MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

盯梢 1.0.APK

APP名称:	盯梢
包名:	com.mufan.app.dingshao
域名线索:	19条
URL线索:	19条
邮箱线索:	0条
分析日期:	2022年1月20日 21:46

文件信息

文件名: dingshao556792.apk
文件大小: 9.59MB
MD5值: bc1ace5a5f6dc398dc5fb4602b71813c
SHA1值: 809249562228b4eee9a766e897455999d0b44dfa
SHA256值: 2306bd10a60f90fa9caa5e8865a943408045b477b098e2afc109586d2d2e7ec8

APP 信息

App名称: 盯梢
包名: com.mufan.app.dingshao
主活动**Activity:** com.mufan.app.dingshao.MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
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
mclient.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
mobilegw.alipay.com	good	**IP:** 203.209.245.78 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
loggw-exsdk.alipay.com	good	**IP:** 110.75.130.122 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
capacitorjs.com	good	**IP:** 76.76.21.164 所属国家: United States of America 地区: California 城市: Walnut 纬度: 34.015400 经度: -117.858223 查看地图: Google Map
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
upload-z2.qiniup.com	good	IP: 119.167.169.225 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941 查看地图: Google Map
mobilegw.stable.alipay.net	good	没有服务器地理信息.
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
github.com	good	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 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

域名	是否危险域名	服务器信息
ce3e75d5.jpush.cn	good	IP: 183.232.58.244 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
m.alipay.com	good	IP: 203.209.245.120 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
h5.m.taobao.com	good	IP: 140.249.89.233 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map
configapi-api.glqa.jpushoa.com	good	IP: 172.17.5.42 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map

域名	是否危险域名	服务器信息
journeyapps.com	good	**IP:** 13.33.210.59 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看地图:** Google Map
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
play.google.com	good	**IP:** 172.217.163.46 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
render.alipay.com	good	**IP:** 106.117.213.117 **所属国家:** China **地区:** Hebei **城市:** Tangshan **纬度:** 39.633331 **经度:** 118.183327 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://capacitorjs.com/docs/apis/splash-screen#hiding-the-splash-screen	com/capacitorjs/plugins/splashscreen/SplashScreen.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java

URL信息	Url所在文件
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/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.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/ay/c.java
https://ce3e75d5.jpush.cn/wi/d8n3hj	cn/jiguang/ay/c.java
https://ce3e75d5.jpush.cn	cn/jiguang/b/b.java
https://upload-z2.qiniup.com	cn/jiguang/bd/a.java
https://ce3e75d5.jpush.cn/wi/op8jdu	cn/jiguang/s/c.java
http://configapi-api.glqa.jpushoa.com/v1/status	cn/jiguang/bc/f.java
http://play.google.com/store/account/subscriptions	cc/fovea/PurchasePlugin.java
http://play.google.com/store/paymentmethods	cc/fovea/PurchasePlugin.java

URL信息	Url所在文件
https://journeyapps.com/	Android String Resource
https://github.com/journeyapps/zxing-android-embedded	Android String Resource

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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
com.mufan.app.dingshao.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	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.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
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.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True

v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=Sichuan, L=Chengdu, O=Chengdu Mufan Technology
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-12-28 13:31:46+00:00
Valid To: 2046-12-22 13:31:46+00:00
Issuer: C=CN, ST=Sichuan, L=Chengdu, O=Chengdu Mufan Technology
Serial Number: 0x3ea4cc64
Hash Algorithm: sha256
md5: 4c4d50006bed47d2cb35702d023448d1
sha1: 53dc039efcd7cbaabd6536941b937ccc5533a510
sha256: 8abfdae8e5d7e94df4d437fea312f0fab4d8a8f09170b869325c92f3bbe2c010
sha512: 4605e33afd1b89147a52b57b457b32b8f7eee27cc60aa3d905a7f7554ba5a9d6a25479f17ad076cab0e006aaf387106d28f25dc25ff3448b15508c7c14ce00c5
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e0de875f0a8328afed6272f3f6698711a0f1eb2099dafbba2829a4dbecf03961

Exodus威胁情报

名称	分类	URL链接
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

硬编码敏感信息

可能的敏感信息
"google_api_key" : "AIzaSyDYuvGWK6a4ZSXS8PDP71uDVAqIQwWPdC4"

可能的敏感信息
"google_crash_reporting_api_key" : "AIzaSyDYuvGWK6a4ZSXS8PDP71uDVAqIQwWPdC4"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.mufan.app.dingshao.MainActivity	Schemes: @string/custom_url_scheme://,

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER 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.hardware check ro.product.device check ro.kernel.qemu check emulator file check possible VM check</td></tr><tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>