MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

兑好物 2.004.APK

APP名称:	兑好物
包名:	com.duigood.dshopscj
域名线索:	3条
URL线索:	3条
邮箱线索:	0条
分析日期:	2022年1月25日 21:41

文件信息

文件名: duihaowu.apk
文件大小: 2.21MB
MD5值: ac0a757aa9993cd9d71a6680779305a8
SHA1值: 5e5d6da6d1524d1b4fc9673fdf872d849b1c45b4
SHA256值: ca25c2c169e3260d26292c082ec81a855316ad6e63f1ba72aeb1660192276867

APP 信息

App名称: 兑好物
包名: com.duigood.dshopscj
主活动**Activity:** com.dui.goodshop.MainActivity1
安卓版本名称: 2.004
安卓版本: 2004

域名线索

域名	是否危险域名	服务器信息
d.alipay.com	good	**IP:** 203.209.245.120 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
schemas.android.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
hwxs.towshop.cn	good	**IP:** 116.62.196.45 **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

URL线索

URL信息	Url所在文件
http://hwxs.towshop.cn/index.html#/account?env=android	com/dui/goodshop/MainActivity1.java
https://d.alipay.com	b/b/a/a/a.java
http://schemas.android.com/apk/res/android	a/b/k/k.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.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_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.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.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_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.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。

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=334622, ST=HZ, L=ZJ, O=CN, OU=ZhongJian, CN=ZhongJian
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-07-27 03:15:32+00:00
Valid To: 2121-07-03 03:15:32+00:00

Issuer: C=334622, ST=HZ, L=ZJ, O=CN, OU=ZhongJian, CN=ZhongJian
Serial Number: 0x3241b60b
Hash Algorithm: sha256
md5: 38ccf5d78a1416ba520fac26f2684408
sha1: 49a6f31a80e18b140f77b7edc5e5b9bb300c9b7e
sha256: fb390de3059b17b889c473407bfeafbcb2cddfbc88909d896f68dfcbf6efe473
sha512: 67fcba74ac686efd51635419b88caf024e95f37920abd9916c05215eb258181ca7791b886e43fc8afe744635df5ce5388b46aeecbe620ff42ca03c8b81149437

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.MANUFACTURER check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
