MoGua

吉林农信 3.1.2.APK 分析报告

APP名称: 吉林农信

包名:	cn.com.nxy.mbank.jilin
域名线索:	29条
URL线索:	2条
邮箱线索:	1条
分析日期:	2025年6月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: nxy_2400android_312.apk
文件大小: 142.29MB
MD5值: 0d13159785755db62591d2e95f6fcec6
SHA1值: cfecb848c961da12d42dfeda2a701730359d0f8b
SHA256值: 59e6f18bd66daa19bbb27d67795d1389d280d14eba3c29929a053f4804ee559b

APP 信息

App名称: 吉林农信
包名: cn.com.nxy.mbank.jilin
主活动Activity: com.yitong.mbank.app.android.activity.SplashActivity
安卓版本名称: 3.1.2
安卓版本: 12

域名线索

域名	服务器信息
h5testing.gx966888.com	**IP**: 221.7.250.229 **所属国家**: China **地区**: Guangxi Zhuangzu **城市**: Nanning **纬度**: 22.816669 **经度**: 108.316673
ybj-ydzfzx.chutianyun.gov.cn	**IP**: 58.48.40.69 **所属国家**: China **地区**: Hubei **城市**: Wuhan **纬度**: 30.583330 **经度**: 114.266853
www.hbjrxx.com	没有服务器地理信息.
	IP: 180.188.26.28

www.mob.com	**所属国家**: China **地区**: Zhejiang **城市**: Taizhou **纬度**: 28.666668 **经度**: 121.349998
play.google.com	**IP**: 93.46.8.90 **所属国家**: Italy **地区**: Lombardia **城市**: Milan **纬度**: 45.464336 **经度**: 9.188547
channel.nhsa.gov.cn	**IP**: 106.39.128.56 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.ietf.org	**IP**: 104.16.45.99 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
36.110.44.29	**IP**: 36.110.44.29 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
58.48.40.69	**IP**: 58.48.40.69 **所属国家**: China **地区**: Hubei **城市**: Wuhan **纬度**: 30.583330 **经度**: 114.266853

ebank2.nongxinyin.com	没有服务器地理信息.
h5.gx966888.com	**IP**: 223.72.156.239 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
web.yiqianlian.com	**IP**: 47.98.67.200 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
orgineyun.1451cn.com	**IP**: 120.79.98.111 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
code.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
mp1.web.liantiao.ofcard.com	**IP**: 49.4.15.134 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 221.7.250.241

zxkf.gx966888.com	**所属国家**: China **地区**: Guangxi Zhuangzu **城市**: Nanning **纬度**: 22.816669 **经度**: 108.316673
android.googlesource.com	**IP**: 74.125.20.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
weixin2.nxyqs.net	**IP**: 223.71.154.161 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ebank.jlnls.com	**IP**: 219.143.226.129 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ebank1.nongxinyin.com	没有服务器地理信息.
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
fuwu-test.nhsa.gov.cn	没有服务器地理信息.
	IP: 60.28.219.32

a.app.qq.com	**所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
libusb.info	**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
124.127.94.236	**IP**: 124.127.94.236 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
weixin.nxyqs.net	**IP**: 111.205.35.129 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.gnu.org	**IP**: 209.51.188.116 **所属国家**: United States of America **地区**: Massachusetts **城市**: Somerville **纬度**: 42.387600

	经度: -71.099503
www.rsasecurity.com	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**
http://124.127.94.236:9081/mshield-inf/	摸瓜V1引擎
https://ybj-ydzfzx.chutianyun.gov.cn:8082/localcfc/	摸瓜V1引擎
http://58.48.40.69:10080/localcfc/	摸瓜V1引擎
https://channel.nhsa.gov.cn/ebus/channel/api/cfc/	摸瓜V1引擎
https://fuwu-test.nhsa.gov.cn/ebus/ggfw_ylz/yc/api/cfc/	摸瓜V1引擎
http://www.hbjrxx.com/JRWG/download/Jrwgh_Android.htm	摸瓜V1引擎
https://web.yiqianlian.com/ats/mobile?menu=gascardrecharge&categoryStyle=1	摸瓜V1引擎
http://mp1.web.liantiao.ofcard.com/ats/mobile?menu=gascardrecharge&categoryStyle=1	摸瓜V1引擎
https://zxkf.gx966888.com:9888/IMClient/appagent.html	摸瓜V1引擎
http://36.110.44.29:8081/IMClient/appagent.html	摸瓜V1引擎
https://h5.gx966888.com:9480/xyd/page/index.html?version=3.0	摸瓜V1引擎
http://h5testing.gx966888.com:9480/xyd/page/index.html?version=3.0	摸瓜V1引擎

https://play.google.com/store/apps/details?id=me.pengpeng.ppme>	摸瓜V1引擎
http://www.gnu.org/licenses/>www.gnu.org/licenses	摸瓜V1引擎
http://code.google.com/p/nfcard/>code.google.com/p/nfcard	摸瓜V1引擎
https://web.yiqianlian.com/ats/mobile?menu=foodrecharge&categoryStyle=1	摸瓜V1引擎
http://mp1.web.liantiao.ofcard.com/ats/mobile?menu=foodrecharge&categoryStyle=1	摸瓜V1引擎
http://a.app.qq.com/o/simple.jsp?pkgname=com.pactera.hbnx.zsnx	摸瓜V1引擎
https://h5.gx966888.com:9480/htmlShop/page/index.html	摸瓜V1引擎
http://h5testing.gx966888.com:9480/htmlShop/page/index.html	摸瓜V1引擎
https://weixin.nxyqs.net/jmlive/nxy/mobile/entrance.do	摸瓜V1引擎
http://ebank1.nongxinyin.com/jmlive/nxy/mobile/entrance.do	摸瓜V1引擎
https://weixin2.nxyqs.net/jwbank/joinup/appointment.do?	摸瓜V1引擎
http://ebank2.nongxinyin.com/jwbank/joinup/appointment.do?	摸瓜V1引擎
https://ebank.jlnls.com:8803/mshield-inf/	摸瓜V1引擎
http://www.mob.com	摸瓜V1引擎
https://web.yiqianlian.com/ats/mobile?menu=viprecharge&categoryStyle=1	摸瓜V1引擎
http://mp1.web.liantiao.ofcard.com/ats/mobile?menu=viprecharge&categoryStyle=1	摸瓜V1引擎
https://orgineyun.1451cn.com/regionmicro/thirdvisitorlogin.html?value=20181029204120@20180522151217558	摸瓜V1引擎
play.googleapis.com	摸瓜V3引擎

play.googleapis.com	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
http://www.openssl.org/support/faq.html	摸瓜V3引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V3引擎
http://libusb.info	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
http://www.ietf.org/rfc/rfc2440.html	摸瓜V3引擎
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-5/index.html	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎

邮箱线索

邮箱地址	所在文件
sinpowei@gmail.com	摸瓜V1引擎

手机线索

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=CN, ST=北京, L=北京, O=农信银, OU=农信银清算中心, CN=吉林省农信手机银行客户端
签名算法: rsassa_pkcs1v15
有效期自: 2015-08-24 06:40:25+00:00
有效期至: 2115-07-31 06:40:25+00:00
发行人: C=CN, ST=北京, L=北京, O=农信银, OU=农信银清算中心, CN=吉林省农信手机银行客户端
序列号: 0x7609a7ed
哈希算法: sha256
md5值: 695a2406d7254ccd8eded66f6060636c
sha1值: 33cad4b86db956a6dfbb80c6ccfee37150fdbc71
sha256值: 4e389fc6ef13c54d4d3d074174fae4f95a2355a5a053d6b37411ad949df25eb7
sha512值: 5739972a86d9ac51f66868c4e607fae27cf23049e2ded57461e5f15fa9e5f7ea4c11ef7616d4fbb619151f4fdfd5e403ddc34cc8b8e723b28909ff394aa815e2
公钥算法: rsa
密钥长度: 2048
指纹: 7e92f5012654a59c7ac01b7b4512c319977434a9e8de659e04357b31be2b7752

🔑 硬编码敏感信息

可能的敏感信息
"dialog_tp_get_pubkey" : "正在获取加密密钥，请稍候..."
"face_appkey" : "MDM1MzEwbm9kZXZpY2Vjd2F1dGhvcml6ZZfn5OXl5+Tq3+bg5efm5ef65OXl4Obg5Yjm5uvl5ubrkeXm5uvl5uai6+Xm5uvl5qTm6+Xm5ufk++bn5uQ="
"login_input_vdunpwd_tip" : "请输入V盾密码"
"ocr_appkey" : "5CAD6F8533A74153UY91h9t7"
"sqsdk_code_on_pay_forget_pwd" : "忘记密码？"
"sqsdk_code_on_pay_input_pwd" : "请输入支付密码"

"sqsdk_code_on_pay_varify_pay_pwd" : "请输入6-20位支付密码"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"str_gesture_pwd_least" : "密码最少要4位"

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.KILL_BACKGROUND_PROCESSES	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.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.MOUNT_FORMAT_FILESYSTEMS	危险	格式化外部存储器	允许应用程序格式化可移动存储
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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_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.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.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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
		Unknown	

android.permission.INTERACT_ACROSS_USERS_FULL	未知	permission	Unknown permission from android reference
android.permission.BAIDU_LOCATION_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.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.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.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.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
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
org.simalliance.openmobileapi.BIND_TERMINAL	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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.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
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.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.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
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.USE_FINGERPRINT	正常	allow use of 指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
		Unknown	

android.hardware.camera.autofocus	未知	permission	Unknown permission from android reference
android.permission.ACCESS_ASSISTED_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_LOCATION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
android.permission.PREVENT_POWER_KEY	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.yitong.mbank.app.android.activity.SplashActivity	Schemes: nxynewbankofjilin://, Hosts: my.app,

	Ports: 8888,
com.yitong.mbank.app.android.activity.SchmeActivty	Schemes: nxymobilejl://, Hosts: bank,
com.yitong.mbank.app.android.activity.OCBWebViewActivity	Schemes: newbindcardjl://, Hosts: my.app, Ports: 8888,

---