MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

由物 1.0.0.APK

APP名称:	由物
包名:	com.miao.ugoods
域名线索:	35条
URL线索:	40条
邮箱线索:	0条
分析日期:	2022年1月25日 22:58

文件信息

文件名: youwu457017.apk
文件大小: 4.65MB
MD5值: 9736332880cc3801d4e1ed3864b02927
SHA1值: 5e76fb15254c927cdb1800a3e652392b68baa5e8
SHA256值: dd8b291f2b7de9dd2c3f33e70dca2cd261cbb11d732e4b432b46d4dbb92b1e35

APP 信息

App名称: 由物
包名: com.miao.ugoods
主活动**Activity:** com.miao.ugoods.BootActivity
安卓版本名称: 1.0.0
安卓版本: 2

域名线索

域名	是否危险域名	服务器信息
log.umsns.com	good	**IP:** 59.82.29.248 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
www.umeng.com	good	**IP:** 59.82.31.154 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
api.github.com	good	**IP:** 192.30.255.116 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
plbslog.umeng.com	good	**IP:** 59.82.43.171 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:** 203.209.250.2 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
d-gt.getui.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
api.weixin.qq.com	good	**IP:** 109.244.145.152 **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
mobilegwpre.alipay.com	good	**IP:** 110.75.138.35 **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:** 203.209.250.6 **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
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

域名	是否危险域名	服务器信息
c.umsns.com	good	**IP:** 59.82.31.92 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
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
oauth2.umeng.com	good	**IP:** 59.82.60.43 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
uat.wanlinjia.cn	good	**IP:** 47.99.138.243 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
aaid.umeng.com	good	IP: 111.225.159.27 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810001 经度: 114.879440 查看地图: Google Map
ouplog.umeng.com	good	IP: 47.74.172.6 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
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
ulogs.umeng.com	good	IP: 106.11.86.69 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
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
open.weixin.qq.com	good	IP: 175.24.219.72 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
render.alipay.com	good	IP: 140.249.240.248 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
developer.umeng.com	good	IP: 59.82.31.210 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
ulogs.umengcloud.com	good	IP: 106.11.40.44 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
pslog.umeng.com	good	IP: 59.82.31.209 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
mobile.umeng.com	good	IP: 59.82.31.210 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
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
pre-c.umsns.com	good	IP: 59.82.29.25 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
long.open.weixin.qq.com	good	IP: 109.244.216.15 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
h5.m.taobao.com	good	IP: 36.99.228.231 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
alogus.umeng.com	good	IP: 106.11.43.144 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
www.wanlinjia.cn	good	IP: 47.114.196.172 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
sdk.open.phone.igexin.com	good	IP: 183.131.7.102 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
alogsus.umeng.com	good	IP: 106.11.43.229 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
c-hzgt2.getui.com	good	IP: 124.160.127.198 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
ai.login.umeng.com	good	IP: 59.82.60.44 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
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

URL信息	Url所在文件
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/m/h/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/m/h/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/m/h/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/m/h/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/h/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/h/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/m/i/a.java
https://mobilegwpre.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://api.github.com/repos/CXZYH/GoDead/readme	com/zhy/http/okhttp/utils/IndexOutOfBounds.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java

URL信息	Url所在文件
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://api.weixin.qq.com/sns/auth?access_token=	com/umeng/socialize/media/WeixinExtra.java
https://mobile.umeng.com/images/pic/home/social/img-1.png	com/umeng/socialize/net/LinkcardRequest.java
https://log.umsns.com/	com/umeng/socialize/net/base/SocializeRequest.java
https://ai.login.umeng.com/api/umed/event	com/umeng/socialize/net/analytics/SocialAnalytics.java
https://c.umsns.com/ulink/getRTC	com/umeng/socialize/tracker/a.java
https://pre-c.umsns.com/ulink/getRTC	com/umeng/socialize/tracker/a.java
https://log.umsns.com/	com/umeng/socialize/view/OauthDialog.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/socialize/utils/UrlUtil.java
https://log.umsns.com/	com/umeng/socialize/common/SocializeConstants.java

URL信息	Url所在文件
https://log.umsns.com/link/qq/download/	com/umeng/socialize/common/SocializeConstants.java
https://log.umsns.com/link/weixin/download/	com/umeng/socialize/common/SocializeConstants.java
http://www.umeng.com/social	com/umeng/socialize/common/SocializeConstants.java
http://log.umsns.com/link/weixin/download/	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?	com/umeng/socialize/handler/UMWXHandler.java
https://oauth2.umeng.com/oauth/token/acquire?	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/access_token?	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/umeng/socialize/handler/UMWXHandler.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
http://uat.wanlinjia.cn/	com/miao/ugoods/UrlUtil.java
https://www.wanlinjia.cn/	com/miao/ugoods/UrlUtil.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java

URL信息	Url所在文件
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://sdk.open.phone.igexin.com/api.php	com/igexin/push/a.java
https://c-hzgt2.getui.com/api.php	com/igexin/push/a.java
https://d-gt.getui.com/api.htm	com/igexin/push/a.java
http://bi.	com/igexin/push/config/b.java
http://config.	com/igexin/push/config/b.java
http://bi.	com/igexin/push/config/g.java
http://config.	com/igexin/push/config/g.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.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_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.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.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.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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器

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
getui.permission.GetuiService.com.miao.ugoods	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: CN=zaimi
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-30 07:18:51+00:00
Valid To: 2045-06-24 07:18:51+00:00
Issuer: CN=zaimi
Serial Number: 0x226f34e9
Hash Algorithm: sha256
md5: 56059a81272a8d2d943874718fb08786
sha1: afa611550b86c9c29f2c1eb1c54b8a67001e827a
sha256: bf42fe0e07b89ce582bb5b6a8fa14c4c8a0cc1b833b72ff3b2d3a6f9fecb595e
sha512: 05194a2ede56a0e24463e940c60396eab854dbe5fa41cc1d4dce10687f589ffeda61016ae73057d6ab0d83226c772891535e6363ba34e47cbdb568a3d931dc6c
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 0b764626ff377ff2ffb3c9a1b6dbb2f1e57d58eb03aa5fc2d820c6d0e75db63a

Exodus威胁情报

名称	分类	URL链接
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"Amap_Apikey" : "9e606bc29a37696dc7ff7b3a8c393a69"
"MiPush_AppKey" : "5341805588566"
"MiPush_AppSecret" : "6Ofx9agOr16FeLn+XQ8UQA=="
"TD_KEY" : "65a4658b585d46e8958f5b5a48059615"

加壳分析

文件列表	分析结果

<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</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
