

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成



♣ 一秒推 1.2.3.APK

APP名称: 一秒推

包名: w2a.W2Am.yimiaotui.com

域名线索: 23条

URL线索: 48条

邮箱线索: 0条

分析日期: 2022年1月26日 20:26

文件名: yimiaodui.apk 文件大小: 4.45MB

MD5值: 76907d2b250662dc3c08ffadc3d34b02

SHA1值: 0b78e94c5014840659b2f90022341027a692baab

\$HA256值: 229a018a5c7ee8754f0571984d366c3be7d469fc7da2ca645ad65f74debb4f6d

i APP 信息

App名称: 一秒推

包名: w2a.W2Am.yimiaotui.com 主活动**Activity**: io.dcloud.PandoraEntry

安卓版本名称: 1.2.3 安卓版本: 16

0 域名线索

域名	是否危险域名	服务器信息
ask.dcloud.net.cn	good	IP: 222.85.26.232 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

域名	是否危险域名	服务器信息
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
uniad-report.dcloud.io	good	IP: 118.31.105.31 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
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
h5.m.taobao.com	good	IP: 218.61.211.231 所属国家: China 地区: Liaoning 城市: Dalian 纬度: 41.069592 经度: 122.598511 查看地图: Google Map

域名	是否危险域名	服务器信息
m3w.cn	good	IP: 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 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
stream.dcloud.net.cn	good	IP: 118.31.103.188 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

域名	是否危险域名	服务器信息
service.dcloud.net.cn	good	IP: 47.97.36.120 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.
schemas.android.com	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.aaa.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
update.dcloud.net.cn	good	IP: 182.254.52.213 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

域名	是否危险域名	服务器信息
streamapp.sinaapp.com	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
wappaygw.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
www.dcloud.io	good	IP: 124.95.157.146 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432777 查看地图: Google Map
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

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.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
stream.mobihtml5.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
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

URL信息	Url所在文件
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/d.java
https://h5.m.taobao.com/mlapp/olist.html	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://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://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
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://m3w.cn/sd/reg	io/dcloud/appstream/b.java

URL信息	Url所在文件
http://m3w.cn/s/	io/dcloud/appstream/share/a.java
http://ask.dcloud.net.cn/article/283	io/dcloud/feature/b.java
http://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://service.dcloud.net.cn/advert/splash	io/dcloud/feature/ad/dcloud/ADHandler.java
https://service.dcloud.net.cn/collect/plusapp/cad	io/dcloud/feature/ad/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/287	<u>io/dcloud/share/IFShareApi.java</u>
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://www.dcloud.io/streamapp/streamapp.apk	io/dcloud/common/util/ShortCutUtil.java
http://stream.dcloud.net.cn/resource/sitemap/v2?appid=	io/dcloud/common/a/d.java
https://service.dcloud.net.cn/collect/plusapp/startup	io/dcloud/common/a/d.java
http://ask.dcloud.net.cn/article/35627	io/dcloud/common/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/common/a/a.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/common/core/a.java
https://service.dcloud.net.cn/collect/plusapp/action	io/dcloud/common/core/b/a.java
https://service.dcloud.net.cn/pdz	io/dcloud/common/core/b/a.java

URL信息	Url所在文件
https://uniad-report.dcloud.io/video/report?p=a&t=r	io/dcloud/common/core/b/a.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://update.dcloud.net.cn/apps/	io/dcloud/common/constant/IntentConst.java
http://streamapp.sinaapp.com	io/dcloud/streamdownload/utils/b.java

畫此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
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_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

向手机申请的权限	是否危险	类型	详细情况
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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。
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.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.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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.READ_LOGS	危 险	读取敏感日志 数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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
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。



APK is signed

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

Found 1 unique certificates

Subject: C=CN, ST=guangdongsheng, L=shenzhen, O=yimiaotui, OU=yimiaotui, CN=yimiaotui

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-04-01 03:31:19+00:00 Valid To: 2120-03-08 03:31:19+00:00

Issuer: C=CN, ST=guangdongsheng, L=shenzhen, O=yimiaotui, OU=yimiaotui, CN=yimiaotui

Serial Number: 0xd5c8ce42e1ef6d9c

Hash Algorithm: sha256

md5: 085b56329de78cb8b1d90dd4fe202fd8

sha1: 9db946ac491b9d1530bb6fa86690964ff68bf36e

sha256: 94ad950f52ed10fafa65a1553a11a09db71fc2414c114ae85125e7476b240ec6

sha512: 39eb00aa5cf0683f685ef392c1b8d0d462e3ffa1e22ffac2cc0cee864ae7624268ecacae8def66a2de45d03d81777ecace5b7261394113833dbfdb35153b115d

PublicKey Algorithm: rsa

Bit Size: 2048

■应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.appstream.StreamAppMainActivity	Schemes: streamapp://, streamappmain://,

命加壳分析

文件列表	分析结果		
	売列表	详细情况	
	反虚拟机	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT 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 ro.kernel.qemu check emulator file check possible VM check	

classes.dex 文件列表	分析结果	详细情况	
	编译器	r8 without marker (suspicious)	

报告由 摸瓜平台 自动生成,并非包含所有检测结果,有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析