MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

优吉美汇 6.7.16.APK

APP名称:	优吉美汇
包名:	com.youjimeiapp.app
域名线索:	42条
URL线索:	51条
邮箱线索:	1条
分析日期:	2022年1月22日 23:34

文件信息

文件名: youjimeihui.apk
文件大小: 3.46MB
MD5值: 47d66474d4af584c5c7cbbb4bbd4f891
SHA1值: 081498beaab8b6eb9f4649a7fd676f9807bc05cc
SHA256值: ed9bad33995a625aacd1ed0944d7c6fbb16147c0d79d9ca44e304f90b0f71d10

APP 信息

App名称: 优吉美汇
包名: com.youjimeiapp.app
主活动**Activity:** com.uzmap.pkg.LauncherUI
安卓版本名称: 6.7.16
安卓版本: 16

域名线索

域名	是否危险域名	服务器信息
wspeed.qq.com	good	没有服务器地理信息.
s.apicloud.com	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
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
mobilegw.alipay.com	good	IP: 203.209.255.238 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
h5.m.taobao.com	good	IP: 140.249.89.233 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map
cgi.connect.qq.com	good	IP: 183.2.144.36 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
mobilegw.stable.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
p.apicloud.com	good	IP: 47.93.154.30 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
r.apicloud.com	good	IP: 182.92.145.58 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: 203.209.250.50 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
webpresence.qq.com	good	IP: 182.254.56.83 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
www.myapp.com	good	IP: 182.254.51.124 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
a.apicloud.com	good	IP: 182.92.145.58 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
ls.map.soso.com	good	IP: 109.244.249.149 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
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
appsupport.qq.com	good	IP: 183.2.143.207 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

域名	是否危险域名	服务器信息
c.isdspeed.qq.com	good	没有服务器地理信息.
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
lstest.map.soso.com	good	**IP:** 125.39.120.62 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
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
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
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
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
d.apicloud.com	good	IP: 47.94.176.24 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.wsq.qq.com	good	IP: 121.51.191.216 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
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
cgi.qplus.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
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
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

域名	是否危险域名	服务器信息
lbs.map.qq.com	good	IP: 182.254.50.117 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
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
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
hydra.alibaba.com	good	IP: 203.119.144.59 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
ce3e75d5.jpush.cn	good	IP: 183.232.58.244 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

域名	是否危险域名	服务器信息
api.mch.weixin.qq.com	good	IP: 182.254.22.146 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
analy.qq.com	good	IP: 182.254.51.124 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
appact.qzone.qq.com	good	IP: 182.254.50.22 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
as.apicloud.com	good	没有服务器地理信息.
qzs.qq.com	good	IP: 121.51.49.44 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
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
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

URL线索

URL信息	Url所在文件
http://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
http://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/c.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&	com/alipay/sdk/data/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java

URL信息	Url所在文件
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mta.qq.com/	com/tencent/stat/StatService.java
http://mta.oa.com/	com/tencent/stat/StatService.java
http://ls.map.soso.com/deflect?c=1	com/tencent/map/b/b.java
http://lstest.map.soso.com/loc?c=1	com/tencent/map/b/f.java
http://lbs.map.qq.com/loc?c=1	com/tencent/map/b/f.java
http://ls.map.soso.com/monitor/monitor.html	com/tencent/map/b/q.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
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/AuthDialog.java

URL信息	Url所在文件
https://openmobile.qq.com/	com/tencent/connect/common/Constants.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiIml.java
http://qzs.qq.com/open/mobile/rate/sdk_rate.html?	com/tencent/open/SocialApiIml.java
http://appact.qzone.qq.com/appstore_activity_task_pcpush_sdk	com/tencent/open/TaskGuide.java
http://fusion.qq.com/cgi-bin/qzapps/mapp_lbs_delete.cgi	com/tencent/open/LocationApi.java
http://fusion.qq.com/cgi-bin/qzapps/mapp_lbs_getnear.cgi	com/tencent/open/LocationApi.java
http://c.isdspeed.qq.com/code.cgi	com/tencent/open/b/d.java
https://openmobile.qq.com/	com/tencent/open/utils/HttpUtils.java
http://cgi.qplus.com/report/report	com/tencent/open/utils/Util.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/OpenConfig.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin/qzapps/mapp_getappinfo.cgi	com/tencent/open/utils/ServerSetting.java
http://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/utils/ServerSetting.java

URL信息	Url所在文件
http://qzs.qq.com/open/mobile/brag/sdk_brag.html?	com/tencent/open/utils/ServerSetting.java
https://openmobile.qq.com/	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/reactive/sdk_reactive.html?	com/tencent/open/utils/ServerSetting.java
http://wspeed.qq.com/w.cgi	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/not_support.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/sdk_common/down_qq.htm?	com/tencent/open/utils/ServerSetting.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin/prize_sharing/exchange_prize.cgi	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin/prize_sharing/get_activity_state.cgi	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin/prize_sharing/make_share_url.cgi	com/tencent/open/utils/ServerSetting.java

URL信息	Url所在文件
http://fusion.qq.com/cgi-bin/prize_sharing/query_unexchange_prize.cgi	com/tencent/open/utils/ServerSetting.java
http://webpresence.qq.com/getonline?Type=1&	com/tencent/open/wpa/WPA.java
http://www.myapp.com/forward/a/45592?g_f=990935	com/tencent/open/wpa/WPA.java
http://m.wsq.qq.com/direct?	com/tencent/open/yyb/AppbarAgent.java
http://qzs.qq.com/open/mobile/jsbridge/demo.htm	com/tencent/open/yyb/AppbarJsBridge.java
http://analy.qq.com/cgi-bin/mapp_apptrace	com/tencent/open/yyb/a.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://hydra.alibaba.com/	com/ta/utdid2/aid/AidRequester.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
https://api.mch.weixin.qq.com/pay/unifiedorder	com/uzmap/pkg/uzmodules/uzWxPay/PayTask.java
https://api.mch.weixin.qq.com/pay/unifiedorder	com/uzmap/pkg/uzmodules/uzWxPay/GetOrderIdTask.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	com/uzmap/pkg/uzmodules/uzWx/tasks/AccessTokenTask.java

URL信息	Url所在文件
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=%s&grant_type=refresh_token&refresh_token=%s	com/uzmap/pkg/uzmodules/uzWx/tasks/AccessTokenTask.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=%s	com/uzmap/pkg/uzmodules/uzWx/tasks/GetUserInfoTask.java
https://tsis.jpush.cn	cn/jiguang/ak/i.java
http://182.92.20.189:9099/	cn/jiguang/r/a.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/ae/b.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/af/d.java
https://a.apicloud.com	compile/Properties.java
https://d.apicloud.com	compile/Properties.java
https://s.apicloud.com	compile/Properties.java
https://p.apicloud.com	compile/Properties.java
https://r.apicloud.com	compile/Properties.java
https://as.apicloud.com	compile/Properties.java

邮箱线索

邮箱地址	所在文件
developer@apicloud.com	com/uzmap/pkg/uzcore/b/d.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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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_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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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。

向手机申请的权限	是否危险	类型	详细情况
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
com.youjimeiapp.app.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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_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。

向手机申请的权限	是否危险	类型	详细情况
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(805599740@qq.com), OU=(805599740@qq.com), CN=(j805599740)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-08-16 02:16:06+00:00
Valid To: 2119-07-23 02:16:06+00:00
Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(805599740@qq.com), OU=(805599740@qq.com), CN=(j805599740)
Serial Number: 0x573ff32a
Hash Algorithm: sha256
md5: a89442eff434f38503fde8e741cb4613
sha1: e5bb2cf506344109da97930d17c18d0c40c469a6
sha256: 002d7071f2a19a2db9cd9028b49d6582f0ef7ec316aabeec2a7a5ccf7e28ead5
sha512: 4b22ccdd7389bfc16ef2d15673f123ce6495d7c21dc98730b75dfb9d17e6bea4731f44e622a7d1c2fd5ebcb63ffe378ad21036fc2a157ccd074f93c5576133f3
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 307aa5149ccdc45ec8415b3c04dbe5832fce803e66d1736327196da21e54cac2

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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.uzmap.pkg.EntranceActivity	Schemes: fdsftre://,
com.tencent.tauth.AuthActivity	Schemes: tencent110555722233://,

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
Build.TAGS check
SIM operator check
network operator name check
device ID check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
emulator file check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>