



MoGua

91看片 8.59.APK 分析报告



APP名称:

91看片

包名:	yqkrr.axee.qpfd.azaa
域名线索:	30条
URL线索:	44条
邮箱线索:	2条
分析日期:	2025年6月4日
分析平台:	摸瓜APK反编译平台

文件名: lsav_app_20250303.apk
文件大小: 22.0MB
MD5值: 67498ab4545bd1b94c4221a41e61efe7
SHA1值: fbc97a46fd967e01f236e4660ac5335e336d512d
SHA256值: d456cf14da5cbc73cf6b6af64a1063d84e6288b5bdbf8e33e523fc31c3872ae1

i APP 信息

App名称: 91看片
包名: yqkrr.axee.qpfd.azaa
主活动Activity: com.paulkman.nova.MainActivity
安卓版本名称: 8.59
安卓版本: 1

🔍 域名线索

域名	服务器信息
bense.tv	没有服务器地理信息.
lsav-api-own6oi.ggpfi.com	IP: 221.194.162.223 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
lsav-api-wx041z.aqpcw.com.eo.dnse3.com	IP: 221.204.43.199 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508

app.nova-traffic-1688.com	没有服务器地理信息.
lsav-api-fb5u2f.mpttn.com	IP: 221.194.162.229 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
lsav-api-pao5tc.dsudm.com.eo.dnse3.com	IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
api.ipify.org	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
lsav-api-pao5tc.dsudm.com	IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
lsav-api-fb5u2f.mpttn.com.w.kunluncan.com	IP: 221.194.162.225 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
	IP: 47.253.28.4 所属国家: United States of America 地区: Virginia

us-east-1.oss-acc.aliyuncs.com	城市: Virginia Beach 纬度: 36.853149 经度: -75.978043
portal.toushibao.com	IP: 49.4.55.205 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.
91kan.one	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
oss-acc-allline.aliyuncs.com	IP: 39.107.216.248 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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
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
lsav-api-o1p9b6.mpttn.com	IP: 221.194.162.225 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
seagull-data.toushibao.com	IP: 119.3.240.48 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
logback.qos.ch	IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge 纬度: 46.180931 经度: 6.138709
lsav-api-o1p9b6.mpttn.com.w.kunluncan.com	IP: 123.125.216.215 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
issuetracker.google.com	IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660 经度: -79.382927
	IP: 104.18.22.19 所属国家: United States of America

www.w3.org	地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.slf4j.org	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
lsav-api-own6oi.ggpfi.com.w.kunluncan.com	IP: 221.194.162.224 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
developer.android.com	IP: 172.217.14.206 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
apm-int.cloudwise.com	IP: 139.162.3.159 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
adc3c15e217fd4f863e346e4c3b9b482.oss-accelerate.aliyuncs.com	IP: 39.107.216.248 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

lsav-api-wx041z.aqpcw.com	IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
oss-acc-allline.aliyuncs.com.gds.alibabadns.com	IP: 39.107.216.248 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
xml.org	IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246

URL线索

URL信息	Url所在文件
https://app.nova-traffic-1688.com	a9/s.java
https://github.com/google/gson/blob/main/Troubleshooting.md	b7/a.java
http://www.slf4j.org/codes.html	ch/qos/logback/classic/turbo/DynamicThresholdFilter.java
http://www.slf4j.org/codes.html	ch/qos/logback/classic/turbo/MDCFilter.java
http://logback.qos.ch/css/classic.css	ch/qos/logback/classic/html/UrlCssBuilder.java

http://logback.qos.ch/codes.html	ch/qos/logback/classic/net/SocketReceiver.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/CoreConstants.java
http://logback.qos.ch/manual/	ch/qos/logback/core/CoreConstants.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/FileAppender.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/OutputStreamAppender.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/net/AbstractSocketAppender.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/net/SyslogAppenderBase.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/net/SMTPAppenderBase.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/joran/action/AppenderRefAction.java
http://xml.org/sax/features/validation	ch/qos/logback/core/joran/event/SaxEventRecorder.java
http://xml.org/sax/features/namespace	ch/qos/logback/core/joran/event/SaxEventRecorder.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/rolling/SizeBasedTriggeringPolicy.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/rolling/TimeBasedRollingPolicy.java
http://logback.qos.ch/manual/appenders.html	ch/qos/logback/core/rolling/SizeAndTimeBasedFNATP.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/rolling/FixedWindowRollingPolicy.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/rolling/TimeBasedFileNamingAndTriggeringPolicyBase.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/rolling/RollingFileAppender.java

http://logback.qos.ch/codes.html	ch/qos/logback/core/rolling/helper/RenameUtil.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/pattern/parser/Parser.java
http://logback.qos.ch/codes.html	ch/qos/logback/core/sift/SiftingJoranConfiguratorBase.java
https://seagull-data.toushibao.com	com/cloudwise/agent/app/constant/SDKConst.java
http://portal.toushibao.com	com/cloudwise/agent/app/constant/SDKConst.java
http://portal.toushibao.com/api/v2/mobile/sdk/user_info	com/cloudwise/agent/app/config/ConfigModel.java
https://seagull-data.toushibao.com/api/v2/mobile/sdk	com/cloudwise/agent/app/config/ConfigModel.java
https://seagull-data.toushibao.com/api/v2/mobile/sdk/cdn_provider	com/cloudwise/agent/app/config/ConfigModel.java
http://portal.toushibao.com/api/v2/mobile/setting	com/cloudwise/agent/app/config/ConfigModel.java
http://portal.toushibao.com/api/v2/mobile/timestamp	com/cloudwise/agent/app/config/ConfigModel.java
https://seagull-data.toushibao.com/api/v70/agent/sessionUpload	com/cloudwise/agent/app/config/ConfigModel.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	e4/h0.java
http://ns.adobe.com/xap/1.0/\u0000	h1/g.java
https://issuetracker.google.com/issues/new?component=413106	o1/d2.java
https://www.slf4j.org/codes.html	oi/e.java
https://developer.android.com/training/articles/direct-boot	o2/f.java
https://exoplayer.dev/issues/cleartext-not-permitted	q5/a0.java
https://app.nova-traffic-1688.com	tf/a.java

https://app.nova-traffic-1688.com	v8/f0.java
https://app.nova-traffic-1688.com	v8/m2.java
https://api.ipify.org	v8/b1.java
https://app.nova-traffic-1688.com	ga/h.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	yb/z.java
https://app.nova-traffic-1688.com	fd/d.java
https://apm-int.cloudwise.com	d8/a.java
https://github.com/google/gson/blob/main/Troubleshooting.md	z6/c.java
https://bense.tv	摸瓜V1引擎
lsav-api-own6oi.ggpfi.com	摸瓜V3引擎
lsav-api-own6oi.ggpfi.com.w.kunluncan.com	摸瓜V3引擎
lsav-api-wx041z.aqpcw.com.eo.dnse3.com	摸瓜V3引擎
91kan.one	摸瓜V3引擎
adc3c15e217fd4f863e346e4c3b9b482.oss-accelerate.aliyuncs.com	摸瓜V3引擎
oss-acc-allline.aliyuncs.com	摸瓜V3引擎
lsav-api-fb5u2f.mpttn.com	摸瓜V3引擎
lsav-api-pao5tc.dsudm.com.eo.dnse3.com	摸瓜V3引擎

api.ipify.org	摸瓜V3引擎
lsav-api-pao5tc.dsudm.com	摸瓜V3引擎
oss-acc-allline.aliyuncs.com.gds.alibabadns.com	摸瓜V3引擎
lsav-api-wx041z.aqpcw.com	摸瓜V3引擎
lsav-api-fb5u2f.mpttn.com.w.kunluncan.com	摸瓜V3引擎
lsav-api-o1p9b6.mpttn.com.w.kunluncan.com	摸瓜V3引擎
us-east-1.oss-acc.aliyuncs.com	摸瓜V3引擎
lsav-api-o1p9b6.mpttn.com	摸瓜V3引擎
http://%s	lib/arm64-v8a/libcf-msc.so
http://%s	lib/armeabi-v7a/libcf-msc.so

 邮箱线索

邮箱地址	所在文件
ftp@example.com	lib/arm64-v8a/libcf-msc.so
ftp@example.com	lib/armeabi-v7a/libcf-msc.so

 手机线索

--	--

手机号	所在文件
15778476000	lh/f.java

🌟 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=US, O=Sun, OU=JavaSoft, CN=Mark Jones
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-03 10:10:32+00:00
有效期至: 2079-12-05 10:10:32+00:00
发行人: C=US, O=Sun, OU=JavaSoft, CN=Mark Jones
序列号: 0xe26ab9a258131348
哈希算法: sha256
md5值: f4df62eb37a640ea22fe470761392ec2
sha1值: 6d0e054aef598448ced98e812aa38679c9051c6f
sha256值: 5bfd1433797cc2d62026c66e884fd333a25a7b7c1292f6d1f294e3dd069fafd7
sha512值: 8d483bee65a86c76a205563dcc94fc2d86b0f9461d070ce0e1e8d7be3f80473f28d32a772f8b037bb61eb5552b6f6478e1af4ef4656330890261016611284dc2
公钥算法: rsa
密钥长度: 2048
指纹: 40223206d88902650fc2db34e999062e2f00a1d7010a3ee2139a326264c02689

🔑 硬编码敏感信息

可能的敏感信息
"nova_app_auth_button_get_phone_number_verify_code": "獲取驗證碼"
"nova_app_auth_button_get_phone_number_verify_code_retry_count_down": "%1\$d秒後重試"

"nova_app_auth_button_sign_up" : "立即註冊"
"nova_app_auth_dialog_qrcode_success" : "歡迎回來"
"nova_app_auth_mywallet" : "我的錢包"
"nova_app_auth_mywallet_recharge" : "去充值"
"nova_app_auth_sign_up_successfully" : "註冊成功"
"nova_app_auth_vip" : "會員VIP"
"nova_app_auth_vip_register" : "去開通"
"nova_app_button_my_purchase_api" : "我的購買(待接API)"
"nova_app_button_user" : "用戶:"
"nova_app_debug_enter_password" : "請輸入密碼"
"nova_app_setting_account_credentials" : "帳號憑證"
"nova_app_auth_button_get_phone_number_verify_code" : "獲取驗證碼"
"nova_app_auth_button_get_phone_number_verify_code_retry_count_down" : "%1\$d秒後重試"
"nova_app_auth_button_sign_up" : "立即註冊"
"nova_app_auth_dialog_qrcode_success" : "歡迎回來"
"nova_app_auth_mywallet" : "我的錢包"
"nova_app_auth_mywallet_recharge" : "去充值"
"nova app auth sign up successfully" : "註冊成功"

"nova_app_auth_vip" : "會員VIP"
"nova_app_auth_vip_register" : "去開通"
"nova_app_button_my_purchase_api" : "我的購買(待接API)"
"nova_app_button_user" : "用戶:"
"nova_app_debug_enter_password" : "請輸入密碼"
"nova_app_setting_account_credentials" : "帳號憑證"

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.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.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.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。
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
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.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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
evokx.ffz.xxgnq.dikt.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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	允许应用程序写入外部存储

		容	
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

应用内通信