MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

助力盟
ZHULIMENG

助力盟 1.0.0.APK

APP名称:	助力盟
包名:	com.hwdj98.zhulimeng
域名线索:	21条
URL线索:	21条
邮箱线索:	1条
分析日期:	2022年2月3日 13:32

文件信息

文件名: zhulimeng580802.apk
文件大小: 3.33MB
MD5值: 68f68e5512744ffee57cfd9b7248a32c
SHA1值: 33e0b3e52333a3d1269b661df40534f89683a757
SHA256值: 229ccc7abb95624c13e9b451c5e9198aa5888824bc95fdb6ce5b96573a994fb7

APP 信息

App名称: 助力盟
包名: com.hwdj98.zhulimeng
主活动**Activity:** com.hwdj98.zhulimeng.page.StartPageActivity
安卓版本名称: 1.0.0
安卓版本: 100

域名线索

域名	是否危险域名	服务器信息
tdid.m.qq.com	good	**IP:** 182.254.51.125 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
dp3.qq.com	good	IP: 120.241.16.16 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
pmir.3g.qq.com	good	IP: 113.96.208.65 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.
www.baidu.com	good	IP: 110.242.68.4 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
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
render.alipay.com	good	**IP:** 42.81.213.243 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
h5.m.taobao.com	good	**IP:** 60.28.226.41 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
zhulimeng.ptyskj.top	good	**IP:** 122.114.161.144 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
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-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
app.heroncms.com	good	IP: 122.114.161.144 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
mobilegw.alipay.com	good	IP: 203.209.245.77 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
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
a.gdt.qq.com	good	IP: 121.51.117.90 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
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
xml.apache.org	good	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
mobilegw.stable.alipay.net	good	没有服务器地理信息.
wappaygw.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
loggw-exsdk.alipay.com	good	IP: 203.209.238.2 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
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

URL线索

URL信息	Url所在文件
www.baidu.com	com/blankj/utilcode/util/NetworkUtils.java
http://xml.apache.org/xslt}indent-amount	com/blankj/utilcode/util/LogUtils.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

URL信息	Url所在文件
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
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java

URL信息	Url所在文件
https://tdid.m.qq.com?mc=2	com/tencent/turingfd/sdk/ams/ad/Cgoto.java
http://pmir.3g.qq.com	com/tencent/turingfd/sdk/ams/ad/Celse.java
http://a.gdt.qq.com/getSdkConf	com/qq/gdt/action/j/b.java
https://a.gdt.qq.com/sdk	com/qq/gdt/action/j/c.java
http://a.gdt.qq.com/sdk	com/qq/gdt/action/j/c.java
http://dp3.qq.com/stdlog	com/qq/gdt/action/j/a.java
https://app.heroncms.com/	com/hwdj98/zhulimeng/http/server/ReleaseServer.java
https://app.heroncms.com/	com/hwdj98/zhulimeng/http/server/TestServer.java
http://zhulimeng.ptyskj.top/	com/hwdj98/zhulimeng/page/MainActivity.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/PermissionUtils.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/PermissionChecker.java

邮箱线索

邮箱地址	所在文件
.apk@classes.dex	com/tencent/turingfd/sdk/ams/ad/Cdouble.java

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.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.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
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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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

向手机申请的权限	是否危险	类型	详细情况
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=410000, ST=Hunan, L=Changsha, O=Hunan huaweida e-commerce Co.Ltd, OU=e-commerce, CN=ZhuLiMeng
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-01-18 07:55:45+00:00
Valid To: 2047-01-12 07:55:45+00:00
Issuer: C=410000, ST=Hunan, L=Changsha, O=Hunan huaweida e-commerce Co.Ltd, OU=e-commerce, CN=ZhuLiMeng
Serial Number: 0x71145370
Hash Algorithm: sha256
md5: ebce3321743782e4e11b91aa48ac66de
sha1: fa94081178ea92929a3b67bd88a8302b88e66f84
sha256: d00b0469d2c8fc338357ec86fcc84b7dea73698ae7a4297f8c496addcf92a235
sha512: bca03f9fdddf0ef1e1dbc329bc91b9e56b93dbf6b20639527b4a48d5b06a17b3a66fb15503a299662f1db612d7c48b2e717dde3a6953653cafe8a80473c75231
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 25537c96d313e5a62d26d5ed5037c6aab509026634f84d31f9a80c3b5c0206b2

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>lib/armeabi/libturingad.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 unknown</td></tr></table></td></tr>
<tr><td>lib/armeabi-v7a/libturingad.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 unknown</td></tr></table></td></tr>
<tr><td>lib/arm64-v8a/libturingad.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 unknown</td></tr></table></td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<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
possible VM check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
