



MoGua

91看片 8.57.APK 分析报告



APP名称:

91看片

包名:	dyqbs.zebd.qriu.nrffq
域名线索:	13条
URL线索:	44条
邮箱线索:	2条
分析日期:	2025年5月2日
分析平台:	摸瓜APK反编译平台

文件名: apk (83).apk
文件大小: 21.24MB
MD5值: 801aaead7b01f85331714cb55843e5ea
SHA1值: 1a5ee0eee9566e749e96ba4c2f054b7229251898
SHA256值: 2d1f7cbe84de6312dc15021532db7ffefc7887d127429931a3cd71ec42ef4a56

i APP 信息

App名称: 91看片
包名: dyqbs.zebd.qriu.nrffq
主活动Activity: com.paulkman.nova.MainActivity
安卓版本名称: 8.57
安卓版本: 1

🔍 域名线索

域名	服务器信息
issuetracker.google.com	IP: 142.250.69.206 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: 172.105.113.87 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
bense.tv	没有服务器地理信息.
	IP: 117.78.31.85

portal.toushibao.com	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.ipify.org	IP: 172.67.74.152 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
logback.qos.ch	IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
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
www.slf4j.org	IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge 纬度: 46.180931 经度: 6.138709
ns.adobe.com	没有服务器地理信息.
	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania

exoplayer.dev	城市: California 纬度: 40.065647 经度: -79.891724
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
app.nova-traffic-1688.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

URL线索

URL信息	Url所在文件
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	b4/n0.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/joran/action/AppenderRefAction.java
http://xml.org/sax/features/validation	ch/qos/logback/core/joran/event/SaxEventRecorder.java
http://xml.org/sax/features/namespaces	ch/qos/logback/core/joran/event/SaxEventRecorder.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/net/SyslogAppenderBase.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/SMTPAppenderBase.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/sift/SiftingJoranConfiguratorBase.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
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://issuetracker.google.com/issues/new?component=413106	j1/v1.java
https://issuetracker.google.com/issues/new?component=413106	j1/u0.java
https://issuetracker.google.com/issues/new?component=413106	j1/q1.java
https://exoplayer.dev/issues/cleartext-not-permitted	j5/w.java
http://ns.adobe.com/xap/1.0/\u0000	e1/a.java
https://www.slf4j.org/codes.html	ki/e.java
https://api.ipify.org	o8/d0.java
https://app.nova-traffic-1688.com	o8/n.java

https://app.nova-traffic-1688.com	o8/z0.java
https://app.nova-traffic-1688.com	t8/m.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	x0/u.java
https://app.nova-traffic-1688.com	z9/e.java
https://app.nova-traffic-1688.com	ea/e.java
https://app.nova-traffic-1688.com	nb/b.java
https://app.nova-traffic-1688.com	pa/c.java
https://apm-int.cloudwise.com	w7/a.java
https://app.nova-traffic-1688.com	yc/c.java
https://bense.tv	摸瓜V1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	gh/c.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: 2024-12-29 02:09:51+00:00
有效期至: 2079-10-02 02:09:51+00:00
发行人: C=US, O=Sun, OU=JavaSoft, CN=Mark Jones
序列号: 0x15ec87bf4c9b86cd
哈希算法: sha256
md5值: b7ffda7a0aabfda25811cf2bc0ba2eb5
sha1值: 1f165a31646b4a206225187bc715eb447f16f472
sha256值: 6ff6565c0d1643220f9b20bf3ee33c79185c3e9220d6796a8e49faeb6a33dc58
sha512值: f57c96df3f1d198f607d8667be747b27a323d1222104a77371c8e6d5a19c9995973985d00922f22418a25b9d19c56893992371e8bd49c63812882fbd033c2143
公钥算法: rsa
密钥长度: 2048
指纹: 007bf08bd3b2ab1693a5710f89fb8ddd0c9eae15de8da6a836d1d6822ce85296

🔑 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 : 我的钱包
"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。
bkxavr.ujj.jyab.qon.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 and 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/删除外部存储内容	允许应用程序写入外部存储
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