MoGua

同城美女交友 1.0.APK 分析报告

APP名称: 同城美女交友

包名:	yct.GTCMNJY
域名线索:	4条
URL线索:	3条
邮箱线索:	0条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: qqqq.apk

文件大小: 1.92MB
MD5值: ccae58c562bcb1cb0cc7aa18c39a7e2d
SHA1值: 5cd3dcab55c1171c078290333521963dcbcc3f61
SHA256值: c53d0f7635098ca641eabc68f854e6ad647fb2edc34697c419a8e21e9c38d888

APP 信息

App名称: 同城美女交友
包名: yct.GTCMNJY
主活动Activity: yct.GTCMNJY.MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
sdk.wiipay.cn	没有服务器地理信息.
192.168.1.102	**IP**: 192.168.1.102 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
app.wiipay.cn	没有服务器地理信息.
192.168.1.128	**IP**: 192.168.1.128 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

URL线索

URL信息	Url所在文件
http://192.168.1.102:80/blaze_op/	com/op/opmanifest/OPClientManifest.java
http://192.168.1.128:8080/blaze_op/bindemail	com/op/opaccount/OPAccountBindEmail.java
http://app.wiipay.cn/common/verfiy.do	com/bx/pay/apkupdate/Env.java
http://sdk.wiipay.cn/common/verfiyPaySdk.do	com/bx/pay/apkupdate/Env.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2013-03-14 02:22:48+00:00
有效期至: 2134-02-13 02:22:48+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x4f9eed81

哈希算法: sha256
md5值: 98770ac7f8e06541b9a969822f9d96aa
sha1值: ea4a1759f70c879a6c6ca5f234e9175f70aebf2a
sha256值: 6665f7025a0e4bc005e0c8166dc311a48df6ec7f02779a63924c73d63492c7c5
sha512值: 55f139e383bbcf0e8f21bbb1f4fbe305212c0b743020b4e27dc5848948ba4c0f97f13a8dcc097ea580a0b57a39487aad514f7814a5c400448b8e3244bd27bdd6

硬编码敏感信息

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.WRITE_APN_SETTINGS	危险	写入访问点名称设置	允许应用程序修改 APN 设置,例如任何 APN 的代理和端口
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
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_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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。
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。

android.permission.MODIFY_PHONE_STATE	系统需要	修改电话状态	允许应用程序控制设备的电话功能。具有此权限的应用程序可以切换网络,打开和关闭电话收音机等,而无需通知您
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.READ_OWNER_DATA	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_OWNER_DATA	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量

应用内通信