MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

安心住民宿PMS 3.6.0.APK

APP名称:	安心住民宿PMS
包名:	anxinzhu.pms
域名线索:	20条
URL线索:	17条
邮箱线索:	0条
分析日期:	2022年1月26日 18:46

文件信息

文件名: axzmsPMS.apk
文件大小: 3.83MB
MD5值: 21805a86b335f55203eecd105e90a526
SHA1值: a482ead43369adfaf810bd331dd309e0159c9b26
SHA256值: fd4a658935e055492b30eab7f88b260b8219b30b58ddb0fc3defb1c54591961c

APP 信息

App名称: 安心住民宿PMS
包名: anxinzhu.pms
主活动**Activity:** cn.yododo.yddpms.ui.WelcomeActivity
安卓版本名称: 3.6.0
安卓版本: 360

域名线索

域名	是否危险域名	服务器信息
alog.umeng.co	good	没有服务器地理信息.
ditu.google.cn	good	**IP:** 220.181.174.226 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
developer.android.com	good	IP: 142.251.43.14 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
ex.umengcloud.com	good	IP: 110.75.96.12 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
ex.puata.info	good	IP: 110.75.96.12 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
oc.umeng.com	good	IP: 203.119.128.55 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
au.umeng.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
ex.mobmore.com	good	IP: 110.75.96.12 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
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
feedback.umeng.com	good	没有服务器地理信息.
schemas.android.com	good	没有服务器地理信息.
alog.umeng.com	good	IP: 106.11.86.69 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
maps.google.com	good	IP: 142.251.43.14 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
oc.umeng.co	good	没有服务器地理信息.
ce3e75d5.jpush.cn	good	IP: 183.232.58.242 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
weixin.yododo.cn	good	没有服务器地理信息.
www.anxinzhu.vip	good	IP: 47.105.146.114 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
au.umeng.co	good	没有服务器地理信息.
www.yododo.cn	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
schemas.polites.com	good	**IP:** 192.0.78.24 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.748425 **经度:** -122.413673 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://au.umeng.com/api/check_app_update	com/umeng/update/b.java
http://au.umeng.co/api/check_app_update	com/umeng/update/b.java
http://feedback.umeng.com/feedback	com/umeng/fb/a/b.java
http://feedback.umeng.com/feedback/reply	com/umeng/fb/a/b.java
http://feedback.umeng.com/feedback/feedbacks	com/umeng/fb/a/b.java
http://alog.umeng.com/app_logs	com/umeng/analytics/g.java
http://alog.umeng.co/app_logs	com/umeng/analytics/g.java
http://oc.umeng.com/check_config_update	com/umeng/analytics/g.java

URL信息	Url所在文件
http://oc.umeng.co/check_config_update	com/umeng/analytics/g.java
http://ex.puata.info/api/q?	com/umeng/newxp/net/b.java
http://ex.umengcloud.com/api/q?	com/umeng/newxp/net/b.java
http://ex.mobmore.com/api/q?	com/umeng/newxp/net/b.java
http://ex.puata.info/api/r?	com/umeng/newxp/net/a.java
http://ex.umengcloud.com/api/r?	com/umeng/newxp/net/a.java
http://ex.mobmore.com/api/r?	com/umeng/newxp/net/a.java
http://developer.android.com	com/umeng/newxp/view/aO.java
http://ex.mobmore.com/api/wap?sdk_version=	com/umeng/newxp/view/H.java
http://ex.puata.info	com/umeng/newxp/common/ExchangeConstants.java
http://ex.umengcloud.com	com/umeng/newxp/common/ExchangeConstants.java
http://ex.mobmore.com	com/umeng/newxp/common/ExchangeConstants.java
http://ex.mobmore.com/api/wap?	com/umeng/newxp/common/ExchangeConstants.java
http://ex.mobmore.com/api/wap?sdk_version=	com/umeng/newxp/common/g.java
http://schemas.android.com/apk/res/android	com/polites/android/GestureImageView.java

URL信息	Url所在文件
http://schemas.polites.com/android	com/polites/android/GestureImageView.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/al/c.java
http://weixin.yododo.cn/hotel/detail.do?hotelId=	cn/yododo/yddpms/ui/weidian/WeidianActivity.java
http://ditu.google.cn/maps/geo?output=csv&key=abcdef&q=%s,%s	cn/yododo/yddpms/utils/MathUtils.java
http://maps.google.com/maps/geo?q=	cn/yododo/yddpms/utils/MathUtils.java
http://maps.google.com/maps/api/geocode/json?latlng=%s,%s&language=zh-CN&sensor=false	cn/yododo/yddpms/utils/MathUtils.java
http://www.anxinzhu.vip:9984	cn/yododo/yddpms/utils/Constant.java
http://www.yododo.cn/hotel/events/mjump.html	cn/yododo/yddpms/utils/Constant.java
https://api.weixin.qq.com/sns/oauth2/access_token	cn/yododo/yddpms/utils/Constant.java
https://api.weixin.qq.com/sns/userinfo	cn/yododo/yddpms/utils/Constant.java
https://api.weixin.qq.com/sns/oauth2/refresh_token	cn/yododo/yddpms/utils/Constant.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_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_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_COARSE_UPDATES	未知	Unknown permission	Unknown permission from android reference
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.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

向手机申请的权限	是否危险	类型	详细情况
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_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.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.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_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.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.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.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.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
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
cn.yododo.yddpms.permission.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
cn.yododo.yddpms.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.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.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

向手机申请的权限	是否危险	类型	详细情况
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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=天津, L=天津, O=安心住, OU=天津安心住酒店管理有限公司, CN=安心住
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-07-03 14:51:01+00:00
Valid To: 2045-06-27 14:51:01+00:00
Issuer: C=CN, ST=天津, L=天津, O=安心住, OU=天津安心住酒店管理有限公司, CN=安心住
Serial Number: 0x33344098
Hash Algorithm: sha256
md5: 3533d34299e05f3ed6c1fc39e0ed9f45
sha1: ed8f377b478a5238ee8e787a2eba009e03f3f3b4
sha256: c3f679d5bab4af1d270e8eb2ebe2226d07b4d953e2b224f257a362a2cb414a1f
sha512: 204248af9d612190cda373d377017e77d57a75e8e75ac4b548fc46575d4dbec041d7af680f733629a3a75f3367fc74d77546c843d315c97fd5c0acb352961bae
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 1b491ad68e40a8ba9d16e89b06bfa0f617c1f52d973b97d329dc37ed9d201e4e

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
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Umeng Feedback		https://reports.exodus-privacy.eu.org/trackers/120

硬编码敏感信息

可能的敏感信息
"modify_password" : "修改密码"
"private_vip" : "隐私政策"
"toast_pwd" : "请输入密码"
"toast_user" : "请输入账号"
"user_name" : "用户名:"
"user_password" : "密码:"

应用内通信

活动(ACTIVITY)	通信(INTENT)
cn.yododo.yddpms.ui.WelcomeActivity	Schemes: http://, Hosts: www.yododo.cn, Path Prefixes: /hotel/events/mjump_02.html,

加壳分析

文件列表	分析结果
classes.dex	<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 network operator name check device ID check subscriber ID check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>