



MoGua

黄瓜视频 8.62.APK 分析报告



APP名称:

黄瓜视频

包名:	ufdca.piwt.pfxpxa.oiee
域名线索:	12条
URL线索:	40条
邮箱线索:	2条
分析日期:	2025年6月14日
分析平台:	摸瓜APK反编译平台

文件名: xlav_app_20250611_fpfs.apk
文件大小: 20.54MB
MD5值: 7320bfa22cecab3f9c95081c10d293eb
SHA1值: beaf3a3a67f6bd10c7e5b093a673daf8a7304182
SHA256值: f3eb818aa0cf14f87f55c12789c100faf8ced380fe43b057985da3fb2613dce7

i APP 信息

App名称: 黄瓜视频
包名: ufdca.piwt.pfxpxa.oiee
主活动Activity: com.paulkman.nova.MainActivity
安卓版本名称: 8.62
安卓版本: 1

🔍 域名线索

域名	服务器信息
developer.android.com	IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
app.nova-traffic-1688.com	IP: 127.0.0.1 所属国家: - 地区: -

	城市: - 纬度: 0.000000 经度: 0.000000
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
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
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
bense.tv	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
api.ipify.org	IP: 104.26.12.205 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
issuetracker.google.com	IP: 142.250.217.78 所属国家: United States of America 地区: California

	城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
www.slf4j.org	IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790

 URL线索

URL信息	Url所在文件
https://github.com/google/gson/blob/main/Troubleshooting.md	a7/a.java
https://app.nova-traffic-1688.com	b9/q.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/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/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/pattern/parser/Parser.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
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	d4/h0.java
http://ns.adobe.com/xap/1.0/\u0000	h1/g.java
https://issuetracker.google.com/issues/new?component=413106	o1/b2.java
https://developer.android.com/training/articles/direct-boot	o2/b.java
https://exoplayer.dev/issues/cleartext-not-permitted	p5/a0.java
https://app.nova-traffic-1688.com	t8/h0.java
https://app.nova-traffic-1688.com	t8/m2.java
https://api.ipify.org	t8/c1.java
https://app.nova-traffic-1688.com	n2/f.java
https://www.slf4j.org/codes.html	qi/e.java
https://app.nova-traffic-1688.com	ha/h.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	ra/v2.java
https://app.nova-traffic-1688.com	gd/d.java
https://github.com/google/gson/blob/main/Troubleshooting.md	y6/c.java
https://bense.tv	摸瓜V1引擎
http://%s	lib/arm64-v8a/libcf-msc.so

http://%s	lib/armeabi-v7a/libcf-misc.so
-----------	-------------------------------

邮箱线索

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

手机线索

手机号	所在文件
15778476000	nh/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: 2025-06-10 23:44:44+00:00
有效期至: 2080-03-13 23:44:44+00:00
发行人: C=US, O=Sun, OU=JavaSoft, CN=Mark Jones
序列号: 0xd92b455a78e80fbe
哈希算法: sha256

md5值: 221cc456305279f4ef261767006bcb95
sha1值: fe0539944e65ada98510d0de9344727ba38d41c4
sha256值: 4202fa5224cb002fc915bb5ec7e3a995be913dac1b056ce0afd15eb856069dab
sha512值: d8667ba43c56a560da869c6ae4caaf591f6aa9448f4c97046315824a13bf9658517a43f14b028ddc79a3e5a6a810af8d0d5e7592c7b759e16afa2a51edb9b3e4
公钥算法: rsa
密钥长度: 2048
指纹: 328475a3562791ef2feee2213cc0b14f94847bcdbf9a4357b29f37f6a8ebee1d

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。
xjc.cmta.rpny.clojg.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

