MoGua

油联合伙人 1.4.APK 分析报告

APP名称: 油联合伙人

包名:	com.yltx.oil.partner
域名线索:	37条
URL线索:	29条
邮箱线索:	0条
分析日期:	2024年10月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 油联合伙人.apk
文件大小: 10.17MB
MD5值: a3cbbefc9028c21f765264d3aa9e2748
SHA1值: 1a85e1945a8118ae270592cf6610fe10a407c916
SHA256值: dd50b275f972253bb2dc53250ad4153e1feb86d8f85e813b4d84cb6a562e1899

APP 信息

App名称: 油联合伙人
包名: com.yltx.oil.partner
主活动Activity: com.yltx.oil.partner.modules.SplashActivity
安卓版本名称: 1.4
安卓版本: 5

域名线索

域名	服务器信息
ouplog.umeng.com	**IP**: 47.246.110.93 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
log.umsns.com	**IP**: 59.82.29.249 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
open.weixin.qq.com	**IP**: 220.196.139.154 **所属国家**: China **地区**: Jiangsu

	城市: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
image.cnamedomain.com	**IP**: 91.195.240.94 **所属国家**: Germany **地区**: Nordrhein-Westfalen **城市**: Koeln **纬度**: 50.933346 **经度**: 6.949720
mcgw.alipay.com	**IP**: 123.125.216.192 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
long.open.weixin.qq.com	**IP**: 112.65.193.170 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
m.alipay.com	**IP**: 203.209.245.120 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

cmnsguider.yunos.com	**IP**: 203.119.169.158 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
wappaygw.alipay.com	**IP**: 123.125.216.191 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
et2-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	**IP**: 203.119.169.82 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
h5.m.taobao.com	**IP**: 60.28.247.215 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
s.s	没有服务器地理信息.
developer.umeng.com	**IP**: 59.82.31.154 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
weixin.ylsp188.com	没有服务器地理信息.

alogsus.umeng.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
mobilegw.stable.alipay.net	没有服务器地理信息.
yltx-x.oss-cn-hangzhou.aliyuncs.com	**IP**: 101.67.62.115 **所属国家**: China **地区**: Zhejiang **城市**: Huzhou **纬度**: 30.870550 **经度**: 120.093300
ulogs.umeng.com	**IP**: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
chinayltx.com	**IP**: 120.26.114.51 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
oss-cn-.aliyuncs.comor	没有服务器地理信息.
mclient.alipay.com	**IP**: 125.39.135.57 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

114.215.220.245	**IP**: 114.215.220.245 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
wx.chinayltx.com	**IP**: 120.26.114.51 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
mobilegw.alipaydev.com	**IP**: 110.75.132.131 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
oss-cn-hangzhou.aliyuncs.com	**IP**: 118.31.219.189 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
ylsp-x.oss-cn-hangzhou.aliyuncs.com	**IP**: 118.31.219.202 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 59.82.29.163 **所属国家**: China

mobile.umeng.com	**地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
alogus.umeng.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
ulogs.umengcloud.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
mobilegw.aaa.alipay.net	没有服务器地理信息.
mobilegw.alipay.com	**IP**: 203.209.255.238 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
weixin.chinayltx.com	**IP**: 47.96.25.119 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
api.weixin.qq.com	**IP**: 112.65.193.153 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333

	经度: 121.468948
www.umeng.com	**IP**: 59.82.29.162 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
plbslog.umeng.com	**IP**: 36.156.202.68 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600

URL线索

URL信息	Url所在文件
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSClient.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/OSSClient.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java

https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/d.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java

http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://mobile.umeng.com/images/pic/home/social/img-1.png	com/umeng/socialize/net/LinkcardRequest.java
https://log.umsns.com/	com/umeng/socialize/net/base/SocializeRequest.java
https://log.umsns.com/	com/umeng/socialize/common/SocializeConstants.java
https://log.umsns.com/link/qq/download/	com/umeng/socialize/common/SocializeConstants.java
https://log.umsns.com/link/weixin/download/	com/umeng/socialize/common/SocializeConstants.java
http://www.umeng.com/social	com/umeng/socialize/common/SocializeConstants.java
http://log.umsns.com/link/weixin/download/	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/access_token?	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/auth?access_token=	com/umeng/socialize/media/WeixinExtra.java
https://developer.umeng.com/docs/66632/detail/66890	com/umeng/socialize/utils/SLog.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/socialize/utils/UrlUtil.java
https://log.umsns.com/	com/umeng/socialize/view/OauthDialog.java
https://chinayltx.com/app	com/yltx/oil/partner/data/network/Config.java
http://weixin.ylsp188.com/?wechat	com/yltx/oil/partner/data/network/Config.java
http://wx.chinayltx.com/	com/yltx/oil/partner/data/network/Config.java

http://weixin.chinayltx.com/?wechat=	com/yltx/oil/partner/data/network/Config.java
http://yltx-x.oss-cn-hangzhou.aliyuncs.com/	com/yltx/oil/partner/data/network/Config.java
http://114.215.220.245	com/yltx/oil/partner/data/network/Config.java
http://wx.chinayltx.com/	com/yltx/oil/partner/modules/home/activity/ShareDetailsActivity.java
http://weixin.ylsp188.com/?wechat	com/yltx/oil/partner/modules/home/activity/ShareDetailsActivity.java
http://weixin.ylsp188.com/	com/yltx/oil/partner/modules/login/activity/RegisterActivity.java
http://yltx-x.oss-cn-hangzhou.aliyuncs.com/	com/yltx/oil/partner/utils/AlbumDisplayUtils.java
http://ylsp-x.oss-cn-hangzhou.aliyuncs.com/	com/yltx/oil/partner/utils/AlbumDisplayUtils.java
http://%s.%s/%s	com/yltx/oil/partner/oss/OSSFileHelper.java
https://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎
log.umsns.com	摸瓜V3引擎
et2-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	摸瓜V3引擎
chinayltx.com	摸瓜V3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: False
找到 1 个唯一证书
主题: C=025, ST=js, L=nj, O=yltx, OU=zh, CN=ding
签名算法: rsassa_pkcs1v15
有效期自: 2019-05-10 02:52:27+00:00
有效期至: 2059-04-30 02:52:27+00:00
发行人: C=025, ST=js, L=nj, O=yltx, OU=zh, CN=ding
序列号: 0x68392148
哈希算法: sha256
md5值: 3711cd29d4471901ca0a8c227f7f0e13
sha1值: 7b448d72f1e938f0d79b347a8cdead32db15c9a8
sha256值: ba4a433784b07db62f7d732cb3c1502e760eb673cdf26a05e583a8f6ce44c680
sha512值: 0aa2322034f4db057ff3bc297ba569931a989e24acc14a15ef9a0ef4bd72719bf8cfda90d3701d3b0708400c7cbd2d40974dea93693dc41ada42c8773842b596
公钥算法: rsa
密钥长度: 2048
指纹: 7be45d8639f0810ce788263e5bd98ac3a92646c135f553d4b52a5f896b02d462

硬编码敏感信息

可能的敏感信息
"forget_password" : "忘记密码?"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

"pls_enter_again_phone_pwd2" : "请再次输入密码"
"pls_enter_phone_pwd1" : "请输入密码"

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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

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.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.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_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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.alipay.sdk.app.AlipayResultActivity	Schemes: alipaysdk://,

---