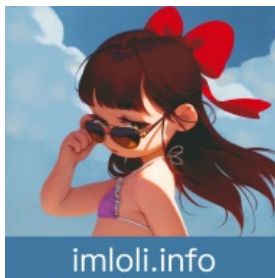




MoGua

91Lolita 3.20.APK 分析报告



APP名称:

91Lolita

包名: `com.huawei.android.kkllapp`

域名线索: 27条

URL线索: 33条

邮箱线索: 2条

分析日期: 2025年8月19日

分析平台: [摸瓜APK反编译平台](#)

文件名: loli.apk
文件大小: 18.45MB
MD5值: 7814674de89b0fe0f43fa52d2c127b62
SHA1值: 836bcfbf402933758068143d74e33aeaf2b31f96
SHA256值: 112df1527f9f6f047f7fa2c089e251e607d9e56ba634d3e7ee9017fa959aaf52

i APP 信息

App名称: 91Lolita
包名: com.huawei.android.kkllapp
主活动Activity: com.ty.app.tongyanrealapp.ui.splash.SplashActivity
安卓版本名称: 3.20
安卓版本: 10

🔍 域名线索

域名	服务器信息
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
lolimn02.xyz	IP: 1.13.9.79 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England

	城市: Warrington 纬度: 52.184460 经度: -0.687590
swybgjapi2.hymailto03.top	IP: 172.67.161.252 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.
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
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
swybgjapi.api20991.top	IP: 103.117.102.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
swybgjapi.hymailto.top	IP: 172.67.164.140 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

dnsrepo-pub.alibaba.com	IP: 106.11.43.250 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
xmlpull.org	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
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
app.iqiyi.com	IP: 202.108.14.128 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
swybgjapi.hncake.top	没有服务器地理信息.
xml.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 113.56.189.162

h.trace.qq.com	所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
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
otheve.beacon.qq.com	IP: 113.56.189.242 所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
swybgjapi4.hymailto03.top	IP: 104.21.15.86 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
swybgjapi2.api20991.top	IP: 103.117.102.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
swybgjapi.hymailto03.top	IP: 104.21.15.86 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

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
swybgjapi3.hymailto03.top	IP: 172.67.161.252 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
othstr.beacon.qq.com	IP: 112.65.194.211 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.binance.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.huobi.com	IP: 199.59.149.204 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
swybgjapi4.api20991.top	IP: 103.117.102.61 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://swybgjapi.api20991.top	defpackage/c41.java
http://swybgjapi2.api20991.top	defpackage/c41.java
http://swybgjapi4.api20991.top	defpackage/c41.java
http://swybgjapi.hymailto03.top	defpackage/c41.java
http://swybgjapi2.hymailto03.top	defpackage/c41.java
http://swybgjapi3.hymailto03.top	defpackage/c41.java
http://swybgjapi4.hymailto03.top	defpackage/c41.java
http://swybgjapi.hncake.top	defpackage/c41.java
http://swybgjapi.hymailto.top	defpackage/c41.java
http://dashif.org/guidelines/last-segment-number	defpackage/cs.java
https://github.com/danikula/AndroidVideoCache/issues/43	defpackage/ei0.java
https://github.com/danikula/AndroidVideoCache/issues	defpackage/ei0.java
https://github.com/danikula/AndroidVideoCache/issues/88	defpackage/ei0.java

https://exoplayer.dev/issues/player-accessed-on-wrong-thread	defpackage/ey1.java
http://%s:%d/%s	defpackage/fh1.java
https://github.com/danikula/AndroidVideoCache/issues/134.	defpackage/fh1.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/im.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/e71.java
https://dnsrepo-pub.alibaba.com/api/internet/putTermData	defpackage/oi2.java
https://dnsrepo-pub.alibaba.com/api/internet/putTermStatusData	defpackage/oi2.java
http://%s:%d/%s	defpackage/rh0.java
http://www.w3.org/ns/ttml	defpackage/r92.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/qy1.java
https://dnsrepo-pub.alibaba.com/api/internet/putTermData	defpackage/wj2.java
https://dnsrepo-pub.alibaba.com/api/internet/putTermStatusData	defpackage/wj2.java
http://xmlpull.org/v1/doc/features.html	defpackage/wk1.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/wv0.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/x60.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java

http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://xml.apache.org/xslt	com/orhanobut/logger/LoggerPrinter.java
https://h.trace.qq.com/kv	com/tencent/beacon/a/b/c.java
https://otheve.beacon.qq.com/analytics/upload	com/tencent/beacon/base/net/c/b.java
https://othstr.beacon.qq.com/analytics/upload	com/tencent/beacon/base/net/c/b.java
http://xmlpull.org/v1/doc/features.html	com/tencent/cos/xml/transfer/XmlBuilder.java
http://www.w3.org/2001/XMLSchema-instance	com/tencent/cos/xml/transfer/XmlBuilder.java
http://xmlpull.org/v1/doc/features.html	com/tencent/cos/xml/transfer/XmlSlimBuilder.java
https://t.me/tysptv001	com/ty/app/tongyanrealapp/ui/splash/SplashActivity\$bindEvent\$2\$1\$1.java
https://t.me/tysptv001	com/ty/app/tongyanrealapp/ui/splash/SplashActivity\$bindEvent\$2.java
http://lolimn02.xyz:6969/api/set/status	com/ty/app/tongyanrealapp/ui/splash/SplashActivity.java
http://app.iqiyi.com	com/ty/app/tongyanrealapp/ui/video/p000long/LongVideoDetailActivity\$videoPlayHeader\$2.java
http://app.iqiyi.com	com/ty/app/tongyanrealapp/ui/video/p001short/ShortListPlayFragment\$videoPlayHeader\$2.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.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
https://www.binance.com	Mogua Engine V1

https://www.huobi.com	Mogua Engine V1

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	defpackage/ei0.java
appro@openssl.org	lib/arm64-v8a/libconscrypt_jni.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=ushdf, ST=dsouyf, L=dhfds, O=kfjxhgv, OU=osdyf, CN=piasu
签名算法: rsassa_pkcs1v15
有效期自: 2023-12-22 07:18:15+00:00
有效期至: 2078-09-24 07:18:15+00:00
发行人: C=ushdf, ST=dsouyf, L=dhfds, O=kfjxhgv, OU=osdyf, CN=piasu

序列号: 0xc54be83444b03567
 哈希算法: sha256
 md5值: 44f5366f9b4270f9b757cb7d57257084
 sha1值: 6c5663013e48395e7af4f2d75fb4aeda58ee02f8
 sha256值: 98b51613e6a4a5d5cb3a7c70fe0f0c1f58a1f22e2bd443b548f8a9ce7ef80c86
 sha512值: d1ec438429edf0c665aed355d0feacc308fbd718cf9205c62c2a8729a0b69c9faf99387b30618e9deec00bbcaab4299893bde3544b3e13499fe16138fab4a7a5
 公钥算法: rsa
 密钥长度: 2048
 指纹: 44c09a3e7673d6907f8588d38fb0f5d41c81e241ae80b5de7246e2e7d47ded2b

硬编码敏感信息

可能的敏感信息
"accountCredentials" : "Account Credentials"
"ordinaryUser" : "I am an ordinary user, only VIP can be redeemed"
"retrieveByCertificate" : "Retrieve by certificate"
"upload_dont_close_token" : "Please do not close this page to obtain uploaded resources"
"user" : "User"
"accountCredentials" : "账号凭证"
"ordinaryUser" : "我是普通用户，购买正式会员才可兑现"
"retrieveByCertificate" : "凭证找回"
"upload_dont_close_token" : "请不要关闭本页面，获取上传资源"
"user" : "用户"

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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

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。