MoGua

快易贷 null.APK 分析报告

APP名称:	快易贷

包名:	lSJhejqkrnJdkwbx.vzdJsnd.ngirjsHsjqk
域名线索:	17条
URL线索:	10条
邮箱线索:	0条
分析日期:	2025年8月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: kyd.apk
文件大小: 35.47MB
MD5值: 6d93305434111cdca3b99a23ba54ab1c

SHA1值: 0bf0d251f3c83bd7b1b782111710ed6050e2530e
SHA256值: 18b5dc9a05bd3499e9cc09577862063e99f013c839294703d80e6696500b621a

APP 信息

App名称: 快易贷
包名: ISJhejqkrnJdkwbx.vzdJsnd.ngirjsHsjqk
主活动Activity: com.xuegao.yhearth.ui.MainActivity
安卓版本名称: null
安卓版本:

域名线索

域名	服务器信息
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
xml.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
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.cn-beijing.aliyuncs.com	IP: 8.141.244.36 **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
android.bugly.qq.com	IP: 124.95.225.169 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
tianshu.alicdn.com	IP: 122.156.130.223 **所属国家**: China **地区**: Heilongjiang **城市**: Heihe **纬度**: 50.266670 **经度**: 127.466667
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
astat.bugly.qcloud.com	IP: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com	IP: 140.206.110.110 **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: 47.118.168.189 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
18.163.3.115	IP: 18.163.3.115 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
render.alipay.com	IP: 101.73.101.227 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
gw.alipayobjects.com	IP: 116.136.134.115 **所属国家**: China **地区**: Nei Mongol **城市**: Tongliao **纬度**: 43.612499 **经度**: 122.265282
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

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
cloudauth.aliyuncs.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

URL线索

URL**信息**	Url**所在文件**
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.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://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://tianshu.alicdn.com/64ce83c2-97db-4024-9af3-ef6ffee08f52.png	com/dtf/face/utils/ModelDownloadUtil.java
https://gw.alipayobjects.com/render/p/yuyan_npm/@alipay_dtfconfig/1.0.1/lib/toyger.face.android.wasm	com/dtf/face/utils/ModelDownloadUtil.java
https://gw.alipayobjects.com/render/p/yuyan_npm/@alipay_dtfconfig/1.0.2/lib/toyger.quality.android.wasm	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://cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com/model/toyger.quality.2.2.7.android.dat	com/dtf/face/utils/ModelDownloadUtil.java
https://mgw.mpaas.cn-hangzhou.aliyuncs.com	com/alipay/alipaysecuritysdk/common/config/Configuration.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java
http://18.163.3.115/api/	com/xuegao/yhearth/store/ConfigStore.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True

v3 签名: False
找到 1 个唯一证书
主题: C=MX, ST=Xokwsfoklujijv, L=Montpellier, O=Xbcanxvhxdgct, OU=jjjakcvfluz, CN=Xvpjntgjwqp
签名算法: rsassa_pkcs1v15
有效期自: 2025-08-01 11:19:07+00:00
有效期至: 2028-07-31 11:19:07+00:00
发行人: C=MX, ST=Xokwsfoklujijv, L=Montpellier, O=Xbcanxvhxdgct, OU=jjjakcvfluz, CN=Xvpjntgjwqp
序列号: 0x3f4bb4c7
哈希算法: sha1
md5值: 2aae06b6a85a3b30f6e60e0a464baa86
sha1值: 855a0a2f413dc3503455a9b6dd39ea3e59c68deb
sha256值: b2b220c725a21f7db52c2e6f84e7dfbecb77f1edd0d6581154bda96b96a96c92
sha512值: 4f006a5297509815aecf0fe41f512490bd0f43f04935633c69b762d5e660e01a871d1eebb10fb799c28d14aeee405c6bd0b397ca4f8d58dd3221150d0fb437ce
公钥算法: rsa
密钥长度: 1024
指纹: 1b2f46b5e35724f12bfdf67cd900d4c19b2e58d69875737ebcb8ddeee4c647b8

🔑 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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
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.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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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_CALL_LOG	危险		允许应用程序读取用户的通话日志
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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
	危		允许应用程序用相机拍照和录像。这允许应用程序收集

android.permission.CAMERA	险	拍照和录像	相机随时看到的图像
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.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
ISJhejqkrnJdkwbx.vzdJsnd.ngirjsHsjqk.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信
