MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

百网通聘 1.0.1.APK

APP名称:	百网通聘
包名:	com.bwtzp.jobapp
域名线索:	15条
URL线索:	29条
邮箱线索:	0条
分析日期:	2022年2月2日 19:28

文件信息

文件名: bwtp.apk
文件大小: 7.94MB
MD5值: 071146e7372ccd6d58eb248c65f2f011
SHA1值: 669f006705c0a9ec33fb23b2e9e62d4b233170a0
SHA256值: 4951b445c89320b72deaec17ed63888210eba3cead12f0dcaa78ed174570d572

APP 信息

App名称: 百网通聘
包名: com.bwtzp.jobapp
主活动**Activity:** com.bwtzp.jobapp.SplashActivity
安卓版本名称: 1.0.1
安卓版本: 2

域名线索

域名	是否危险域名	服务器信息
xml.apache.org	good	**IP:** 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
p.share.mob.com	good	没有服务器地理信息.

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
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
app.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
www.bwtzp.com	good	IP: 120.26.47.16 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
loc.map.baidu.com	good	IP: 111.206.209.175 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
graph.qq.com	good	IP: 113.96.208.232 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
www.baidu.com	good	IP: 110.242.68.3 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
api.map.baidu.com	good	IP: 111.206.209.166 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
daup.map.baidu.com	good	IP: 153.3.236.86 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777779 查看地图: Google Map
m.bwtzp.com	good	IP: 120.26.47.16 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
itsdata.map.baidu.com	good	IP: 111.206.209.180 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
qzs.qq.com	good	IP: 182.254.54.167 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
ofloc.map.baidu.com	good	**IP:** 111.206.209.193 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
www.baidu.com	com/blankj/utilcode/util/NetworkUtils.java
http://xml.apache.org/xslt}indent-amount	com/blankj/utilcode/util/LogUtils.java
https://ofloc.map.baidu.com/locnu	com/baidu/location/b/aa.java
https://loc.map.baidu.com/cc.php	com/baidu/location/b/g.java
https://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/b/i.java
https://loc.map.baidu.com/cfgs/loc/commcfgs	com/baidu/location/b/a.java
https://loc.map.baidu.com/indoorlocbuildinginfo.php	com/baidu/location/indoor/a.java
https://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet	com/baidu/location/indoor/mapversion/b/a.java

URL信息	Url所在文件
http://loc.map.baidu.com/sdk.php	com/baidu/location/h/n.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/h/n.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/h/n.java
https://loc.map.baidu.com/tcu.php	com/baidu/location/h/n.java
http://loc.map.baidu.com/rtbu.php	com/baidu/location/h/n.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/h/n.java
http://loc.map.baidu.com/wloc	com/baidu/location/h/n.java
https://loc.map.baidu.com/sdk_ep.php	com/baidu/location/h/n.java
https://loc.map.baidu.com/sdk.php	com/baidu/location/h/n.java
https://daup.map.baidu.com/cltr/rcvr	com/baidu/location/h/n.java
https://loc.map.baidu.com/cfgs/loc/commcfgs	com/baidu/location/c/e.java
https://loc.map.baidu.com/gpsz	com/baidu/location/c/a.java
https://ofloc.map.baidu.com/offline_loc	com/baidu/location/e/k.java
http://ofloc.map.baidu.com/offline_loc	com/baidu/location/e/h.java
https://ofloc.map.baidu.com/offline_loc	com/baidu/location/e/g.java

URL信息	Url所在文件
http://%s/%s	com/baidu/location/e/c.java
https://ofloc.map.baidu.com/offline_loc	com/baidu/location/e/c.java
https://api.map.baidu.com/sdkproxy/v2/lbs_locsdk/geocoding/v3/	com/baidu/geofence/a/b.java
https://api.map.baidu.com/sdkproxy/v2/lbs_locsdk/geocoding/v3/?	com/baidu/geofence/a/b.java
https://api.map.baidu.com/sdkproxy/v2/lbs_locsdk/place/v2/search	com/baidu/geofence/a/f.java
https://api.map.baidu.com/sdkproxy/v2/lbs_locsdk/place/v2/search?	com/baidu/geofence/a/f.java
https://api.map.baidu.com/sdkcs/verify	com/baidu/lbsapi/auth/LBSAuthManager.java
https://www.bwtzp.com/treaty.html	com/bwtzp/jobapp/PrivacyFragment.java
http://m.bwtzp.com/?from=appload&appcid=	com/bwtzp/jobapp/SplashActivity.java
http://m.bwtzp.com/api/	com/bwtzp/jobapp/service/http/HttpConstants.java
http://m.bwtzp.com/	com/bwtzp/jobapp/service/http/HttpConstants.java
http://m.bwtzp.com/?from=app&appcid=	com/bwtzp/jobapp/service/http/HttpConstants.java
https://){1}	cn/sharesdk/framework/b/a.java
http://p.share.mob.com/tags/getTagList	cn/sharesdk/framework/authorize/f.java
https://graph.qq.com/oauth2.0/me	cn/sharesdk/tencent/qq/c.java

URL信息	Url所在文件
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com	cn/sharesdk/tencent/qq/c.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?sdkv=3.3.0.lite&display=mobile	cn/sharesdk/tencent/qq/a.java
http://app.qq.com/detail/com.tencent.mobileqq?autodownload=1&norecommend=1&rootvia=opensdk	cn/sharesdk/tencent/qq/a.java
https://api.weixin.qq.com/sns/oauth2/access_token	cn/sharesdk/wechat/utils/h.java
https://api.weixin.qq.com/sns/oauth2/refresh_token	cn/sharesdk/wechat/utils/h.java
https://api.weixin.qq.com/sns/userinfo	cn/sharesdk/wechat/utils/h.java
http://www.mob.com/policy/en	Android String Resource
http://www.mob.com/about/policy	Android String Resource
http://www.mob.com	Android String Resource
http://www.mob.com/about/policy/en	Android String Resource
http://www.mob.com/policy/zh	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.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_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_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.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.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.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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=cn, ST=hz, L=zj, O=lee, OU=lee, CN=lee
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-12-13 11:35:29+00:00
Valid To: 2075-09-16 11:35:29+00:00
Issuer: C=cn, ST=hz, L=zj, O=lee, OU=lee, CN=lee
Serial Number: 0x4f9082d4
Hash Algorithm: sha256
md5: c30246c85a7ae3e4416930216c7e1c96
sha1: 395ccfda67617f43d3030c262dac1c922623092f
sha256: 26599d1da9c794d5de4a8d391d226cde9f58933d8a6328e22699d9ab8ffacb7e
sha512: 8d6091b5ee6d1a817c62b6fb3f0a1a05f217e7e726c06324f704817d29e248081e25f9f8373490884fd0605543660ab72e793b466b48940dfe1e47a1b89c6721
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 02e7f41713d56bbe4b3f6e652b4c4e239ca94e85cbf00e2019dd13b8cbed21e2

Exodus威胁情报

名称	分类	URL链接
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97

硬编码敏感信息

可能的敏感信息
"input_pwd" : "请输入密码"
"input_user_name" : "用户名/邮箱/手机号"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/about/policy。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobdemo_authorize_dialog_title" : "服务授权"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"mobcommon_authorize_dialog_accept" : "Accept"

可能的敏感信息
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see detailshttp://www.mob.com/about/policy/en.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."
"mobdemo_authorize_dialog_title" : "service authority"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"mobcommon_authorize_dialog_accept" : "同意"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/policy/zh。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobcommon_authorize_dialog_reject" : "拒绝"
"mobcommon_authorize_dialog_title" : "服务授权"

应用内通信

活动(ACTIVITY)	通信(INTENT)
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent101931962://,

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机：Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check Build.TAGS check subscriber ID check emulator file check possible VM check 编译器：r8

<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>反虚拟机</td><td>Build.MODEL check
Build.MANUFACTURER check
possible Build.SERIAL check
Build.TAGS check
subscriber ID check
possible ro.secure check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
