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
exoplayer.dev	**IP**: 185.199.108.153 **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
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
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
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/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://clsp.fun	com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java
https://mh.tzgmbg.xyz	com/grass/mh/ui/SplashActivity.java
https://mh.u4tblg.xyz	com/grass/mh/ui/SplashActivity.java
https://mh.u68hn2.xyz	com/grass/mh/ui/SplashActivity.java
https://d2yvno3b6unw4p.cloudfront.net/mh.json	com/grass/mh/ui/SplashActivity.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/h/a/a/t0.java
http://dashif.org/guidelines/last-segment-number	e/h/a/a/h1/j0/j/c.java
http://www.w3.org/ns/ttml	e/h/a/a/i1/q/a.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	o/a/a/f.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	org/dsq/library/widget/tablayout/SlidingTabLayout.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
16222222222	e/h/a/a/c1/a0/d.java
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: 2022-03-25 13:01:42+00:00
有效期至: 2047-03-19 13:01:42+00:00
发行人: C=24, ST=24, L=24, O=24, OU=24, CN=24
序列号: 0x797b824
哈希算法: sha256
md5值: 5448189ea4647045f735df55eb60fdfd
sha1值: b85d995154b20da9f874eb18add66052a9b246b8
sha256值: f406c7482dda52357d592a8aae0a74141414b5d1a3db8ae3c7aeec3641d3d790
sha512值: 43082bbc7b0b443dde9df011d1351ccd48563bd4e4ab38be6d91168fad9098f8854fbf7a0df7c90f062c734bdf78ea3d56eaca60121f216e002b5264631b5544
公钥算法: rsa
密钥长度: 2048
指纹: a49d0e68a41eb147ebb8983c8b8f704ff558cd1bd3aa1727ca8185e959533f58

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
