MoGua

失乐园 1.0.3.APK 分析报告

APP名称:	失乐园

包名:	com.androidjks.sly.d17047627034640911143
域名线索:	15条
URL线索:	22条
邮箱线索:	2条
分析日期:	2025年6月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: sly_1.0.3_62817865.apk
文件大小: 13.74MB
MD5值: c59be21e4116eefc49bfcf892aef0637
SHA1值: e9261c7d1257d187243558afed02ef25d4bce18d
SHA256值: 99bbde20e441f7672a3162d69c1a61d630ae16bdcef305db106f8843c08f4f94

APP 信息

App名称: 失乐园
包名: com.androidjks.sly.d1704762703464091143
主活动Activity: com.grass.mh.SplashActivity
安卓版本名称: 1.0.3
安卓版本: 103

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**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
schemas.android.com	没有服务器地理信息.
	IP: 104.18.22.19

www.w3.org	**所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ly.yhuyvv.xyz	**IP**: 172.67.133.194 **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.
exoplayer.dev	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
d2yvno3b6unw4p.cloudfront.net	**IP**: 54.230.174.144 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
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
ly.ktlggh.xyz	IP: 104.21.40.224 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ly.83o6vb.xyz	IP: 104.21.94.37 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
schemas.microsoft.com	IP: 13.107.213.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
www.openssl.org	IP: 184.50.93.94 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

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://ly.yhuyvv.xyz	com/grass/mh/SplashActivity.java
https://ly.ktlggh.xyz	com/grass/mh/SplashActivity.java
https://ly.83o6vb.xyz	com/grass/mh/SplashActivity.java
https://d2yvno3b6unw4p.cloudfront.net/sly.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
http://www.w3.org/ns/ttml	e/g/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	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/CommonTabLayout.java
http://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/SegmentTabLayout.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
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
16222222222	e/g/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: 2023-09-07 12:02:06+00:00
有效期至: 2048-08-31 12:02:06+00:00
发行人: C=24, ST=24, L=24, O=24, OU=24, CN=24
序列号: 0x6d1000e8
哈希算法: sha256
md5值: 469ef0779dcbf1bdad605750871ae31a
sha1值: 525e85bce1cdf81c8ccf7b3149285f0fb4a49538
sha256值: 9271fd09f25085a216f942fb5c0960f0c8fdd8dabb2215d3796ba17c4456afae
sha512值: fa0fdeb0aad5c40589a4f00d90ca7990b9b42dcb55e168ccb6395ca3834d40d8d5cb25ca11aade07bd19976f2a529528c3e465a9efbea6a06b485ceca3a04bf4
公钥算法: rsa
密钥长度: 2048
指纹: 3d17924f3d632ae083449083ebcfbad63883b670c081ce992e442c4678b91a08

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