MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

多宝掌柜 1.1.0.APK

APP名称:	多宝掌柜
包名:	cn.trechina.duobao.industry
域名线索:	1条
URL线索:	1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: duobaozhanggui589946.apk
文件大小: 8.14MB
MD5值: 9a5fd6e0c3c837482c57e7363bca0c3d
SHA1值: 995437192849b806ea9b7f32cf9ffe05127a80a3
SHA256值: fd307696954070b52fb96d36ad1f77f339cd893ea195aa4e2f845ba36e8a5014

APP 信息

App名称: 多宝掌柜
包名: cn.trechina.duobao.industry
主活动**Activity:** cn.trechina.duobao.industry.MainActivity
安卓版本名称: 1.1.0
安卓版本: 10100

域名线索

域名	是否危险域名	服务器信息
192.168.3.102	good	**IP:** 192.168.3.102 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://192.168.3.102:8080/update_apk/version.xml	com/vaenow/appupdate/android/UpdateManager.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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_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
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.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.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

向手机申请的权限	是否危险	类型	详细情况
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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=china, ST=sd, L=yt, O=duobao, OU=trechina, CN=dev
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-12-21 01:10:42+00:00
Valid To: 2032-12-03 01:10:42+00:00
Issuer: C=china, ST=sd, L=yt, O=duobao, OU=trechina, CN=dev
Serial Number: 0x3567dd92
Hash Algorithm: sha256
md5: f854d6ca78434379a2b85669eb585f90
sha1: 98e56ba9f04c328daa0d10c7e43b6fa7cca13cd7
sha256: 12d70468b95683c94b1a9a2ddf8a65399434ecc81f4c8b677b6583c3411b4a79
sha512: c3b9b8e26b7a7ac6799cbd7a5c0e0a0787083f0298b2d4147700918e932b5a20580305ad0b21b00e0f9708035155812a2021e5b23a58ddc700634dd7d37eddbb

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
