MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

福物通
智 慧 社 区

福物通店铺 1.0.3.APK

APP名称:	福物通店铺
包名:	com.ykh.o2oprovider
域名线索:	34条
URL线索:	41条
邮箱线索:	1条
分析日期:	2022年2月2日 19:58

文件信息

文件名: fwtdp.apk
文件大小: 7.04MB
MD5值: 23519302f118b116db03e0a749af7665
SHA1值: e0d7e67523ce498f03fe36d1d60335333e0aec37
SHA256值: a5ebb99005b611cfbca64952332047991053c34ee59848fa4a4a7c1800ed194e33

APP 信息

App名称: 福物通店铺
包名: com.ykh.o2oprovider
主活动**Activity:** com.ykh.o2oprovider.MainActivity
安卓版本名称: 1.0.3
安卓版本: 10003

域名线索

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

域名	是否危险域名	服务器信息
test.ykhcn.net	good	**IP:** 42.193.245.161 **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
notification.aizachi.com	good	没有服务器地理信息.
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
ccc.sys.miui.com	good	**IP:** 183.84.5.14 **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.jivesoftware.com	good	**IP:** 35.238.7.255 **所属国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860832 **查看地图:** Google Map

域名	是否危险域名	服务器信息
api.xmpush.xiaomi.com	good	**IP:** 117.48.116.220 **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.aizatao.com	good	**IP:** 154.37.46.84 **所属国家:** United States of America **地区:** Pennsylvania **城市:** Bellefonte **纬度:** 40.938061 **经度:** -77.721718 **查看地图:** Google Map
api.aizatao.com	good	**IP:** 154.37.46.84 **所属国家:** United States of America **地区:** Pennsylvania **城市:** Bellefonte **纬度:** 40.938061 **经度:** -77.721718 **查看地图:** Google Map
www.baidu.com	good	**IP:** 110.242.68.4 **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
graph.qq.com	good	**IP:** 223.166.152.195 **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
open.weixin.qq.com	good	**IP:** 175.24.209.30 **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
xmlpull.org	good	**IP:** 74.50.61.58 **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
182.254.116.117	good	**IP:** 182.254.116.117 **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
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
fr.register.xmpush.global.xiaomi.com	good	**IP:** 18.185.221.188 **所属国家:** Germany **地区:** Hessen **城市:** Frankfurt am Main **纬度:** 50.115520 **经度:** 8.684170 **查看地图:** Google Map
register.xmpush.global.xiaomi.com	good	**IP:** 47.88.199.5 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
qzs.qq.com	good	**IP:** 121.51.49.29 **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
cgi.connect.qq.com	good	**IP:** 183.2.144.86 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map
huatuocode.huatuo.qq.com	good	没有服务器地理信息.
www.midlib	good	没有服务器地理信息.
ru.register.xmpush.global.xiaomi.com	good	**IP:** 107.155.52.56 **所属国家:** Russian Federation **地区:** Moskva **城市:** Moscow **纬度:** 55.752220 **经度:** 37.615559 **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

域名	是否危险域名	服务器信息
metok.sys.miui.com	good	**IP:** 124.251.100.14 **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
api.aizachi.com	good	**IP:** 59.63.166.114 **所属国家:** China **地区:** Jiangxi **城市:** Nanchang **纬度:** 28.683331 **经度:** 115.883331 **查看地图:** Google Map
openmobile.qq.com	good	**IP:** 113.96.208.233 **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
cn.register.xmpush.xiaomi.com	good	**IP:** 118.26.252.220 **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
api.weixin.qq.com	good	**IP:** 109.244.145.152 **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.mob.com	good	**IP:** 116.62.130.46 **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
mta.qq.com	good	**IP:** 123.125.46.222 **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
idmb.register.xmpush.global.xiaomi.com	good	**IP:** 3.109.136.30 **所属国家:** United States of America **地区:** Washington **城市:** Seattle **纬度:** 47.627499 **经度:** -122.346199 **查看地图:** Google Map

域名	是否危险域名	服务器信息
fusion.qq.com	good	**IP:** 121.51.36.15 **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
appsupport.qq.com	good	**IP:** 183.2.144.86 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map
resolver.msg.xiaomi.net	good	**IP:** 120.92.96.13 **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://api.aizatao.com/Mall/Upload.ashx	com/aizatao/api/host/UploadFileEndpoint.java

URL信息	Url所在文件
https://test.ykhcn.net/Platform/Json/VersionService.svc/Add	com/aizatao/api/service/VersionService.java
https://test.ykhcn.net/Platform/Json/VersionService.svc/Get	com/aizatao/api/service/VersionService.java
https://test.ykhcn.net/Platform/Json/VersionService.svc/Modify	com/aizatao/api/service/VersionService.java
https://test.ykhcn.net/Platform/Json/VersionService.svc/Query	com/aizatao/api/service/VersionService.java
https://test.ykhcn.net/Platform/Json/VersionService.svc/Remove	com/aizatao/api/service/VersionService.java
https://api.aizatao.com/Mall/Json/ParameterService.svc/Add	com/aizatao/api/service/ParameterService.java
https://api.aizatao.com/Mall/Json/ParameterService.svc/Get	com/aizatao/api/service/ParameterService.java
https://api.aizatao.com/Mall/Json/ParameterService.svc/Modify	com/aizatao/api/service/ParameterService.java
https://api.aizatao.com/Mall/Json/ParameterService.svc/Query	com/aizatao/api/service/ParameterService.java
https://api.aizatao.com/Mall/Json/ParameterService.svc/Remove	com/aizatao/api/service/ParameterService.java
www.midlib;	com/tencent/www/midlib/BuildConfig.java
www.midlib	com/tencent/www/midlib/BuildConfig.java
http://182.254.116.117/d?dn=99e2d153e4d0527186ebed5ac5608367&id=6&ttl=1	com/tencent/android/tpush/service/b/b.java
www.qq.com	com/tencent/android/tpush/service/e/a.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java

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/d.java
https://graph.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/connect/share/QQShare.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/connect/share/QzoneShare.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/auth/a.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/common/BaseApi.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiIml.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiIml.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApiIml.java
http://qzs.qq.com	com/tencent/open/SocialApiIml.java

URL信息	Url所在文件
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	com/tencent/open/b/g.java
https://huatuocode.huatuo.qq.com	com/tencent/open/b/d.java
https://openmobile.qq.com/	com/tencent/open/utils/HttpUtils.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/f.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
http://www.qq.com	com/ykh/o2oprovider/ui/activity/ShareMiniProgramActivity.java
https://api.aizachi.com/MallConsumer	com/ykh/o2oprovider/utils/NetConst.java
https://api.aizatao.com/MallConsumer	com/ykh/o2oprovider/utils/NetConst.java
http://notification.aizachi.com:8888/jpush/send_sendAllMessage.action	com/ykh/o2oprovider/utils/NetConst.java
http://notification.aizachi.com:8888/jpush/send_sendWaiterMessage.action	com/ykh/o2oprovider/utils/NetConst.java
http://api.aizachi.com/Restaurant/Json/	com/ykh/o2oprovider/utils/NetConst.java
http://www.aizatao.com	com/ykh/o2oprovider/utils/NetConst.java
http://api.aizatao.com	com/ykh/o2oprovider/utils/NetConst.java

URL信息	Url所在文件
https://api.aizatao.com/Mall/Picture.ashx	com/ykh/o2oprovider/utils/NetConst.java
https://api.aizachi.com/Mall/Picture.ashx	com/ykh/o2oprovider/utils/NetConst.java
http://www.aizatao.com/maintenance.html	com/ykh/o2oprovider/utils/NetConst.java
https://api.aizatao.com/Upload/Mall/App/Logo/Mall_Android_Consumer.png	com/ykh/o2oprovider/utils/NetConst.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=APPID&secret=SECRET&code=CODE&grant_type=authorization_code	com/ykh/o2oprovider/utils/wxlogin/WechatHandler.java
https://api.weixin.qq.com/sns/userinfo?access_token=ACCESS_TOKEN&openid=OPENID	com/ykh/o2oprovider/utils/wxlogin/WechatHandler.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/ft.java
https://metok.sys.miui.com	com/xiaomi/push/ao.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gx.java
http://ccc.sys.miui.com	com/xiaomi/push/au.java
http://www.jivesoftware.com/xmlns/xmpp/properties	com/xiaomi/push/gp.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gd.java
http://%1$s/gslb/?ver=4.0	com/xiaomi/push/cx.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gw.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/be.java

URL信息	Url所在文件
https://register.xmpush.global.xiaomi.com	com/xiaomi/push/service/be.java
https://fr.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/be.java
https://ru.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/be.java
https://idmb.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/be.java
http://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/ad.java
www.baidu.com:80	com/xiaomi/push/service/e.java
https://api.xmpush.xiaomi.com/upload/xmsf_log?file=	com/xiaomi/mipush/sdk/w.java
https://api.xmpush.xiaomi.com/upload/app_log?file=	com/xiaomi/mipush/sdk/w.java
https://api.xmpush.xiaomi.com/upload/crash_log?file=	com/xiaomi/mipush/sdk/y.java
http://www.mob.com	Android String Resource

邮箱线索

邮箱地址	所在文件
ctwap@mycdma.cn	com/tencent/mid/core/HttpConnectClient.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.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.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_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_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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.	未知	Unknown permission	Unknown permission from android reference
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.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

向手机申请的权限	是否危险	类型	详细情况
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.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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
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_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.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.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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference

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.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.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用
com.ykh.o2oprovider.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates

Subject: C=China, ST=JiangXi, L=NanChang, O=flm158, OU=flm158, CN=flm158
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-12-25 02:23:06+00:00
Valid To: 2118-12-01 02:23:06+00:00
Issuer: C=China, ST=JiangXi, L=NanChang, O=flm158, OU=flm158, CN=flm158
Serial Number: 0xced6b5
Hash Algorithm: sha256
md5: a5f11d4ed498fb429d8837029dcaff0c
sha1: 30bb043e0564fad4ce1f385548e6092312b24a01
sha256: e07c82685613bd71ee9cecfc9ab1acec073c0cb865136ef1c7619f9d8f9d014d
sha512: 90b85598e7627cf8e96e40244afcb1526687a7ecbf8b63497be21b28086f3548993708901fa1e01e862716d36bcff404238e74e2d610a5238634c1d8a3747945

Exodus威胁情报

名称	分类	URL链接
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
"dtp_deleted_key" : "%1$s deleted"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"third_party_toast_auth_canceled" : "取消授权"

可能的敏感信息
"third_party_toast_auth_failed" : "授权失败"
"third_party_toast_auth_success" : "授权成功"
"dtp_deleted_key" : "已删除 %1$s"
"dtp_deleted_key" : "已删除 %1$s"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1109597708://,

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.BOARD check
possible Build.SERIAL check
SIM operator check
subscriber ID check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
