MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

店铺管理 1.13.APK

APP名称:	店铺管理
包名:	com.kyb.seller
域名线索:	15条
URL线索:	12条
邮箱线索:	0条
分析日期:	2022年2月2日 19:31

文件信息

文件名: dianpuguanli535782.apk
文件大小: 1.83MB
MD5值: 58854cc0cd3925a3c5daf7305e715ec7
SHA1值: 0ae8e1dd9d7dd03a21e09c0d7c113abd2e059106
SHA256值: eb6f427c707cd6f9af8401d6fcce7609abb5f281ebaa413c4cec6350833292e5

APP 信息

App名称: 店铺管理
包名: com.kyb.seller
主活动**Activity:** com.kyb.seller.SplashActivity
安卓版本名称: 1.13
安卓版本: 13

域名线索

域名	是否危险域名	服务器信息
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
mobilegw.alipaydev.com	good	**IP:** 110.75.132.131 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
kyb.vip	good	IP: 42.193.13.10 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
mobilegw.alipay.com	good	IP: 203.209.245.78 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
hydra.alibaba.com	good	IP: 203.119.169.88 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
www.cd-zq.com	good	IP: 8.129.180.254 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
mclient.alipay.com	good	IP: 203.209.250.6 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
mobilegw.stable.alipay.net	good	没有服务器地理信息.
wappaygw.alipay.com	good	IP: 203.209.250.6 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
mcgw.alipay.com	good	IP: 203.209.250.6 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
m.alipay.com	good	IP: 203.209.245.74 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
xmlpull.org	good	**IP:** 74.50.61.58 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map
h5.m.taobao.com	good	**IP:** 60.28.226.41 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res-auto	com/zq/core/view/RotateTextView.java
http://www.cd-zq.com/	com/zq/core/utils/Constants.java
http://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java

URL信息	Url所在文件
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
http://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/c.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&	com/alipay/sdk/data/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://kyb.vip/kyb_files/apk_update/	com/kyb/seller/MyApplication.java
http://hydra.alibaba.com/	com/ta/utdid2/aid/AidRequester.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/XmlUtils.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/FastXmlSerializer.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
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_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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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
com.cdzq.hongtu.permission.RECV_NETWORK_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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

向手机申请的权限	是否危险	类型	详细情况
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
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.GET_TOP_ACTIVITY_INFO	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
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证令牌
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.AUTHENTICATE_ACCOUNTS	危险	充当帐户验证器	允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码
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.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: ST=1, L=1, O=1, OU=1, CN=11
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-01-12 10:38:57+00:00
Valid To: 2065-12-30 10:38:57+00:00
Issuer: ST=1, L=1, O=1, OU=1, CN=11
Serial Number: 0x5e5a8a08
Hash Algorithm: sha256
md5: dbbaade17748ba1cde5dd5b2411786a7
sha1: cf3888aaae2e84e4a86873b8961c60d13b68cffe
sha256: bd3cc59f79c6e3caa0f649f7689aa34d8a47f9e751cb4150ea053050b72eefb1
sha512: ad4a42cf7a2bfb58b313d4d4db5056003c21ca46e07fe47d8a1d622034b10230f3e37b90f35aea7f3ddab5e166ab451974aac831181f6808b0b741c9dadb64d6

加壳分析

文件列表	分析结果

<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.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
device ID check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>模糊器</td><td>unreadable field names</td></tr>
</table>
</td></tr>
</table>