MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

博商管理 1.2.23.APK

APP名称:	博商管理
包名:	org.boshang.erpapp
域名线索:	26条
URL线索:	31条
邮箱线索:	0条
分析日期:	2022年2月2日 17:06

文件信息

文件名: boshangguanli485987.apk

文件大小: 8.71MB
MD5值: 83b46cc6096e52fe2eb6a49d068d1d94
SHA1值: 4c74ac745557f72469e0a67e73baf95d4080ef2e
SHA256值: 659e8d277b891713adde1a19e4917c0b720352cd7af77735a64405976e4a4291

APP 信息

App名称: 博商管理
包名: org.boshang.erpapp
主活动Activity: org.boshang.erpapp.ui.module.other.activity.SplashActivity
安卓版本名称: 1.2.23
安卓版本: 20211109

域名线索

域名	是否危险域名	服务器信息
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
aip.baidubce.com	good	IP: 111.206.210.12 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
cfg.imtt.qq.com	good	**IP:** 121.51.158.70 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
mqqad.html5.qq.com	good	**IP:** 0.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
mta.qq.com	good	**IP:** 220.194.87.235 **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
bjuser.jpush.cn	good	**IP:** 122.9.9.94 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map

域名	是否危险域名	服务器信息
debugtbs.qq.com	good	**IP:** 175.27.9.46 **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
127.0.0.1	good	**IP:** 127.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
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
debugx5.qq.com	good	**IP:** 175.27.9.46 **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
oss.aliyuncs.com	good	**IP:** 118.178.29.5 **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
erp.bosum.com	good	**IP:** 119.23.75.57 **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
image.cnamedomain.com	good	没有服务器地理信息.
wup.imtt.qq.com	good	**IP:** 182.254.57.56 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.105 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map

域名	是否危险域名	服务器信息
oss-cn-.aliyuncs.comor	good	没有服务器地理信息.
log.tbs.qq.com	good	**IP:** 109.244.244.32 **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
www.qq.com	good	**IP:** 175.27.8.138 **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
mdc.html5.qq.com	good	**IP:** 175.27.9.46 **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
182.92.20.189	good	**IP:** 182.92.20.189 **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
tsis.jpush.cn	good	**IP:** 103.230.236.38 **所属国家:** China **地区:** Fujian **城市:** Xiamen **纬度:** 24.479790 **经度:** 118.081871 **查看地图:** Google Map
pms.mb.qq.com	good	**IP:** 121.51.158.70 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **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
oss-cn-hangzhou.aliyuncs.com	good	**IP:** 118.31.219.248 **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
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
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

URL线索

URL信息	Url所在文件
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
www.qq.com	com/tencent/smtt/sdk/j.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/j.java

URL信息	Url所在文件
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/c.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.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
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java

URL信息	Url所在文件
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/liulishuo/filedownloader/services/BaseFileServiceUIGuard.java
https://ip.	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSImpl.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss.aliyuncs.com	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://127.0.0.1	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
http://erp.bosum.com/	org/boshang/erpapp/BuildConfig.java
http://erp.bosum.com/erp/phone/	org/boshang/erpapp/BuildConfig.java
http://erp.bosum.com/wechat/private_agreement.html	org/boshang/erpapp/ui/module/mine/setting/activity/LoginActivity.java
https://aip.baidubce.com/rest/2.0/ocr/v1/business_card?access_token=	org/boshang/erpapp/ui/module/home/contact/presenter/ContactListPresenter.java
http://erp.bosum.com/erp/phone/	org/boshang/erpapp/backend/network/ErpRetrofitService.java

URL信息	Url所在文件
https://tsis.jpush.cn	cn/jiguang/c/a.java
http://182.92.20.189:9099/	cn/jiguang/a/a/c/i.java
http://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/d/i/c.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.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.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
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.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_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_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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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
org.boshang.erpapp.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=GuangDong, L=ShenZhen, O=bosum, OU=bosum, CN=bosum
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-07-01 09:35:30+00:00
Valid To: 2044-06-24 09:35:30+00:00
Issuer: C=CN, ST=GuangDong, L=ShenZhen, O=bosum, OU=bosum, CN=bosum
Serial Number: 0x1cbd7c9
Hash Algorithm: sha256
md5: 30a2f089d2ec62c4aaa66c471791b479
sha1: d0edd5730fa89035e5506254f1da6060e4590d90
sha256: 124bfd106e0d25fb1e40e653501710aca5bc997cfef06b0af454df376de04162
sha512: 99f9f7f0e7145ea4539cd92ef1b50eac5650be971fd5e73ae39287e148d17516061a0579a1306aadd84e868e62c16a2603381aac1dd7cf26e096a297ea0582bf
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d13398500e3839eab6f178181660ab42357fb063631357ce858763710f474e80

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

硬编码敏感信息

可能的敏感信息
"choose_user" : "请选择用户！"
"pwd_no_same" : "两次密码输入不一致！"
"reset_pwd_successful" : "重设密码成功！"
"setting_pwd" : "设置密码"
"sure_pwd" : "再次输入"
"user_name" : "用户名称"

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
possible Build.SERIAL check
SIM operator check
network operator name check
device ID check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</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>
