MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

打卡提醒 1.0.0.APK

APP名称:	打卡提醒
包名:	com.weixikeji.clockreminder
域名线索:	3条
URL线索:	3条
邮箱线索:	0条
分析日期:	2022年2月2日 19:43

文件信息

文件名: dktx.apk
文件大小: 10.13MB
MD5值: 21c239b91cc5e21ce3d5e392f9994bcd
SHA1值: 365ba81169748d9044fdb3e12a5194574a6c0eea
SHA256值: 9c547cc3a442f28b6a9a0e41223777cfbc7abc898ae5f6be2e0b3882c822eba0

APP 信息

App名称: 打卡提醒
包名: com.weixikeji.clockreminder
主活动**Activity:** com.weixikeji.clockreminder.activity.SplashActivity
安卓版本名称: 1.0.0
安卓版本: 100

域名线索

域名	是否危险域名	服务器信息
www.hzweixi.cn	good	**IP:** 101.37.119.95 **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
errlog.umeng.com	good	**IP:** 106.8.130.60 **所属国家:** China **地区:** Hebei **城市:** Zhangjiakou **纬度:** 40.810001 **经度:** 114.879440 **查看地图:** Google Map
errlogos.umeng.com	good	**IP:** 47.246.110.18 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://www.hzweixi.cn/quanduoduo	Android String Resource
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi/libcrashsdk.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.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.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_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

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.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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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_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_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.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.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.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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
com.weixikeji.clockreminder.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=hangzhou, ST=zhejiang, L=china, O=weixi, OU=weixi, CN=xufang
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-01-01 13:31:06+00:00
Valid To: 2042-12-26 13:31:06+00:00
Issuer: C=hangzhou, ST=zhejiang, L=china, O=weixi, OU=weixi, CN=xufang
Serial Number: 0x2a45e658
Hash Algorithm: sha256
md5: 82fdf3f8f341efb1e95b7473f3525c01
sha1: 7b56f5f4bc48c08396e8df5ff500d46100d96834
sha256: 8af7c9996e5f3ace23337960e28cec5f25ce886ba518003e4f2f96babe71ccd9
sha512: c4e7dca31cca3ab4475e33dcf0dffcf87cc6e22717095d2fb83298717c94e01176e10cc4bc5a058695211decc990e59640e712e4292eb22e22ede870fcd855bf
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4b29a8a2c44d098ff4143a3c66478b46b051dd0c8009951584a1e2dfaa1994bc

硬编码敏感信息

可能的敏感信息
"feedback_app_key" : "ce14032d747129b04779c763b6218503"
"feedback_qq_not_installed_or_api_not_support" : "您还未安装手机QQ或版本不支持"
"need_auth_to_use" : "抱歉，该功能仅限VIP会员用户使用"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent100424468://, tencent101963624://,

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
