



MoGua

None 1.0.APK 分析报告



APP名称:

None

包名:

域名线索:

40条

URL线索:

41条

邮箱线索:

1条

分析日期:

2025年7月2日

分析平台:

[摸瓜APK反编译平台](#)

文件名: kyddappsats.apk
文件大小: 85.66MB
MD5值: 49f17c1c216d2d23355993e9e784ea91
SHA1值: 166529bf1c43ec145cfb2aa4ed02bcef4173fd32
SHA256值: 25b3b14c1b6cd7dc6f8dc498acb10807995d95016983c87ac668d6da73ba5829

i APP 信息

App名称: None
包名:
主活动Activity: []
安卓版本名称: 1.0
安卓版本: []

🔍 域名线索

域名	服务器信息
android.bugly.qq.com	IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
m.alipay.com	IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
182.92.20.189	IP: 182.92.20.189 所属国家: China 地区: Beijing

	城市: Beijing 纬度: 39.907501 经度: 116.397102
h.trace.qq.com	IP: 113.56.189.162 所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
bjuser.jpush.cn	IP: 122.9.11.195 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
shehona.cn	没有服务器地理信息.
mdc.html5.qq.com	IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
debugx5.qq.com	IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
	IP: 112.65.193.170 所属国家: China 地区: Shanghai

long.open.weixin.qq.com	城市: Shanghai 纬度: 31.224333 经度: 121.468948
h5.m.taobao.com	IP: 125.38.11.98 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
render.alipay.com	IP: 124.165.219.237 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
fusion.qq.com	IP: 116.130.228.157 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
qzs.qq.com	IP: 42.231.138.64 所属国家: China 地区: Henan 城市: Nanyang 纬度: 32.994720 经度: 112.532784
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418

mobilegw.aaa.alipay.net	没有服务器地理信息.
cgi.connect.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
pms.mb.qq.com	IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
astat.bugly.qcloud.com	IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
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: 120.161583
tbs.imtt.qq.com	IP: 211.90.132.201 所属国家: China 地区: Jiangsu 城市: Wuxi 纬度: 31.569349 经度: 120.288788
mobilegw.stable.alipay.net	没有服务器地理信息.

cgi.qplus.com	没有服务器地理信息.
log.tbs.qq.com	IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
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
mclient.alipay.com	IP: 124.95.170.204 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
open.weixin.qq.com	IP: 140.207.121.14 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
appsupport.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
	IP: 116.142.245.205 所属国家: China

mcgw.alipay.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
loggw-exsdk.alipay.com	IP: 119.42.231.20 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
debugtbs.qq.com	IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
graph.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
api.sharetrace.com	IP: 39.98.67.122 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
cfg.imtt.qq.com	IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102

www.baidu.com	IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
mobilegw.alipay.com	IP: 203.209.250.2 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
wappaygw.alipay.com	IP: 116.142.245.206 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
huatuocode.huatuo.qq.com	没有服务器地理信息.
openmobile.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
tsis.jpush.cn	IP: 1.94.113.76 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
https://tsis.jpush.cn	cn/jiguang/ad/i.java
http://182.92.20.189:9099/	cn/jiguang/o/c.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/aa/b.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/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.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java

https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/k.java

https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utls/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utls/o.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utls/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utls/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utls/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utls/d.java
https://graph.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/common/BaseApi.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/share/QQShare.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/share/QzoneShare.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/auth/a.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.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

https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=%s	com/tencent/mm/opensdk/diffdev/a/c.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
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiml.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiml.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApiml.java
http://qzs.qq.com	com/tencent/open/SocialApiml.java
https://graph.qq.com/cgi-bin/qunopensdk/check_group	com/tencent/open/SocialOperation.java
https://graph.qq.com/cgi-bin/qunopensdk/unbind	com/tencent/open/SocialOperation.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utis/f.java
http://cgi.qplus.com/report/report	com/tencent/open/utis/k.java
https://huatuocode.huatuo.qq.com	com/tencent/open/b/d.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java

https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://www.baidu.com?	org/cocos2dx/javascript/AppActivity.java
https://shehona.cn/creator/344qp/version.manifest	org/cocos2dx/lib/Cocos2dxDownloader.java
https://api.sharetrace.com	肌絹/肌絹/肌絹/肌絹/蒟申漳胝映鎗籽惚鎗瑜/C0079.java

邮箱线索

邮箱地址	所在文件
x5tbs@tencent.com	com/tencent/smtt/sdk/X5Downloader.java

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=Fujian, ST=adminlexeeTa, L=adminlexeeTa, O=adminlexeeTa, OU=adminlexeeTa, CN=adminlexeeTa
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-30 08:27:48+00:00
有效期至: 2125-06-06 08:27:48+00:00
发行人: C=Fujian, ST=adminlexeeTa, L=adminlexeeTa, O=adminlexeeTa, OU=adminlexeeTa, CN=adminlexeeTa
序列号: 0x302bc7a0
哈希算法: sha512
md5值: bf7313c4e3d79ba82ad8a1ccb15fd7a7

sha1值: d860ac7ad507fdb4cf75aa1b96852c829e08da10

sha256值: bd3f0b503714c4d9328517c1a8d850197b3d8b077216a7f60ff5d7294831d91a

sha512值: 0e20801a277102415ec72b2b98beff58761b7ef4edc0a988124e41b640ba7bf92cd20f06157302be49e6795d14344a1c8dc6f5a662e7336185cdf614df37107c

公钥算法: rsa

密钥长度: 2048

指纹: d6e8a251ebe4c0c78723c0cfb32539caedb99e74827ef012392848ef4056b0f7

 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

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。