MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

新商盟 2.0.3.APK

APP名称:	新商盟
包名:	com.hengtiansoft.xinyunlian
域名线索:	16条
URL线索:	18条
邮箱线索:	1条
分析日期:	2022年1月22日 23:32

文件信息

文件名: xinshangmeng.apk
文件大小: 3.45MB
MD5值: 38d3b27229d1356e61aeede62b4635ed
SHA1值: d67503d2c1d9b30c28ff107dc5d17b56d21a56a3
SHA256值: ccbc240db8f310471386cab84ae2987d0f0575adeb2372960ce2b1461f2c91ff

APP 信息

App名称: 新商盟
包名: com.hengtiansoft.xinyunlian
主活动**Activity:** com.hengtiansoft.xinyunlian.activity.LoadingActivity
安卓版本名称: 2.0.3
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
mta.qq.com	good	**IP:** 125.39.171.64 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map

域名	是否危险域名	服务器信息
www.alipay.com	good	IP: 203.209.250.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
pingma.qq.com	good	IP: 119.45.78.184 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
wappaygw.alipay.com	good	IP: 203.209.250.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
admin.baiwandian.cn	good	IP: 223.4.220.102 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
xmlpull.org	good	IP: 74.50.62.60 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map
mobilegw.alipay.com	good	IP: 203.209.247.65 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
mcgw.alipay.com	good	IP: 203.209.250.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
m.alipay.com	good	IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
mclient.alipay.com	good	IP: 203.209.250.50 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
xyl-qa.hengtiansoft.com	good	没有服务器地理信息.
www.baiwandian.cn	good	IP: 223.4.220.102 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
www.alidao.com	good	IP: 121.40.146.254 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
ditu.google.cn	good	IP: 180.163.151.162 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061 查看地图: Google Map

域名	是否危险域名	服务器信息
mta.oa.com	good	IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://mcgw.alipay.com/gateway.do	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
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/sdkErrorlog.do	com/alipay/sdk/util/d.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/security/mobile/module/a/a/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/face/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/mobilesecuritysdk/face/a.java

URL信息	Url所在文件
http://mta.qq.com/	com/tencent/wxop/stat/e.java
http://mta.oa.com/	com/tencent/wxop/stat/e.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/c.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/XmlUtils.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/FastXmlSerializer.java
http://xyl-qa.hengtiansoft.com/xinyunlian-app-ecom/app/payment/notify/async.jhtml	com/hengtiansoft/xinyunlian/alipay/AliPayUtil.java
https://www.alipay.com/	com/hengtiansoft/xinyunlian/activity/WebPageAipayActivity.java
http://schemas.android.com/apk/res/android	com/hengtiansoft/xinyunlian/widget/AlignTextView.java
http://skip?type=x&param=a,b,c,d	com/hengtiansoft/xinyunlian/utils/StringUtils.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/sign.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/asyncNotifyForAlipayTest.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/searchProductByBarcode.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/cancel.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/cart/cartInfo.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/cart/cart_operate.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java

URL信息	Url所在文件
http://www.baiwandian.cn/xinyunlian-app-ecom/app/register/checkMobile.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/register/checkSecurity.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/login/checkVersion.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/login/createToken.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/dealer/getDealerIndex.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/dealer/getDealerInfo.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/dealer/getDealerProduct.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/discountCoupon/list.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/cart/edit_cart_plus.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/notice/fetchCurrentSeq.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/notice/fetchNoticeByUser.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/notice/fetchCurrentUnRead.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/register/findAreas.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/findPaymentPlugins.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/undertake/getUnderTakeById.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java

URL信息	Url所在文件
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/getNavs.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/getPromotionNavs.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/member/getQrCodeData.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/getHotWords.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/login/userLogin.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/login/checkMobile.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/login/userLoginOut.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/member/loginUpdate.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/notice/markRead.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/member/findAreas.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/dealer/getNavCount.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/notice/fetchNoticeDetail.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/create.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/order_info.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java

URL信息	Url所在文件
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/list.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/orderquery.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/pick_coupon.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/product/searchProductByDealer.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/product/saleInfo.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/member/profile/update.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/member/profile/upload.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/product/getPromotionPage.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/discountCoupon/appReceived.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/register/registAgreement.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/product/searchProduct.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/login/securityLogin.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/paymentPluginSelect.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/register/sendMessage.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/register/submit.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java

URL信息	Url所在文件
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/unifiedorder.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/notice/fechUnreadeNotice.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/member/update.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/register/upload.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/member/userCenter.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/view.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/order/asyncNotifyForWxTest.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://admin.baiwandian.cn/xinyunlian-admin/static/upload/image	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/getIndexAds.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/getIndexNav.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/getIndexProduct.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/getProducts.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://www.baiwandian.cn/xinyunlian-app-ecom/app/index/getPromotionPage.jhtml	com/hengtiansoft/xinyunlian/constant/Urls.java
http://ditu.google.cn/maps?hl=	com/alidao/android/common/utils/IntentUtils.java
www.alidao.com	com/alidao/android/common/entity/AppInfoBean.java

邮箱线索

邮箱地址	所在文件
u0014nz@9.vrr	cn/jpush/android/api/r.java

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.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.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.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_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

向手机申请的权限	是否危险	类型	详细情况
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.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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_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.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

向手机申请的权限	是否危险	类型	详细情况
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_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_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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-06-23 03:33:58+00:00
Valid To: 2045-06-15 03:33:58+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x133c3208
Hash Algorithm: sha256
md5: 8817dc6fc3de1dc191fd471ef2f88dca
sha1: 4d012f5904f9c4ca1a8dd55c3c239a5218c6cfaa
sha256: 061f5c60c702100a07aac29f30c61013c0b5426d89552813fbbbace2073c8942
sha512: 8d3b95c6c01a3bd2cb79a49b67c3e4693dc2a558a7f2fef070aa3a1efafc6e05c1f099d70b2f41ba6d4f542ab5b3cf8a02268948fa4d0a54916af9c824d7ecea

Exodus威胁情报

名称	分类	URL链接
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

加壳分析

文件列表	分析结果

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
SIM operator check
device ID check
subscriber ID check
ro.kernel.qemu check</td></tr>
<tr><td>编译器</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>
