

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♣ 拱钱猪 1.0.6.APK

APP名称: 拱钱猪

包名: com.jianzhipig.zhaopin

域名线索: 19条

URL线索: 51条

邮箱线索: 0条

分析日期: 2022年2月2日 19:59

文件名: gongqianzhu.apk

文件大小: 4.84MB

MD5值: 37d0a6d0e58afc09237527066cca9a83

SHA1值: 6e830d5f0ad2e93bbc81d24d2663a23af0497c38

\$HA256值: fb77c3dd76df60c8698395c4b3a525f664778469bc80ef218b91b6c328bf749a

i APP 信息

App名称: 拱钱猪

包名: com.jianzhipig.zhaopin

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

安卓版本名称: 1.0.6 安卓版本: 106

0 域名线索

域名	是否危险域名	服务器信息
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

域名	是否危险域名	服务器信息
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
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
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
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
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
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
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
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

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
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
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
schemas.android.com	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
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
stream.mobihtml5.com	good	没有服务器地理信息.
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
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



URL信息	Url所在文件
http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/b.java
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://openapi.openspeech.cn/webapi/wfr.do	com/iflytek/thirdparty/C0029ae.java
http://imfv.openspeech.cn/msp.do	com/iflytek/thirdparty/C0027ac.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog	com/iflytek/thirdparty/C0042b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog	com/iflytek/thirdparty/C0042b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog	com/iflytek/thirdparty/C0042b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog	com/iflytek/thirdparty/C0042b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:specposteventlog	com/iflytek/thirdparty/C0042b.java
http://wke.openspeech.cn/wakeup/	com/iflytek/thirdparty/C0059s.java
http://hxqd.openspeech.cn/launchconfig	com/iflytek/thirdparty/aF.java
http://iss.openspeech.cn/v?	com/iflytek/speech/UtilityConfig.java

URL信息	Url所在文件
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
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/thirdConfig	io/dcloud/feature/ad/AdFlowMgr.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
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/ad/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.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

URL信息	Url所在文件
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
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	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/CommitPointData.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.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.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_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

向手机申请的权限	是否危险	类型	详细情况
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.RECORD_AUDIO	危 险	录音	允许应用程序访问音频记录路径
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.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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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

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
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

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-07-21 07:00:54+00:00 Valid To: 2030-07-19 07:00:54+00:00

Serial Number: 0x2f426c01 Hash Algorithm: sha256

md5: b76226d7f087bc571431439853a6a928

sha1: 36398554fde15a76d7a7e2aa55e32c0a3fa22998

sha256: 2d5a0dcbd5ae9c75b434a48f5c502b567d5bd21bc94085eb0adead3662f0c9cd

sha512: 370e8b88f9fe3abda8edec80dbffbd83d22da6a536d66ec97465428da8184ce9bc3d29cf82a20e8d6bc966541d55ed85f17f8b350e4361b60d1c99aa8e41a416

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: f0e656f171556095d0e73e94855cbfcf9555e2f85134437916d01bef37cf6ac9



活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h5cada0dd://,
io.dcloud.appstream.StreamAppMainActivity	Schemes: streamapp://, streamappmain://,

命加壳分析

文件列表	分析结果
------	------