



MoGua

撸撸社 8.4.82b9593a.APK 分析报告



APP名称:

撸撸社

包名:	vyyk.mxg.gpis.anxl
域名线索:	5条
URL线索:	7条
邮箱线索:	0条
分析日期:	2025年9月28日
分析平台:	摸瓜APK反编译平台

文件名: lls_app_20230620_6vrz.apk
文件大小: 19.58MB
MD5值: cf7eeeba539860d4c0adb28fbbebbf238
SHA1值: 1c4d2326aa5058d859ff7afff0870a9a501cbc05
SHA256值: ffb62675273db2ab735f12af1a786f26c38cdda0419df182e3ec8ab2ed3a1fc6

i APP 信息

App名称: 撸撸社
包名: vvyk.mxg.gpis.anxl
主活动Activity: com.paulkman.nova.MainActivity
安卓版本名称: 8.4.82b9593a
安卓版本: 1

🔍 域名线索

域名	服务器信息
www.google.com	IP: 199.59.148.96 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
app.nova-traffic-1688.com	没有服务器地理信息.
xmlpull.org	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724

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

 URL线索

URL信息	Url所在文件
https://www.google.com	com/paulkman/nova/core/ui/component/Dialog_AppUpdateKt.java
https://app.nova-traffic-1688.com	com/paulkman/nova/core/common/OSSProtectionKt.java
http://xmlpull.org/v1/doc/features.html	org/codehaus/plexus/util/xml/pull/XmlPullParser.java
http://xmlpull.org/v1/doc/properties.html	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/MXParser.java
http://xmlpull.org/v1/doc/properties.html	org/codehaus/plexus/util/xml/pull/MXParser.java
https://bense.tv	摸瓜V1引擎

 邮箱线索

☰ 手机线索

手机号	所在文件
15222222222	com/paulkman/nova/feature/game/ui/component/MarqueeTextKt.java
15778800000	org/joda/time/chrono/BasicFixedMonthChronology.java
15778476000	org/joda/time/chrono/GregorianChronology.java
15778800000	org/joda/time/chrono/JulianChronology.java
15308640144	org/joda/time/chrono/IslamicChronology.java
17179869184	org/tukaani/xz/common/Util.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: 2023-06-20 01:07:46+00:00
有效期至: 2078-03-23 01:07:46+00:00
发行人: C=US, O=Sun, OU=JavaSoft, CN=Mark Jones
序列号: 0x1dc124d7bed70dde
哈希算法: sha256
md5值: 62b2768a8f3565a4608fe6f2db2a9996
sha1值: 30baef026d137e1f8e1910252db3d74de52c6b7d
sha256值: 73f93ef36e99d3405a5510e146ef26f43d3fbeat1d4d4878886fb9c822192e155
sha512值: 7fa2c574d1f1830337f75d845c790fd84d20c0f1aa353d1ccb7a4557a283b5900c67534821c6eccc9d003e92c5bde5254dc8435cad992cb0f431ec05edf67be2

公钥算法: rsa
密钥长度: 2048
指纹: 08879d023e9918ef7c039d06da18557e23297e6ae8aac9b1327cf649704808af

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
vyyk.mxg.gpis.anxl.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown	Unknown permission from android reference

		permission	
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