MoGua

ABC加速器 3.0.4.APK 分析报告

APP名称: ABC加速器

包名:	com.zfast.xyz
域名线索:	29条
URL线索:	21条
邮箱线索:	2条
分析日期:	2025年7月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: abc304.apk
文件大小: 39.59MB
MD5值: b79a1a1ed4aec3de3d6684daf5adc360
SHA1值: 0b70b1e59f30dd701643cd3ecfd1571056a953c9
SHA256值: e19921a36244e9500076db61439e44c5b9e37f38d95c9cc4fda00128032db9bd

APP 信息

App名称: ABC加速器
包名: com.zfast.xyz
主活动Activity: com.faster.cheetah.ui.GuideActivity
安卓版本名称: 3.0.4
安卓版本: 1

域名线索

域名	服务器信息
netty.io	**IP**: 104.21.3.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
mobilegw.stable.alipay.net	没有服务器地理信息.
ask.gosupport.cc	**IP**: 154.23.223.8 **所属国家**: United States of America **地区**: District of Columbia **城市**: Washington **纬度**: 38.901566 **经度**: -77.050781

h5.m.taobao.com	**IP**: 27.128.222.51 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
shadowsocks.org	**IP**: 37.61.54.158 **所属国家**: Azerbaijan **地区**: Baki **城市**: Baku **纬度**: 40.377670 **经度**: 49.892010
www.zetetic.net	**IP**: 13.227.62.26 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
open.weixin.qq.com	**IP**: 175.24.209.30 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mobilegw.alipay.com	**IP**: 203.209.245.129 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
api.gsdfe3520zfa.com	没有服务器地理信息.
	IP: 124.239.239.236 **所属国家**: China **地区**: Hebei

wappaygw.alipay.com	**城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
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
api.askjdhsdjh.com	没有服务器地理信息.
secure.ccavenue.com	**IP**: 23.37.148.163 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
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**: 120.161423
www.openssl.org	**IP**: 104.71.138.221 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
mclient.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
long.open.weixin.qq.com	**IP**: 109.244.216.15 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mcgw.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
api.as2kjdhs1djh.com	**IP**: 8.210.76.85 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
loggw-exsdk.alipay.com	**IP**: 110.76.3.2 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
testapi.allpayx.com	**IP**: 101.132.157.66 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
	IP: 42.81.147.159 **所属国家**: China

appcashier.test.95516.com	**地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
api.as26sfsadjh.com	**IP**: 8.210.76.85 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
api.gsdsd52sf4a.com	没有服务器地理信息.
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
mobilegw.aaa.alipay.net	没有服务器地理信息.
cashier.95516.com	**IP**: 222.79.76.149 **所属国家**: China **地区**: Fujian **城市**: Xiamen **纬度**: 24.479790 **经度**: 118.081871
api.allpayx.com	**IP**: 47.101.160.96 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
appcashier256.95516.com	**IP**: 222.79.76.149 **所属国家**: China **地区**: Fujian **城市**: Xiamen **纬度**: 24.479790 **经度**: 118.081871

URL线索

URL信息	Url所在文件
https://netty.io/wiki/reference-counted-objects.html	io/netty/util/ResourceLeakDetector.java
https://shadowsocks.org/acl/android/v1/	com/github/shadowsocks/acl/AclSyncer.java
http://api.gsdsd52sf4a.com:3306/client.php	com/faster/cheetah/MainApplication.java
http://api.gsdfe3520zfa.com:3306/client.php	com/faster/cheetah/MainApplication.java
http://api.askjdhsdjh.com:3306/client.php	com/faster/cheetah/MainApplication.java
http://api.as2kjdhs1djh.com:3306/client.php	com/faster/cheetah/MainApplication.java
http://api.as26sfsadjh.com:3306/client.php	com/faster/cheetah/MainApplication.java
http://%s:%s@%s	com/faster/cheetah/sdk/shadowsocks/tunnel/httpconnect/HttpConnectConfig.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/util/l.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://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/packet/impl/e.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/d.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
https://api.allpayx.com	com/allpayx/sdk/util/ServerUtil.java
https://testapi.allpayx.com	com/allpayx/sdk/util/ServerUtil.java
https://secure.ccavenue.com/transaction/initTrans	com/allpayx/sdk/util/Constants.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://cashier.95516.com/b2c/api/sdkPay.action\	com/unionpay/UPPayAssistEx.java
https://ask.gosupport.cc/	net/xfkefu/sdk/retrofit/A.java
https://github.com/shadowsocks/shadowsocks-android/blob/master/.github/faq.md	Mogua Engine V1
https://www.zetetic.net/sqlcipher/	Mogua Engine V1
https://www.zetetic.net/sqlcipher/license/	Mogua Engine V1
https://github.com/sqlcipher/android-database-sqlcipher	Mogua Engine V1
https://github.com/shadowsocks/shadowsocks-android/blob/master/.github/faq.ru.md	Mogua Engine V1
https://appcashier.test.95516.com/gateway/mobile/json	lib/armeabi/libentryexpro.so
https://appcashier256.95516.com/gateway/mobile/json	lib/armeabi/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/json	lib/armeabi/libentryexpro.so
https://appcashier256.95516.com/app/mobile/json	lib/armeabi/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/hft	lib/armeabi/libentryexpro.so
https://appcashier256.95516.com/app/mobile/hft	lib/armeabi/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/conf	lib/armeabi/libentryexpro.so
https://appcashier256.95516.com/app/mobile/conf	lib/armeabi/libentryexpro.so
http://www.openssl.org/support/faq.html	lib/armeabi/libuptsmaddon.so
https://appcashier256.95516.com/gateway/mobile/json	lib/x86/libentryexpro.so

https://appcashier.test.95516.com/gateway/mobile/json	lib/x86/libentryexpro.so
https://appcashier256.95516.com/app/mobile/hft	lib/x86/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/hft	lib/x86/libentryexpro.so
https://appcashier256.95516.com/app/mobile/json	lib/x86/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/json	lib/x86/libentryexpro.so
https://appcashier256.95516.com/app/mobile/conf	lib/x86/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/conf	lib/x86/libentryexpro.so
http://www.openssl.org/support/faq.html	lib/x86/libuptsmaddon.so

邮箱线索

邮箱地址	所在文件
ambrop7@gmail.com	lib/x86/libtun2socks.so
ambrop7@gmail.com	lib/arm64-v8a/libtun2socks.so

手机线索

手机号	所在文件
14774490842	com/faster/cheetah/service/AlcedoService.java

13918766593	com/faster/cheetah/service/AlcedoService.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: CN=abc
签名算法: rsassa_pkcs1v15
有效期自: 2021-03-15 08:28:06+00:00
有效期至: 2051-03-08 08:28:06+00:00
发行人: CN=abc
序列号: 0x431facd4
哈希算法: sha256
md5值: 49e39bdc5eb14f79e5ae9b655165c20e
sha1值: 1c9b7b8a2eedeb143834e840ba41c315dc93fb2d
sha256值: 2928a794fdf9faf328fae5ddc34c5b1eb10cce1686ea4333b81c0e8bb453d97e
sha512值: 4fe44e09888237f5065a8573c5b20e6fc59e17f7d1e553c310aa94c89ae66bc007b78e8b6abbcc96eb6cc95258cf4c2125c037d78410eda5e71b1b5b718cdbde
公钥算法: rsa
密钥长度: 2048
指纹: eef37bc1f2f4730577ac2997568aafd1e80cbbb8cc15613af4d2dddfede27981

硬编码敏感信息

可能的敏感信息
"buy_private" : "新购独享线路"
"input_account_pwd" : "验证码"
"library_android_database_sqlcipher_author" : "Zetetic, LLC"

"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"

"line_free_user" : "无限访问"

"line_private_buy" : "立即购买"

"line_private_buy_amount" : "充值金额"

"line_private_buy_area" : "选择地区"

"line_private_buy_day" : "购买时长"

"line_private_buy_null" : "当前地区没有线路可购买"

"line_private_buy_num" : "购买数量"

"line_private_buy_pay" : "确认"

"line_private_buy_paytype" : "支付方式"

"line_private_buy_pro" : "选择产品"

"line_private_buy_quan" : "使用兑换券"

"line_private_buy_svip" : "送会员服务"

"line_private_list_ctrl" : "操作"

"line_private_list_name" : "线路"

"line_private_title" : "开通/续费"

"line_try_user" : "体验用户"

"remember_password" : "记住密码"

"sitekey" : "Password"
"withdraw_pwd" : "验证码"
"sitekey" : "كلمه عبور"
"sitekey" : "パスワード"
"sitekey" : "비밀번호"
"sitekey" : "كلمة المرور"
"sitekey" : "Mot de passe"
"sitekey" : "Şifre"
"sitekey" : "Contraseña"
"sitekey" : "Пароль"
"sitekey" : "密码"
"buy_private" : "新购独享线路"
"input_account_pwd" : "驗證碼"
"line_free_user" : "無限訪問"
"line_private_buy" : "立即购买"
"line_private_buy_amount" : "充值金额"
"line_private_buy_area" : "选择地区"

"line_private_buy_day" : "购买时长"
"line_private_buy_null" : "当前地区没有线路可购买"
"line_private_buy_num" : "购买数量"
"line_private_buy_pay" : "确认"
"line_private_buy_paytype" : "支付方式"
"line_private_buy_pro" : "选择产品"
"line_private_buy_quan" : "使用兑换券"
"line_private_buy_svip" : "送会员服务"
"line_private_list_name" : "线路"
"line_private_title" : "开通/续费"
"line_try_user" : "體驗用戶"
"remember_password" : "记住密码"
"sitekey" : "密碼"
"withdraw_pwd" : "驗證碼"
"buy_private" : "新购独享线路"
"input_account_pwd" : "Please enter Verification Code"
"line_free_user" : "Unlimited access"
"line_private_buy" : "立即购买"

"line_private_buy_amount" : "充值金额"
"line_private_buy_area" : "选择地区"
"line_private_buy_day" : "购买时长"
"line_private_buy_null" : "当前地区没有线路可购买"
"line_private_buy_num" : "购买数量"
"line_private_buy_pay" : "确认"
"line_private_buy_paytype" : "支付方式"
"line_private_buy_pro" : "选择产品"
"line_private_buy_quan" : "使用兑换券"
"line_private_buy_svip" : "送会员服务"
"line_private_list_name" : "线路"
"line_private_title" : "开通/续费"
"line_try_user" : "Experience user"
"remember_password" : "记住密码"
"withdraw_pwd" : "Verification Code"

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。