MoGua

幻影分身 3.0.1.APK 分析报告

APP名称:	幻影分身
包名:	com.hy.clone

域名线索:	108条
URL线索:	90条
邮箱线索:	2条
分析日期:	2024年4月26日
分析平台:	摸瓜反编译平台

文件信息

文件名: 幻影分身.apk
文件大小: 22.72MB
MD5值: 297ebc22c6a1dfb74b91dc37c86ae6a9
SHA1值: 4daef169196c6ae8d7c0c096d72890ab69463c98
SHA256值: a78975600225412a716cdb743302ff627bfd81b37ab1e06baa8018fc0a9699ea

APP 信息

App名称: 幻影分身
包名: com.hy.clone
主活动Activity: wd.BR
安卓版本名称: 3.0.1
安卓版本: 301

域名线索

域名	服务器信息
mobilegw.aaa.alipay.net	没有服务器地理信息.
appcdn.ddyun.com	**IP**: 36.102.212.36 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
apiinit.amap.com	**IP**: 106.11.43.113 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
ulogs.umeng.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
yybdata.ddyun123.com	**IP**: 124.71.13.61 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou

	纬度: 23.116671 **经度**: 113.250000
www.coolapk.com	**IP**: 123.125.46.70 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
zhuoyao.wangandi.com	没有服务器地理信息.
zhushou.360.cn	**IP**: 112.65.208.95 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
wb.amap.com	**IP**: 59.82.31.164 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mobilegw.stable.alipay.net	没有服务器地理信息.
hyapi.huanyings.com	**IP**: 36.103.176.212 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
pslog.umeng.com	**IP**: 59.82.112.112 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423

mst01.is.autonavi.com	**IP**: 59.82.9.86 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
www.bilibili.com	**IP**: 117.23.60.13 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280
wappaygw.alipay.com	**IP**: 124.239.239.237 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
work.weixin.qq.com	**IP**: 106.55.127.35 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
yybdata.ddyun.com	**IP**: 124.71.13.61 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
lbs.amap.com	**IP**: 59.82.60.60 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423

i.snssdk.com	**IP**: 36.104.139.237 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
open.weixin.qq.com	**IP**: 175.24.219.72 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
api.xposed.info	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
yybapp.ddyun.com	**IP**: 124.71.13.61 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
long.open.weixin.qq.com	**IP**: 109.244.217.35 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
plbslog.umeng.com	**IP**: 36.156.202.68 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 59.82.39.12

c-adash.m.taobao.com	**所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
mobilegw.alipay.com	**IP**: 203.209.245.77 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
gdapi.ddyun.com	**IP**: 124.70.152.179 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
apilocate.amap.com	**IP**: 106.11.43.81 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
ulogs.umengcloud.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
app.ddyun.com	**IP**: 123.60.176.153 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
	IP: 203.119.175.208 **所属国家**: China **地区**: Beijing

m.pp.cn	**城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mpsapi.amap.com	**IP**: 106.11.43.68 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
gameapp.ddyun.com	**IP**: 117.27.139.140 **所属国家**: China **地区**: Fujian **城市**: Fuzhou **纬度**: 26.061390 **经度**: 119.306107
weixin.qq.com	**IP**: 101.226.94.124 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
test.ifengwoo.com.obs.myhwclouds.com	**IP**: 122.112.208.64 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
121.37.208.5	**IP**: 121.37.208.5 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
init.sms.mob.com	**IP**: 45.120.103.138 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou

	纬度: 32.397221 **经度**: 119.435829
gapp1.ddyun.com	**IP**: 124.70.152.179 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
sj.qq.com	**IP**: 109.244.244.91 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
instagram.com	**IP**: 31.13.112.4 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.343990 **经度**: -6.267190
dualstack-arestapi.amap.com	**IP**: 39.98.22.142 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
alogsus.umeng.com	**IP**: 223.109.148.130 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
apps.oceanengine.com	**IP**: 124.238.245.115 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717

abroad.apilocate.amap.com	**IP**: 59.82.44.11 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
mobilegw.alipaydev.com	**IP**: 110.75.132.131 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
h5coml.vivo.com.cn	**IP**: 123.151.120.205 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
android.bugly.qq.com	**IP**: 109.244.244.137 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
yybess.ddyun.com	**IP**: 124.71.13.61 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
gamedapi.ddyun.com	**IP**: 117.27.139.140 **所属国家**: China **地区**: Fujian **城市**: Fuzhou **纬度**: 26.061390 **经度**: 119.306107

alogus.umeng.com	**IP**: 223.109.148.130 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
sf6-ttcdn-tos.pstatp.com	**IP**: 61.147.216.109 **所属国家**: China **地区**: Jiangsu **城市**: Nantong **纬度**: 32.030281 **经度**: 120.874718
adiu.amap.com	**IP**: 59.82.31.203 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
wprd0d.is.autonavi.com	没有服务器地理信息.
xmlpull.org	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
ouplog.umeng.com	**IP**: 47.246.110.94 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
www.hyer.vip	**IP**: 59.49.89.55 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280

restsdk.amap.com	**IP**: 203.119.175.194 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
adash.m.taobao.com	**IP**: 59.82.39.12 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
gdapi1.ddyun.com	没有服务器地理信息.
m.facebook.com	**IP**: 128.242.240.212 **所属国家**: United States of America **地区**: California **城市**: Milpitas **纬度**: 37.428268 **经度**: -121.906616
hy.gwgo.qq.com	**IP**: 182.254.60.48 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545540 **经度**: 114.068298
pv.sohu.com	**IP**: 150.138.233.198 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
124.70.152.179	**IP**: 124.70.152.179 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000

gess1.ddyun.com	**IP**: 124.70.152.179 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
hydra.alibaba.com	**IP**: 203.119.169.88 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
gamedata.ddyun.com	**IP**: 117.27.139.140 **所属国家**: China **地区**: Fujian **城市**: Fuzhou **纬度**: 26.061390 **经度**: 119.306107
yybess.ddyun123.com	**IP**: 124.71.13.61 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
esscdn.ddyun.com	**IP**: 36.102.212.39 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
github.com	**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

identify.verify.mob.com	**IP**: 45.120.103.138 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435829
app.huanyings.com	**IP**: 36.103.176.216 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
dualstack-a.apilocate.amap.com	**IP**: 106.11.40.50 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
www.slf4j.org	**IP**: 83.173.251.158 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366669 **经度**: 8.550000
webcast.amemv.com	**IP**: 106.117.244.233 **所属国家**: China **地区**: Hebei **城市**: Tangshan **纬度**: 39.633331 **经度**: 118.183327
mclient.alipay.com	**IP**: 124.239.239.237 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
	IP: 106.11.35.98 **所属国家**: China

m5.amap.com	**地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
www.mob.com	**IP**: 116.62.130.46 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
gdata.ddyun.com	**IP**: 124.70.152.179 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
data.ddyun.com	**IP**: 123.60.176.153 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
aaid.umeng.com	**IP**: 218.91.197.67 **所属国家**: China **地区**: Jiangsu **城市**: Nantong **纬度**: 32.030281 **经度**: 120.874718
xml.apache.org	**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
ess.ddyun.com	**IP**: 119.3.10.58 **所属国家**: China **地区**: Shanghai **城市**: Shanghai

	纬度: 31.222219 **经度**: 121.458061
rqd.uu.qq.com	**IP**: 175.27.12.121 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
obs.ddyun.com	**IP**: 139.9.163.244 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
weibo.com	**IP**: 49.7.37.76 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
developer.umeng.com	**IP**: 59.82.29.248 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
mcgw.alipay.com	**IP**: 124.239.239.236 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
wap.amap.com	**IP**: 106.117.214.243 **所属国家**: China **地区**: Hebei **城市**: Tangshan **纬度**: 39.633331

	经度: 118.183327
m.alipay.com	**IP**: 203.209.245.74 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
webcast-open.douyin.com	**IP**: 124.238.245.115 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
yybapp.ddyun123.com	**IP**: 124.71.13.61 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
h5.m.taobao.com	**IP**: 111.225.210.165 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
www.wandoujia.com	**IP**: 203.119.175.233 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.lanzouy.com	**IP**: 150.138.233.199 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223

gess.ddyun.com	**IP**: 36.102.212.36 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
gapp.ddyun.com	**IP**: 36.102.212.37 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
yybdapi.ddyun123.com	**IP**: 124.71.13.61 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
dapi.ddyun.com	**IP**: 123.60.176.153 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
twitter.com	**IP**: 104.244.42.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
yuntuapi.amap.com	没有服务器地理信息.
www.samsungapps.com	**IP**: 52.31.24.56 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.343990 **经度**: -6.267190

appstore.huawei.com	没有服务器地理信息.
www.huanyings.com	**IP**: 36.103.176.219 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
url.cn	**IP**: 101.226.141.21 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
youtube.com	**IP**: 108.160.170.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
cgicol.amap.com	**IP**: 59.82.31.164 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
yybdapi.ddyun.com	**IP**: 124.71.13.61 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000

URL线索

URL信息	Url所在文件
http://api.xposed.info/using.html	de/robv/android/xposed/XposedInit.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	z1/rg0.java
https://h5.m.taobao.com/mlapp/olist.html	z1/v.java
https://url.cn/P1mNQodn?_type=wpa&qidian=true	z1/wb1.java
http://www.slf4j.org/codes.html	z1/kh2.java
https://mobilegw.alipay.com/mgw.htm	z1/s.java
https://mobilegw.alipaydev.com/mgw.htm	z1/s.java
http://m.alipay.com/?action=h5quit	z1/s.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	z1/s.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	z1/s.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	z1/te0.java
https://mcgw.alipay.com/sdklog.do	z1/n0.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	z1/ke0.java
http://xmlpull.org/v1/doc/features.html	z1/i60.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	z1/jf0.java
http://xml.apache.org/xslt	z1/x90.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	z1/sf0.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	z1/af0.java

https://github.com/ReactiveX/RxJava/wiki/Error-Handling	z1/pg0.java
http://www.slf4j.org/codes.html	z1/lh2.java
https://hy.gwgo.qq.com/sync/pet/	io/virtualapp/fake/modules/SpriteInfo.java
https://sj.qq.com/myapp/detail.htm?apkName=com.hy.clone	io/virtualapp/fake/fragment/MarktetDialogFragment.java
https://appstore.huawei.com/app/C101370217	io/virtualapp/fake/fragment/MarktetDialogFragment.java
http://zhushou.360.cn/detail/index/soft_id/4158860	io/virtualapp/fake/fragment/MarktetDialogFragment.java
https://m.pp.cn/detail.html?appid=8087804	io/virtualapp/fake/fragment/MarktetDialogFragment.java
https://www.wandoujia.com/apps/8087804	io/virtualapp/fake/fragment/MarktetDialogFragment.java
https://h5coml.vivo.com.cn/h5coml/appdetail_h5/browser_v2/index.html?appId=2841770&resource=301&source=7	io/virtualapp/fake/fragment/MarktetDialogFragment.java
http://www.huanyings.com/sdk-policy.html	io/virtualapp/fake/fragment/PrivateDialogFragment.java
http://www.huanyings.com/dy_help.html	io/virtualapp/fake/fragment/MineFragment.java
http://www.huanyings.com/wx_card_help.html	io/virtualapp/fake/fragment/MineFragment.java
https://weibo.com/p/1005057304191399	io/virtualapp/fake/fragment/MineFragment.java
http://www.huanyings.com/momo_help.html	io/virtualapp/fake/fragment/MomoDialogFragment.java
http://www.huanyings.com/findvip_help.html	zg/BK.java
https://www.bilibili.com/video/av71652893	zg/Bl.java
https://weibo.com/p/1005057304191399	zg/CV.java
https://www.coolapk.com/apk/	zg/r.java
https://work.weixin.qq.com/u/vcaf600352319bd6aa?v=4.0.0.80223	zg/r.java

http://hyapi.huanyings.com	zg/r.java
http://apilocate.amap.com	zg/r.java
http://zhuoyao.wangandi.com	zg/r.java
https://hy.gwgo.qq.com/sync/pet/	zg/r.java
https://weixin.qq.com	zg/r.java
https://www.lanzouy.com/huan90s	zg/r.java
https://www.lanzouy.com/plugin64301	zg/r.java
https://www.lanzouy.com/feclone	zg/r.java
https://www.lanzouy.com/plugin32301	zg/r.java
https://www.lanzouy.com/liantong12	zg/r.java
https://www.lanzouy.com/clone64	zg/r.java
http://www.huanyings.com/help.html	zg/r.java
https://www.lanzouy.com/clone	zg/r.java
http://www.hyer.vip	zg/r.java
http://www.huanyings.com	zg/r.java
http://www.huanyings.com/momo_help.html	le/CB.java
http://init.sms.mob.com/v3/sdk/init	cn/smssdk/utils/a.java
http://www.mob.com/about/policy\	cn/smssdk/utils/b.java
http://www.mob.com/about/policy	cn/smssdk/utils/b.java

http://identify.verify.mob.com/auth/verify/mobile\nparams:	cn/smssdk/net/h/e.java
http://identify.verify.mob.com/auth/verify/mobile	cn/smssdk/net/h/e.java
https://github.com/xuuhaoo/OkSocket	com/xuhao/didi/socket/client/impl/client/ManagerHolder.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/k0.java
https://adiu.amap.com/ws/device/adius	com/amap/api/col/p0003sl/a9.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003sl/q1.java
http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0	com/amap/api/col/p0003sl/h6.java
http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0	com/amap/api/col/p0003sl/h6.java
http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0	com/amap/api/col/p0003sl/h6.java
http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0	com/amap/api/col/p0003sl/h6.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/amap/api/col/p0003sl/wa.java
http://apiinit.amap.com/v3/log/init	com/amap/api/col/p0003sl/u6.java
http://restsdk.amap.com/v3/place/text?	com/amap/api/col/p0003sl/a.java
http://restsdk.amap.com/v3/place/around?	com/amap/api/col/p0003sl/a.java
http://restsdk.amap.com/v3/config/district?	com/amap/api/col/p0003sl/a.java
http://restsdk.amap.com/v3	com/amap/api/col/p0003sl/h4.java
https://restsdk.amap.com/v3	com/amap/api/col/p0003sl/h4.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003sl/h4.java
https://restsdk.amap.com/v4	com/amap/api/col/p0003sl/h4.java

http://yuntuapi.amap.com	com/amap/api/col/p0003sl/h4.java
https://yuntuapi.amap.com	com/amap/api/col/p0003sl/h4.java
http://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/p0003sl/h4.java
https://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/p0003sl/h4.java
http://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/p0003sl/h4.java
https://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/p0003sl/h4.java
http://apilocate.amap.com/mobile/binary	com/amap/api/col/p0003sl/vc.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/amap/api/col/p0003sl/vc.java
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\	com/amap/api/col/p0003sl/j9.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003sl/be.java
http://restsdk.amap.com/v4/grasproad/driving?	com/amap/api/col/p0003sl/n6.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/col/p0003sl/f2.java
https://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/p0003sl/e8.java
http://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/p0003sl/e8.java
http://wprd0%d.is.autonavi.com/appmaptile?	com/amap/api/col/p0003sl/e2.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/col/p0003sl/e2.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/amap/api/col/p0003sl/t6.java
https://restsdk.amap.com/v3/iasdkauth	com/amap/api/col/p0003sl/t6.java
http://restsdk.amap.com	com/amap/api/col/p0003sl/d7.java

http://wap.amap.com/	com/amap/api/maps/AMapUtils.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.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
http://121.37.208.5:8080/api/v3/EncodeService	com/cyjh/ddysdk/order/base/constants/a.java
http://121.37.208.5:8080/api/v3/EncodeService	com/cyjh/ddysdk/order/base/model/a.java
http://test.ifengwoo.com.obs.myhwclouds.com/DevOps/App/android/JUnit4/new/deviceEnvirCheck.tar	com/cyjh/ddysdk/device/command/DeviceToolModule$1.java
http://pv.sohu.com/cityjson?ie=utf-8	com/cyjh/ddy/base/utils/g.java
http://ess.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://124.70.152.179:8082/	com/cyjh/ddy/net/utils/a.java
http://gess.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://gess1.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://yybess.ddyun123.com/	com/cyjh/ddy/net/utils/a.java
http://yybess.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://esscdn.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://gamedata.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://gdata.ddyun.com/	com/cyjh/ddy/net/utils/a.java

http://yybdata.ddyun123.com/	com/cyjh/ddy/net/utils/a.java
http://yybdata.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://data.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://obs.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://gamedapi.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://gdapi.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://gdapi1.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://yybdapi.ddyun123.com/	com/cyjh/ddy/net/utils/a.java
http://yybdapi.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://dapi.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://gameapp.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://yybapp.ddyun123.com/	com/cyjh/ddy/net/utils/a.java
http://yybapp.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://appcdn.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://app.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://124.70.152.179:8081/	com/cyjh/ddy/net/utils/a.java
http://gapp.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://gapp1.ddyun.com/	com/cyjh/ddy/net/utils/a.java
http://xmlpull.org/v1/doc/features.html	com/lody/virtual/server/content/e.java

http://xmlpull.org/v1/doc/features.html	com/lody/virtual/server/pm/n.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/c/a/e.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/c/a/a.java
http://hydra.alibaba.com/	com/ta/utdid2/a/b.java
http://adash.m.taobao.com/rest/abtest	com/alibaba/sdk/android/tbrest/rest/RestConstants.java
http://c-adash.m.taobao.com/rest/gc	com/alibaba/sdk/android/tbrest/rest/RestConstants.java
http://adash.m.taobao.com/rest/sur	com/alibaba/sdk/android/tbrest/rest/RestConstants.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/autonavi/amap/mapcore/Inner_3dMap_location.java
http://m5.amap.com/	com/autonavi/base/amap/mapcore/maploader/AMapLoader.java
http://restsdk.amap.com/rest/lbs/dem/dataservice?z=%d&x=%d&y=%d&type=2	com/autonavi/base/ae/gmap/TerrainOverlayProvider.java
http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh_cn&size=1&scale=1&style=6	com/autonavi/base/ae/gmap/TerrainOverlayProvider.java
http://mpsapi.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java
http://m5.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java
http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/utils/g.java
http://apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/utils/b.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/utils/b.java
http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/utils/b.java
http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/trans/a.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/autonavi/aps/amapapi/trans/c.java

http://restsdk.amap.com/v3/geocode/regeo	com/autonavi/aps/amapapi/trans/c.java
https://webcast-open.douyin.com	com/bytedance/android/openliveplugin/material/LiveInitMaterialManager.java
https://webcast-open.douyin.com/webcast/openapi/pangle/setting/?app_id=	com/bytedance/android/openliveplugin/material/LiveInitMaterialManager.java
https://webcast.amemv.com/falcon/webcast_douyin/page/anchor_task_v2/panel/index.html?web_bg_color=%23ff161823	com/bytedance/android/live/base/api/BuildConfig.java
https://webcast.amemv.com/falcon/webcast_douyin/page/recharge_v1/index.html	com/bytedance/android/live/base/api/BuildConfig.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.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://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java

http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/beta/upgrade/BetaUploadStrategy.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
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://www.samsungapps.com/appquery/appDetail.as?appId=	com/ss/android/downloadlib/utils/g.java
https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/downloadlib/addownload/compliance/b.java
https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java
http://m.facebook.com/	mehdi/sakout/aboutpage/a.java
https://github.com/%s	mehdi/sakout/aboutpage/a.java
http://instagram.com/_u/	mehdi/sakout/aboutpage/a.java
http://twitter.com/intent/user?screen_name=%s	mehdi/sakout/aboutpage/a.java
http://youtube.com/channel/%s	mehdi/sakout/aboutpage/a.java
http://www.huanyings.com	Mogua Engine V1
http://app.huanyings.com/huan90s	Mogua Engine V1

邮箱线索

邮箱地址	所在文件

huan90s@163.com	zg/CV.java
发送到邮件huan90s@163.com	Mogua Engine V1

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=QD, ST=山东省, L=青岛市, O=海尔, OU=中国, CN=Huan
签名算法: rsassa_pkcs1v15
有效期自: 2018-12-15 11:47:04+00:00
有效期至: 2117-11-21 11:47:04+00:00
发行人: C=QD, ST=山东省, L=青岛市, O=海尔, OU=中国, CN=Huan
序列号: 0x6378bf70
哈希算法: sha256
md5值: a1ccb0d670efba1bc4353b1bc8ddf4f7
sha1值: f60eda7015da4c0e4d7b72a0bc509df7cd16429f
sha256值: 73d839943f868bd049f21ce6d96cff1dafab7e0e2d47d37e47b59fd06856b1cc
sha512值: d7dd8aa40f5bb099b50aaaa106beab45f1c1e7441b62ba89065a5b8b90db4306f9e51afd6f3fc0abbfa14b06678892878726eb1b4e26c7fb755fcde53e104dfe
公钥算法: rsa
密钥长度: 2048
指纹: 84e3ac84eeff5f677342d6d168c39101797aa5c72af5353ff65b859438dbe361

硬编码敏感信息

可能的敏感信息
"get_wxtoken_tip" : "1.可通过抓包工具获取微信小程序“捉妖雷达”的身份码，填写后即可共享。 2.年费用户共享成功一次，可以获得1天VIP时间奖励。 3.普通用户共享成功一次，可以获得两小时的雷达使用时间。 4.身份码获取方法可进入售后群或者王者群查看"

"gey_appkey_failure" : "连接服务器失败，请重新打开APP，若仍未解决，请联系客服"
"google_maps_key" : "AIzaSyDBMDDx4Yz7SNCm_Kq6MRZiKEGdapFfU44"
"input_pwd" : "请输入密码"
"share_wxtoken" : "填写身份码"
"smssdk_authorize_dialog_accept" : "同意"
"smssdk_authorize_dialog_reject" : "拒绝"
"smssdk_authorize_dialog_title" : "服务授权"
"token_expire" : "登录token过期或账号已在其他设备登录，请重新登录。"
"smssdk_authorize_dialog_accept" : "同意"
"smssdk_authorize_dialog_reject" : "拒绝"
"smssdk_authorize_dialog_title" : "服务授权"
"smssdk_authorize_dialog_accept" : "Agree"
"smssdk_authorize_dialog_reject" : "Disagree"
"smssdk_authorize_dialog_title" : "Terms of Use"
"get_wxtoken_tip" : "1.可通过抓包工具获取微信小程序“捉妖雷达”的身份码，填写后即可共享。 2.年费用户共享成功一次，可以获得1天VIP时间奖励。 3.普通用户共享成功一次，可以获得两小时的雷达使用时间。 4.身份码获取方法可进入售后群或者王者群查看"
"gey_appkey_failure" : "连接服务器失败，请重新打开APP，若仍未解决，请联系客服"
"input_pwd" : "请输入密码"
"share_wxtoken" : "填写身份码"
"token_expire" : "登录token过期或账号已在其他设备登录，请重新登录。"

加壳分析

第三方SDK

名称	分类	URL链接
Bugly	数据分析	https://reports.exodus-privacy.eu.org/trackers/190
Pangle	广告管理	https://reports.exodus-privacy.eu.org/trackers/363
友盟统计	数据分析	https://reports.exodus-privacy.eu.org/trackers/119
支付宝	身份识别, 支付平台, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/445
腾讯微信	身份识别, 支付平台, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/447
高德地图	位置服务	https://reports.exodus-privacy.eu.org/trackers/361

此APP的危险动作

应用内通信