




APP线索分析报告

报告由 [摸瓜APP分析平台\(mogua.co\)](http://mogua.co) 生成



 Many优惠券 1.0.4.APK

APP名称:	Many优惠券
包名:	com.weili.wtcouponapp
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2022年1月22日 23:21

文件名: manyyhq413759.apk
文件大小: 7.33MB
MD5值: 658d4b50e9d81503c962084534c4e51f
SHA1值: b9e280e7bdeb70581ae7d455e887848f826178df
SHA256值: 4dff350f450b7d8b08fc2a2421aa897422851d4f09e33831bb09a7a39bdc9f15

i APP 信息

App名称: Many优惠券
包名: com.weili.wtcouponapp
主活动Activity: com.weili.wtcouponapp.ui.WelComeActivity
安卓版本名称: 1.0.4
安卓版本: 4

☰ 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.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_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

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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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.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.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.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_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_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.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.RUN_INSTRUMENTATION	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: C=CN, L=XM, OU=ywl, CN=wl

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2018-10-24 07:24:05+00:00

Valid To: 2043-10-18 07:24:05+00:00

Issuer: C=CN, L=XM, OU=ywl, CN=wl

Serial Number: 0x78a76c4d

Hash Algorithm: sha256

md5: 214ca664b8e0bcfec3337066e089f14

sha1: 1640ef7b2fa660e0cf6379cc6ccc312360c6a25f

sha256: 2acdfe160d02a7e991aa420d03afcb361113ce9cdfe6bf968e547bef43e22182

sha512: 2317cb3502e598e6de2f838243c99c320cfa6aed6c6278d47c39c5af8e5131bf6aa39aead8cb01e79db9e5fb2c4eaa635fe5bf2691ae23ca0f9a0215e2db7259

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: cd2a7e71bbf987fc87615fb307af8a07d10976e9154a96438439d9df5144526b

硬编码敏感信息

可能的敏感信息
"com_alibc_auth_actiivty_auth_ok": "确认授权"
"com_alibc_auth_actiivty_cancel": "取消"
"com_alibc_auth_actiivty_get": "获取"
"com_taobao_tae_sdk_authorize_title": "登录授权"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.alibaba.baichuan.android.trade.ui.AlibcBackActivity	Schemes: alisdk://,

加壳分析

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

文件列表	分析结果						
lib/arm64-v8a/libsgmain.so!classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>subscriber ID check</td></tr><tr><td>编译器</td><td>dx</td></tr></table>	壳列表	详细情况	反虚拟机	subscriber ID check	编译器	dx
壳列表	详细情况						
反虚拟机	subscriber ID check						
编译器	dx						
lib/arm64-v8a/libsgmain.so!lib/arm64-v8a/libsgmainso-5.1.81.so	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr></table>	壳列表	详细情况	模糊器	Obfuscator-LLVM version 3.4		
壳列表	详细情况						
模糊器	Obfuscator-LLVM version 3.4						
lib/armeabi-v7a/libsgmain.so!classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>subscriber ID check</td></tr><tr><td>编译器</td><td>dx</td></tr></table>	壳列表	详细情况	反虚拟机	subscriber ID check	编译器	dx
壳列表	详细情况						
反虚拟机	subscriber ID check						
编译器	dx						
lib/armeabi-v7a/libsgmain.so!lib/armeabi-v7a/libsgmainso-5.1.81.so	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr></table>	壳列表	详细情况	模糊器	Obfuscator-LLVM version 3.4		
壳列表	详细情况						
模糊器	Obfuscator-LLVM version 3.4						

文件列表	分析结果						
lib/armeabi/libsgmain.so!classes.dex	<table><tr><td>壳列表</td><td>详细情况</td></tr><tr><td>反虚拟机</td><td>subscriber ID check</td></tr><tr><td>编译器</td><td>dx</td></tr></table>	壳列表	详细情况	反虚拟机	subscriber ID check	编译器	dx
壳列表	详细情况						
反虚拟机	subscriber ID check						
编译器	dx						
lib/armeabi/libsgmain.so!lib/armeabi/libsgmainso-5.1.81.so	<table><tr><td>壳列表</td><td>详细情况</td></tr><tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr></table>	壳列表	详细情况	模糊器	Obfuscator-LLVM version 3.4		
壳列表	详细情况						
模糊器	Obfuscator-LLVM version 3.4						
lib/x86/libsgmain.so!classes.dex	<table><tr><td>壳列表</td><td>详细情况</td></tr><tr><td>反虚拟机</td><td>subscriber ID check</td></tr><tr><td>编译器</td><td>dx</td></tr></table>	壳列表	详细情况	反虚拟机	subscriber ID check	编译器	dx
壳列表	详细情况						
反虚拟机	subscriber ID check						
编译器	dx						
lib/x86/libsgmain.so!lib/x86/libsgmainso-5.1.81.so	<table><tr><td>壳列表</td><td>详细情况</td></tr><tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr></table>	壳列表	详细情况	模糊器	Obfuscator-LLVM version 3.4		
壳列表	详细情况						
模糊器	Obfuscator-LLVM version 3.4						

文件列表	分析结果						
lib/x86_64/libsgmain.so!classes.dex	<table><tr><td>壳列表</td><td>详细情况</td></tr><tr><td>反虚拟机</td><td>subscriber ID check</td></tr><tr><td>编译器</td><td>dx</td></tr></table>	壳列表	详细情况	反虚拟机	subscriber ID check	编译器	dx
壳列表	详细情况						
反虚拟机	subscriber ID check						
编译器	dx						
lib/x86_64/libsgmain.so!lib/x86_64/libsgmainso-5.1.81.so	<table><tr><td>壳列表</td><td>详细情况</td></tr><tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr></table>	壳列表	详细情况	模糊器	Obfuscator-LLVM version 3.4		
壳列表	详细情况						
模糊器	Obfuscator-LLVM version 3.4						

报告由 [摸瓜平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。

[查诈骗APP](#) | [查木马APP](#) | [违法APP分析](#) | [APK代码分析](#)