MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

小明排班 1.0.APK

APP名称:	小明排班
包名:	com.shandong.xs.paiban
域名线索:	3条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年2月3日 12:44

文件信息

文件名: xiaomingpaiban.apk

文件大小: 8.95MB
MD5值: fed3cafa9276bb984b56e2b394878c8d
SHA1值: a71086727b4009cb9aca80f36c8c1512993331f4
SHA256值: 26b8102fbd5a793b2e05c4339293f9e05caa02ab4c8e98ee6a3faf1d83d6cf43

APP 信息

App名称: 小明排班
包名: com.shandong.xs.paiban
主活动**Activity:** com.shandong.xs.paiban.ym.YSZCActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
appgallery.cloud.huawei.com	good	**IP:** 117.78.15.51 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
store.hispace.hicloud.com	good	**IP:** 49.4.44.164 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
play.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

URL线索

URL信息	Url所在文件
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	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

向手机申请的权限	是否危险	类型	详细情况
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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_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_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.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_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.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.READ_SETTINGS	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

向手机申请的权限	是否危险	类型	详细情况
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.SET_ALARM	正常	在闹钟中设置闹钟	允许应用程序在已安装的闹钟应用程序中设置闹钟。某些闹钟应用程序可能无法实现此功能
android.permission.NOTIFICATION_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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.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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	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
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
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.shandong.xs.paiban.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.shandong.xs.paiban.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.shandong.xs.paiban.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.shandong.xs.paiban.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	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.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.shandong.xs.paiban.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=bu
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-02-26 14:22:43+00:00
Valid To: 2042-02-20 14:22:43+00:00
Issuer: CN=bu
Serial Number: 0x433f000d
Hash Algorithm: sha256

md5: 7ba3c13f5af15c9fffb29882570b1aa1
sha1: ee469b1865a12514a4566f019d01c303e631b4e8
sha256: 3188f09cf1d2727cfa90798f9a5be4d21868fb7418ccce8fbac3ea008b5c90de
sha512: 89ab26fac1f2e1e424fdc0c95c3a1339b1eaf7a96b48b880261fecfa4b9fa399b0d838108f031df6ce7d7e8d06f9bfc126eeac031ec0794b49ae562489f45881
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 111a59303997915e6f390501924a1069eee68c755fb15086a31dd820500720e0

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.shandong.xs.paiban.mfr.MfrMessageActivity	Schemes: agoo://, Hosts: com.shandong.xs.paiban, Paths: /thirdpush,

加壳分析

文件列表	分析结果
APK包	壳列表 / 详细情况 打包 / Jiagu
classes.dex	壳列表 / 详细情况 编译器 / dexlib 2.x