

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成



♣ 艾美丽 0.0.6.APK

APP名称: 艾美丽

包名: com.hk.tz023

域名线索: 32条

URL线索: 30条

邮箱线索: 1条

分析日期: 2022年2月2日 11:35

文件名: aimeili.apk 文件大小: 4.68MB

MD5值: 40e13e95aff132d5ba8ccbba512b4963

SHA1值: 65b3ad7588fffb7992aedc292ccd9e63062ee9ca

\$HA256值: 2d92bc178ae7dcbed7176b6b907ccf6c6c886af5b99bad9e2da2d12cf9b8d4ff

i APP 信息

App名称: 艾美丽 包名: com.hk.tz023

主活动**Activity:** com.uzmap.pkg.LauncherUI

安卓版本名称: 0.0.6

安卓版本: 6

0 域名线索

域名	是否危险域名	服务器信息
debugtbs.qq.com	good	IP: 175.27.9.46 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
soft.tbs.imtt.qq.com	good	IP: 121.51.175.105 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
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.
cfg.imtt.qq.com	good	IP: 121.51.158.70 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
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
mta.qq.com	good	IP: 220.194.87.235 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
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
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
p.apicloud.com	good	IP: 47.93.154.30 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
s.apicloud.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
api.weixin.qq.com	good	IP: 81.69.216.43 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
mqqad.html5.qq.com	good	P: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
api.mch.weixin.qq.com	good	IP: 182.254.22.146 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
h5.m.taobao.com	good	IP: 140.249.89.232 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map

域名	是否危险域名	服务器信息
d.apicloud.com	good	IP: 47.94.176.24 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
as.apicloud.com	good	没有服务器地理信息.
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
hydra.alibaba.com	good	IP: 203.119.169.5 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
a.apicloud.com	good	IP: 182.92.145.58 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
long.open.weixin.qq.com	good	IP: 109.244.216.15 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
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
r.apicloud.com	good	IP: 182.92.145.58 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
mdc.html5.qq.com	good	IP: 175.27.9.46 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
log.tbs.qq.com	good	IP: 109.244.244.37 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
wup.imtt.qq.com	good	IP: 182.254.56.113 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
mobilegw.alipay.com	good	IP: 203.209.245.77 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.
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
www.qq.com	good	IP: 175.27.8.138 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
pms.mb.qq.com	good	IP: 121.51.158.70 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
debugx5.qq.com	good	IP: 175.27.9.46 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://mobilegw.alipay.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
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
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
www.qq.com	com/tencent/smtt/sdk/j.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/j.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/c.java

URL信息	Url所在文件
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://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://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://hydra.alibaba.com/	com/ta/utdid2/aid/AidRequester.java

URL信息	Url所在文件
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
https://api.mch.weixin.qq.com/pay/unifiedorder	com/uzmap/pkg/uzmodules/uzWxPay/PayTask.java
https://api.mch.weixin.qq.com/pay/unifiedorder	com/uzmap/pkg/uzmodules/uzWxPay/GetOrderIdTask.java
https://api.weixin.qq.com/sns/oauth2/access_token? appid=%s&secret=%s&code=%s&grant_type=authorization_code	com/uzmap/pkg/uzmodules/uzWx/tasks/AccessTokenTask.java
https://api.weixin.qq.com/sns/oauth2/refresh_token? appid=%s&grant_type=refresh_token&refresh_token=%s	com/uzmap/pkg/uzmodules/uzWx/tasks/AccessTokenTask.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s⟨=%s	com/uzmap/pkg/uzmodules/uzWx/tasks/GetUserInfoTask.java
https://a.apicloud.com	compile/Properties.java
https://d.apicloud.com	compile/Properties.java
https://s.apicloud.com	compile/Properties.java
https://p.apicloud.com	compile/Properties.java
https://r.apicloud.com	compile/Properties.java
https://as.apicloud.com	compile/Properties.java



邮箱地址	所在文件
developer@apicloud.com	com/uzmap/pkg/uzcore/b/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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上 显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
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_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.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_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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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。

向手机申请的权限	是否危险	类型	详细情况
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



APK is signed v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(544295996@qq.com), OU=(comhktz023), CN=(comhktz023)

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-06-23 03:28:32+00:00 Valid To: 2120-05-30 03:28:32+00:00

Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(544295996@qq.com), OU=(comhktz023), CN=(comhktz023)

Serial Number: 0x7af26eab Hash Algorithm: sha256

md5: 75a01fb0594aa5ffd4360611082630f8

sha1: dfd9cf60eb64ad7d8d02eb657fe47cf7b7c065b3

sha256: 65c1d719b9559bd8c735ce534757d6f252454a1c0d7a521c85ddc300963aaebc

sha512: 954d2a9778a04abedacfa8c2d4bf870a90c87e2baf0128d7ee11945ba5b9e2859fd2082a1816971e1c6c7131f10ffd4473f9286e337e0999cc9d94db2c628966

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: 7a7607b449501ae0880c0b4c8b645446295e522d1f0a7e4b3c5beeb30971f919



名称	分类	URL链接
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

命 加壳分析

文件列表	分析结果					
文件列表 classes.dex	売列表 反虚拟机	详细情况 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 SIM operator check network operator name check device ID check subscriber ID check ro.product.device 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