MoGua

APP线索分析报告

报告由 [摸瓜APP分析平台(mogua.co)](https://mogua.co) 生成

跟屁虫 7.91.APK

APP名称:	跟屁虫
包名:	com.mobileann.mafamily
域名线索:	56条
URL线索:	67条
邮箱线索:	0条
分析日期:	2022年1月26日 18:57

文件信息

文件名: genpizhong.apk
文件大小: 7.32MB
MD5值: 806b43637f086c3b46d80db6eed82259
SHA1值: 7db97e222cbf30ffaf662a7e1141573d9372c43e
SHA256值: 42e46846fc1c7ecb949f175a2670043c8801fed117b0cebd3ee398c1508e68eb

APP 信息

App名称: 跟屁虫
包名: com.mobileann.mafamily
主活动**Activity:** mobileann.mafamily.act.main.WelcomeActivity
安卓版本名称: 7.91
安卓版本: 313

域名线索

域名	是否危险域名	服务器信息
d1.client.map.bdimg.com	good	**IP:** 221.194.182.35 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
alog.umeng.co	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
fusion.qq.com	good	**IP:** 121.51.36.15 **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
init.sms.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
openmobile.qq.com	good	**IP:** 113.96.208.233 **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
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

域名	是否危险域名	服务器信息
itsdata.map.baidu.com	good	**IP:** 111.206.209.180 **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
client.mobileann.com	good	没有服务器地理信息.
dev.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
cgi.qplus.com	good	**IP:** 0.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
its.map.baidu.com	good	**IP:** 112.80.248.49 **所属国家:** China **地区:** Jiangsu **城市:** Nanjing **纬度:** 32.061668 **经度:** 118.777779 **查看地图:** Google Map

域名	是否危险域名	服务器信息
oc.umeng.com	good	**IP:** 203.119.128.55 **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
www.mobileann.com	good	**IP:** 217.194.134.138 **所属国家:** United Kingdom of Great Britain and Northern Ireland **地区:** England **城市:** London **纬度:** 51.508530 **经度:** -0.125740 **查看地图:** Google Map
log.sms.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
url.cn	good	**IP:** 58.60.9.100 **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
wap.mobileann.com记得安装注册后填写推荐码	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
sapi.map.baidu.com	good	**IP:** 163.177.151.253 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
loc.map.baidu.com	good	**IP:** 111.206.209.175 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
mo.baidu.com	good	**IP:** 111.206.209.136 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
qzs.qq.com	good	**IP:** 182.254.48.164 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
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
v.map.baidu.com	good	**IP:** 111.206.209.185 **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
wp.map.baidu.com	good	**IP:** 111.206.209.185 **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
devs.data.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
api.mobileann.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
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
wspeed.qq.com	good	没有服务器地理信息.
api.exc.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
sv.map.baidu.com	good	**IP:** 111.206.209.186 **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
lba.baidu.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
sdkapi.sms.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
appsupport.qq.com	good	IP: 183.2.144.86 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
client.map.baidu.com	good	IP: 111.206.209.119 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.umeng.com	good	IP: 59.82.29.162 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
skyhookwireless.com	good	**IP:** 96.45.82.232 **所属国家:** United States of America **地区:** Virginia **城市:** Reston **纬度:** 38.938862 **经度:** -77.346191 **查看地图:** Google Map
code.sms.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
www.bjtime.cn	good	没有服务器地理信息.
app.navi.baidu.com	good	**IP:** 111.206.209.213 **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
c.isdspeed.qq.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
sns.whalecloud.com	good	IP: 203.119.244.125 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
vector0.map.bdimg.com	good	IP: 221.194.182.35 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
alog.umeng.com	good	IP: 59.82.29.246 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
sapi.skyhookwireless.com	good	IP: 54.169.126.245 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
shang.qq.com	good	**IP:** 121.51.8.34 **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
log.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
daohang.map.baidu.com	good	**IP:** 111.206.209.190 **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
sv0.map.bdimg.com	good	**IP:** 111.206.209.186 **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
oc.umeng.co	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
sdk.e.qq.com	good	IP: 58.250.137.37 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
addrlist.sms.mob.com	good	没有服务器地理信息.
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.map.baidu.com	good	IP: 111.206.208.72 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
wap.mobileann.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
newvector.map.baidu.com	good	**IP:** 111.206.209.177 **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
cgi.connect.qq.com	good	**IP:** 183.2.144.86 **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
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://api.exc.mob.com:80	com/mob/commons/logcollector/c.java

URL信息	Url所在文件
http://devs.data.mob.com:80/dinfo	com/mob/commons/authorize/a.java
http://devs.data.mob.com:80/dsign	com/mob/commons/authorize/a.java
http://api.exc.mob.com:80	com/mob/logcollector/a.java
http://或者https://开头	com/umeng/socialize/media/QQShareContent.java
http://log.umsns.com/	com/umeng/socialize/net/base/SocializeClient.java
http://log.umsns.com/share/auth/	com/umeng/socialize/view/j.java
http://dev.umeng.com/social/android/share/quick-integration#social_weixin	com/umeng/socialize/weixin/controller/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=	com/umeng/socialize/weixin/controller/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=	com/umeng/socialize/weixin/controller/UMWXHandler.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/umeng/socialize/weixin/controller/UMWXHandler.java
http://www.umeng.com/social	com/umeng/socialize/common/SocializeConstants.java
http://sns.whalecloud.com	com/umeng/socialize/sso/SinaSsoHandler.java
http://dev.umeng.com/social/android/share/quick-integration#social_qzone_sso	com/umeng/socialize/sso/QZoneSsoHandler.java
http://dev.umeng.com/social/android/share/quick-integration#social_qq_sso	com/umeng/socialize/sso/UMQQSsoHandler.java
http://www.umeng.com/social	com/umeng/socialize/sso/UMSsoHandler.java

URL信息	Url所在文件
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umeng.co/app_logs	com/umeng/analytics/a.java
http://oc.umeng.com/check_config_update	com/umeng/analytics/a.java
http://oc.umeng.co/check_config_update	com/umeng/analytics/a.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/f.java
http://log.umsns.com/	com/umeng/analytics/social/e.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/umeng/message/proguard/C0074l.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/umeng/message/proguard/C0070h.java
http://%s/rest/api3.do	com/umeng/message/proguard/C0047ad.java
http://pingma.qq.com:80/mstat/report	com/tencent/stat/StatConfig.java
http://mta.qq.com/	com/tencent/stat/StatService.java
http://mta.oa.com/	com/tencent/stat/StatService.java
http://openmobile.qq.com/api/check?page=shareindex.html&style=9	com/tencent/connect/share/QQShare.java
http://openmobile.qq.com/api/check2?page=qzshare.html&loginpage=loginindex.html&logintype=qzone	com/tencent/connect/share/QzoneShare.java

URL信息	Url所在文件
http://cgi.connect.qq.com/qqconnectutil/sdk	com/tencent/connect/a/a.java
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/auth/AuthDialog.java
https://openmobile.qq.com/	com/tencent/connect/common/Constants.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiIml.java
http://c.isdspeed.qq.com/code.cgi	com/tencent/open/b/d.java
https://openmobile.qq.com/	com/tencent/open/utils/HttpUtils.java
http://cgi.qplus.com/report/report	com/tencent/open/utils/Util.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/OpenConfig.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin/qzapps/mapp_getappinfo.cgi	com/tencent/open/utils/ServerSetting.java
http://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com	com/tencent/open/utils/ServerSetting.java

URL信息	Url所在文件
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/brag/sdk_brag.html?	com/tencent/open/utils/ServerSetting.java
https://openmobile.qq.com/	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/reactive/sdk_reactive.html?	com/tencent/open/utils/ServerSetting.java
http://wspeed.qq.com/w.cgi	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/not_support.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/open/utils/ServerSetting.java
http://qzs.qq.com/open/mobile/sdk_common/down_qq.htm?	com/tencent/open/utils/ServerSetting.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin/prize_sharing/exchange_prize.cgi	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin/prize_sharing/get_activity_state.cgi	com/tencent/open/utils/ServerSetting.java

URL信息	Url所在文件
http://fusion.qq.com/cgi-bin/prize_sharing/make_share_url.cgi	com/tencent/open/utils/ServerSetting.java
http://fusion.qq.com/cgi-bin/prize_sharing/query_unexchange_prize.cgi	com/tencent/open/utils/ServerSetting.java
http://lba.baidu.com/	com/baidu/location/BDLocation.java
https://sapi.skyhookwireless.com/wps2/reverse-geo	com/baidu/location/h/a.java
http://skyhookwireless.com/wps/2005	com/baidu/location/h/a.java
http://loc.map.baidu.com/statloc	com/baidu/location/c/f.java
http://loc.map.baidu.com/cc.php	com/baidu/location/c/e.java
http://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/c/e.java
http://%s/%s	com/baidu/location/e/b.java
http://loc.map.baidu.com/offline_loc	com/baidu/location/e/d.java
https://loc.map.baidu.com/sdk.php	com/baidu/location/i/f.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/i/i.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/i/i.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/i/i.java
http://loc.map.baidu.com/tcu.php	com/baidu/location/i/i.java

URL信息	Url所在文件
http://loc.map.baidu.com/rtbu.php	com/baidu/location/i/i.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/i/i.java
https://sapi.skyhookwireless.com/wps2/location	com/baidu/location/i/i.java
http://loc.map.baidu.com/wloc	com/baidu/location/i/i.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/i/i.java
http://app.navi.baidu.com/mobile/#navi/naving/	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://daohang.map.baidu.com/mobile/#navi/naving/start=	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://daohang.map.baidu.com/mobile/#search/search/qt=nav&sn=2$$$$$$	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://mo.baidu.com/map/	com/baidu/mapapi/utils/OpenClientUtil.java
http://api.map.baidu.com/place/detail?	com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java
http://api.map.baidu.com/place/search?	com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java
http://api.map.baidu.com/direction?	com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java
https://sapi.map.baidu.com/sdkcs/verify	com/baidu/lbsapi/auth/i.java
http://c.isdspeed.qq.com/code.cgi	com/qq/e/comm/services/RetCodeService.java
http://sdk.e.qq.com/err	com/qq/e/comm/services/a.java

URL信息	Url所在文件
http://sdk.e.qq.com/launch	com/qq/e/comm/services/a.java
http://sdk.e.qq.com/activate	com/qq/e/comm/services/a.java
http://wap.mobileann.com记得安装注册后填写推荐码	mobileann/mafamily/act/member/AddByAcountActivity.java
http://www.mobileann.com	mobileann/mafamily/act/setup/AboutActivity.java
http://www.mobileann.com/	mobileann/mafamily/act/setup/ContactFragment.java
http://client.mobileann.com/page/gpc_security.php	mobileann/mafamily/act/eye/SafeSettingActivity.java
http://api.mobileann.com//api/gpc_get_api.phps?1_list_desktop	mobileann/mafamily/utils/AppDetailsManager.java
http://api.map.baidu.com/marker?location=	mobileann/mafamily/utils/MySelfUtils.java
http://www.bjtime.cn	mobileann/mafamily/utils/MySelfUtils.java
http://api.map.baidu.com/geocoder/v2/?ak=%s&location=%s,%s&output=json	mobileann/mafamily/utils/BaiduLocationUtils.java
http://wap.mobileann.com	mobileann/mafamily/utils/ShareUtil.java
http://wap.mobileann.com记得安装注册后填写推荐码	mobileann/mafamily/utils/ShareUtil.java
http://client.mobileann.com/api/gpc_activity.php	mobileann/mafamily/utils/URLUtils.java
http://api.mobileann.com/	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/api/gpc_update.php	mobileann/mafamily/utils/URLUtils.java

URL信息	Url所在文件
http://client.mobileann.com/	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/page/gpc_protocol.php	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/api/gpc_feedback.php	mobileann/mafamily/utils/URLUtils.java
http://api.mobileann.com/api/gpc_set_api.php	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/page/gpc_help.php	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/page/gpc_help.php?os=android&open=1	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/page/gpc_help.php?os=android&open=2	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/page/gpc_help.php?os=android&open=3	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/page/gpc_help.php?os=android	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/api/gpc_get_promotion.php	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/api/gpc_online.php	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/api/gpc_device.php	mobileann/mafamily/utils/URLUtils.java
http://api.mobileann.com//api/gpc_get_api.phps?	mobileann/mafamily/utils/URLUtils.java
http://client.mobileann.com/page/gpc_manual.php	mobileann/mafamily/utils/URLUtils.java
http://www.mobileann.com	mobileann/mafamily/utils/code/CodeUtils.java

URL信息	Url所在文件
http://%s/rest/api3.do	org/android/agoo/client/AgooSettings.java
http://%s/activeip/	org/android/agoo/client/AgooSettings.java
http://sdkapi.sms.mob.com/utils/zonelist	cn/smssdk/net/a.java
http://log.sms.mob.com/log/install	cn/smssdk/net/a.java
http://log.sms.mob.com/log/collect	cn/smssdk/net/a.java
http://addrlist.sms.mob.com/relat/fm	cn/smssdk/net/a.java
http://addrlist.sms.mob.com/relat/apply	cn/smssdk/net/a.java
http://code.sms.mob.com/voice/verify/code	cn/smssdk/net/a.java
http://code.sms.mob.com/verify/code	cn/smssdk/net/a.java
http://sdkapi.sms.mob.com/app/submituserinfo	cn/smssdk/net/a.java
http://sdkapi.sms.mob.com/token/get	cn/smssdk/net/a.java
http://code.sms.mob.com/client/verification	cn/smssdk/net/a.java
http://init.sms.mob.com/sdk/init	cn/smssdk/utils/a.java
http://url.cn/M2fpgJ	Android String Resource
http://shang.qq.com/wpa/qunwpa?idkey=5fc3732afbe8027acf8a3abdc7ebb49393f5e38ecfd408f1627d936a079feb6f	Android String Resource

URL信息	Url所在文件
www.umeng.com/social	Android String Resource
http://client.map.baidu.com/imap/sdk/tj?qt=vmap	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://v.map.baidu.com/low/	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://v.map.baidu.com/indoorinside/	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://v.map.baidu.com/high/	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://newvector.map.baidu.com/grid_vc/	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://vector0.map.bdimg.com/vecdata/	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://its.map.baidu.com:8003/its.php	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://wp.map.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://api.map.baidu.com/sdkws/heatmap?	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/footmap/image.php?	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://sv.map.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://sv0.map.bdimg.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/phpui2/?	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/offline-search/?	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so

URL信息	Url所在文件
http://d1.client.map.bdimg.com/offline-search/?	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi-v7a/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_base_v3_6_1.so
http://client.map.baidu.com/phpui2/	lib/armeabi-v7a/libBaiduMapSDK_base_v3_6_1.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi-v7a/libBaiduMapSDK_base_v3_6_1.so
http://client.map.baidu.com/imap/sdk/tj?qt=vmap	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://v.map.baidu.com/low/	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://v.map.baidu.com/indoorinside/	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://v.map.baidu.com/high/	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://newvector.map.baidu.com/grid_vc/	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://vector0.map.bdimg.com/vecdata/	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://its.map.baidu.com:8003/its.php	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://wp.map.baidu.com/	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://api.map.baidu.com/sdkws/heatmap?	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/footmap/image.php?	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so

URL信息	Url所在文件
http://sv.map.baidu.com/	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://sv0.map.bdimg.com/	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/phpui2/?	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/offline-search/?	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://d1.client.map.bdimg.com/offline-search/?	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi/libBaiduMapSDK_map_v3_6_1.so
http://client.map.baidu.com/	lib/armeabi/libBaiduMapSDK_base_v3_6_1.so
http://client.map.baidu.com/phpui2/	lib/armeabi/libBaiduMapSDK_base_v3_6_1.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi/libBaiduMapSDK_base_v3_6_1.so

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.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作

向手机申请的权限	是否危险	类型	详细情况
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.BAIDU_LOCATION_SERVICE	未知	Unknown permission	Unknown permission from android reference
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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_MOCK_LOCATION	危险	用于测试的模拟位置源	创建模拟位置源进行测试。恶意应用程序可以使用它来覆盖由真实位置源（如GPS 或网络提供商）返回的位置和/或状态
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.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
com.android.launcher.permission.READ_SETTINGS	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.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
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_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息

向手机申请的权限	是否危险	类型	详细情况
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
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
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定

向手机申请的权限	是否危险	类型	详细情况
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
org.agoo.android.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统

向手机申请的权限	是否危险	类型	详细情况
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.ACCESS_COARSE_UPDATES	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=Beijing, L=Beijing, O=MobileAnn Information Technology (Beijing) Co.Ltd, OU=MobileAnn Information Technology (Beijing) Co.Ltd, CN=Mobile Ann
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-01-22 07:49:32+00:00

Valid To: 2036-01-16 07:49:32+00:00
Issuer: C=86, ST=Beijing, L=Beijing, O=MobileAnn Information Technology (Beijing) Co.Ltd, OU=MobileAnn Information Technology (Beijing) Co.Ltd, CN=Mobile Ann
Serial Number: 0x4d3a8c0c
Hash Algorithm: sha1
md5: f42eb940971445adcc0a3853e8088008
sha1: 270f41df373663c6e4541ae378236f064df6b5e1
sha256: c938839b5c2b9ade097c191bf935e1fcd57dea89ee963a5ee1b9d2cf31db540c
sha512: 17d85bb65487f31e49813270bf4b7e112f20800cc84284fd4a03de6c7b20706b96877d82ea1a690e6d1bdfe7659368574a68eb176b2931edca2519be7d8588f3

Exodus威胁情报

名称	分类	URL链接
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"password" : "密 码"
"input_password" : "请输入密码"
"remember_password" : "记住密码"

可能的敏感信息
"map_fragment_no_user" : "系统中不存在此用户"
"one_key_reg" : "一键注册并登录"
"login_pwd" : "初始密码为手机号"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent101027754://,

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>APK包</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>unknown (please file detection issue!)</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.BOARD check
SIM operator check
network operator name check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!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.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>

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