MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

订货小助手 1.1.8.APK

APP名称:	订货小助手
包名:	com.dsx.dinghuobao
域名线索:	7条
URL线索:	22条
邮箱线索:	0条
分析日期:	2022年1月25日 21:41

文件信息

文件名: dhxzs169740.apk
文件大小: 9.05MB
MD5值: 82d07634f8a07883f924b545f84a30c5
SHA1值: cb2d17f3df1d0af4ccbec9f1f0f1168c36e8925a
SHA256值: 5fb3eb4dc878493eef4aad84c186815c55a10bf5d8a6f3966339bec1633e5c58

APP 信息

App名称: 订货小助手
包名: com.dsx.dinghuobao
主活动**Activity:** com.dsx.dinghuobao.activity.SpaleActivity
安卓版本名称: 1.1.8
安卓版本: 18

域名线索

域名	是否危险域名	服务器信息
github.com	good	**IP:** 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 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
long.open.weixin.qq.com	good	**IP:** 109.244.217.35 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
app.suoposhengpin.net	good	**IP:** 121.89.247.3 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
open.weixin.qq.com	good	**IP:** 175.24.219.72 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
app.diansanxia.com	good	**IP:** 39.105.231.123 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
api.weixin.qq.com	good	**IP:** 81.69.216.43 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

URL线索

URL信息	Url所在文件
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://app.diansanxia.com/api/	com/dsx/dinghuobao/http/URLContacts.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=wx6c51c74ed7b19b37&secret=d12ccc16c71b0eeb25484e1b6974f99a&code=	com/dsx/dinghuobao/wxapi/WXEntryActivity.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/dsx/dinghuobao/wxapi/WXEntryActivity.java
https://app.diansanxia.com/dhb_web/login_pro.html	com/dsx/dinghuobao/activity/LoginActivity.java
https://app.diansanxia.com/dhb_web/yinsi.html	com/dsx/dinghuobao/activity/LoginActivity.java
https://app.suoposhengpin.net/sp_mobile/xieyi/login_pro.html	com/dsx/dinghuobao/widget/YSDialog.java

URL信息	Url所在文件
https://app.suoposhengpin.net/sp_mobile/xieyi/yinsi.html	com/dsx/dinghuobao/widget/YSDialog.java
https://app.diansanxia.com/dhb_web/shouhou.html	com/dsx/dinghuobao/fragment/Fragment4.java
http://schemas.android.com/apk/res/android	com/xuexiang/xui/widget/banner/widget/banner/base/BaseBanner.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=wu, ST=wu, L=wu, O=wu, OU=wu, CN=wu
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-07-01 03:19:06+00:00
Valid To: 2046-06-25 03:19:06+00:00
Issuer: C=wu, ST=wu, L=wu, O=wu, OU=wu, CN=wu
Serial Number: 0x400d39e2
Hash Algorithm: sha256
md5: aafb137f891b416010fccb3dae6384ee
sha1: a42347f9cb45d7e984c571dac281c0eb3f879193
sha256: 2a6f27d8f22e5acd3f6b5fa62bc9461391b746b27aff20885d57ec2ed9351250
sha512: 4a85b5a778cfeead274d4485d1511d66622eebda5259886050a219562149f1331289cf7c2a05e07dd7132ba45f0e64bb304697675d8457f18bf12ef83c022d02
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 389811b3567e6ded8fd9a28c1c32fe21d2b5665593fb0af3a8abc91effde954a

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></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.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
