MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

logo设计大师 1.0.1.APK

APP名称:	logo设计大师
包名:	com.mnt.logo
域名线索:	33条
URL线索:	37条
邮箱线索:	0条
分析日期:	2022年1月26日 19:29

文件信息

文件名: logosjds.apk
文件大小: 4.15MB
MD5值: 6f2fb02b0666e975aa287055e2a5708f
SHA1值: 0434f763e9a3d835226391b7c53d87cf03e8da64
SHA256值: bccc09e95ff7c6b28a6afdebba143369cf82a3f53321febd11b9cde987ccb4b2

APP 信息

App名称: logo设计大师
包名: com.mnt.logo
主活动Activity: com.mnt.logo.ui.MainActivity
安卓版本名称: 1.0.1
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
118.178.227.81	good	IP: 118.178.227.81 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
service.weibo.com	good	IP: 180.149.139.248 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
pingma.qq.com	good	IP: 119.45.78.184 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
kuaihua.cn	good	IP: 123.56.9.102 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
api.weibo.com	good	IP: 180.149.153.83 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
app.qq.com	good	IP: 182.254.63.77 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.mob.com	good	IP: 116.62.130.46 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
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
api.utag.mob.com	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
qzs.qq.com	good	IP: 182.254.48.158 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
api.weixin.qq.com	good	IP: 81.69.216.43 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: 74.50.61.58 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
51taohao.com	good	IP: 8.212.24.67 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
paygate-yf.meituan.com	good	**IP:** 101.236.12.31 **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
lks.share.mob.com	good	没有服务器地理信息.
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
mobilegw.stable.alipay.net	good	没有服务器地理信息.
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
up.sdk.mob.com	good	**IP:** 203.107.55.19 **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
weibo.com	good	IP: 180.149.138.246 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
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
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
open.weibo.cn	good	IP: 180.149.153.83 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
mta.oa.com	good	**IP:** 193.123.33.15 **所属国家:** Netherlands **地区:** Noord-Holland **城市:** Amsterdam **纬度:** 52.374031 **经度:** 4.889690 **查看地图:** Google Map
api.u.mob.com	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
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
p.share.mob.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
graph.qq.com	good	**IP:** 113.96.208.232 **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
ka90.net	good	**IP:** 123.56.9.102 **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
mta.qq.com	good	**IP:** 125.39.171.64 **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

🌐 URL线索

URL信息	Url所在文件
http://kuaihua.cn/interface/act?id=20	com/mnt/logo/ui/MainActivity.java

URL信息	Url所在文件
http://kuaihua.cn/interface/act?id=21	com/mnt/logo/ui/MainActivity.java
http://51taohao.com/51taohao/xieyi.html	com/mnt/logo/ui/ShopInfoActivity.java
http://118.178.227.81/renmai/interface/act?id=30	com/mnt/logo/ui/RegActivity.java
http://118.178.227.81/renmai/interface/act?id=31	com/mnt/logo/ui/RegActivity.java
http://ka90.net:8080/shop/wap/apppoint	com/mnt/logo/ui/fragment/FaXianFragment.java
http://51taohao.com/51taohao/about.html	com/mnt/logo/ui/fragment/MineFragment.java
http://ka90.net:8080/shop/wap/complain	com/mnt/logo/ui/fragment/MineFragment.java
http://ka90.net:8080/shop/wap/contact	com/mnt/logo/ui/fragment/MineFragment.java
http://ka90.net:8080/shop/interface/downloadapp/	com/mnt/logo/util/ShareUtil.java
http://ka90.net:8080/shop	com/mnt/logo/util/ShareUtil.java
http://ka90.net:8080/shop/imgs/app_logo.png	com/mnt/logo/util/ShareUtil.java
http://51taohao.com/web/shoplist	com/mnt/logo/service/YkjService.java
http://51taohao.com/web/shoplist	com/mnt/logo/service/DbService.java
http://51taohao.com/web/paimai_shoplist	com/mnt/logo/service/PmService.java
http://kuaihua.cn	com/mnt/logo/service/base/BaseService.java

URL信息	Url所在文件
http://kuaihua.cn/interface	com/mnt/logo/service/base/BaseService.java
http://api.u.mob.com	com/mob/MobUser.java
http://api.utag.mob.com/bdata	com/mob/commons/utag/UserTager.java
http://api.utag.mob.com/conf	com/mob/commons/utag/TagRequester.java
http://up.sdk.mob.com	com/mob/commons/filesys/FileUploader.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
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://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/c.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&	com/alipay/sdk/data/a.java
https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple	com/alipay/test/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

URL信息	Url所在文件
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
http://mta.qq.com/	com/tencent/wxop/stat/e.java
http://mta.oa.com/	com/tencent/wxop/stat/e.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/c.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/a.java
https://){1}	cn/sharesdk/framework/b/a.java
http://p.share.mob.com/tags/getTagList	cn/sharesdk/framework/authorize/f.java
https://graph.qq.com/oauth2.0/me	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com	cn/sharesdk/tencent/qq/c.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?sdkv=3.3.0.lite&display=mobile	cn/sharesdk/tencent/qq/a.java
http://app.qq.com/detail/com.tencent.mobileqq?autodownload=1&norecommend=1&rootvia=opensdk	cn/sharesdk/tencent/qq/a.java

URL信息	Url所在文件
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com/oauth2.0/me	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com/photo/upload_pic	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com	cn/sharesdk/tencent/qzone/b.java
http://lks.share.mob.com/share/genShareInfo	cn/sharesdk/sina/weibo/b.java
http://weibo.com/	cn/sharesdk/sina/weibo/SinaWeibo.java
https://open.weibo.cn/oauth2/authorize?	cn/sharesdk/sina/weibo/f.java
https://api.weibo.com/oauth2/default.html	cn/sharesdk/sina/weibo/h.java
https://api.weibo.com/oauth2/access_token	cn/sharesdk/sina/weibo/h.java
https://api.weibo.com/2/users/show.json	cn/sharesdk/sina/weibo/h.java
https://api.weibo.com/2/friendships/create.json	cn/sharesdk/sina/weibo/h.java
https://api.weibo.com/2/statuses/user_timeline.json	cn/sharesdk/sina/weibo/h.java
https://api.weibo.com/2/friendships/friends.json	cn/sharesdk/sina/weibo/h.java
https://api.weibo.com/2/friendships/friends/bilateral.json	cn/sharesdk/sina/weibo/h.java

URL信息	Url所在文件
https://api.weibo.com/2/friendships/followers.json	cn/sharesdk/sina/weibo/h.java
http://service.weibo.com/share/mobilesdk.php?	cn/sharesdk/sina/weibo/g.java
http://service.weibo.com/share/mobilesdk_uppic.php	cn/sharesdk/sina/weibo/g.java
http://lks.share.mob.com/share/shareLog	cn/sharesdk/sina/weibo/c.java
https://api.weixin.qq.com/sns/oauth2/access_token	cn/sharesdk/wechat/utils/h.java
https://api.weixin.qq.com/sns/oauth2/refresh_token	cn/sharesdk/wechat/utils/h.java
https://api.weixin.qq.com/sns/userinfo	cn/sharesdk/wechat/utils/h.java
http://www.mob.com/policy/en	Android String Resource
http://www.mob.com	Android String Resource
http://www.mob.com/policy/zh	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

向手机申请的权限	是否危险	类型	详细情况
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.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
com.mnt.logo.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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

签名证书

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=jiangsu, L=nanjing, O=rongdong, OU=rongdong, CN=rongdong
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-08-01 09:45:35+00:00
Valid To: 2045-07-26 09:45:35+00:00
Issuer: C=86, ST=jiangsu, L=nanjing, O=rongdong, OU=rongdong, CN=rongdong
Serial Number: 0xee1980a
Hash Algorithm: sha256
md5: 4078f2559cb4fdcae8afee8d6579261b
sha1: 642eb77608267eca8f0cc7d4a8eaeb13e3fe841b
sha256: 9e50105ea77fb39ad120f98086481165f6a4480015a935c88ddbad08f9e42da0
```

sha512: a704744eebaef83ce33843d2cedf248b7fb83de767d0b3c353a4587a4d59d6b8ec4f08b18199e4f18485d345ffd3f9ad88a73647b6c76bfb3ad6e1115fd63cae
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6a9b1ab9e4a56b6eac33597bbf07aa920c37bfc3464aeb7a715d1ca1480c2c25

Exodus威胁情报

名称	分类	URL链接
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

硬编码敏感信息

可能的敏感信息
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href="http://www.mob.com/policy/en">http://www.mob.com/policy/en</a>. If you agree with our service policy, please click "accept", if you do not agree with our service policy, please click "reject""
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"

可能的敏感信息
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href="http://www.mob.com/policy/en">http://www.mob.com/policy/en</a>. If you agree with our service policy, please click "accept", if you do not agree with our service policy, please click "reject""
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"mobcommon_authorize_dialog_accept" : "同意"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href="http://www.mob.com/policy/zh">http://www.mob.com/policy/zh</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobcommon_authorize_dialog_reject" : "拒绝"
"mobcommon_authorize_dialog_title" : "服务授权"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.mob.tools.MobUIShell	Schemes: tencent1109428623://,
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent1109428623://,

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td></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
possible ro.secure check
emulator file check</td></tr>
</table>
</td></tr>
</table>

文件列表	分析结果
classes.dex	

分析结果	详细情况
编译器	r8

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