MoGua

91重口 1.6.0.APK 分析报告

APP名称: 91重口

包名:	gov.juyov.jrbplx
域名线索:	20条
URL线索:	16条
邮箱线索:	4条
分析日期:	2025年7月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 51lieqi_1.6.0_250701_6.apk
文件大小: 30.0MB
MD5值: 3b77a56c4ff517faefd8809ed74bb6e9
SHA1值: 4aa98f0c453d9e790974ec8b944a36cecd4e399f
SHA256值: 8e094b3aa229ae90bb3dbbbe03198162a529f7023614d09c603abbf533b5022e

APP 信息

App名称: 91重口
包名: gov.juyov.jrbplx
主活动Activity: com.tbone.novelty.MainActivity
安卓版本名称: 1.6.0
安卓版本: 7

域名线索

域名	服务器信息
flutter.dev	**IP**: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
raw.githubusercontent.com	**IP**: 185.199.109.133 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
developer.apple.com	**IP**: 17.253.85.205 **所属国家**: Hong Kong **地区**: Hong Kong

	城市: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
127.0.0.1	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
exoplayer.dev	**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
www.jsdelivr.com	**IP**: 104.21.23.24 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
51lqapi1.wwmtcdbm.xyz	**IP**: 156.255.123.51 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
developer.android.com	**IP**: 142.250.73.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
	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
aomedia.org	**IP**: 157.240.10.36 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604
www.google.cn	**IP**: 114.250.69.34 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ns.adobe.com	没有服务器地理信息.
api.flutter.dev	**IP**: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.ibm.com	**IP**: 23.1.167.82 **所属国家**: Japan **地区**: Osaka **城市**: Ibaraki **纬度**: 34.816425 **经度**: 135.568909
	IP: 156.255.123.51 **所属国家**: Hong Kong **地区**: Hong Kong

51lqapi2.wwmtcdbm.xyz	**城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
developer.mozilla.org	IP: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
51lqapi3.wwmtcdbm.xyz	IP: 154.207.77.51 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
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
staff.tea123.me	IP: 172.67.169.1 **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

URL线索

URL信息	Url所在文件
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	f/d/a/a/e2.java
https://x</LA_URL>	f/d/a/a/w3/k0.java
https://x	f/d/a/a/w3/k0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	f/d/a/a/w3/l0.java
http://ns.adobe.com/xap/1.0/	f/d/a/a/x3/m0/a.java
https://exoplayer.dev/issues/cleartext-not-permitted	f/d/a/a/e4/d0.java
https://aomedia.org/emsg/ID3	f/d/a/a/z3/j/a.java
https://developer.apple.com/streaming/emsg-id3	f/d/a/a/z3/j/a.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/d/t.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/e.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/l.java
http://ns.adobe.com/xap/1.0/\u0000	e/d/a/a.java
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	摸瓜V2引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎

https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://www.google.cn/intl/zh-CN/chrome	摸瓜V2引擎
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so
https://51lqapi3.wwmtcdbm.xyz/api.php	lib/armeabi-v7a/libapp.so
http://127.0.0.1:	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
https://raw.githubusercontent.com/little-5/backup/master/51lq.txt	lib/armeabi-v7a/libapp.so
https://staff.tea123.me/e.jpg	lib/armeabi-v7a/libapp.so
https://51lqapi1.wwmtcdbm.xyz/api.php	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://51lqapi2.wwmtcdbm.xyz/api.php	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new.	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so
m_immutablelist@0150898._xib _double@0150898.fromintege _growablelist@0150898._literal _casterror@0150898._create _growablelist@0150898._withdata n_typeerror@0150898._create eo_bytebuffer@7027147._new _assertionerror@0150898._create	lib/armeabi-v7a/libapp.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
appro@openssl.org	lib/arm64-v8a/libijkffmpeg.so

手机线索

手机号	所在文件
17512775099	f/d/b/c/a.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: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2022-11-03 10:16:02+00:00

有效期至: 2052-10-26 10:16:02+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
md5值: 7d8a2c0d2493e5d6d85c3865d0918482
sha1值: 7682ef35f017d1b3d352557971c295a6885fae4c
sha256值: 7b86e6199d7c910d075153a0fe61cf241a4b390dd5f4dd0a74381dab7cf42b6f
sha512值: 5d1a8d09f651ee318f3411e559df66a5439dfea5538839f3bc527c6fa3a0671d1326e28949e56f2766e9f716b69ff5ecb1298370c4bb59b7701a43ef4744178b
公钥算法: rsa
密钥长度: 2048
指纹: a715c81d7c87ff29afca669875aed119aeed1a6f489b5d567f6e4c3922f04e1f

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.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.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.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_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.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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度

应用内通信
