MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

U智荟 1.1.10.APK

APP名称:	U智荟
包名:	com.baoying.android.shopping
域名线索:	19条
URL线索:	29条
邮箱线索:	0条
分析日期:	2022年1月22日 23:30

文件信息

文件名: uzhihui361618.apk
文件大小: 6.93MB
MD5值: b5913ce355eadc664921eacca9b3e952
SHA1值: 7f6caeff9490d5dfb903ece6c4eb696ec92689cc
SHA256值: 25e1d369c84f86f243e029c6d71c8a57b7668d57d2d01c4ae99a626897a61984

APP 信息

App名称: U智荟
包名: com.baoying.android.shopping
主活动**Activity:** com.baoying.android.shopping.ui.SplashActivity
安卓版本名称: 1.1.10
安卓版本: 10

域名线索

域名	是否危险域名	服务器信息
hmma.baidu.com	good	**IP:** 110.242.68.196 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map

域名	是否危险域名	服务器信息
www.baoying.com	good	IP: 36.102.212.89 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
esb.baoying.com	good	IP: 119.254.197.82 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
shop.baoying.com	good	IP: 125.37.206.220 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
api.baoying.com	good	IP: 140.249.60.213 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941 查看地图: Google Map

域名	是否危险域名	服务器信息
image.eum-appdynamics.com	good	**IP:** 35.161.226.28 **所属国家:** United States of America **地区:** Oregon **城市:** Portland **纬度:** 45.523449 **经度:** -122.676208 **查看地图:** Google Map
mobile.eum-appdynamics.com	good	**IP:** 34.215.125.8 **所属国家:** United States of America **地区:** Oregon **城市:** Portland **纬度:** 45.523449 **经度:** -122.676208 **查看地图:** Google Map
s-s.s	good	没有服务器地理信息.
intelcc-user.icsoc.net	good	**IP:** 182.92.53.37 **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
datax.baidu.com	good	**IP:** 111.206.210.170 **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

域名	是否危险域名	服务器信息
openrcv.baidu.com	good	**IP:** 111.206.209.112 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
play.google.com	good	**IP:** 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 查看地图: Google Map
long.open.weixin.qq.com	good	**IP:** 109.244.216.15 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
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

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
today.baoying.com	good	**IP:** 61.168.100.185 所属国家: China 地区: Henan 城市: Luoyang 纬度: 34.683609 经度: 112.453613 查看地图: Google Map
dxp.baidu.com	good	**IP:** 110.242.68.94 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
survey.qualtrics.com	good	**IP:** 23.197.180.107 所属国家: United States of America 地区: Massachusetts 城市: Billerica 纬度: 42.558430 经度: -71.268951 查看地图: Google Map

域名	是否危险域名	服务器信息
cms.baoying.com	good	**IP:** 36.102.212.77 **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

URL线索

URL信息	Url所在文件
https://survey.qualtrics.com	com/qualtrics/digital/LatencyReportingService.java
https://play.google.com/store/apps/details?id=	com/qualtrics/digital/QualtricsPopOverActivity.java
https://mobile.eum-appdynamics.com	com/appdynamics/eumagent/runtime/AgentConfiguration.java
https://image.eum-appdynamics.com	com/appdynamics/eumagent/runtime/AgentConfiguration.java
https://api.baoying.com/cn-shopping-gateway	com/baoying/android/shopping/BuildConfig.java
https://cms.baoying.com/	com/baoying/android/shopping/BuildConfig.java
https://shop.baoying.com/shop/checkout/ShippingAndPaymentInfo.action	com/baoying/android/shopping/BuildConfig.java
https://shop.baoying.com/shop/spring/phoenix/initializeShop/CN-APP-ANDROID	com/baoying/android/shopping/BuildConfig.java

URL信息	Url所在文件
https://www.baoying.com	com/baoying/android/shopping/BuildConfig.java
https://esb.baoying.com/i18n/graphql	com/baoying/android/shopping/BuildConfig.java
https://esb.baoying.com/cart/cart/validateCart	com/baoying/android/shopping/BuildConfig.java
https://www.baoying.com/ux/mall/shopping-download	com/baoying/android/shopping/ui/profile/SettingActivity.java
https://cms.baoying.com/BaoyingShopping.apk	com/baoying/android/shopping/api/AppUpgradeApi.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/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://hmma.baidu.com/auto.gif	com/baidu/mobstat/Config.java
http://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://dxp.baidu.com/vizParser	com/baidu/mobstat/db.java
https://dxp.baidu.com/autoTracker	com/baidu/mobstat/db.java
https://dxp.baidu.com/circleConfig?	com/baidu/mobstat/db.java
http://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/r.java
https://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/r.java

URL信息	Url所在文件
http://datax.baidu.com/xs.gif	com/baidu/mobstat/y.java
https://datax.baidu.com/xs.gif	com/baidu/mobstat/y.java
http://dxp.baidu.com/upgrade	com/baidu/mobstat/y.java
https://dxp.baidu.com/upgrade	com/baidu/mobstat/y.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	Android String Resource
https://today.baoying.com/ux/dotcom/zhs-CN/privacy-policy	Android String Resource

URL信息	Url所在文件
http://intelcc-user.icsoc.net?channelKey=f5e9d3e983d3fb98f7a4d9acf6ca7178&init=1	Android String Resource

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.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.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_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_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.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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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=CN, ST=beijing, L=beijing, O=com, OU=baoying, CN=YI
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-07-17 16:15:13+00:00
Valid To: 5851-08-12 16:15:13+00:00
Issuer: C=CN, ST=beijing, L=beijing, O=com, OU=baoying, CN=YI
Serial Number: 0x67cc01c1
Hash Algorithm: sha256
md5: 990e7a094bec8c34e905b18c0bb14c3d
sha1: 0f376005564773b7a98c5fa42eec1879ced54d55
sha256: ca2b3d6c8aae0b65f1ae62482c62cd6deb768601d2f27a5a2ff1dbb5b6dd13f1
sha512: db8fcb174cca2d4eedde5fa6b981f276e32ddc82fe238c50eca21573ad661fd7def29214b5c5faf62aa8da4d4b85ec1d9c450248221dda48de35202511fd738e
PublicKey Algorithm: rsa
Bit Size: 2048

Fingerprint: 7212061e82fe8e757d65bbe087be8f9dc922cac239f6b89a66b003530e597d73

Exodus威胁情报

名称	分类	URL链接
Appdynamics	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/194
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101
Qualtrics		https://reports.exodus-privacy.eu.org/trackers/306

硬编码敏感信息

可能的敏感信息
"forget_password" : "忘记密码"
"incomplete_username_or_pwd" : "账号或密码不能为空"
"input_password" : "密码"
"input_username" : "请输入您的用户名"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

可能的敏感信息
"send_to_wechat_session" : "发给微信朋友"
"incomplete_username_or_pwd" : "账号或密码不能为空"
"input_password" : "密码"
"send_to_wechat_session" : "发给微信朋友"

加壳分析

<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.MANUFACTURER check
Build.BOARD check
device ID check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></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>
</table>