

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



Picasso 1.0.APK

APP名称: Picasso

包名: plus.a00d8170dec4dfe5e

域名线索: 18条

URL线索: 45条

邮箱线索: 0条

分析日期: 2022年1月25日 21:33

文件名: 7d381e199a84910a1247dba695d0939c.apk

文件大小: 5.19MB

MD5值: 39ce53819d6654351160869bf2c4afdd

SHA1值: 109de91d9ba187260b6bde447fd3ee5387a39457

SHA256值: ae75e22f0f6a47eb991229878a6b91daf1724cc245d3dae8b8b95899810d6bd8

i APP 信息

App名称: Picasso

包名: plus.a00d8170dec4dfe5e

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

安卓版本名称: 1.0 安卓版本: 1

0 域名线索

域名	是否危险域名	服务器信息
update.dcloud.net.cn	good	IP: 121.51.175.120 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
schemas.android.com	good	没有服务器地理信息.

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
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
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
m3w.cn	good	IP: 222.85.26.230 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
ask.dcloud.net.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
hxqd.openspeech.cn	good	IP: 42.62.116.134 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
stream.mobihtml5.com	good	没有服务器地理信息.
wke.openspeech.cn	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
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
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
imfv.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
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

域名	是否危险域名	服务器信息
www.dcloud.io	good	IP: 124.239.227.205 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
dev.voicecloud.cn	good	IP: 58.67.223.138 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
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

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://imfv.openspeech.cn/msp.do	com/iflytek/thirdparty/C0018ac.java
http://wke.openspeech.cn/wakeup/	com/iflytek/thirdparty/C0050s.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog	com/iflytek/thirdparty/C0033b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog	com/iflytek/thirdparty/C0033b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog	com/iflytek/thirdparty/C0033b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog	com/iflytek/thirdparty/C0033b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:specposteventlog	com/iflytek/thirdparty/C0033b.java
http://openapi.openspeech.cn/webapi/wfr.do	com/iflytek/thirdparty/C0020ae.java
http://hxqd.openspeech.cn/launchconfig	com/iflytek/thirdparty/aF.java
http://iss.openspeech.cn/v?	com/iflytek/speech/UtilityConfig.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java

URL信息	Url所在文件
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
http://m3w.cn/s/	io/dcloud/appstream/c/b.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/a/a.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://service.dcloud.net.cn/collect/plusapp/action?	io/dcloud/common/util/TestUtil.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://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

URL信息	Url所在文件
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/common/core/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.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.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.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.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_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

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
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。
android.permission.GET_ACCOUNTS	危 险	列出帐户	允许访问账户服务中的账户列表

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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_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
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
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.android.launcher.permission.INSTALL_SHORTCUT	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.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcherL.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.bbk.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序 上显示通知 计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序 上显示通知 计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.qiku.launcher.permission.READ_SETTINGS	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.READ_SETTINGS	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.zte.mifavor.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lenovo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.google.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcher3.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.qihoo360.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lge.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
net.qihoo.launcher.permission.READ_SETTINGS	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
org.adwfreak.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher_donut.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.fede.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.sec.android.app.twlauncher.settings.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.tencent.qqlauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ebproductions.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.nd.android.launcher.permission.READ_SETTINGS	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.yulong.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.mylauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ztemt.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
cn.nubia.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.gionee.amisystem.permission.READ_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
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.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



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

Found 1 unique certificates

Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2008-02-29 01:33:46+00:00 Valid To: 2035-07-17 01:33:46+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

Serial Number: 0x936eacbe07f201df

Hash Algorithm: sha1

md5: e89b158e4bcf988ebd09eb83f5378e87

sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81

sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc

sha512: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

☑应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: a00d8170dec4dfe5e://,
io.dcloud.PandoraEntryActivity	Schemes: h56131bcf://,
io.dcloud.appstream.StreamAppMainActivity	Schemes: streamapp://, streamappmain://,

命加壳分析

文件列表	分析结果	
------	------	--

文件列表	分析结果	
	売列表	详细情况
classes.dex	反虚拟机	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check SIM operator check network operator name check device ID check subscriber ID check possible VM check
	编译器	dexlib 2.x

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