



APP线索分析报告

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



 中质物联 1.01.APK

APP名称:	中质物联
包名:	com.ct.hzjtbase
域名线索:	1条
URL线索:	12条
邮箱线索:	0条
分析日期:	2022年2月3日 13:32

文件名: zhongzhiwulian.apk
文件大小: 2.95MB
MD5值: 04187971143c585d71ad4da92974acee
SHA1值: 6305d4a573c6915343964a4df30578e3f295cb8b
SHA256值: f762697a7b52d8c8c54619b5d448439757ba68e3c6246a70a3f5aff984405a42

i APP 信息

App名称: 中质物联
包名: com.ct.hzjtbase
主活动Activity: com.ct.hzjtbase.LoginActivity
安卓版本名称: 1.01
安卓版本: 2

🔍 域名线索

域名	是否危险域名	服务器信息
sz.songhuang-tea.com	good	IP: 47.112.147.133 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

🌐 URL 线索

URL信息	Url所在文件
https://sz.songhuang-tea.com/core/v1/scanner/addgoodsreturn	com/ct/hzjtbase/BackkOrderActivity.java
https://sz.songhuang-tea.com/core/v1/scanner/updategoodsreturn	com/ct/hzjtbase/BackkOrderActivity.java
https://sz.songhuang-tea.com/core/v1/scanner/goodsreturnscantag	com/ct/hzjtbase/BackkOrderActivity.java
https://sz.songhuang-tea.com/core/v1/tag/decodetagno?tagCode=	com/ct/hzjtbase/BackkOrderActivity.java
https://sz.songhuang-tea.com/core/v1/sysstaff/logout	com/ct/hzjtbase/MainActivity.java
https://sz.songhuang-tea.com/core/v1/production/rework/getpendingreworks	com/ct/hzjtbase/ReturnOrderListActivity.java
https://sz.songhuang-tea.com/core/v1/product/getproducts	com/ct/hzjtbase/ReturnOrderListActivity.java
https://sz.songhuang-tea.com/core/v1/production/rework/submitrework	com/ct/hzjtbase/ReturnOrderActivity.java
https://sz.songhuang-tea.com/core/v1/production/rework/confirmscantag?tagCode=	com/ct/hzjtbase/ReturnOrderActivity.java
https://sz.songhuang-tea.com/core/v1/scanner/getpendingoutstocks	com/ct/hzjtbase/OrderListActivity.java
https://sz.songhuang-tea.com/core/v1/scanner/getpendingoutstockbycouriernumber?courierNumber=	com/ct/hzjtbase/OrderListActivity.java
https://sz.songhuang-tea.com/core/v1/inventory/inventoryscantag	com/ct/hzjtbase/CheckOrderActivity.java
https://sz.songhuang-tea.com/core/v1/inventory/completeinventory	com/ct/hzjtbase/CheckOrderActivity.java
https://sz.songhuang-tea.com/core/v1/production/rework/addrework	com/ct/hzjtbase/NewReturnOrderActivity.java
https://sz.songhuang-tea.com/core/v1/production/rework/reworkscantag?tagCode=	com/ct/hzjtbase/NewReturnOrderActivity.java

URL信息	Url所在文件
https://sz.songhuang-tea.com/core/v1/inventory/getpendinginventoryplans	com/ct/hzjtbase/CheckOrderListActivity.java
https://sz.songhuang-tea.com/core/v1/scanner/getpendinggoodsreturns	com/ct/hzjtbase/BcakOrderListActivity.java
https://sz.songhuang-tea.com/core/v1/scanner/outstockscantag	com/ct/hzjtbase/OrderActivity.java
https://sz.songhuang-tea.com/core/v1/scanner/submitoutstockitems	com/ct/hzjtbase/OrderActivity.java
https://sz.songhuang-tea.com/core/v1/tag/decodetagno?tagCode=	com/ct/hzjtbase/OrderActivity.java
https://sz.songhuang-tea.com/core/v1/sysstaff/login	com/ct/hzjtbase/LoginActivity.java
https://sz.songhuang-tea.com/core	com/ct/hzjtbase/util/Constants.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

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
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
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.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.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.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.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.WRITE_SETTING	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

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: O=j, OU=j, CN=w
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-23 06:11:21+00:00
Valid To: 2045-11-17 06:11:21+00:00
Issuer: O=j, OU=j, CN=w
Serial Number: 0x7a95a394
Hash Algorithm: sha256
md5: f2cde2d763cd9337202ba8662a5287bc
sha1: 5cc57bf6585c1928f8c98a4df2094f09afca623f
sha256: 4255f115e23dd5cf8d732d8971764c99ee13c9e6ddddd73730919e748a41143d
sha512: edddf15fc68dd1d6a27f0557d200b579d5c61008dfd416f8896f92b8cfbd1d33da7af0abe9b0a7c401df721141fa031af28d7aa8f0e6a2d74f1236811d3dd7e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a69d41ba3f0ac473dc64edb4d2cde626dcad728cd4d9b32865c3f13a82678fdb

加壳分析

文件列表	分析结果	
classes.dex	壳列表	详细情况
	反虚拟机	Build.FINGERPRINT check Build.MANUFACTURER check
	编译器	r8

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