MoGua

牛牛分期 4.1.1.APK 分析报告

APP名称: 牛牛分期

包名:	com.rwvvgt.watilykd
域名线索:	17条
URL线索:	11条
邮箱线索:	0条
分析日期:	2025年8月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: fnnfq.apk
文件大小: 20.56MB
MD5值: d789f66cbc5790770995885d78280a08
SHA1值: 51bf75798e5f7812dbfcf28d45cfb68bbde8a614
SHA256值: 25b2a34c37e0b9f8d13dc6ec7bf5227b7483e5ec06a93f6e59187fe3b80fa45a

APP 信息

App名称: 牛牛分期
包名: com.rwvvgt.watilykd
主活动Activity: com.nnfq.ui.activitys.JDXF0ACT
安卓版本名称: 4.1.1
安卓版本: 52

域名线索

域名	服务器信息
www.beizhuabao.com	没有服务器地理信息.
h5.dafsdfdfuy.cn	没有服务器地理信息.
render.alipay.com	**IP**: 101.72.221.202 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
tianshu.alicdn.com	**IP**: 1.25.68.237 **所属国家**: China **地区**: Nei Mongol **城市**: Baotou **纬度**: 40.651909 **经度**: 109.822922

nice800.com	**IP**: 43.132.110.135 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
zxcvnlasdf-1326599440.cos.ap-guangzhou.myqcloud.com	**IP**: 36.248.13.150 **所属国家**: China **地区**: Fujian **城市**: Fuzhou **纬度**: 26.061390 **经度**: 119.306107
pop.yuncloudauth.com	**IP**: 59.82.44.22 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
mgw.mpaas.cn-hangzhou.aliyuncs.com	**IP**: 47.118.173.165 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
cloudauth-dualstack.aliyuncs.com	**IP**: 106.11.172.8 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com	**IP**: 3.5.236.180 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong

	纬度: 22.285521 **经度**: 114.157692
cloudauth.cn-beijing.aliyuncs.com	**IP**: 39.97.154.134 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
cloudauth-dualstack.cn-beijing.aliyuncs.com	**IP**: 39.97.154.8 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
cloudauth.aliyuncs.com	**IP**: 59.82.44.22 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
auth.yunverify.com	**IP**: 106.11.232.51 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com	**IP**: 36.248.13.149 **所属国家**: China **地区**: Fujian **城市**: Fuzhou **纬度**: 26.061390 **经度**: 119.306107
	IP: 139.227.226.244

cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com	**所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
android-donwload.oss-cn-hangzhou.aliyuncs.com	**IP**: 101.67.62.58 **所属国家**: China **地区**: Zhejiang **城市**: Huzhou **纬度**: 30.870550 **经度**: 120.093300

URL线索

URL**信息**	Url**所在文件**
https://mgw.mpaas.cn-hangzhou.aliyuncs.com	com/alipay/alipaysecuritysdk/common/config/Configuration.java
https://render.alipay.com/p/f/fd-j8l9yjja/index.html	com/dtf/face/config/NavigatePage.java
https://tianshu.alicdn.com/7504f3f0-aca8-4636-b486-e396559d3efb.png	com/dtf/face/utils/ModelDownloadUtil.java
https://cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com/model/toyger.face.dat	com/dtf/face/utils/ModelDownloadUtil.java
https://cloudauth-dualstack.aliyuncs.com	com/dtf/face/api/DTFacadeExt.java
https://cloudauth.aliyuncs.com	com/dtf/face/api/DTFacadeExt.java
https://cloudauth-dualstack.cn-beijing.aliyuncs.com	com/dtf/face/api/DTFacadeExt.java
https://cloudauth.cn-beijing.aliyuncs.com	com/dtf/face/api/DTFacadeExt.java
https://auth.yunverify.com	com/dtf/face/api/DTFacadeExt.java

https://pop.yuncloudauth.com	com/dtf/face/api/DTFacadeExt.java
https://nice800.com	com/nnfq/ui/activitys/MT7ACT.java
https://nice800.com/	com/nnfq/ui/activitys/MT10ACT.java
https://zxcvnlasdf-1326599440.cos.ap-guangzhou.myqcloud.com	com/nnfq/mjyp/BuildConfig.java
https://ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com	com/nnfq/mjyp/BuildConfig.java
https://jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com	com/nnfq/mjyp/BuildConfig.java
http://h5.dafsdfdfuy.cn:9005/	com/nnfq/mjyp/BuildConfig.java
https://android-donwload.oss-cn-hangzhou.aliyuncs.com/domai0dsfnName/5100sdfh0635.text/	com/nnfq/mjyp/BuildConfig.java
http://www.beizhuabao.com	com/nnfq/mjyp/app/api/Api2.java
http://www.beizhuabao.com	com/nnfq/mjyp/app/api/Api.java
https://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html	摸瓜V1引擎

邮箱线索

手机线索

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=YnfLREmw, ST=hrsuQZyj, L=LTreYRMU, O=HctBJZos, OU=okPlDqmN, CN=UmaEFfvf
签名算法: rsassa_pkcs1v15
有效期自: 2024-11-28 13:28:01+00:00
有效期至: 2034-11-26 13:28:01+00:00
发行人: C=YnfLREmw, ST=hrsuQZyj, L=LTreYRMU, O=HctBJZos, OU=okPlDqmN, CN=UmaEFfvf
序列号: 0x8f1e54e9c6743bbb
哈希算法: sha256
md5值: bd1dbc3360db99b5399f28180ad2fb56
sha1值: ed675094e1094ba96eb97b37638d54827f9c81f9
sha256值: a72e141384d2bc7135686e5254cfeafb4bb1b64afa85b64b6c0aa757d8c4d6fb
sha512值: c663dd5fcbba134f846a1064b2aab0cc9817076a2d87dafe28025b24a7383ee264ebf0f329abd985582823b13372377b4fdfb6cac29e556d417629a4957b5c6f
公钥算法: rsa
密钥长度: 2048
指纹: 861cba4f72e8e37a7a3711514329b88ef1ecc27cb747a6ffb30c8e095b5dc9cb

🔑 硬编码敏感信息

可能的敏感信息
"agreee_user" : "请先同意并勾选用户协议"
"check_gesture_pwd" : "验证手势密码"
"check_login_pwd" : "验证登录密码"
"dear_user" : "尊敬的用户:"
"find_pwd" : "找回密码"
"gesture_pwd" : "手势密码"
"has_authd" : "已授权"

"info_auth_fee" : "信息认证费： "
"info_auth_fee2" : "信息认证费"
"input_orgin_pwd" : "请输入原密码"
"input_pwd" : "请输入验证码"
"input_pwd_number" : "请输入新密码(6-16位数字字母组合)"
"modify_pwd" : "修改密码"
"ple_agree_auth_agreement" : "请先同意授权及借款协议"
"ple_input_service_pwd" : "请输入服务密码"
"real_auth" : "实名认证"
"reset_service_pwd" : "重置服务密码"
"service_pwd" : "服务密码:"
"to_authorize" : "去授权"
"user" : "用户"

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.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.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.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_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.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.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.WRITE_CALL_LOG	危险		允许应用程序写入（但不读取）用户号召日志数据。
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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。
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference

应用内通信