



# MoGua

## 騷狐視頻 7.12.3811eb86.APK 分析報告



APP名称:

騷狐視頻

包名:

ixmcb.fbwod.iezq.ccf

域名线索:	11条
URL线索:	18条
邮箱线索:	0条
分析日期:	2024年9月18日
分析平台:	<a href="#">摸瓜APK反编译平台</a>

## 文件信息

文件名: saohu\_app\_20230416\_y9gp.apk

文件大小: 17.46MB

MD5值: c1cfe0e556217920159afa919dc22177

SHA1值: 7bdb64c0e212d50dcd9346c71cd94d4bf3354881

SHA256值: c00fd57f8d4b835448cd07b4551d3748bd5605b22ca2b2faed532a680a614368

## APP 信息

App名称: 騷狐視頻

包名: ixmcb.fbwod.iezq.cef

主活动Activity: com.paulkman.nova.MainActivity

安卓版本名称: 7.12.3811eb86

安卓版本: 1

## 🔍 域名线索

域名	服务器信息
swebtoon-phinf.pstatic.net	IP: 23.47.50.9 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.783058 经度: -96.806671
cdn.readmoo.com	IP: 78.16.49.15 所属国家: Ireland 地区: Waterford 城市: Kill 纬度: 52.176109 经度: -7.335000
saohu.live	IP: 175.29.155.193 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
cdnec.sanmin.com.tw	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
app.nova-traffic-1688.com	没有服务器地理信息.
	IP: 192.133.77.191

www.google.com	<b>所属国家:</b> United States of America <b>地区:</b> California <b>城市:</b> San Francisco <b>纬度:</b> 37.773968 <b>经度:</b> -122.410446
xmlpull.org	<b>IP:</b> 185.199.109.153 <b>所属国家:</b> United States of America <b>地区:</b> Pennsylvania <b>城市:</b> California <b>纬度:</b> 40.065632 <b>经度:</b> -79.891708
www.w3.org	<b>IP:</b> 104.18.22.19 <b>所属国家:</b> United States of America <b>地区:</b> California <b>城市:</b> San Francisco <b>纬度:</b> 37.775700 <b>经度:</b> -122.395203
cdn.shopify.com	<b>IP:</b> 23.227.60.200 <b>所属国家:</b> Canada <b>地区:</b> Ontario <b>城市:</b> Ottawa <b>纬度:</b> 45.418877 <b>经度:</b> -75.696510
bense.tv	<b>IP:</b> 175.29.155.193 <b>所属国家:</b> Hong Kong <b>地区:</b> Hong Kong <b>城市:</b> Hong Kong <b>纬度:</b> 22.285521 <b>经度:</b> 114.157692
blog.myvideo.net.tw	<b>IP:</b> 31.13.70.9 <b>所属国家:</b> United States of America <b>地区:</b> California <b>城市:</b> Los Angeles <b>纬度:</b> 34.052231 <b>经度:</b> -118.243683

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html	org/codehaus/plexus/util/xml/pull/MXParser.java
http://xmlpull.org/v1/doc/properties.html	org/codehaus/plexus/util/xml/pull/MXParser.java
http://www.w3.org/2000/xmlns/	org/codehaus/plexus/util/xml/pull/MXParser.java
http://www.w3.org/XML/1998/namespace	org/codehaus/plexus/util/xml/pull/MXParser.java
http://xmlpull.org/v1/doc/properties.html	org/codehaus/plexus/util/xml/pull/MXSerializer.java
http://www.w3.org/2000/xmlns/	org/codehaus/plexus/util/xml/pull/MXSerializer.java
http://www.w3.org/XML/1998/namespace	org/codehaus/plexus/util/xml/pull/MXSerializer.java
http://xmlpull.org/v1/doc/features.html	org/codehaus/plexus/util/xml/pull/MXSerializer.java
http://xmlpull.org/v1/doc/features.html	org/codehaus/plexus/util/xml/pull/XMLPullParser.java
https://app.nova-traffic-1688.com	com/paulkman/nova/BuildConfig.java
https://app.nova-traffic-1688.com	com/paulkman/nova/NovaOSSProtectionHeaderInterceptor.java
https://app.nova-traffic-1688.com	com/paulkman/nova/data/CDNRepositoryImpl.java
https://app.nova-traffic-1688.com	com/paulkman/nova/player/HttpVideoDataSource\$ossProtectionHeader\$2.java
https://www.google.com	com/paulkman/nova/feature/develop/ui/ComposableSingletons\$TestAppUpdateScreenKt\$lambda3\$1.java
https://app.nova-traffic-1688.com	com/paulkman/nova/feature/develop/ui/AdvertisementBenchmarkViewModel\$startTest\$1.java
https://app.nova-traffic-1688.com	com/paulkman/nova/feature/comic/data/ComicRepositoryImpl.java
https://cdnec.sanmin.com.tw/product_images/626/626340434.jpg	com/paulkman/nova/feature/comic/ui/component/ComicDetail.java
https://cdn.shopify.com/s/files/1/0613/7030/2681/files/office_1800x1000_1b8864f9-845d-4173-bcba-24db1eb15f34_1800x1000_crop_center.jpg?v=1675905269	com/paulkman/nova/feature/comic/ui/component/ComicDetail.java

https://swebtoon-phinf.pstatic.net/20220527_228/1653654172831ifO8w_JPEG/thumbnail.jpg	com/paulkman/nova/feature/comic/ui/component/ComicDetail.java
https://cdn.readmoo.com/cover/po/vmzfujk_210x315.jpg?v=1653898485	com/paulkman/nova/feature/comic/ui/component/ComicDetail.java
https://blog.myvideo.net.tw/assets/2022/12-15/blog9988532510.png	com/paulkman/nova/feature/comic/ui/component/ComicDetail.java
https://app.nova-traffic-1688.com	com/paulkman/nova/core/common/OSSProtectionKt.java
https://www.google.com	com/paulkman/nova/core/ui/component/Dialog_AppUpdateKt.java
https://www.google.com	com/paulkman/nova/ui/components/ComposableSingletons\$DialogKt\$lambda2\$1.java
https://saohu.live	com/paulkman/nova/ui/components/ShowIdCardDialogKt.java
https://saohu.live	com/paulkman/nova/ui/components/ShowIdCardDialogKt\$DialogContent\$1\$1\$3.java
https://bense.tv	Mogua Engine V1

## 邮箱线索

## 手机线索

手机号	所在文件
15778800000	org/joda/time/chrono/BasicFixedMonthChronology.java
15778800000	org/joda/time/chrono/JulianChronology.java
15778476000	org/joda/time/chrono/GregorianChronology.java
15308640144	org/joda/time/chrono/IslamicChronology.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=US, O=Sun, OU=JavaSoft, CN=Mark Jones

签名算法: rsassa\_pkcs1v15

有效期自: 2023-04-16 09:30:19+00:00

有效期至: 2078-01-17 09:30:19+00:00

发行人: C=US, O=Sun, OU=JavaSoft, CN=Mark Jones

序列号: 0x2257a268

哈希算法: sha256

md5值: 1ca5471f3f9977b86a3c96b07c73106a

sha1值: 139a8c54f7033ba185a49ffbd7fb34c527d3a356

sha256值: 1d517270fe4da739273d6edb961e7b71805f6ae743b16038e578d190d36a936e

sha512值: cc6d170b329254ee6c93239550398f3e788df0966354c0731da509b5377e782bff004f87bb304a82163730bdee16b408ef4c19c9380210da3861cd4d7de2130a

公钥算法: rsa

密钥长度: 2048

指纹: 066c03c4c20ed42e9616568d8dfb4bbca2843f21b6d5a2990273f88a2ceb1ea7

# 🔑 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
登录摸瓜网站后查看	

## 第三方插件

名称	分类	URL链接
登录摸瓜网站后查看		

## 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
		...	

ixmcb.fbwod.iezq.cef.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

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。