



MoGua

69视频 8.55.APK 分析报告



APP名称:

69视频

包名:	tnh.sfayfm.nsntpe.sjgt
域名线索:	14条
URL线索:	46条
邮箱线索:	2条
分析日期:	2025年9月29日
分析平台:	摸瓜APK反编译平台

文件名: 69视频.apk
文件大小: 19.81MB
MD5值: e3ac361f98cfbf469d45eb23d87cd132
SHA1值: 933c08389ec3a8d2cf177934de7233f4c7779e85
SHA256值: 79389a16c592156d3d3393dad6c0ba8f45d9e1c1340ebfa33207ab6b49627759

i APP 信息

App名称: 69视频
包名: tnh.sfayfm.nsntpe.sjgt
主活动Activity: com.paulkman.nova.MainActivity
安卓版本名称: 8.55
安卓版本: 1

🔍 域名线索

域名	服务器信息
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
issuetracker.google.com	IP: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660 经度: -79.382927
app.nova-traffic-1688.com	没有服务器地理信息.
	IP: 104.239.240.11

xml.org	所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
ns.adobe.com	没有服务器地理信息.
logback.qps.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
www.slf4j.org	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
bense.tv	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
api.ipify.org	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

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
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
69tv.tw	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
exoplayer.dev	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724

 URL线索

URL信息	Url所在文件
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	a4/e1.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/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/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

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://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	com/cloudwise/agent/app/constant/SDKConst.java
http://portal.toushibao.com	com/cloudwise/agent/app/constant/SDKConst.java
https://69tv.tw	c9/a2.java
https://www.slf4j.org/codes.html	di/f.java
https://exoplayer.dev/issues/cleartext-not-permitted	i5/w.java
https://issuetracker.google.com/issues/new?component=413106	i1/u1.java
https://issuetracker.google.com/issues/new?component=413106	i1/u0.java
https://issuetracker.google.com/issues/new?component=413106	i1/q1.java

https://api.ipify.org	n8/e0.java
https://app.nova-traffic-1688.com	n8/b1.java
https://app.nova-traffic-1688.com	n8/n.java
https://app.nova-traffic-1688.com	s8/m.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	w0/s.java
https://app.nova-traffic-1688.com	y9/d.java
https://app.nova-traffic-1688.com	da/e.java
http://ns.adobe.com/xap/1.0/\u0000	d1/a.java
https://app.nova-traffic-1688.com	mb/b.java
https://app.nova-traffic-1688.com	oa/c.java
https://69tv.tw	zc/g.java
https://apm-int.cloudwise.com	v7/a.java
https://app.nova-traffic-1688.com	xc/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	zg/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: 2024-10-24 06:35:42+00:00
有效期至: 2079-07-28 06:35:42+00:00
发行人: C=US, O=Sun, OU=JavaSoft, CN=Mark Jones
序列号: 0xa6d117174409b04f
哈希算法: sha256
md5值: 3a3e590b5c0779be5b88d32acc64ed3c
sha1值: 35a96042a10d1662ecc91fd504a5f1085b56962e
sha256值: 2b351df7433daffbf799d4acfd769ba294173ae3470606294872120f89534e81
sha512值: 4dfef7b7e9d56eff6698186ee98a4bc6e1a2e1d7a39bb4e4a2ccdaa4e7c92cc7312e1697eb875e2329135f93bd6ab6b6ff5ff51dfc5d90b3899e98831c08cf0d
公钥算法: rsa
密钥长度: 2048
指纹: 14ace8d699fb1a264739335c205f599d948bbe0303af00e684d5f680938d2007

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。

svez.wdq.xff.xmsoc.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