MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

易宝支付 2.0.APK

APP名称:	易宝支付
包名:	com.zhongsou.qyappzym
域名线索:	11条
URL线索:	7条
邮箱线索:	0条
分析日期:	2022年2月2日 14:58

文件信息

文件名: yibaozhifu.apk
文件大小: 1.62MB
MD5值: e3408b9f84021b4cfb5a656b0476b834
SHA1值: cbc36037bd7043575d5db60df119312c057a98c2
SHA256值: 252455c0568582980f1c189a0acb9825908e8f020da6899b38b0f2cffeb7f706

APP 信息

App名称: 易宝支付
包名: com.zhongsou.qyappzym
主活动**Activity:** com.zhongsou.mobile_ticket.activity.StartActivity
安卓版本名称: 2.0
安卓版本: 14093013

域名线索

域名	是否危险域名	服务器信息
ds.mapabc.com	good	没有服务器地理信息.
restapi.amap.com	good	**IP:** 203.119.175.194 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
tm.mapabc.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
pigimg.zhongso.com	good	**IP:** 202.108.1.39 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.zhongsou.net	good	**IP:** 47.91.170.222 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692 查看地图: Google Map
uid.zhongsou.net	good	**IP:** 47.91.170.222 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692 查看地图: Google Map
mst01.is.autonavi.com	good	**IP:** 203.119.211.251 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
m.amap.com	good	**IP:** 59.82.60.45 **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
tmds.mapabc.com	good	没有服务器地理信息.
webrd01.is.autonavi.com	good	**IP:** 140.249.61.194 **所属国家:** China **地区:** Shandong **城市:** Qingdao **纬度:** 36.098610 **经度:** 120.371941 **查看地图:** Google Map
aps.amap.com	good	**IP:** 59.82.31.156 **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://aps.amap.com/APS/r	com/autonavi/aps/api/Constant.java
http://webrd01.is.autonavi.com	com/amap/api/location/core/j.java
http://tm.mapabc.com	com/amap/api/location/core/j.java
http://restapi.amap.com	com/amap/api/location/core/j.java
http://ds.mapabc.com:8888	com/amap/api/location/core/j.java
http://mst01.is.autonavi.com	com/amap/api/location/core/j.java
http://tmds.mapabc.com	com/amap/api/location/core/j.java
http://restapi.amap.com/log/init	com/amap/api/a/f.java
http://m.amap.com	com/amap/api/a/a.java
http://restapi.amap.com	com/amap/api/search/core/k.java
http://www.zhongsou.net/space/interface/ydcp_getBranch.php?kw=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/space/interface/ydcp_getBranch.php?getaddr=1&kw=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/space/interface/ydcp_getBranch.php?getscnt=1&kw=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/space/interface/ydcp_getBranch.php?gettel=1&kw=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/np/mobile?t=catelist&key=	com/zhongsou/config/UrlConfig.java

URL信息	Url所在文件
http://www.zhongsou.net/space/interface/ydcp_getSections.php?kw=	com/zhongsou/config/UrlConfig.java
http://uid.zhongsou.net/soaweb/handler.aspx?apikey=ba5169615c854abf9516fc492a566f1c&method=people.get&type=m&userid=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/space/interface/ydcp_homepagedata.php?t=android&kw=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/space/interface/searchInfosByKw.php?cn=10&kw=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/space/interface/getInfoById.php?kw=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/np/mobile?t=list&app=s&ig=	com/zhongsou/config/UrlConfig.java
http://www.zhongsou.net/np/mobile?t=detail&app=s&fmt=json&id=	com/zhongsou/config/UrlConfig.java
http://pigimg.zhongso.com/space/gallery/2013/04/08/19/b2b_20130308072901995119_120.png	com/zhongsou/model/IndexData_Products.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.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.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.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.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.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.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.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.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_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_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: CN=app_release
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-07-01 09:51:57+00:00
Valid To: 2113-06-07 09:51:57+00:00
Issuer: CN=app_release
Serial Number: 0x51d1513d
Hash Algorithm: sha1
md5: cd32c64efab4bb29a1ff29af165dc781
sha1: b46237abcf02a84fadc4c9a690114d1275171cbd
sha256: 38c98b5ba92665c6eda21f03d983e7c16219a343152f1e6734b5c29ac2ff039b
sha512: 31c3163a97e07818db446ba4cb432227ad8538fc20e0b589402421aabd05aca70cad1b2b578afea1aa21c204aceaa07923e2b5b84305a0060d29be3040c42b49

Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机 / subscriber ID check 编译器 / dx (possible dexmerge) Manipulator Found / dexmerge

---