

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♠ 汇森速运 v2.1.0.APK

APP名称: 汇森速运

包名: cn.com.longbang.kdy.huisen

域名线索: 56条

URL线索: 43条

邮箱线索: 1条

分析日期: 2022年1月26日 18:58

文件名: huissy.apk 文件大小: 5.66MB

MD5值: 7cd264faafb39c0d64e658f224e413a9

SHA1值: 5841323090ba089f2056a6ed9ac15d055330b319

\$HA256值: 283ac3dc37d274e2a3ee356d6f2cf1c7fec42fd48cfce430e664ec6d09e1cbfa

i APP 信息

App名称: 汇森速运

包名: cn.com.longbang.kdy.huisen

主活动**Activity:** cn.com.longbang.kdy.ui.activity.LaunchActivity

安卓版本名称: v2.1.0

安卓版本: 210

0 域名线索

域名	是否危险域名	服务器信息
ulogs.umeng.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

域名	是否危险域名	服务器信息
lbzb1103.3322.org	good	IP: 222.69.151.58 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061 查看地图: Google Map
fusion.qq.com	good	IP: 121.51.36.15 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
test.lborder.mlick.cn	good	没有服务器地理信息.
openmobile.qq.com	good	IP: 113.96.208.233 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
liuyan.lbscm.com.cn	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
vip.lbzhilian.com	good	IP: 101.133.165.83 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
ddlogin.longbangcdn.com	good	IP: 42.157.195.19 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
apilocate.amap.com	good	IP: 59.82.31.183 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
pingma.qq.com	good	IP: 119.45.78.184 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
version.longbangcdn.com	good	IP: 42.157.195.51 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
alogus.umeng.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
lark.alipay.com	good	IP: 103.52.199.80 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
ouplog.umeng.com	good	IP: 47.74.172.6 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map

域名	是否危险域名	服务器信息
192.168.1.110	good	IP: 192.168.1.110 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
app.lbscm.net	good	没有服务器地理信息.
logs.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
alogsus.umeng.com	good	IP: 203.119.174.133 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: 203.209.255.248 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
www.huisenky.com	good	IP: 113.229.254.8 所属国家: China 地区: Liaoning 城市: Dandong 纬度: 40.129169 经度: 124.394722 查看地图: Google Map
k801.lbex.com.cn	good	IP: 42.157.195.62 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
open.weixin.qq.com	good	IP: 175.24.219.72 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
k901.lbex.com.cn	good	IP: 42.157.195.12 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map

域名	是否危险域名	服务器信息
h5.m.taobao.com	good	IP: 125.39.135.241 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
ulogs.umengcloud.com	good	IP: 106.11.86.69 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
abroad.apilocate.amap.com	good	IP: 59.82.39.53 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
hsgis.longbangcdn.com	good	IP: 47.116.100.115 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
restapi.amap.com	good	IP: 106.11.43.113 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
cgicol.amap.com	good	IP: 59.82.60.56 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
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
hsapp.longbangcdn.com	good	IP: 42.157.195.51 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map

域名	是否危险域名	服务器信息
apilocatesrc.amap.com	good	IP: 106.11.43.81 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: 203.209.250.50 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.
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
lbs.amap.com	good	IP: 59.82.29.155 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
c.isdspeed.qq.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
vip.huisenky.com	good	IP: 222.85.26.234 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613 查看地图: Google Map
developer.umeng.com	good	IP: 59.82.31.160 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.w3.org	good	IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge 纬度: 42.365078 经度: -71.104523 查看地图: Google Map
122.225.104.218	good	IP: 122.225.104.218 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
www.slf4j.org	good	IP: 83.166.144.67 所属国家: Switzerland 地区: Geneve 城市: Carouge 纬度: 46.180962 经度: 6.139210 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
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
a.lbex.com.cn	good	IP: 42.157.195.19 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
plbslog.umeng.com	good	IP: 59.82.43.171 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
127.0.0.1	good	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
long.open.weixin.qq.com	good	IP: 109.244.217.35 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
mta.oa.com	good	IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map
ddm.longbangcdn.com	good	IP: 122.225.104.205 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
appsetting.longbangcdn.com	good	IP: 122.225.105.103 所属国家: China 地区: Zhejiang 城市: Huzhou 纬度: 30.870300 经度: 120.093300 查看地图: Google Map
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
lbzhilian.com	good	IP: 47.116.133.173 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
cmnsguider.yunos.com	good	IP: 203.119.169.44 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
cgi.connect.qq.com	good	IP: 183.2.144.36 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
mta.qq.com	good	IP: 123.125.46.111 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://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&	com/alipay/sdk/b/b.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&	com/alipay/sdk/b/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/util/k.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/util/j.java
http://mcgw.alipay.com/sdklog.do	com/alipay/sdk/e/a/c.java

URL信息	Url所在文件
http://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/a/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/b/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/b/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/b/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/b/b/a.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://lark.alipay.com/yj131525/byt0wl/ufnf3i#A10200	com/umeng/commonsdk/statistics/internal/c.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://developer.umeng.com/docs/66632/detail/70018?um_channel=sdk	com/umeng/analytics/b.java

URL信息	Url所在文件
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
http://cgicol.amap.com/collection/writedata?ver=v1.0_ali&	com/loc/ax.java
http://restapi.amap.com/v3/geocode/regeo	com/loc/ax.java
http://logs.amap.com/ws/log/upload?product=%s&type=%s&platform=%s&channel=%s&sign=%s	com/loc/ct.java
http://restapi.amap.com	com/loc/cp.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/bq.java
https://restapi.amap.com/v3/iasdkauth	com/loc/ck.java
http://apilocate.amap.com/mobile/binary	com/loc/cf.java
http://apilocatesrc.amap.com/mobile/binary	com/loc/cf.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/cf.java
http://restapi.amap.com/v3/place/around?	com/loc/a.java
http://restapi.amap.com/v3/place/text?	com/loc/a.java
http://restapi.amap.com/v3/config/district?	com/loc/a.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/a/a/b/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/a/a/b/a/a.java

URL信息	Url所在文件
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
http://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/c/a.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/a.java
http://c.isdspeed.qq.com/code.cgi	com/tencent/open/b/d.java
https://openmobile.qq.com/	com/tencent/open/utils/HttpUtils.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/d.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/StatConfig.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/amap/api/location/AMapLocation.java
http://www.slf4j.org/codes.html#unsuccessfullnit	org/slf4j/c.java
http://www.slf4j.org/codes.html#multiple_bindings	org/slf4j/c.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	org/slf4j/c.java

URL信息	Url所在文件
http://www.slf4j.org/codes.html#substituteLogger	org/slf4j/c.java
http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/c.java
http://www.slf4j.org/codes.html#log4j_version	org/slf4j/impl/b.java
http://www.w3.org/2000/xmlns/	org/mozilla/javascript/xmlimpl/XmlNode.java
http://restapi.amap.com/v3/geocode/geo?	cn/com/longbang/kdy/contacts/a.java
http://192.168.1.110:8106/app/dealWithOrder.json	cn/com/longbang/kdy/contacts/a.java
http://lbzb1103.3322.org:8106/login/getAppld.json	cn/com/longbang/kdy/contacts/a.java
http://appsetting.longbangcdn.com/appsetting/getSettings	cn/com/longbang/kdy/contacts/a.java
http://122.225.104.218:8096/GetBillCode/getBillCode	cn/com/longbang/kdy/contacts/a.java
http://test.lborder.mlick.cn/	cn/com/longbang/kdy/contacts/a.java
http://vip.huisenky.com/h5/#/pages/mailing/mailing?empCode=	cn/com/longbang/kdy/contacts/a.java
http://hsapp.longbangcdn.com/	cn/com/longbang/kdy/contacts/a.java
http://ddm.longbangcdn.com/	cn/com/longbang/kdy/contacts/a.java
http://hsgis.longbangcdn.com/beauty_ssm/	cn/com/longbang/kdy/contacts/a.java
http://ddlogin.longbangcdn.com:9889/	cn/com/longbang/kdy/contacts/a.java

URL信息	Url所在文件
http://version.longbangcdn.com/	cn/com/longbang/kdy/contacts/a.java
http://vip.lbzhilian.com:7003/	cn/com/longbang/kdy/contacts/a.java
http://a.lbex.com.cn:7006/	cn/com/longbang/kdy/contacts/a.java
http://k801.lbex.com.cn:8620/	cn/com/longbang/kdy/contacts/a.java
http://122.225.104.218:8081/Ftp/Pic/	cn/com/longbang/kdy/contacts/a.java
http://lbzhilian.com/hsapp/updater/version.json	cn/com/longbang/kdy/contacts/a.java
http://k901.lbex.com.cn:8122	cn/com/longbang/kdy/contacts/a.java
http://122.225.104.218:8096/K8Service/k8/qryDestinationBySiteName.do	cn/com/longbang/kdy/contacts/a.java
http://liuyan.lbscm.com.cn?empCode=	cn/com/longbang/kdy/ui/activity/WebActivity.java
http://www.huisenky.com/site/appIndex	cn/com/longbang/kdy/ui/activity/WebActivity.java
http://ddlogin.longbangcdn.com/lbpic/uploads/lbappdownload.png	cn/com/longbang/kdy/ui/view/a/d.java
http://app.lbscm.net/	cn/com/longbang/kdy/ui/view/a/d.java
http://127.0.0.1:43689/进行测试	Android String Resource



邮箱地址	所在文件
j3cq.@3op.c3	cn/jpush/android/a/e.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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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

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
cn.com.longbang.kdy.huisen.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
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.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_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。
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.ACCESS_BACKGROUND_LOCATION	危 险	后台访问位置	允许应用程序在后台访问位置
android.permission.SYSTEM_ALERT_WINDOW	危 险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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_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.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_LOCATION_EXTRA_COMMANDS	正常	访问额外的位 置提供程序命 令	访问额外的位置提供程序命令,恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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

向手机申请的权限	是否危险	类型	详细情况
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.INTERACT_ACROSS_USERS	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频 设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.SEND_SMS	危 险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送 消息,从而使您付出代价
android.permission.READ_CONTACTS	危 险	读取联系人数 据	允许应用程序读取您手机上存储的所有联系人(地址)数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.RECORD_AUDIO	危 险	录音	允许应用程序访问音频记录路径
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。

常签名证书

APK is signed

v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: C=CN, ST=上海, L=上海, O=个人, OU=私企, CN=daiyao

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2014-10-07 10:58:32+00:00 Valid To: 2069-07-10 10:58:32+00:00

Issuer: C=CN, ST=上海, L=上海, O=个人, OU=私企, CN=daiyao

Serial Number: 0x5433c758 Hash Algorithm: sha1

md5: 5001895054ab8877afb89b2007589c57

sha1: ad0dcbcaa72d0a6c1202e8b41666957195d7a467

sha256: c54c72d1dc757323c77450f5ceef2eab0f96503608e02624976a5f819a8da314

sha512: ad0b80c73aa4691a7984a397cda52fba01684afbba43d91ee648e76c20ea898c12e1aeecb90b50630c6413c99cee61419dad52cc0d91f688eb93617ff9a60d45

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: 349ab271ff07c3c887c30457754f4b17ea446db8e3ba3b1aa9ff646eaf91daf4

在 Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119



可能的敏感信息

"setMsgPwd_title":"设置密码"

■应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: \ 1106372875://,

命加壳分析

文件列表	分析结果		
------	------	--	--

文件列表	分析结果				
大行列衣 Classes.dex	売列表 详细情况 Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check device ID check subscriber ID check ro.product.device check ro.kernel.gemu check emulator file check 编译器 dx				

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析