MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

宜兴人才网 1.0.0.APK

APP名称:	宜兴人才网
包名:	com.kgmttn.kmbqiuj
域名线索:	32条
URL线索:	47条
邮箱线索:	1条
分析日期:	2022年2月3日 13:05

文件信息

文件名: yixrcwang.apk
文件大小: 4.85MB
MD5值: 00c145e8a562fe14d8684c729fda7a98
SHA1值: cd8bc6c9aad53a8225d5d48fe39e0d48182b3f16
SHA256值: 6509c46a830364e7d30b62216fd17f2100455a436afc5ad7b14b6f5ce924b025

APP 信息

App名称: 宜兴人才网
包名: com.kgmttn.kmbqiuj
主活动**Activity:** com.bslyun.app.activity.MainActivity
安卓版本名称: 1.0.0
安卓版本: 2

域名线索

域名	是否危险域名	服务器信息
com.thoughtworks.xstream	good	没有服务器地理信息.
interface.shareinstall.com.cn	good	**IP:** 106.75.20.108 **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

域名	是否危险域名	服务器信息
iploc.market.alicloudapi.com	good	**IP:** 119.23.169.39 **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
pv.sohu.com	good	**IP:** 211.159.191.96 **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
adv.ppf.kim	good	**IP:** 119.8.233.196 **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
cc.map.qq.com	good	**IP:** 182.254.57.47 **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
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
config.shareinstall.com.cn	good	**IP:** 124.71.238.62 **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
www.appk6.com	good	**IP:** 116.62.66.31 **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
adblocker.appbsl.net	good	没有服务器地理信息.
maplbs-40171.sh.gfp.tencent-cloud.com	good	**IP:** 121.51.57.206 **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
astat.bugly.cros.wr.pvp.net	good	**IP:** 170.106.135.32 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.774929 **经度:** -122.419418 **查看地图:** Google Map
analytics.map.qq.com	good	**IP:** 182.254.63.54 **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
statlog.shareinstall.com.cn	good	**IP:** 114.116.251.190 **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
android.bugly.qq.com	good	**IP:** 109.244.244.35 **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

域名	是否危险域名	服务器信息
auth.appbsl.com	good	**IP:** 116.62.66.31 **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
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 **所属国家:** Korea (Republic of) **地区:** Seoul-teukbyeolsi **城市:** Seoul **纬度:** 37.568260 **经度:** 126.977829 **查看地图:** Google Map
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
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
wx.tenpay.com	good	**IP:** 182.254.88.167 **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
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
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
check.shareinstall.com.cn	good	**IP:** 124.71.238.62 **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
my.wlwx.com	good	**IP:** 120.24.95.120 **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
xml.org	good	**IP:** 104.239.240.11 **所属国家:** United States of America **地区:** Texas **城市:** Windcrest **纬度:** 29.499678 **经度:** -98.399246 **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
api.weibo.com	good	**IP:** 180.149.153.83 **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
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
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
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.84 **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
rqd.uu.qq.com	good	**IP:** 182.254.88.185 **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
maps.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

URL线索

URL信息	Url所在文件
https://statlog.shareinstall.com.cn/shareinstall_log/online	com/sh/sdk/shareinstall/helper/n.java
https://statlog.shareinstall.com.cn/shareinstall_log/install	com/sh/sdk/shareinstall/helper/k.java
https://check.shareinstall.com.cn/wwwroot	com/sh/sdk/shareinstall/helper/f.java
http://iploc.market.alicloudapi.com/v3/ip	com/sh/sdk/shareinstall/helper/g.java
https://statlog.shareinstall.com.cn/shareinstall_log/si	com/sh/sdk/shareinstall/helper/l.java
https://config.shareinstall.com.cn/signal/config	com/sh/sdk/shareinstall/helper/c.java
http://pv.sohu.com/cityjson?ie=utf-8	com/sh/sdk/shareinstall/helper/i.java
https://statlog.shareinstall.com.cn/shareinstall_log/register	com/sh/sdk/shareinstall/helper/p.java

URL信息	Url所在文件
https://statlog.shareinstall.com.cn/sdkinfoscollection/startover	com/sh/sdk/shareinstall/helper/d.java
https://interface.shareinstall.com.cn/hike/exce	com/sh/sdk/shareinstall/helper/o.java
https://statlog.shareinstall.com.cn/shareinstall_log/active	com/sh/sdk/shareinstall/helper/a.java
https://config.shareinstall.com.cn/signal/config	com/sh/sdk/shareinstall/d/a/b.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
http://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://analytics.map.qq.com/tr?mllc	com/tencent/map/geolocation/a/a/e.java
https://maplbs-40171.sh.gfp.tencent-cloud.com/Index/	com/tencent/map/geolocation/a/a/c.java
https://cc.map.qq.com?desc_c	com/tencent/map/geolocation/a/a/i.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java

URL信息	Url所在文件
www.qq.com	com/tencent/smtt/sdk/j.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/j.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/m.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/m.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/m.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
http://www.appk6.com	com/bslyun/app/MainApplication.java

URL信息	Url所在文件
https://wx.tenpay.com/	com/bslyun/app/browser/WebViewUtils.java
http://maps.google.com/maps?saddr=	com/bslyun/app/browser/Bridge.java
https://api.weibo.com/2/users/	com/bslyun/app/component/WeiboComponent.java
http://auth.appbsl.com/index.php/app/sms/check_code	com/bslyun/app/component/quicklogin/QuickLoginComponent.java
http://auth.appbsl.com/index.php/app/api/record	com/bslyun/app/component/quicklogin/QuickLoginComponent.java
http://my.wlwx.com:6006	com/bslyun/app/component/quicklogin/QuickLoginComponent.java
http://auth.appbsl.com/index.php/app/sms/send_sms_code	com/bslyun/app/component/quicklogin/QuickLoginComponent.java
http://auth.appbsl.com	com/bslyun/app/component/quicklogin/QuickLoginComponent.java
http://adv.ppf.kim/public/adv/index/appcount	com/bslyun/app/e/a.java
https://adblocker.appbsl.net/index.php?g=port&m=unionadvblock&a=get	com/bslyun/app/service/UpdateFilterIpService.java
https://wx.tenpay.com/	com/bslyun/app/fragment/WebFragment.java
http://com.thoughtworks.xstream/XStreamSource/feature	com/thoughtworks/xstream/io/xml/TraxSource.java
http://com.thoughtworks.xstream/sax/property/configured-xstream	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://com.thoughtworks.xstream/sax/property/source-object-list	com/thoughtworks/xstream/io/xml/SaxWriter.java
http://xml.org/sax/features/namespaces	com/thoughtworks/xstream/io/xml/SaxWriter.java

URL信息	Url所在文件
http://xml.org/sax/features/namespace-prefixes	com/thoughtworks/xstream/io/xml/SaxWriter.java

邮箱线索

邮箱地址	所在文件
null@null.xml	com/thoughtworks/xstream/persistence/FilePersistenceStrategy.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.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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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

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_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.RESTART_PACKAGES	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.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.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.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.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

向手机申请的权限	是否危险	类型	详细情况
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.SET_DEBUG_APP	危险	启用应用程序调试	允许一个应用程序打开另一个应用程序的调试。恶意应用程序可以使用它来杀死其他应用程序
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表

向手机申请的权限	是否危险	类型	详细情况
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证令牌
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
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.CLEAR_APP_CACHE	系统需要	删除所有应用程序缓存数据	允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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
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_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ASSISTED_GPS	未知	Unknown permission	Unknown permission from android reference
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.fingerprints.service.ACCESS_FINGERPRINT_MANAGER	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
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	Unknown permission	Unknown permission from android reference
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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, O=����������������, OU=����������������, CN=352951
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-02-15 06:25:35+00:00
Valid To: 2119-09-10 06:25:35+00:00
Issuer: C=CN, O=����������������, OU=����������������, CN=352951
Serial Number: 0x3460382a
Hash Algorithm: sha256
md5: f489491645a04d5ed45d9744b78b6c10
sha1: afd02aa154fefd9f465e5b9dfb215e68a6f430fb
sha256: 59e815c5a1643f5e8614bc6a2bef3556141ae79203a5c27c021dc4fa5179f6b1
sha512: 023cc49ec5441f6f63eb53fd4cd9cc076bbd53d1c7dacf9eb1eafb624d2566187b30636d70c6466dd8dd4c0db844e7491317d14f3e50492199cb9202f771aedd
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a38712bcdb701cfc620d28c49b8aba6b98f4cbfc0fb60307d2fee290cb0443f4

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
WeChat Location		https://reports.exodus-privacy.eu.org/trackers/76

硬编码敏感信息

可能的敏感信息
"QQ_AppSecret" : "_QQ_AppSecret"
"SINA_APP_KEY" : "_SINA_APP_KEY"
"WX_AppSecret" : "_WX_AppSecret"
"baid_ai_app_key" : "_baid_ai_app_key"
"baid_ai_secret_key" : "_baid_ai_secret_key"
"baidu_face_api_key" : ""
"baidu_face_secret_key" : ""
"hw_app_key" : "_hw_app_key"

可能的敏感信息
"lebo_app_secret" : "_lebo_app_secret"
"linked_me_key" : ""
"mi_app_key" : "_mi_app_key"
"my_app_secret" : ""
"my_master_secret" : ""
"oppo_app_key" : ""
"shareinstall_appkey" : ""
"zb_license_key" : ""

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.bslyun.app.activity.MainActivity	Schemes: @string/wx_app_id://, @string/shareinstall_scheme://,
com.tencent.tauth.AuthActivity	Schemes: @string/tencent://,
com.bslyun.app.activity.HtmlOpenApp	Schemes: bslapp://,

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.BRAND check
Build.DEVICE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
subscriber ID check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
