MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

RTHS展业 1.0.11.APK

APP名称:	RTHS展业
包名:	com.tangtang.pos
域名线索:	7条
URL线索:	6条
邮箱线索:	0条
分析日期:	2022年2月2日 22:24

文件信息

文件名: rthszy.apk
文件大小: 2.48MB
MD5值: 9c7a86a44e85ef7c2ca07124ce90df7f
SHA1值: 5785481b3e9b07d33631aa32830bfb63da575027
SHA256值: d0495aaafce07a6949ecd86001d687360579c9a4baef0d27d3c801796f745633

APP 信息

App名称: RTHS展业
包名: com.tangtang.pos
主活动**Activity:** com.tangtang.pos.LoginActivity
安卓版本名称: 1.0.11
安卓版本: 11

域名线索

域名	是否危险域名	服务器信息
cmnsguider.yunos.com	good	**IP:** 203.119.169.69 **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

域名	是否危险域名	服务器信息
api.bestmpos.com	good	**IP:** 47.100.9.83 **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
b.bestmpos.com	good	**IP:** 47.100.9.83 **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
uop.umeng.com	good	没有服务器地理信息.
alog.umengcloud.com	good	**IP:** 106.11.86.76 **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
log.umsns.com	good	**IP:** 59.82.60.44 **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
alog.umeng.com	good	**IP:** 59.82.29.246 **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
http://api.bestmpos.com/	com/tangtang/f/c.java
http://b.bestmpos.com/wap/InVist/Index.aspx?u=	com/tangtang/pos/AddFriendsActivity.java
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umengcloud.com/app_logs	com/umeng/analytics/a.java
https://uop.umeng.com	com/umeng/analytics/a.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/analytics/c/p.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java
http://log.umsns.com/	com/umeng/analytics/social/d.java

URL信息	Url所在文件
http://log.umsns.com/share/api/	com/umeng/analytics/social/d.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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_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。

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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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.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: True
v3 signature: False
Found 1 unique certificates
Subject: C=xxx, ST=xxx, L=xxx, O=xxx, OU=XXX, CN=LiXinTang
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-01-07 09:35:14+00:00
Valid To: 2044-01-01 09:35:14+00:00
Issuer: C=xxx, ST=xxx, L=xxx, O=xxx, OU=XXX, CN=LiXinTang
Serial Number: 0x29ea4dd8
Hash Algorithm: sha256
md5: 42643f2260467585a65971707ec79a05
sha1: af3090a159bff52d6d6ac16ea4cf35067807885a
sha256: d3c5ad168a69e769a035b3d8aac828cf04a52c85ffe4e27031d911bc2444456b
sha512: 1eb2c15ac97ee3ba2266bb3e9329dc3ac84079dadfc74cbf352f1321847ef7af4d5ff7abefbc1c838a3dda26440aa3f44fee91a92d1abb438fc8c8dae45f9666
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 817e5034b4c039890e34711228789c27ba8bf50e153699dc6b4b20c37f8fd032

Exodus威胁情报

名称	分类	URL链接
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

加壳分析

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check network operator name check subscriber ID check</td></tr><tr><td>编译器</td><td>dx</td></tr></table>
