MoGua

智能工厂 1.0.67.APK 分析报告

APP名称:	智能工厂
包名:	com.cordova.ifapp
域名线索:	18条
URL线索:	19条
邮箱线索:	1条
分析日期:	2022年9月26日
分析平台:	摸瓜反编译平台

文件信息

文件名: 1.0.67.apk
文件大小: 15.96MB
MD5值: 7fcf0ab7320cde05c52e48eac7572a2d
SHA1值: 66c30f498931327bd5782d353d33f7e062cb75b5
SHA256值: f08078ba4ef71a4d283cc2a6504589bec9e3d71dc8e354457e45dbc4e0e5cd73

APP 信息

App名称: 智能工厂
包名: com.cordova.ifapp
主活动**Activity:** com.cordova.ifapp.MainActivity
安卓版本名称: 1.0.67
安卓版本: 100673

域名线索

域名	服务器信息
tbsrecovery.imtt.qq.com	**IP:** 109.244.244.237 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

域名	服务器信息
soft.tbs.imtt.qq.com	**IP:** 121.51.175.105 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
tts.baidu.com	**IP:** 111.206.208.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
s3.amazonaws.com	**IP:** 52.217.80.230 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488
yuyin.baidu.com	**IP:** 153.3.236.85 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777779

域名	服务器信息
pms.mb.qq.com	**IP:** 109.244.173.227 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
cfg.imtt.qq.com	**IP:** 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
www.qq.com	**IP:** 175.27.8.138 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
mqqad.html5.qq.com	**IP:** 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

域名	服务器信息
debugx5.qq.com	**IP:** 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
vop.baidu.com	**IP:** 111.206.209.68 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
vse.baidu.com	**IP:** 111.206.208.71 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
log.tbs.qq.com	**IP:** 109.244.244.37 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

域名	服务器信息
mdc.html5.qq.com	**IP:** 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
openapi.baidu.com	**IP:** 110.242.69.36 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
ce3e75d5.jpush.cn	**IP:** 183.232.58.242 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
upl.baidu.com	**IP:** 111.206.208.71 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

域名	服务器信息
debugtbs.qq.com	**IP:** 175.27.9.46 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232

URL线索

URL信息	Url所在文件
www.qq.com	com/tencent/smtt/sdk/m.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/m.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.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

URL信息	Url所在文件
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/n.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
https://upl.baidu.com/voice?osname=voiceopen&action=usereventflow&	com/baidu/tts/e/a.java
https://tts.baidu.com/text2audio	com/baidu/tts/f/o.java
https://tts.baidu.com/bos/story.php?	com/baidu/tts/f/o.java
https://upl.baidu.com/ttsdlstats.php	com/baidu/tts/f/o.java
https://openapi.baidu.com/oauth/2.0/token?	com/baidu/tts/auth/c.java
https://vse.baidu.com/v2	com/baidu/speech/asr/SpeechConstant.java

URL信息	Url所在文件
https://vse.baidu.com/echo.fcgi	com/baidu/speech/asr/SpeechConstant.java
https://upl.baidu.com//words/add	com/baidu/speech/asr/SlotControl.java
https://yuyin.baidu.com/voice?osname=voiceopen&action=usereventflow&	com/baidu/speech/utils/analysis/Analysis.java
https://vop.baidu.com/v2	com/baidu/speech/core/ASREngine.java
https://s3.amazonaws.com/android-beacon-library/android-distance.json	org/altbeacon/beacon/BeaconManager.java
https://www.	org/altbeacon/beacon/utils/UrlBeaconUrlCompressor.java
http://www.	org/altbeacon/beacon/utils/UrlBeaconUrlCompressor.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/al/c.java

邮箱线索

邮箱地址	所在文件
6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/arm64-v8a/libiconv.so

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=xian, L=china, O=am, OU=am, CN=am
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-06-27 04:50:24+00:00
Valid To: 2044-11-12 04:50:24+00:00
Issuer: C=86, ST=xian, L=china, O=am, OU=am, CN=am
Serial Number: 0x6e41b6be
Hash Algorithm: sha256
md5: 4ff0e39a0fc5e6382bf2684736b81def
sha1: 6c3a18699b6ee0f064cb4ca65ff846375be2289d
sha256: f6edb8bf94ebab1180f56067c3039009383d144fb07f183e40c3dbd7c89cc009
sha512: e9726a28e2afd0ee8542c5a5419ca4263d85702534214db6fdc69d267741e7bff6df0b5b7abbb73f5b75d878d6e02980647d3884e1749ec5f6670c2e4fc44d82
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6c9c3319547c31fa6b0defaf7fe2eb958de86f13debf2224751f6f8d431d74a4

硬编码敏感信息

加壳分析

第三方SDK

名称	分类	URL链接
AltBeacon		https://reports.exodus-privacy.eu.org/trackers/219
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

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.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
com.cordova.ifapp.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_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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器

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
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.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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.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.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
com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信

向手机申请的权限	是否危险	类型	详细情况
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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.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
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.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.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.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
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。

向手机申请的权限	是否危险	类型	详细情况
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。
com.huawei.android.launcher.permission.READ_SETTINGS	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
com.huawei.android.launcher.permission.WRITE_SETTINGS	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
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.cordova.ifapp.MainActivity	Schemes: ifapp://, https://, Hosts: www.kshzn.net, Path Patterns: /ifapp/.*,