MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

海王聊天 2.5.6.APK

APP名称:	海王聊天
包名:	com.yc.verbaltalk
域名线索:	78条
URL线索:	74条
邮箱线索:	0条

分析日期: 2022年1月28日 23:59

文件信息

文件名: hwlt.apk
文件大小: 7.74MB
MD5值: 9b1e786dd8da56466ac27142187dcd8c
SHA1值: 30e4bdc55e717adaecb246c30012e8a288f6dbb1
SHA256值: 2290a8079e9773f4dedce589cdb5db91e81263f746c36acc86a2d5a31b0e5538

APP 信息

App名称: 海王聊天
包名: com.yc.verbaltalk
主活动Activity: com.yc.verbaltalk.base.activity.SpecializedActivity
安卓版本名称: 2.5.6
安卓版本: 23

域名线索

域名	是否危险域名	服务器信息
i.snssdk.com	good	**IP:** 125.39.216.238 **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

域名	是否危险域名	服务器信息
toblog.itobsnssdk.com	good	**IP:** 104.116.243.152 **所属国家:** Taiwan (Province of China) **地区:** Taipei **城市:** Taipei **纬度:** 25.047760 **经度:** 121.531853 **查看地图:** Google Map
sdfp-sg.byteoversea.com	good	**IP:** 104.74.70.171 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **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
ytx.wk2.com	good	**IP:** 60.28.196.240 **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
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
qzs.qq.com	good	**IP:** 182.254.54.201 **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
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

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
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
log.umsns.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
schemas.android.com	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.
extlog.snssdk.com	good	**IP:** 60.28.226.31 **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
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
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
bds-va.byteoversea.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
rqd.uu.qq.com	good	**IP:** 182.254.88.185 **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
toppic-mszs.oss-cn-hangzhou.aliyuncs.com	good	**IP:** 118.31.219.222 **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
sj.qq.com	good	**IP:** 109.244.244.91 **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
success.ctobsnssdk.com	good	**IP:** 150.223.251.229 **所属国家:** China **地区:** Shandong **城市:** Jinan **纬度:** 36.668331 **经度:** 116.997223 **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
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
stats.umsns.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
service.weibo.com	good	**IP:** 39.156.6.59 **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
tic.upkao.com	good	**IP:** 106.225.229.16 **所属国家:** China **地区:** Jiangxi **城市:** Nanchang **纬度:** 28.683331 **经度:** 115.883331 **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
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
alogsus.umeng.com	good	**IP:** 106.11.43.142 **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
nz.qqtn.com	good	**IP:** 125.39.135.110 **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
log.snssdk.com	good	**IP:** 42.81.213.193 **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

域名	是否危险域名	服务器信息
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
c.isdspeed.qq.com	good	没有服务器地理信息.
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 **所属国家:** Korea (Republic of) **地区:** Seoul-teukbyeolsi **城市:** Seoul **纬度:** 37.568260 **经度:** 126.977829 **查看地图:** Google Map
developer.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
sf3-ttcdn-tos.pstatp.com	good	**IP:** 42.81.213.228 **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
alogus.umeng.com	good	**IP:** 106.11.86.76 **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

域名	是否危险域名	服务器信息
toblog.tobsnssdk.com	good	**IP:** 103.136.220.204 **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
tobapplog.tobsnssdk.com	good	**IP:** 103.136.220.204 **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
en.qqtn.com	good	**IP:** 106.225.229.42 **所属国家:** China **地区:** Jiangxi **城市:** Nanchang **纬度:** 28.683331 **经度:** 115.883331 **查看地图:** Google Map
h5.m.taobao.com	good	**IP:** 125.39.135.240 **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
ulogs.umengcloud.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
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
is.snssdk.com	good	**IP:** 42.81.213.191 **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

域名	是否危险域名	服务器信息
p3-tt.byteimg.com	good	**IP:** 60.28.216.240 **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
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
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
cmnsguider.yunos.com	good	**IP:** 203.119.169.224 **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
ulogs.umeng.com	good	**IP:** 106.11.86.77 **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
success.tobsnssdk.com	good	**IP:** 103.136.220.204 **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
sdfp-va.byteoversea.com	good	**IP:** 104.116.243.25 **所属国家:** Taiwan (Province of China) **地区:** Taipei **城市:** Taipei **纬度:** 25.047760 **经度:** 121.531853 **查看地图:** Google Map

域名	是否危险域名	服务器信息
tobapplog.ctobsnssdk.com	good	**IP:** 42.81.156.229 **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
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
love.bshu.com	good	**IP:** 112.74.184.143 **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
crm.bytedance.com	good	**IP:** 36.99.228.224 **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.chengzijianzhan.com	good	**IP:** 36.99.32.248 **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
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
open.weixin.qq.com	good	**IP:** 175.24.209.30 **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
127.0.0.1	good	**IP:** 127.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
sdfp.snssdk.com	good	**IP:** 58.49.162.227 **所属国家:** China **地区:** Hubei **城市:** Wuhan **纬度:** 30.583330 **经度:** 114.266670 **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
bds-sg.byteoversea.com	good	**IP:** 103.136.220.204 **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
mobilegw.stable.alipay.net	good	没有服务器地理信息.
sns.whalecloud.com	good	**IP:** 203.119.214.125 **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
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

域名	是否危险域名	服务器信息
sf1-ttcdn-tos.pstatp.com	good	**IP:** 60.28.216.242 **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
success.itobsnssdk.com	good	**IP:** 104.116.243.154 **所属国家:** Taiwan (Province of China) **地区:** Taipei **城市:** Taipei **纬度:** 25.047760 **经度:** 121.531853 **查看地图:** Google Map
www.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
at.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
mobilegw.alipay.com	good	**IP:** 203.209.245.129 **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
huatuocode.huatuo.qq.com	good	没有服务器地理信息.
android.bugly.qq.com	good	**IP:** 109.244.244.35 **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
tobapplog.itobsnssdk.com	good	**IP:** 23.199.34.226 **所属国家:** Taiwan (Province of China) **地区:** Taipei **城市:** Taipei **纬度:** 25.047760 **经度:** 121.531853 **查看地图:** Google Map
bds.snssdk.com	good	**IP:** 42.81.156.229 **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
aexception.bugly.qq.com	good	**IP:** 101.226.233.161 **所属国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.222219 **经度:** 121.458061 **查看地图:** Google Map
toblog.ctobsnssdk.com	good	**IP:** 140.249.159.221 **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
wspeed.qq.com	good	没有服务器地理信息.

URL线索

URL信息
http://sns.whalecloud.com
https://sj.qq.com/myapp/detail.htm?apkName=com.yc.verbaltalk
https://bds-va.byteoversea.com
https://bds-sg.byteoversea.com
https://bds.snssdk.com
https://sdfp-va.byteoversea.com
https://sdfp-sg.byteoversea.com

URL信息
https://sdfp.snssdk.com
https://mobilegw.alipay.com/mgw.htm
https://mobilegw.alipaydev.com/mgw.htm
http://m.alipay.com/?action=h5quit
https://wappaygw.alipay.com/home/exterfaceAssign.htm?
https://mclient.alipay.com/home/exterfaceAssign.htm?
https://mcgw.alipay.com/sdklog.do
https://h5.m.taobao.com/mlapp/olist.html
https://mobilegw.alipay.com/mgw.htm
http://mobilegw.aaa.alipay.net/mgw.htm
http://mobilegw-1-64.test.alipay.net/mgw.htm
http://mobilegw.stable.alipay.net/mgw.htm
http://tic.upkao.com/apk/love.apk
https://sj.qq.com/myapp/detail.htm?apkName=com.yc.verbaltalk
http://nz.qqtn.com/zbsq/index.php?m=Home&c=zbsq&a=getCateList
http://nz.qqtn.com/zbsq/index.php?m=Home&c=Zbsq&a=start_zb
http://nz.qqtn.com/zbsq/index.php?
http://love.bshu.com/
http://en.qqtn.com/api/
http://toppic-mszs.oss-cn-hangzhou.aliyuncs.com/xfzs.apk
http://ytx.wk2.com/static/ueditor/php/upload1//20190308/15520293621027.jpg
http://127.0.0.1:
https://is.snssdk.com/api/ad/union/sdk/get_ads/
https://is.snssdk.com/api/ad/union/sdk/stats/
https://extlog.snssdk.com/service/2/app_log/
https://is.snssdk.com/api/ad/union/dislike_event/

URL信息
https://is.snssdk.com/api/ad/union/sdk/reward_video/reward/
https://is.snssdk.com/union/service/sdk/upload/
https://is.snssdk.com/api/ad/union/sdk/material/check/
https://i.snssdk.com/inspect/aegis/client/page/
https://sf3-ttcdn-tos.pstatp.com/obj/ad-pattern/renderer/package.json
http://p3-tt.byteimg.com/img/web.business.image/201907245d0d495a0568785742e0b940~100x100.image
http://sf3-ttcdn-tos.pstatp.com/obj/mosaic-legacy/2b96e0005c6b6019f8a5b
https://www.chengzijianzhan.com/tetris/page/1639938884171780/? ad_id=1639940885031987&_toutiao_params=%7B%22cid%22%3A1639941324071955%2C%22device_id%22%3A38167681029%2C%22log_extra%22%3A%22%7B%5C%22ad_price%5C%22%3A%5C%22XThCVgADKYpdOEJWAAMpijdExKKDLYCp1GNXWw%5C%22%2C%5C%22c bf4b-4ff8-be68-9149e288a420u6714%5C%22%2C%5C%22rit%5C%22%3A901121375%7D%22%2C%22orit%22%3A900000000%2C%22req_id%22%3A%220781feb2-bf4b-4ff8-be68-9149e288a420u6714%22%2C%22rit%22%3A901121375%2C%22sign%22%3A%22D41D8CD98F
http://sf3-ttcdn-tos.pstatp.com/img/mosaic-legacy/2b96e0005c6b6019f8a5b~noop.jpg
https://sf1-ttcdn-tos.pstatp.com/obj/union-fe/playable/97699c8fb31e7836e828cffdd428bc80/index.html?toutiao_card_params=%7B%22name%22%3A%20%22%5Cu5168%5Cu6c11%5Cu6f02%5Cu79fb- 3D%5Cu98d9%5Cu8f66%22%2C%20%22pkg_name%22%3A%20%22com.joyfort.merge.car%22%2C%20%22id%22%3A%20163929997932851 6%2C%20%22download_url%22%3A%20%22https%3A//itunes.apple.com/cn/app/%25E5%2585%25A8%25E6%25B0%2591%25E6%2
http://sf1-ttcdn-tos.pstatp.com/obj/ttfe/adfe/union_endcard/union_test_tool.mp4
http://sf1-ttcdn-tos.pstatp.com/obj/ttfe/adfe/union_endcard/Lark20190725-175511.png
https://i.snssdk.com/api/ad/union/sdk/stats/
https://is.snssdk.com/api/ad/union/sdk/upload/app_info/
https://is.snssdk.com/api/ad/union/sdk/settings/
https://toblog.ctobsnssdk.com
https://tobapplog.ctobsnssdk.com
https://toblog.tobsnssdk.com
https://tobapplog.tobsnssdk.com
https://toblog.itobsnssdk.com
https://tobapplog.itobsnssdk.com
https://toblog.ctobsnssdk.com/service/2/device_register_only/
https://toblog.ctobsnssdk.com/service/2/app_alert_check/
https://toblog.ctobsnssdk.com/service/2/log_settings/

URL信息
https://toblog.ctobsnssdk.com/service/2/abtest_config/
https://success.ctobsnssdk.com
https://toblog.tobsnssdk.com/service/2/device_register_only/
https://toblog.tobsnssdk.com/service/2/app_alert_check/
https://toblog.tobsnssdk.com/service/2/log_settings/
https://toblog.tobsnssdk.com/service/2/abtest_config/
https://success.tobsnssdk.com
https://toblog.itobsnssdk.com/service/2/device_register_only/
https://toblog.itobsnssdk.com/service/2/app_alert_check/
https://toblog.itobsnssdk.com/service/2/log_settings/
https://toblog.itobsnssdk.com/service/2/abtest_config/
https://success.itobsnssdk.com
https://ulogs.umeng.com/unify_logs
https://alogus.umeng.com/unify_logs
https://alogsus.umeng.com/unify_logs
https://ulogs.umengcloud.com/unify_logs
https://cmnsguider.yunos.com:443/genDeviceToken
https://developer.umeng.com/docs/66632/detail/
https://plbslog.umeng.com
https://ouplog.umeng.com
https://at.umeng.com/0fqeCy?cid=476
https://api.weibo.com/2/users/show.json
https://api.weibo.com/oauth2/revokeoauth2
https://api.weibo.com/oauth2/getaid.json
https://log.umsns.com/
https://stats.umsns.com/

URL信息
https://log.umsns.com/
https://at.umeng.com/0fqeCy?cid=476
https://at.umeng.com/CuKXbi?cid=476
https://at.umeng.com/1HTzyC?cid=476
https://at.umeng.com/i8Dy8n?cid=476
https://at.umeng.com/ya4Dmy?cid=476
https://at.umeng.com/aOzmWf?cid=476
https://at.umeng.com/5P9baC?cid=476
https://at.umeng.com/ve4Pbm?cid=476
https://at.umeng.com/bObWzC?cid=476
https://at.umeng.com/8Tfmei?cid=476
https://at.umeng.com/9T595j?cid=476
https://at.umeng.com/CCiOHv?cid=476
https://at.umeng.com/KzKfWz?cid=476
https://at.umeng.com/LXzm8D?cid=476
https://at.umeng.com/Pn0TTr?cid=476
https://at.umeng.com/KD4zOf?cid=476
https://at.umeng.com/OTnqea?cid=476
https://at.umeng.com/jiia8D?cid=476
https://at.umeng.com/WT95za?cid=476
https://at.umeng.com/iWvmGD?cid=476
https://at.umeng.com/19HTvC?cid=476
https://at.umeng.com/iqmK1D?cid=476
https://at.umeng.com/CC0LLz?cid=476
https://at.umeng.com/9XX5ry?cid=476
https://at.umeng.com/4v4XPn?cid=476

URL信息
https://at.umeng.com/GPruqi?cid=476
https://at.umeng.com/9XXbCm?cid=476
https://at.umeng.com/KHDGXb?cid=476
https://at.umeng.com/HL1T9j?cid=476
https://at.umeng.com/iiuOHz?cid=476
https://at.umeng.com/SLDG5z?cid=476
https://at.umeng.com/f8HHDi?cid=476
https://at.umeng.com/H5vGLj?cid=476
https://at.umeng.com/uOjyCu?cid=476
https://at.umeng.com/9D49bu?cid=476
https://at.umeng.com/KfWLzu?cid=476
http://service.weibo.com/share/mobilesdk.php
http://service.weibo.com/share/mobilesdk_uppic.php
http://log.umsns.com/link/qq/download/
http://log.umsns.com/link/weixin/download/
http://www.umeng.com/social
https://open.weibo.cn/oauth2/authorize?
https://graph.qq.com/oauth2.0/me?access_token=
https://openmobile.qq.com/user/get_simple_userinfo?status_os=
https://graph.qq.com/oauth2.0/me?access_token=
https://api.weixin.qq.com/sns/userinfo?access_token=
https://api.weixin.qq.com/sns/oauth2/access_token?
https://api.weixin.qq.com/sns/oauth2/refresh_token?
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=
http://developer.umeng.com/docs/66650/cate/66650
http://android.bugly.qq.com/rqd/async

URL信息
http://astat.bugly.qcloud.com/rqd/async
http://rqd.uu.qq.com/rqd/sync
http://android.bugly.qq.com/rqd/async
http://android.bugly.qq.com/rqd/async
http://aexception.bugly.qq.com:8012/rqd/async
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s
https://graph.qq.com/oauth2.0/me
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1
https://openmobile.qq.com/oauth2.0/m_authorize?
https://openmobile.qq.com/user/user_login_statis
https://openmobile.qq.com/v3/user/get_info
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi
http://qzs.qq.com/open/mobile/login/qzsjump.html?
http://openmobile.qq.com/oauth2.0/m_jump_by_version?
http://qzs.qq.com/open/mobile/login/qzsjump.html?
http://qzs.qq.com/open/mobile/request/sdk_request.html?
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?
http://qzs.qq.com
https://huatuocode.huatuo.qq.com
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf
http://wspeed.qq.com/w.cgi
http://c.isdspeed.qq.com/code.cgi
http://sdk.e.qq.com/err

URL信息
http://sdk.e.qq.com/activate
http://sdk.e.qq.com/launch
http://xmlpull.org/v1/doc/features.html#indent-output
http://xmlpull.org/v1/doc/features.html#indent-output
http://xml.apache.org/xslt}indent-amount
https://crm.bytedance.com/audit/inspect/client/app/resend/
http://log.snssdk.com/service/2/app_log_exception/
http://schemas.android.com/apk/res/android
http://schemas.android.com/apk/res/android
http://schemas.android.com/apk/res/android

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.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_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.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_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.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.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.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
android.permission.REQUEST_PERMISSIONS	未知	Unknown permission	Unknown permission from android reference
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

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
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=123456, ST=china, L=china, O=yc, OU=com.yc.love, CN=Hello World
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-05-15 10:15:37+00:00
Valid To: 2049-05-07 10:15:37+00:00
Issuer: C=123456, ST=china, L=china, O=yc, OU=com.yc.love, CN=Hello World
Serial Number: 0x49bba5ca
Hash Algorithm: sha256
md5: 3ae24446daf815d1c9286cec4c699ba3
sha1: af7129eb5d3f365554c2ca23c3102a5da784a705
sha256: bfe4482c19e77885f590d5e31dd282c4c49b3a7c2a956aca13e3f8037bb35200
sha512: 1b321a5299b0c130c40a2d1e6e5d8982452d11f547a8bd5f359754b6e2dbd8c692be167c483b00f69b43b608a0b73f636f75be70059f3cc24676e6bf71b89d12

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"set_pwd" : "设置密码"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1109275009://,
com.umeng.qq.tencent.AuthActivity	Schemes: tencent1106261461://,
com.alipay.sdk.app.AlipayResultActivity	Schemes: alipaysdk://,

加壳分析

<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
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>lib/arm64-v8a/libnms.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>ByteGuard 0.9.3</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libnms.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>ByteGuard 0.9.3</td></tr>
</table>
</td></tr>
</table>

文件列表	分析结果
lib/armeabi/libnms.so	壳列表 | 详细情况 模糊器 | ByteGuard 0.9.3
lib/x86/libnms.so	壳列表 | 详细情况 模糊器 | ByteGuard 0.9.3
lib/x86_64/libnms.so	壳列表 | 详细情况 模糊器 | ByteGuard 0.9.3