MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

华地 1.0.6.APK

APP名称:	华地
包名:	com.huadi.w
域名线索:	31条
URL线索:	31条
邮箱线索:	0条
分析日期:	2022年1月22日 17:50

文件信息

文件名: huadi546729.apk
文件大小: 4.43MB
MD5值: 9a0f5f1637232636740354 6153b8a1ca
SHA1值: 291d8a3dbd5a2a13f499efb061a2b51919e744c5
SHA256值: 51b0a8344dbdad554234ba04c557e5f6aff40425a4cad6a69c35104e837dca66

APP 信息

App名称: 华地
包名: com.huadi.w
主活动**Activity:** com.lt.app.MainActivity
安卓版本名称: 1.0.6
安卓版本: 106

域名线索

域名	是否危险域名	服务器信息
idmb.register.xmpush.global.xiaomi.com	good	**IP:** 15.206.99.29 **所属国家:** India **地区:** Maharashtra **城市:** Mumbai **纬度:** 19.014410 **经度:** 72.847939 **查看地图:** Google Map

域名	是否危险域名	服务器信息
render.alipay.com	good	**IP:** 182.40.18.117 **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
resolver.msg.xiaomi.net	good	**IP:** 183.84.5.221 **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
schemas.android.com	good	没有服务器地理信息.
mobilegw.alipay.com	good	**IP:** 203.209.247.65 **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:** 59.47.236.231 **所属国家:** China **地区:** Liaoning **城市:** Benxi **纬度:** 41.288609 **经度:** 123.764999 **查看地图:** Google Map

域名	是否危险域名	服务器信息
appgallery.cloud.huawei.com	good	**IP:** 49.4.35.33 **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.jivesoftware.com	good	**IP:** 35.238.7.255 **所属国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860832 **查看地图:** Google Map
api-push.meizu.com	good	**IP:** 125.94.213.129 **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
resolver.msg.global.xiaomi.net	good	**IP:** 47.241.174.254 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map

域名	是否危险域名	服务器信息
api-push.in.meizu.com	good	**IP:** 206.161.233.191 **所属国家:** United States of America **地区:** Virginia **城市:** Herndon **纬度:** 38.978210 **经度:** -77.386993 **查看地图:** Google Map
mobilegw.stable.alipay.net	good	没有服务器地理信息.
xml.org	good	**IP:** 104.239.240.11 **所属国家:** United States of America **地区:** Texas **城市:** Windcrest **纬度:** 29.499678 **经度:** -98.399246 **查看地图:** Google Map
fr.register.xmpush.global.xiaomi.com	good	**IP:** 3.122.66.25 **所属国家:** Germany **地区:** Hessen **城市:** Frankfurt am Main **纬度:** 50.115520 **经度:** 8.684170 **查看地图:** Google Map
loggw-exsdk.alipay.com	good	**IP:** 110.75.134.8 **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
mcgw.alipay.com	good	**IP:** 203.209.250.6 **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
ru.register.xmpush.global.xiaomi.com	good	**IP:** 107.155.52.56 **所属国家:** Russian Federation **地区:** Moskva **城市:** Moscow **纬度:** 55.752220 **经度:** 37.615559 **查看地图:** Google Map
norma-external-collect.meizu.com	good	**IP:** 113.106.27.98 **所属国家:** China **地区:** Guangdong **城市:** Zhongshan **纬度:** 22.520580 **经度:** 113.382317 **查看地图:** Google Map
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
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
play.google.com	good	**IP:** 172.217.160.110 **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
register.xmpush.global.xiaomi.com	good	**IP:** 47.88.199.5 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
cn.register.xmpush.xiaomi.com	good	**IP:** 118.26.252.220 **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
xmlpull.org	good	**IP:** 74.50.62.60 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.814899 **经度:** -96.879204 **查看地图:** Google Map
mobilegw.aaa.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
m.alipay.com	good	**IP:** 203.209.245.74 **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
mclient.alipay.com	good	**IP:** 203.209.250.6 **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.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
hydra.alibaba.com	good	**IP:** 203.119.169.227 **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
store.hispace.hicloud.com	good	**IP:** 49.4.18.123 **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.baidu.com	good	**IP:** 110.242.68.3 **所属国家:** China **地区:** Hebei **城市:** Baoding **纬度:** 38.851109 **经度:** 115.490280 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
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

URL信息	Url所在文件
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
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

URL信息	Url所在文件
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://schemas.android.com/apk/res/android	com/baidu/techain/i/c.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/c/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/c/a/a.java
http://hydra.alibaba.com/	com/ta/utdid2/a/b.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.meizu.com/garcia/api/client/log/upload	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.meizu.com/garcia/api/server/getPublicKey	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.in.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
http://xml.org/sax/features/namespaces	com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java
http://xml.org/sax/features/validation	com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java

URL信息	Url所在文件
http://xml.org/sax/features/namespaces	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/namespace-prefixes	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/validation	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/external-general-entities	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/external-parameter-entities	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/string-interning	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html#report-namespace-prefixes	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html#process-docdecl	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html#validation	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://www.jivesoftware.com/xmlns/xmpp/properties	com/xiaomi/push/gg.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gn.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/fj.java
https://%1$s/gslb/?ver=4.0	com/xiaomi/push/cv.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/fv.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/go.java
https://resolver.msg.global.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bt.java
https://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bt.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/s.java
https://register.xmpush.global.xiaomi.com	com/xiaomi/push/service/s.java
https://fr.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/s.java
https://ru.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/s.java
https://idmb.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/s.java
www.baidu.com:80	com/xiaomi/push/service/an.java
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	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.RECEIVE_USER_PRESENT	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
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
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.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.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
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。

向手机申请的权限	是否危险	类型	详细情况
com.huadi.w.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
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.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.huadi.w.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.huadi.w.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	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.huadi.w.permission.techain.RECEIVE	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.huadi.w.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.huadi.w.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
com.huadi.w.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
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

签名证书

APK is signed
v1 signature: True
v2 signature: True

v3 signature: False
Found 1 unique certificates
Subject: C=NL, ST=NL, L=NL, O=NL, OU=NLJK, CN=NL
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-11-25 08:25:03+00:00
Valid To: 2121-11-01 08:25:03+00:00
Issuer: C=NL, ST=NL, L=NL, O=NL, OU=NLJK, CN=NL
Serial Number: 0x55ba7d34
Hash Algorithm: sha256
md5: aae621b1a8c9678c3c710351fc1c7517
sha1: f753c63dfcacf6e5b9f6d7697ed34df581570f8c
sha256: efb154340ce058a513ce3d2e7269f3df6fb5bf9baae3c7eef2a034720af025b8
sha512: cceeee343f1cca31c5bb23be51eb0ba9af3a6182ad4942bccfc283af1a8f230377b701fcb83df32fa90135a6d8f59f6a24ab4578200b32d565de15e51bcf88eb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4676cf2326d5dce1a0dddc9477af36e4273ca740fe96dde81ddc47a65f23ed36

Exodus威胁情报

名称	分类	URL链接
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

硬编码敏感信息

可能的敏感信息
"p_ht_appkey" : "700024262"
"p_ht_mz_appkey" : ""

可能的敏感信息
"p_ht_op_appkey" : ""
"p_ht_op_appsecret" : ""
"p_ht_vv_appkey" : ""
"p_ht_xm_appkey" : ""
"p_rcpush_mzAppKey" : ""
"p_rcpush_opAppKey" : ""
"p_rcpush_opAppSecret" : ""
"p_rcpush_vvAppKey" : ""
"p_rcpush_xmAppKey" : ""
"p_weibo_appkey" : ""

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.lt.app.JumpActivity	Schemes: ltapp280385://,

活动(ACTIVITY)	通信(INTENT)
com.baidu.techain.push.VivoPushActivity	Schemes: vpushscheme://, Hosts: com.huadi.w, Paths: /detail,

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.product.device check ro.kernel.qemu check emulator file check</td></tr><tr><td>编译器</td><td>r8</td></tr><tr><td>模糊器</td><td>unreadable field names unreadable method names</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>lib/arm64-v8a/libtechain.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libtechain.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr>
</table>
</td></tr>
</table>
