



MoGua

부자가 null.APK 分析报告



APP名称:	부자가
包名:	im.ohedddikca.messenger
域名线索:	59条
URL线索:	66条
邮箱线索:	8条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 부자가
文件大小: 65.38MB
MD5值: 197a5781f953265ba6aa352c81bb9b62
SHA1值: 8c8f2010084db5f1bb8ac9bc3a340cf877c6af93
SHA256值: 6d051901be0b9a0cdf16004d8970d3984557f62145077b203acab5372013de14

i APP 信息

App名称: 부자가
包名: im.ohedddikca.messenger
主活动Activity: im.ohedddikca.ui.LaunchActivity
安卓版本名称: null
安卓版本:

域名线索

域名	服务器信息
dxdnbtobr08h6.cloudfront.net	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
wealthextend.huanhuit.com	IP: 103.224.212.216 所属国家: Australia 地区: Victoria 城市: Beaumaris 纬度: -37.982201

	经度: 145.038940
www.aparat.com	IP: 185.147.178.14 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran 纬度: 35.694241 经度: 51.421310
www.example.com	IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
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
daohang.map.baidu.com	IP: 111.206.209.190 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
coub.com	IP: 95.213.253.85 所属国家: Russian Federation 地区: Sankt-Peterburg 城市: Saint Petersburg 纬度: 59.894440 经度: 30.264200
daup.map.baidu.com	IP: 110.242.69.98 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
player.vimeo.com	IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
www.shareinstall.com.cn	IP: 101.28.249.78 所属国家: China 地区: Hebei 城市: Handan 纬度: 36.600559 经度: 114.467781
	IP: 3.165.102.57

api.twitch.tv	所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
youtube.googleapis.com	IP: 142.251.33.106 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660 经度: -79.382927
192.168.1.4	IP: 192.168.1.4 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
map.baidu.com	IP: 111.206.208.32 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
192.168.31.38	IP: 192.168.31.38 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.sl4j.org	IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge 纬度: 46.180931 经度: 6.138709
impyq.gz.bcebos.com	IP: 153.3.238.105 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
stripe.com	IP: 54.92.90.44 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
usher.ttvnw.net	IP: 65.9.42.9 所属国家: Japan 地区: Tokyo 城市: Tokyo

	纬度: 35.689499 经度: 139.692322
www.youtube.com	IP: 31.13.68.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
live.caillao.im	没有服务器地理信息.
www.ntsc.ac.cn	IP: 159.226.242.43 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.stripe.com	IP: 13.230.11.13 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
app.navi.baidu.com	IP: 111.206.209.213 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
m12345.cc	IP: 106.74.25.198 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
game.caillao.im	没有服务器地理信息.
106.13.253.35	IP: 106.13.253.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
m12345.com	IP: 75.2.19.62 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
	IP: 111.206.209.180 所属国家: China 地区: Beijing

itsdata.map.baidu.com	城市: Beijing 纬度: 39.907501 经度: 116.397102
wapmap.baidu.com	IP: 111.206.209.212 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
maps.googleapis	没有服务器地理信息.
ip-api.com	IP: 208.95.112.1 所属国家: United States of America 地区: North Carolina 城市: Skyland 纬度: 35.483757 经度: -82.521996
d.alipay.com	IP: 116.136.204.220 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
m.bjz.com	没有服务器地理信息.
game.bjz.com	没有服务器地理信息.
d20f1mv4ccrawx.cloudfront.net	IP: 3.165.91.17 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
bbs.lbsyun.baidu.com	没有服务器地理信息.
client.map.baidu.com	IP: 111.206.209.120 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
loc.map.baidu.com	IP: 111.206.209.175 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 213.180.204.41 所属国家: Russian Federation 地区: Moskva

static-maps.yandex.ru	城市: Moscow 纬度: 55.752258 经度: 37.615471
www.instagram.com	IP: 199.59.149.232 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
ss3.4sql.net	IP: 151.101.90.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
attheme.org	IP: 204.152.214.30 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
instagram.com	IP: 108.160.169.186 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
vop.baidu.com	IP: 111.206.209.68 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.smpte-ra.org	IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
twitter.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
192.200.1.242	IP: 192.200.1.242 所属国家: United States of America 地区: New Jersey 城市: Jersey City 纬度: 40.721169 经度: -74.044960

maps.google.com	IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
api.map.baidu.com	IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
schemas.android.com	没有服务器地理信息.
www.google.com	IP: 31.13.88.26 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
106.13.253.90	IP: 106.13.253.90 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
shibatch.sourceforge.net	IP: 104.18.12.149 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
youtube.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

openapi.baidu.com	IP: 110.242.69.36 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
j.map.baidu.com	IP: 111.206.209.187 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

 URL线索

URL信息	Url所在文件
http://app.navi.baidu.com/mobile/	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://daohang.map.baidu.com/mobile/	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://map.baidu.com/zt/client/index?fr=sdk_	com/baidu/mapapi/utlis/OpenClientUtil.java
http://api.map.baidu.com/direction?	com/baidu/mapapi/utlis/route/BaiduMapRoutePlan.java
http://api.map.baidu.com/place/detail?uid=	com/baidu/mapapi/utlis/poi/BaiduMapPoiSearch.java
http://api.map.baidu.com/place/search?	com/baidu/mapapi/utlis/poi/BaiduMapPoiSearch.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/g/k.java
https://loc.map.baidu.com/tcu.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/rtbu.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/g/k.java
http://loc.map.baidu.com/wloc	com/baidu/location/g/k.java
https://loc.map.baidu.com/sdk.php	com/baidu/location/g/k.java
https://daup.map.baidu.com/cltr/rcvr	com/baidu/location/g/k.java

http://loc.map.baidu.com/indoorlocbuildinginfo.php	com/baidu/location/indoor/a.java
http://loc.map.baidu.com/check_indoor_data_update	com/baidu/location/indoor/mapversion/a/e.java
https://loc.map.baidu.com/ios_indoorloc	com/baidu/location/indoor/mapversion/a/a.java
http://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet	com/baidu/location/indoor/mapversion/c/a.java
http://loc.map.baidu.com/cc.php	com/baidu/location/b/d.java
https://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/b/f.java
https://loc.map.baidu.com/cfgs/loc/commcfgs	com/baidu/location/c/e.java
http://loc.map.baidu.com/gpsz	com/baidu/location/c/a.java
https://api.map.baidu.com/lbs_sdkcc/report	com/baidu/mapsdkplatform/comapi/b/a/c.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/custom/v2/getjsonstyle	com/baidu/mapsdkplatform/comapi/map/h.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/custom/v2/getjsonstyle	com/baidu/mapsdkplatform/comapi/map/h.java
http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n=====\\n	com/baidu/mapsdkplatform/comapi/util/PermissionCheck.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/search	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/detail	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/indoor/v1/	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/suggestion	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/geocoder/v2	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/pathplan/v2/transit	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/phpui2/v1/	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/pathplan/v2/riding	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/	com/baidu/platform/domain/b.java
https://j.map.baidu.com/	com/baidu/platform/domain/b.java
https://client.map.baidu.com/imap/share/ps	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/s	com/baidu/platform/domain/b.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/search	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/detail	com/baidu/platform/domain/a.java

http://api.map.baidu.com/sdkproxy/lbs_androidsdk/indoor/v1/	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/suggestion	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/geocoder/v2	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/pathplan/v2/transit	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/phpui2/v1/	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/pathplan/v2/riding	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/	com/baidu/platform/domain/a.java
http://j.map.baidu.com/	com/baidu/platform/domain/a.java
http://client.map.baidu.com/imap/share/ps	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/s	com/baidu/platform/domain/a.java
http://wapmap.baidu.com/s?tn=Detail&pid=	com/baidu/platform/core/e/c.java
http://map.baidu.com/?newmap=1&s=	com/baidu/platform/core/e/e.java
https://api.map.baidu.com/sdkcs/verify	com/baidu/lbsapi/auth/LBSAuthManager.java
http://192.200.1.242:1999/	com/bjz/comm/net/UrlConstant.java
http://m.bjz.com/	com/bjz/comm/net/UrlConstant.java
https://106.13.253.35/	com/bjz/comm/net/UrlConstant.java
https://live.cailliao.im/	com/bjz/comm/net/UrlConstant.java
http://game.bjz.com/	com/bjz/comm/net/UrlConstant.java
https://game.cailliao.im	com/bjz/comm/net/UrlConstant.java
http://192.168.1.4:20000/	com/bjz/comm/net/UrlConstant.java
https://106.13.253.90/	com/bjz/comm/net/UrlConstant.java
https://impyq.gz.bcebos.com/	com/bjz/comm/net/UrlConstant.java
http://ip-api.com/json/	com/bjz/comm/net/UrlConstant.java
https://wealthextend.huanhuit.com/	com/bjz/comm/net/UrlConstant.java
https://vop.baidu.com/	com/bjz/comm/net/factory/ApiTranslateAudioFactory.java
https://impyq.gz.bcebos.com/	com/bjz/comm/net/utis/HttpUtils.java

http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videoCache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videoCache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videoCache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videoCache/Pinger.java
http://%s:%d/%s	com/danikula/videoCache/Pinger.java
http://%s:%d/%s	com/danikula/videoCache/HttpProxyCacheServer.java
http://www.smpte-ra.org/schemas/2052-1/2010/smp-te	com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java
http://schemas.android.com/apk/res/android	com/tablayout/SlidingScaleTabLayout.java
http://schemas.android.com/apk/res/android	com/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/tablayout/SlidingTabLayout.java
http://xml.apache.org/xslt	com/socks/library/klog/XmlLog.java
https://stripe.com/docs/stripe.js.	com/stripe/android/Stripe.java
https://stripe.com/docs/stripe.js	com/stripe/android/Stripe.java
https://api.stripe.com	com/stripe/android/net/StripeApiHandler.java
https://stripe.com/api	com/stripe/android/net/StripeApiHandler.java
https://twitter.com/stripestatus,	com/stripe/android/net/StripeApiHandler.java
https://static-maps.yandex.ru/1.x/?ll=%6f,%6f&z=%d&size=%d,%d&l=map&scale=%d&pt=%6f,%6f,vk&km&lang=%s	im/ohedddikka/messenger/AndroidUtilities.java
https://static-maps.yandex.ru/1.x/?ll=%6f,%6f&z=%d&size=%d,%d&l=map&scale=%d&lang=%s	im/ohedddikka/messenger/AndroidUtilities.java
http://api.map.baidu.com/staticimage/v2?ak=%s&mcode=%s¢er=%6f,%6f&width=%d&height=%d&zoom=%d&scale=%d&coordtype=gcj02ll©right=1&dpiType=ph&markers=%6f,%6f&markerStyle=l,,red	im/ohedddikka/messenger/AndroidUtilities.java
http://api.map.baidu.com/staticimage/v2?ak=%s&mcode=%s¢er=%6f,%6f&width=%d&height=%d&zoom=%d&scale=%d&coordtype=gcj02ll©right=1&dpiType=ph	im/ohedddikka/messenger/AndroidUtilities.java
https://instagram.com/	im/ohedddikka/messenger/MessageObject.java
https://www.instagram.com/explore/tags/	im/ohedddikka/messenger/MessageObject.java
https://twitter.com/	im/ohedddikka/messenger/MessageObject.java

https://twitter.com/hashtag/	im/ohedddikca/messenger/MessageObject.java
https://static-maps	im/ohedddikca/messenger/ImageLoader.java
https://maps.googleapis	im/ohedddikca/messenger/ImageLoader.java
https://m12345.com/dl	im/ohedddikca/messenger/ContactsController.java
https://m12345.cc/install.html?appkey=aa717156fa6e34325d3d4a7004a6647a	im/ohedddikca/messenger/MessagesController.java
http://www.shareinstall.com.cn/js-test.html?appkey=aa717156fa6e34325d3d4a7004a6647a	im/ohedddikca/messenger/MessagesController.java
http://www.example.com	im/ohedddikca/messenger/support/customtabsclient/shared/CustomTabsHelper.java
https://www.youtube.com/embed/	im/ohedddikca/messenger/utils/PlayerUtils.java
https://youtube.googleapis.com/v/	im/ohedddikca/messenger/utils/PlayerUtils.java
https://www.youtube.com/get_video_info?	im/ohedddikca/messenger/utils/PlayerUtils.java
https://www.youtube.com	im/ohedddikca/messenger/utils/PlayerUtils.java
https://player.vimeo.com/video/%s/config	im/ohedddikca/messenger/utils/PlayerUtils.java
http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s	im/ohedddikca/messenger/utils/PlayerUtils.java
https://api.twitch.tv/kraken/streams/%s?stream_type=all	im/ohedddikca/messenger/utils/PlayerUtils.java
https://api.twitch.tv/api/channels/%s/access_token	im/ohedddikca/messenger/utils/PlayerUtils.java
https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s	im/ohedddikca/messenger/utils/PlayerUtils.java
https://coub.com/api/v2/coubs/%s.json	im/ohedddikca/messenger/utils/PlayerUtils.java
http://www.google.com	im/ohedddikca/messenger/browser/Browser.java
https://www.google.com/resolve?name=	im/ohedddikca/tgnet/ConnectionsManager.java
https://dxdnbtobr08h6.cloudfront.net/dns-query	im/ohedddikca/tgnet/NetworkConfig.java
https://d20f1mv4ccrawx.cloudfront.net/dns-query	im/ohedddikca/tgnet/NetworkConfig.java
https://m12345.com/deactivate?phone=	im/ohedddikca/ui/TwoStepVerificationActivity.java
https://m12345.cc/deactivate?phone=	im/ohedddikca/ui/TwoStepVerificationActivity2.java
http://maps.google.com/maps?saddr=%f,%f&daddr=%f,%f	im/ohedddikca/ui/LocationActivity.java
http://youtube.com	im/ohedddikca/ui/ArticleViewer.java
https://m12345.com/embed	im/ohedddikca/ui/ArticleViewer.java

https://m12345.com/deactivate?phone=	im/ohedddikca/ui/PassportActivity.java
https://m12345.com/proxy?	im/ohedddikca/ui/ProxySettingsActivity.java
https://m12345.com/socks?	im/ohedddikca/ui/ProxySettingsActivity.java
https://m12345.com	im/ohedddikca/ui/ChatActivity.java
http://m12345.com	im/ohedddikca/ui/ChatActivity.java
https://m12345.com/authtoken/	im/ohedddikca/ui/ChatActivity.java
https://openapi.baidu.com/oauth/2.0/token	im/ohedddikca/ui/ChatActivity.java
https://vop.baidu.com/pro_api	im/ohedddikca/ui/ChatActivity.java
https://www.youtube.com/iframe_api\	im/ohedddikca/ui/components/EmbedBottomSheet.java
http://youtube.com	im/ohedddikca/ui/components/EmbedBottomSheet.java
https://www.youtube.com	im/ohedddikca/ui/components/EmbedBottomSheet.java
https://m12345.com/	im/ohedddikca/ui/components/URLSpanNoUnderline.java
https://www.youtube.com/embed/	im/ohedddikca/ui/components/WebPlayerView.java
https://youtube.googleapis.com/v/	im/ohedddikca/ui/components/WebPlayerView.java
https://www.youtube.com/get_video_info?	im/ohedddikca/ui/components/WebPlayerView.java
https://www.youtube.com	im/ohedddikca/ui/components/WebPlayerView.java
https://player.vimeo.com/video/%s/config	im/ohedddikca/ui/components/WebPlayerView.java
http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s	im/ohedddikca/ui/components/WebPlayerView.java
https://api.twitch.tv/kraken/streams/%s?stream_type=all	im/ohedddikca/ui/components/WebPlayerView.java
https://api.twitch.tv/api/channels/%s/access_token	im/ohedddikca/ui/components/WebPlayerView.java
https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s	im/ohedddikca/ui/components/WebPlayerView.java
https://coub.com/api/v2/coubs/%s.json	im/ohedddikca/ui/components/WebPlayerView.java
https://192.168.31.38:8080/v1/token	im/ohedddikca/ui/hui/visualcall/AlIRtcConstants.java
https://m12345.com	im/ohedddikca/ui/hui/discovery/QrScanActivity.java
http://m12345.com	im/ohedddikca/ui/hui/discovery/QrScanActivity.java
https://m12345.com/authtoken/	im/ohedddikca/ui/hui/discovery/QrScanActivity.java

http://www.ntsc.ac.cn	im/ohedddikca/ui/utls/timer/OrderCountDownHelper.java
http://shibatch.sourceforge.net/\n\n	im/ohedddikca/ui/utls/translate/ssrc/SSRC.java
https://d.alipay.com	im/ohedddikca/ui/wallet/WalletRechargeH5Activity.java
https://attheme.org?slug=	im/ohedddikca/ui/actionbar/Theme.java
https://ss3.4sqi.net/img/categories_v2/	im/ohedddikca/ui/adapters/BaseLocationAdapter.java
http://www.slf4j.org/codes.html	org.slf4j/MDC.java
http://www.slf4j.org/codes.html	org.slf4j/LoggerFactory.java

 邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java
support@stripe.com	com/stripe/android/net/StripeApiHandler.java
sms@stel.com	im/ohedddikca/ui/ChangePhoneActivity.java
login@stel.com sms@stel.com	im/ohedddikca/ui/LoginActivity.java
sms@stel.com	im/ohedddikca/ui/PassportActivity.java
sms@stel.com	im/ohedddikca/ui/CancelAccountDeletionActivity.java
login@stel.com sms@stel.com	im/ohedddikca/ui/hui/login/HloginActivity.java
login@stel.com	im/ohedddikca/ui/hui/login/LoginContronllerBaseActivity.java

 手机线索

手机号	所在文件
18345352118	com/baidu/mapsdkplatform/comapi/util/b.java
14058229493	im/ohedddikca/messenger/Utilities.java

 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=re2jyxRhFa2bDb9nhHnx, ST=VBIEH1T5Dxx5ISdYbLzX, L=u4Z0fiSCZ6S94Ww3tzQo, O=8Ldg9aG2i6VFdkksumR8, OU=jOlefNN5gL2lLOslwtRf, CN=I81RknrAubN8NIU1sMuf
签名算法: rsassa_pkcs1v15
有效期自: 2024-11-17 08:44:46+00:00
有效期至: 2052-04-04 08:44:46+00:00
发行人: C=re2jyxRhFa2bDb9nhHnx, ST=VBIEH1T5Dxx5ISdYbLzX, L=u4Z0fiSCZ6S94Ww3tzQo, O=8Ldg9aG2i6VFdkksumR8, OU=jOlefNN5gL2lLOslwtRf, CN=I81RknrAubN8NIU1sMuf
序列号: 0x7ff72319
哈希算法: sha256
md5值: ad7d66e556e6b511cf73d58374125ff6
sha1值: 0ae8d69bab507468fe6d807065396362ad020840
sha256值: 3cb55fd463be9c867711e3b1123ba89224d31675184350c6d9f407196ddfe0bf
sha512值: c5d0f4be2e875ef733244a8a6a91ab50d194882b600c06db1030d31fa902a5ef15ede8162cb9a6af612766d9e84b9059a440d287b6b77f2494ce794259d51215
公钥算法: rsa
密钥长度: 2048
指纹: 9932a87485b8f2f0daf03d12caf35e18c6391510bd81a1a2ceac7b43f2daec03

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

应用内通信