MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

AVIC

智慧物业平台 4.0.4.APK

APP名称:	智慧物业平台
包名:	com.zh.wuye
域名线索:	31条
URL线索:	29条
邮箱线索:	0条
分析日期:	2022年2月3日 13:32

文件信息

文件名: zhwypt339312.apk
文件大小: 8.5MB
MD5值: 6c804989b0e05975ed6d89c8c5ecbd56
SHA1值: e86bf3c6c11cf37503ca8f0ba5d84aa7343dcb0f
SHA256值: a81a76702bbe0f31d4e6c84e9e99fd8a34ca155eb49ba52f577163cd70f4568a

APP 信息

App名称: 智慧物业平台
包名: com.zh.wuye
主活动**Activity:** com.zh.wuye.SplashActivity
安卓版本名称: 4.0.4
安卓版本: 63

域名线索

域名	是否危险域名	服务器信息
114.67.22.172	good	**IP:** 114.67.22.172 **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
114.67.23.144	good	**IP:** 114.67.23.144 **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
applog.zhihuiwuye.com.cn	good	**IP:** 47.106.70.42 **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
hmma.baidu.com	good	**IP:** 110.242.68.195 **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
schemas.android.com	good	没有服务器地理信息.
192.168.0.4	good	**IP:** 192.168.0.4 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map

域名	是否危险域名	服务器信息
java.sun.com	good	**IP:** 23.206.238.121 **所属国家:** Malaysia **地区:** Wilayah Persekutuan Kuala Lumpur **城市:** Kuala Lumpur **纬度:** 3.141200 **经度:** 101.686531 **查看地图:** Google Map
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
oss-cn-.aliyuncs.comor	good	没有服务器地理信息.
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
file.zhihuiwuye.com.cn	good	**IP:** 119.23.82.181 **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
lame.sf.net	good	**IP:** 204.68.111.100 **所属国家:** United States of America **地区:** California **城市:** San Diego **纬度:** 32.799797 **经度:** -117.137047 **查看地图:** Google Map
android.bugly.qq.com	good	**IP:** 109.244.244.137 **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
openrcv.baidu.com	good	**IP:** 111.206.209.112 **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
supervisor.zhihuiwuye.com.cn	good	**IP:** 120.78.185.8 **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
datax.baidu.com	good	**IP:** 111.206.210.170 **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.javaeye.com	good	没有服务器地理信息.
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
www.w3.org	good	**IP:** 128.30.52.100 **所属国家:** United States of America **地区:** Massachusetts **城市:** Cambridge **纬度:** 42.365078 **经度:** -71.104523 **查看地图:** Google Map
api.zhihuiwuye.com.cn	good	**IP:** 119.23.82.181 **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
114.67.22.212	good	**IP:** 114.67.22.212 **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
dxp.baidu.com	good	**IP:** 110.242.68.94 **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
120.78.150.247	good	**IP:** 120.78.150.247 **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
192.168.0.99	good	**IP:** 192.168.0.99 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
avic-paixiu-2019.oss-cn-shenzhen.aliyuncs.com	good	**IP:** 120.77.166.71 **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
freemarker.org	good	**IP:** 192.64.119.217 **所属国家:** United States of America **地区:** Georgia **城市:** Atlanta **纬度:** 33.727291 **经度:** -84.425377 **查看地图:** Google Map
oss-cn-shenzhen.aliyuncs.com	good	**IP:** 120.77.166.207 **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
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
image.cnamedomain.com	good	没有服务器地理信息.
192.168.0.198	good	**IP:** 192.168.0.198 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
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://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/al.java
https://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/al.java

URL信息	Url所在文件
http://datax.baidu.com/xs.gif	com/baidu/mobstat/bb.java
https://datax.baidu.com/xs.gif	com/baidu/mobstat/bb.java
http://dxp.baidu.com/upgrade	com/baidu/mobstat/bb.java
https://dxp.baidu.com/upgrade	com/baidu/mobstat/bb.java
http://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://dxp.baidu.com/autoTracker	com/baidu/mobstat/autotrace/Common.java
https://dxp.baidu.com/circleConfig	com/baidu/mobstat/autotrace/Common.java
https://dxp.baidu.com/vizParser	com/baidu/mobstat/autotrace/Common.java
http://www.javaeye.com/custom	com/zh/wuye/ui/activity/keyEvent/TimePicker/ImageTextButton.java
http://schemas.android.com/apk/res/android	com/zh/wuye/widget/SlidingTabLayout/CommonTabLayout.java
http://api.zhihuiwuye.com.cn/	com/zh/wuye/Manager/PreferenceManager.java
http://114.67.23.144:8031	com/zh/wuye/Manager/PreferenceManager.java
http://file.zhihuiwuye.com.cn/	com/zh/wuye/Manager/PreferenceManager.java
http://120.78.150.247:9066/	com/zh/wuye/Manager/PreferenceManager.java

URL信息	Url所在文件
http://114.67.22.172:8026/	com/zh/wuye/Manager/PreferenceManager.java
http://supervisor.zhihuiwuye.com.cn:6031/	com/zh/wuye/Manager/PreferenceManager.java
https://avic-paixiu-2019.oss-cn-shenzhen.aliyuncs.com/	com/zh/wuye/constants/UriConstant.java
http://192.168.0.99:8080/zhwuye/	com/zh/wuye/constants/UriConstant.java
http://oss-cn-shenzhen.aliyuncs.com	com/zh/wuye/constants/UriConstant.java
http://114.67.22.212:9080/	com/zh/wuye/constants/UriConstant.java
http://192.168.0.198:8026/zhwuye/	com/zh/wuye/constants/UriConstant.java
http://120.78.150.247:9066/	com/zh/wuye/constants/UriConstant.java
http://applog.zhihuiwuye.com.cn:8098/	com/zh/wuye/constants/UriConstant.java
http://192.168.0.4:8031/	com/zhwy/zhwy_chart/constants/Doman.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

URL信息	Url所在文件
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://182.92.20.189:9099/	cn/jiguang/a/a/c/h.java
http://java.sun.com/dtd/web-jsptaglibrary_1_2.dtd	freemarker/ext/jsp/TaglibFactory.java
http://java.sun.com/j2ee/dtds/web-jsptaglibrary_1_1.dtd	freemarker/ext/jsp/TaglibFactory.java
http://java.sun.com/dtd/web-app_2_3.dtd	freemarker/ext/jsp/TaglibFactory.java
http://java.sun.com/j2ee/dtds/web-app_2_2.dtd	freemarker/ext/jsp/TaglibFactory.java
http://www.w3.org/XML/1998/namespace	freemarker/ext/xml/Namespaces.java
http://freemarker.org/docs/ref_builtins.html;	freemarker/core/BuiltIn.java
http://freemarker.org/docs/ref_directive_list.html).	freemarker/core/FMParserTokenManager.java
http://freemarker.org/docs/ref_directive_alphaidx.html;	freemarker/core/FMParserTokenManager.java
http://freemarker.org/	freemarker/core/CommandLine.java
http://lame.sf.net	lib/mips64/libmp3lame.so
http://lame.sf.net	lib/x86_64/libmp3lame.so

URL信息	Url所在文件
http://lame.sf.net	lib/x86/libmp3lame.so
http://lame.sf.net	lib/mips/libmp3lame.so
http://lame.sf.net	lib/arm64-v8a/libmp3lame.so

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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

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.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.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.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.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_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.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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.REPLACE_EXISTING_PACKAGE	未知	Unknown permission	Unknown permission from android reference
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。
com.blackcard.collector.collectorplugin.permissions.BRUSHCARD	未知	Unknown permission	Unknown permission from android reference
com.zh.wuye.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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=GD, L=SZ, O=AVIC, OU=AVIC, CN=AVIC
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-08-25 05:16:11+00:00
Valid To: 2042-08-19 05:16:11+00:00
Issuer: C=86, ST=GD, L=SZ, O=AVIC, OU=AVIC, CN=AVIC
Serial Number: 0x4c0ddfb1
Hash Algorithm: sha256
md5: 9082b2222ddee7ee03a8f87944c13c56
sha1: 4560de6556926f0bb4155464e94601f47606c3a4
sha256: 45e4f6c7fe2b97757457dbd053fab5f32aff7b51ede33c98d12a34fc190a1a0d
sha512: c3279756475dfba819a856678d93a014aa5d4abc443ed57b4d05b0827ce4263ef03a48581fb65c0ae469d5739839a4a84c00d0eb6e5ab945f725479d74189362
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 48c1c5552b5fa0fc207e7c91aa362e8f22f891edd8ba1593f97bcb236703633a

Exodus威胁情报

名称	分类	URL链接
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

硬编码敏感信息

可能的敏感信息
"type_certificate" : "证书"

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.MANUFACTURER check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
device ID check
subscriber ID check
possible ro.secure check
emulator file 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>