

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成



♣ 一采通 3.6.2.APK

APP名称: 一采通

包名: bj.yicaitong.H58CD123A

域名线索: 22条

URL线索: 49条

邮箱线索: 0条

分析日期: 2022年1月22日 23:34

文件名: yicaitong511326.apk

文件大小: 5.5MB

MD5值: 7de0b65d4aaeb42b23582edc431b8c23

SHA1值: 1a1110bf3b91f9c3923352592c49f86d53e24573

\$HA256值: e25a9a08766c7702b9d84b5d7e0fc677489ad99cf5049c28c015c6ef7e117332

i APP 信息

App名称: 一采通

包名: bj.yicaitong.H58CD123A

主活动**Activity:** io.dcloud.PandoraEntry

安卓版本名称: 3.6.2

安卓版本:83

Q 域名线索

域名	是否危险域名	服务器信息
sdk.open.lbs.igexin.com	good	IP: 183.134.98.68 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
imfv.openspeech.cn	good	IP: 42.62.116.18 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.dcloud.io	good	IP: 125.76.247.187 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.560280 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.
scs.openspeech.cn	good	IP: 220.248.230.134 所属国家: China 地区: Anhui 城市: Hefei 纬度: 31.863890 经度: 117.280830 查看地图: Google Map
stream.mobihtml5.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
ask.dcloud.net.cn	good	IP: 125.76.247.240 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.560280 查看地图: Google Map
iss.openspeech.cn	good	IP: 42.62.43.147 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
c-hzgt2.getui.com	good	IP: 124.160.127.198 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
wke.openspeech.cn	good	没有服务器地理信息.
openapi.openspeech.cn	good	IP: 42.62.116.34 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
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	good	IP: 47.93.95.208 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
data.openspeech.cn	good	IP: 220.248.230.134 所属国家: China 地区: Anhui 城市: Hefei 纬度: 31.863890 经度: 117.280830 查看地图: Google Map
d.gt.igexin.com	good	IP: 183.134.98.71 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.dcloud.net.cn	good	IP: 118.31.188.88 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
m3w.cn	good	IP: 125.76.247.187 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.560280 查看地图: Google Map
dev.voicecloud.cn	good	IP: 42.62.116.34 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
s-gt.getui.com	good	IP: 124.160.127.198 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
da.mmarket.com	good	IP: 120.232.188.83 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
service.dcloud.net.cn	good	IP: 120.26.1.80 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
sdk.open.phone.igexin.com	good	IP: 124.160.127.196 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
hxqd.openspeech.cn	good	IP: 114.118.64.119 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://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/b.java

URL信息	Url所在文件
http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/c.java
http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/a.java
http://scs.openspeech.cn/scs	com/iflytek/thirdparty/Z.java
http://data.openspeech.cn/index.php/clientrequest/clientcollect/isCollect	com/iflytek/thirdparty/Z.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog	com/iflytek/thirdparty/C0062b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog	com/iflytek/thirdparty/C0062b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog	com/iflytek/thirdparty/C0062b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog	com/iflytek/thirdparty/C0062b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:specposteventlog	com/iflytek/thirdparty/C0062b.java
http://openapi.openspeech.cn/webapi/wfr.do	com/iflytek/thirdparty/C0049ae.java
http://imfv.openspeech.cn/msp.do	com/iflytek/thirdparty/C0047ac.java
http://hxqd.openspeech.cn/launchconfig	com/iflytek/thirdparty/aF.java
http://wke.openspeech.cn/wakeup/	com/iflytek/thirdparty/C0079s.java
http://iss.openspeech.cn/v?	com/iflytek/speech/UtilityConfig.java
http://bi.	com/igexin/push/config/n.java

URL信息	Url所在文件
http://config.	com/igexin/push/config/n.java
http://stat.	com/igexin/push/config/n.java
http://log.	com/igexin/push/config/n.java
http://lbs.	com/igexin/push/config/n.java
http://sdk.open.phone.igexin.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://c-hzgt2.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.lbs.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://d.gt.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://s-gt.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.phone.igexin.com/api/addr.htm	com/igexin/push/extension/distribution/gbd/d/d.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://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/ad/dcloud/ADHandler.java

URL信息	Url所在文件
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/f/b/b.java
https://service.dcloud.net.cn/pdz	io/dcloud/f/b/d/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/b/d/a.java
http://ask.dcloud.net.cn/article/35627	io/dcloud/f/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/f/a/a.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://www.dcloud.io/streamapp/streamapp.apk	io/dcloud/common/util/ShortCutUtil.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/36199	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://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java

缸此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
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

向手机申请的权限	是否危险	类型	详细情况
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
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.GET_ACCOUNTS	危 险	列出帐户	允许访问账户服务中的账户列表
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.READ_SMS	危 险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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.RECORD_AUDIO	危 险	录音	允许应用程序访问音频记录路径
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.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.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_CONTACTS	危 险	写入联系人数 据	允许应用程序修改您手机上存储的联系人(地址)数据。恶意应用程序可以使用 它来删除或修改您的联系人数据
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.WRITE_SMS	危 险	编辑短信或彩 信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
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.RECEIVE_SMS	危 险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其 删除而不向您显示
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
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。
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
getui.permission.GetuiService.bj.yicaitong.H58CD123A	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
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。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference



APK is signed v1 signature: True

v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: C=CN, ST=chaoyang, L=beijing, O=1caitong, OU=1caitong, CN=magegnshun

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2015-11-17 01:59:28+00:00 Valid To: 2115-10-24 01:59:28+00:00

Issuer: C=CN, ST=chaoyang, L=beijing, O=1caitong, OU=1caitong, CN=magegnshun

Serial Number: 0x21a8ed6d Hash Algorithm: sha256

md5: 290f63c45b8d5cb5cb76fa7800ac4093

sha1: d14caa6fbc4f545f0374898d462e119398c470b2

sha256: 3b478528b53ef8d866f4189a7fdb0e4ea6b1fd54e6408230dee85999a3db9a5f

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 6c7f2866e34bb0847a4c9b5856dbbbd75442d4da4b4ee4fcc9e8a944d35169c3

■应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h58cd123a://,

命加壳分析

文件列表	分析结果	
classes.dex	売列表 元列表	详细情况 Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check Build.BOARD check
	编译器	possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check device ID check subscriber ID check possible VM check

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