

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♣ 飙升网 2.28.APK

APP名称: 飙升网

包名: app.biaoshengwang.com

域名线索: 22条

URL线索: 51条

邮箱线索: 1条

分析日期: 2022年2月2日 11:35

文件名: biaoshengwnag.apk

文件大小: 7.45MB

MD5值: 90bb52cce2fcb330f48f742e19823632

SHA1值: ddecd0052cd9ad588d81046c21c318398335dd8e

\$HA256值: 9ccf2caeb331a24ec738f5d84908dbbb4b7bce9dc95aca14d773556e4727c444

i APP 信息

App名称: 飙升网

包名: app.biaoshengwang.com

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

安卓版本名称: 2.28 安卓版本: 228

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: <u>Google Map</u>
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
upload.ffmpeg.org	good	IP: 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris 纬度: 48.853409 经度: 2.348800 查看地图: Google Map
schemas.android.com	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

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

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
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
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
log.tbs.qq.com	good	IP: 109.244.244.32 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
wup.imtt.qq.com	good	IP: 182.254.57.56 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
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
www.openssl.org	good	IP: 104.118.68.19 所属国家: Japan 地区: Osaka 城市: Osaka 纬度: 34.693890 经度: 135.502213 查看地图: Google Map
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 査看地图: 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 査看地图: 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://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java

URL信息	Url所在文件
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/i.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/i.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
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

URL信息	Url所在文件
http://soft.tbs.imtt.qq.com/17421/tbs res imtt tbs DebugPlugin DebugPlugin.tbs	com/tencent/smtt/utils/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://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

URL信息	Url所在文件
http://stream.dcloud.net.cn/resource/sitemap/v2?appid=	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
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
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libijkplayer.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so



邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

₩ 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。

向手机申请的权限	是否危险	类型	详细情况
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
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

向手机申请的权限	是否危险	类型	详细情况
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
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_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。
com.asus.msa.SupplementaryDID.ACCESS	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
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=SH, L=SH, O=tmsapp, OU=tmsapp, CN=tmsapp

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-07-09 08:23:03+00:00 Valid To: 2030-07-07 08:23:03+00:00

Issuer: C=CN, ST=SH, L=SH, O=tmsapp, OU=tmsapp, CN=tmsapp

Serial Number: 0x2ecf2552 Hash Algorithm: sha256

md5: 57a36f9028f68598e0545301cbb6d510

sha1: 1baf47186355f4a81a3d1378b017c80abed9b5ad

sha256: f59975b8a8336ed9b441def155272d096e183cb14cf6fee97c95b9b4ca62d40c

sha512: 461249561c7e52cde4f1bdd08313ce8b0cf57f4508994fd6facfa2456262133cbf36f401fe3ed430497e3acc4f4b19fd7c8338448bcf0d80e75b79463fa92bf3

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 9f8350eeed9ff6dc9be2f90210ea4331869818a7e4cf692ddbbc69f636d61808

■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	
classes.dex	反虚拟机	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check SIM operator check device ID check subscriber ID check possible VM check	
	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