



MoGua

YeMaoYX1.2003 1.1.18.APK 分析报告



APP名称:

YeMaoYX1.2003

包名:	com.yymmj.wymmjx
域名线索:	50条
URL线索:	54条
邮箱线索:	4条
分析日期:	2025年6月9日
分析平台:	摸瓜APK反编译平台

文件名: d6f2d0f884da450f8815c6dee8c50673.apk
文件大小: 60.53MB
MD5值: ace393734117b7587e1333522c985b72
SHA1值: 51873f9708f1427bb3dec6a92fbad9701c775857
SHA256值: b0d4948cb588fad14b1714021af08d29eefceafcabfa515b7f8bb7c04d8d147

i APP 信息

App名称: YeMaoYX1.2003
包名: com.ymmj.wymmjx
主活动Activity: org.cocos2dx.lua.AppActivity
安卓版本名称: 1.1.18
安卓版本: 1001018

🔍 域名线索

域名	服务器信息
119.29.29.29	IP: 119.29.29.29 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
collision.shareinstall.com	没有服务器地理信息.
mobilegw.aaa.alipay.net	没有服务器地理信息.
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: 120.161583

abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
log.umsns.com	IP: 59.82.29.248 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
restapi.amap.com	IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.openssl.org	IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
dualstack-a.apilocate.amap.com	IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mobilegw.alipay.com	IP: 203.209.255.248 所属国家: China 地区: Zhejiang 城市: Hangzhou

	纬度: 30.293650 经度: 120.161583
statlog.shareinstall.com	没有服务器地理信息.
sim.qudao.info	没有服务器地理信息.
oc.umeng.com	IP: 59.82.23.79 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
alogus.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
config.shareinstall.com	没有服务器地理信息.
pay.anysdk.com	IP: 211.151.20.124 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
	IP: 54.241.49.5 所属国家: United States of America

www.cocos2d-x.org	地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
api.line.me	IP: 154.83.14.134 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
lbs.amap.com	IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
adiu.amap.com	IP: 110.253.189.146 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
tools.ietf.org	IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
mcbgw.alipay.com	IP: 111.202.5.210 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
cgicol.amap.com	IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
112.74.215.224	IP: 112.74.215.224 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
ipay.iapppay.com	IP: 107.163.197.110 所属国家: United States of America 地区: California 城市: Westlake Village 纬度: 34.192921 经度: -118.822617
hydra.alibaba.com	IP: 203.119.169.241 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
iapppay-data.iapppay.com	IP: 107.163.197.110 所属国家: United States of America 地区: California 城市: Westlake Village 纬度: 34.192921 经度: -118.822617
iapppay.halodigit.com	没有服务器地理信息.

www.mp3dev.org	IP: 142.251.215.243 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
mobilegw.stable.alipay.net	没有服务器地理信息.
www.apple.com	IP: 184.25.87.45 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.566311 经度: 126.977203
data.iapppay.com	IP: 107.163.197.110 所属国家: United States of America 地区: California 城市: Westlake Village 纬度: 34.192921 经度: -118.822617
payment.iapppay.com	IP: 107.163.197.110 所属国家: United States of America 地区: California 城市: Westlake Village 纬度: 34.192921 经度: -118.822617
github.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 59.82.132.217 所属国家: China

restsdk.amap.com	地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
dm-81.data.aliyun.com	IP: 121.199.165.253 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
alog.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
dualstack-arestapi.amap.com	IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
access.line.me	IP: 202.160.130.52 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281

xmlpull.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
c.kp747.com	IP: 46.175.135.11 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
alog.umeng.co	没有服务器地理信息.
rqd.uu.qq.com	IP: 60.29.240.104 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
h5.m.taobao.com	IP: 125.39.135.147 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
apilocate.amap.com	IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
	IP: 123.12.235.54 所属国家: China

pv.sohu.com	地区: Henan 城市: Hebi 纬度: 35.899170 经度: 114.192497
www.winimage.com	IP: 205.251.81.217 所属国家: United States of America 地区: New Jersey 城市: Parsippany 纬度: 40.862041 经度: -74.406120

URL线索

URL信息	Url所在文件
http://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
http://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/c.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&	com/alipay/sdk/data/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/b/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/b/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/b/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/b/b/a.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.java

http://pay.	com/anysdk/framework/UserWrapper.java
http://oauth.	com/anysdk/framework/UserWrapper.java
http://sh-pay.	com/anysdk/framework/UserWrapper.java
http://sh-oauth.	com/anysdk/framework/UserWrapper.java
http://c.kp747.com/k.js	com/anysdk/framework/Statistics.java
http://sim.qudao.info/account/login	com/anysdk/framework/UserDebug.java
http://sim.qudao.info/account/logout	com/anysdk/framework/UserDebug.java
http://sim.qudao.info/account/login	com/anysdk/framework/SocialDebug.java
http://sim.qudao.info/account/logout	com/anysdk/framework/SocialDebug.java
http://sim.qudao.info/account/login	com/anysdk/framework/IAPDebug.java
http://sim.qudao.info/api/pay/exec	com/anysdk/framework/IAPDebug.java
http://pay.anysdk.com/v5/SimsdkPayNotice/SimsdkPayNotice/	com/anysdk/framework/IAPDebug.java
http://pay.anysdk.com/v5/Order/getOrderId/	com/anysdk/Util/a.java
http://pay.anysdk.com/v5/Unit/payment_switch/	com/anysdk/Util/a.java
http://112.74.215.224:9090/zjgapi/api.php	com/basic/pay/ali/AiBeiPay.java
https://data.iapppay.com/useractive	com/iapppay/e/a/d.java
https://iapppay-data.iapppay.com/useractive	com/iapppay/e/a/d.java

http://127.0.0.1/	com/iapppay/interfaces/bean/OrderBean.java
https://ipay.iapppay.com	com/iapppay/interfaces/network/HttpReqTask.java
https://payment.iapppay.com	com/iapppay/interfaces/network/HttpReqTask.java
https://iapppay.halodigit.com	com/iapppay/interfaces/network/HttpReqTask.java
https://data.iapppay.com/useractive	com/iapppay/utls/t.java
https://iapppay-data.iapppay.com/useractive	com/iapppay/utls/t.java
http://data.iapppay.com:8048/domain?dn=data.iapppay.com	com/iapppay/b/e.java
http://119.29.29.29/d?dn=	com/iapppay/b/e.java
https://api.line.me/	com/linecorp/linesdk/BuildConfig.java
https://access.line.me/.well-known/openid-configuration	com/linecorp/linesdk/BuildConfig.java
https://access.line.me/oauth2/v2.1/login	com/linecorp/linesdk/BuildConfig.java
https://adiu.amap.com/ws/device/adius	com/loc/bn.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/dd.java
http://apilocate.amap.com/mobile/binary	com/loc/fr.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/loc/fr.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fr.java
https://restsdk.amap.com/sdk/compliance/params	com/loc/ax.java
http://restsdk.amap.com/sdk/compliance/params	com/loc/ax.java

http://restsdk.amap.com	com/loc/v.java
http://restsdk.amap.com/v3/place/text?	com/loc/a.java
http://restsdk.amap.com/v3/config/district?	com/loc/a.java
http://restsdk.amap.com/v3/place/around?	com/loc/a.java
https://restapi.amap.com/rest/aaid/get	com/loc/af.java
http://restapi.amap.com/rest/aaid/get	com/loc/af.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fw.java
https://restsdk.amap.com/v3/iasdkauth	com/loc/m.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/loc/m.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fk.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/loc/fm.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/fm.java
https://dm-81.data.aliyun.com/rest/160601/ip/getIpInfo.json	com/sh/sdk/shareinstall/helper/e.java
http://pv.sohu.com/cityjson?ie=utf-8	com/sh/sdk/shareinstall/helper/g.java
https://statlog.shareinstall.com/shareinstall_log/active	com/sh/sdk/shareinstall/helper/a.java
https://statlog.shareinstall.com/shareinstall_log/online	com/sh/sdk/shareinstall/helper/l.java
https://statlog.shareinstall.com/shareinstall_log/register	com/sh/sdk/shareinstall/helper/m.java

https://statlog.shareinstall.com/shareinstall_log/install	com/sh/sdk/shareinstall/helper/i.java
https://statlog.shareinstall.com/shareinstall_log/si	com/sh/sdk/shareinstall/helper/j.java
https://collision.shareinstall.com/shareinstall/check.s	com/sh/sdk/shareinstall/helper/b.java
https://config.shareinstall.com/signal/config	com/sh/sdk/shareinstall/helper/c.java
https://collision.shareinstall.com/shareinstall/app.h	com/sh/sdk/shareinstall/helper/d.java
https://config.shareinstall.com/signal/config	com/sh/sdk/shareinstall/b/a/b.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://alogus.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umeng.co/app_logs	com/umeng/analytics/a.java
http://log.umsns.com/	com/umeng/analytics/social/e.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/f.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/core/persistent/FastXmlSerializer.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/core/persistent/XmlUtils.java
http://hydra.alibaba.com/	com/ta/utdid2/aid/AidRequester.java
https://tools.ietf.org/html/rfc7518	io/jsonwebtoken/SignatureAlgorithm.java

https://github.com/jwtkt/jjwt	io/jsonwebtoken/impl/DefaultClaims.java
https://tools.ietf.org/html/rfc7518	io/jsonwebtoken/security/Keys.java
http://www.mp3dev.org/	lib/armeabi/libcocos2dlua.so
http://www.openssl.org/support/faq.html	lib/armeabi/libcocos2dlua.so
http://127.0.0.1:8080	lib/armeabi/libcocos2dlua.so
http://www.winimage.com/zLibDll	lib/armeabi/libcocos2dlua.so
http://www.cocos2d-x.org/filedown/cocos-reader	lib/armeabi/libcocos2dlua.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi/libcocos2dlua.so
http://oc.umeng.com/v2/get_update_time	lib/armeabi/libmobclickcpp.so
http://oc.umeng.com/v2/check_config_update	lib/armeabi/libmobclickcpp.so
http://alog.umeng.co/app_logs	lib/armeabi/libmobclickcpp.so
http://alog.umeng.com/app_logs	lib/armeabi/libmobclickcpp.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi/libmobclickcpp.so
http://www.openssl.org/support/faq.html	lib/armeabi/libmobclickcpp.so
http://www.mp3dev.org/	lib/armeabi-v7a/libcocos2dlua.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libcocos2dlua.so
http://127.0.0.1:8080	lib/armeabi-v7a/libcocos2dlua.so

http://www.winimage.com/zLibDll	lib/armeabi-v7a/libcocos2dlua.so
http://www.cocos2d-x.org/filedown/cocos-reader	lib/armeabi-v7a/libcocos2dlua.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libcocos2dlua.so
http://oc.umeng.com/v2/get_update_time	lib/armeabi-v7a/libmobclickcpp.so
http://oc.umeng.com/v2/check_config_update	lib/armeabi-v7a/libmobclickcpp.so
http://alog.umeng.co/app_logs	lib/armeabi-v7a/libmobclickcpp.so
http://alog.umeng.com/app_logs	lib/armeabi-v7a/libmobclickcpp.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libmobclickcpp.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libmobclickcpp.so

 邮箱线索

邮箱地址	所在文件
ftp@example.com 6h@fo.lwft w9oi_2nhels4u@dlilycclghl.5jlcg_bqh yay@y.u5vcghyy	lib/armeabi/libcocos2dlua.so
ftp@example.com	lib/armeabi/libmobclickcpp.so
ftp@example.com 6h@fo.lwft w9oi_2nhels4u@dlilycclghl.5jlcg_bqh yay@y.u5vcghyy	lib/armeabi-v7a/libcocos2dlua.so

ftp@example.com	lib/armeabi-v7a/libmobclickcpp.so
-----------------	-----------------------------------

手机线索

手机号	所在文件
14222222222	com/loc/m.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=CN, ST=beijing, L=beijing, CN=yemao
签名算法: rsassa_pkcs1v15
有效期自: 2023-10-24 10:12:17+00:00
有效期至: 2048-10-17 10:12:17+00:00
发行人: C=CN, ST=beijing, L=beijing, CN=yemao
序列号: 0x3ea6a4ab
哈希算法: sha256
md5值: 8e3ac4f5ce2bea5beae46a5640a437cb
sha1值: b00a6bd369c7c78538ada5670e1fc95fa65947a1
sha256值: bb3e1fd7523d79046c6cc1ddf9bd6a18040713a3d66a572cc78d17cf3dce7017
sha512值: 2d3fe75557d52b920c8f4686f950e251da31e4cd31f685baf7b332332566b2d74da833680bea28f0ecd223f00098d04665bc977f5f2fe4fe01801c08e2f51f29
公钥算法: rsa
密钥长度: 2048
指纹: 02ecbec7834d2cee93b6d701cd5284a3e0310b69f25ecb599245f89fcc524d9d

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

向手机申请的权限	是否危险	类型	详细情况
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_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.default	未知	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.WRITE_EXTERNAL_STORAGE	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_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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.RECORD_VIDEO	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
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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。

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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用

应用内通信

活动(ACTIVITY)	通信(INTENT)
org.cocos2dx.lua.AppActivity	Schemes: egpq5088://,
com.linecorp.linesdk.auth.internal.LineAuthenticationCallbackActivity	Schemes: lineauth://,