MoGua

枪战英雄 0.6.4.077.APK 分析报告

APP名称:	枪战英雄

包名:	com.sy4399.zjqz
域名线索:	62条
URL线索:	69条
邮箱线索:	1条
分析日期:	2025年9月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: qiangzhanyingxiong.apk
文件大小: 233.95MB
MD5值: 1509567f61e21703027044ec3c96e536
SHA1值: f3398b36dee089c1ee5378f16a72c8ad9af48989
SHA256值: b607dc68d81b3c873926d5846d9497d75698eead96f9cb3c8c0d15d402dac1cd

APP 信息

App名称: 枪战英雄
包名: com.sy4399.zjqz
主活动Activity: com.fnsdk.unity.FnSdkUnityActivity
安卓版本名称: 0.6.4.077
安卓版本: 2108231130

域名线索

域名	服务器信息
wap.cmpassport.com	**IP**: 120.232.169.168 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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
fusion.qq.com	**IP**: 116.130.229.204 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
collect.ux.21cn.com	**IP**: 222.93.106.185 **所属国家**: China **地区**: Jiangsu **城市**: Suzhou **纬度**: 31.311365 **经度**: 120.617691
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
sdk.open.phone.igexin.com	**IP**: 101.68.218.177 **所属国家**: China **地区**: Zhejiang **城市**: Jiaxing **纬度**: 30.752199 **经度**: 120.750000
cdn.h5wan.4399sj.com	**IP**: 123.117.133.190 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
cdp.cloud.unity3d.com	**IP**: 43.156.88.56 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

qzs.qq.com	**IP**: 221.204.20.189 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
api-test.4399sy.com	没有服务器地理信息.
xmlpull.org	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
sdk.open.inc2.igexin.com	没有服务器地理信息.
cdn.4399sj.com	**IP**: 123.126.74.113 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
dev.voicecloud.cn	**IP**: 125.254.169.47 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
openapi.openspeech.cn	**IP**: 125.254.169.47 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

mta.qq.com	**IP**: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
service.weibo.com	**IP**: 116.133.8.18 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
c.isdspeed.qq.com	没有服务器地理信息.
e.189.cn	**IP**: 42.123.76.65 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mobilegw.stable.alipay.net	没有服务器地理信息.
hxqd.openspeech.cn	**IP**: 114.118.75.245 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.yqbgn.com	**IP**: 42.62.62.45 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

m.weibo.cn	**IP**: 116.133.8.18 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
dldir1.qq.com	**IP**: 118.212.139.65 **所属国家**: China **地区**: Jiangxi **城市**: Nanchang **纬度**: 28.683331 **经度**: 115.883331
api.uca.cloud.unity3d.com	**IP**: 101.32.104.143 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
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
api.4399sy.com	**IP**: 211.159.158.242 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
mobile.unionpay.com	没有服务器地理信息.
4399sy.com	**IP**: 111.161.121.98 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
media.weibo.cn	**IP**: 123.125.107.14 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.23x32y.com	**IP**: 119.28.226.139 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
config.uca.cloud.unity3d.com	**IP**: 34.111.113.40 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
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

open.weibo.cn	IP: 123.125.107.13 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
fnsdk.4399sy.com	IP: 62.234.43.132 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mobilegw.aaa.alipay.net	没有服务器地理信息.
appcashier256.95516.com	IP: 180.130.108.165 **所属国家**: China **地区**: Yunnan **城市**: Zhaotong **纬度**: 27.316669 **经度**: 103.716667
open.weixin.qq.com	IP: 116.128.171.214 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
ms.zzx9.cn	IP: 124.64.196.28 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 123.125.107.13

api.weibo.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
dpdcs.4399sy.com	IP: 109.244.60.70 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
wlc.4399sy.com	IP: 109.244.51.115 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mcgw.alipay.com	IP: 119.188.53.105 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
mobilegw.alipay.com	IP: 203.209.243.27 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
pingma.qq.com	IP: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

sdk.open.lbs.igexin.com	没有服务器地理信息.
h5.m.taobao.com	**IP**: 121.29.103.126 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
www.4399.cn	**IP**: 123.117.133.134 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mta.oa.com	**IP**: 141.144.196.217 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.378502 **经度**: 4.899980
sdk.open.amp.igexin.com	**IP**: 124.160.124.197 **所属国家**: China **地区**: Zhejiang **城市**: Wenzhou **纬度**: 27.999420 **经度**: 120.666817
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
opencloud.wostore.cn	**IP**: 210.22.123.92 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948

appcashier.test.95516.com	**IP**: 180.95.171.99 **所属国家**: China **地区**: Gansu **城市**: Jinchang **纬度**: 33.616810 **经度**: 104.896332
fnsdk.demo.4399sy.com	**IP**: 109.244.51.33 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.xfyun.cn	**IP**: 42.62.43.219 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
open.e.189.cn	**IP**: 42.123.76.75 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
router.g263.com	**IP**: 42.62.62.45 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
fnapi.4399sy.com	**IP**: 211.159.174.33 **所属国家**: China **地区**: Beijing **城市**: Beijing

	纬度: 39.907501 **经度**: 116.397102
long.open.weixin.qq.com	**IP**: 112.65.193.170 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
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
www.go-mono.com	**IP**: 13.68.229.189 **所属国家**: United States of America **地区**: Virginia **城市**: Washington **纬度**: 38.713848 **经度**: -78.159439

URL线索

URL**信息**	Url**所在文件**
http://dpdcs.4399sy.com/sdk_error.php	com/ssjjsy/net/ak.java
http://dpdcs.4399sy.com/front_error.php	com/ssjjsy/net/al.java
http://api-test.4399sy.com/plugin/config?	com/ssjjsy/net/Ssjjsy.java

http://api-test.4399sy.com/service/version/plugin?	com/ssjjsy/net/Ssjjsy.java
https://api.4399sy.com/plugin/config?	com/ssjjsy/net/Ssjjsy.java
http://api.4399sy.com/service/version/plugin?	com/ssjjsy/net/Ssjjsy.java
https://api.yqbgn.com/plugin/config?	com/ssjjsy/net/Ssjjsy.java
http://api.yqbgn.com/service/version/plugin?	com/ssjjsy/net/Ssjjsy.java
http://router.g263.com/r.php	com/ssjjsy/net/BgpMgr.java
http://dpdcs.4399sy.com/sdk_error.php	com/ssjjsy/net/an.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&	com/alipay/sdk/data/a.java
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://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://opencloud.wostore.cn/openapi/netauth/precheck/wp?	com/unicom/xiaowo/account/shield/c/b.java
http://fnsdk.4399sy.com/sdk/api/login.php	com/fnsdk/unity/FnSdkUnityActivity.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/core/persistent/XmlUtils.java

http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/core/persistent/FastXmlSerializer.java
http://hydra.alibaba.com/	com/ta/utdid2/aid/AidRequester.java
https://api.weibo.com/2/proxy/sdk/statistic.json	com/sina/weibo/sdk/statistic/LogReport.java
https://api.weibo.com/oauth2/getaid.json	com/sina/weibo/sdk/utils/AidTask.java
https://api.weibo.com/oauth2/getaid.json	com/sina/weibo/sdk/utils/AidTask4Plug.java
http://m.weibo.cn/u/	com/sina/weibo/sdk/web/WeiboPageUtils.java
http://media.weibo.cn/article?	com/sina/weibo/sdk/web/WeiboPageUtils.java
http://m.weibo.cn/comment?	com/sina/weibo/sdk/web/WeiboPageUtils.java
http://m.weibo.cn/	com/sina/weibo/sdk/web/WeiboPageUtils.java
http://m.weibo.cn/index/router?	com/sina/weibo/sdk/web/WeiboPageUtils.java
https://m.weibo.cn/p/100103type=1&	com/sina/weibo/sdk/web/WeiboPageUtils.java
http://m.weibo.cn/mblog?	com/sina/weibo/sdk/web/WeiboPageUtils.java
http://service.weibo.com/share/mobilesdk.php	com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java
http://service.weibo.com/share/mobilesdk_uppic.php	com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java
https://open.weibo.cn/oauth2/authorize?	com/sina/weibo/sdk/auth/BaseSsoHandler.java
https://api.weibo.com/oauth2/access_token	com/sina/weibo/sdk/auth/AccessTokenKeeper.java
http://dldir1.qq.com/gamesafe/mobile/app/android/tpsafe.apk	com/tencent/tersafe2/res/Res.java

http://dldir1.qq.com/gamesafe/mobile/app/android/base.ini	com/tencent/tersafe2/res/Res.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/sdk/diffdev/a/f.java
http://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/sdk/diffdev/a/d.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://fusion.qq.com/cgi-bin/qzapps/unified_jump? appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/connect/share/QQShare.java
https://openmobile.qq.com/	com/tencent/connect/common/Constants.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
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
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/auth/a.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiIml.java

http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiIml.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApiIml.java
http://qzs.qq.com	com/tencent/open/SocialApiIml.java
http://c.isdspeed.qq.com/code.cgi	com/tencent/open/b/d.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/e.java
http://sdk.open.inc2.igexin.com/api.php	com/igexin/getuiext/data/Consts.java
http://sdk.open.phone.igexin.com/api.php	com/igexin/getuiext/data/Consts.java
http://sdk.open.phone.igexin.com/api.php?format=json&t=1	com/igexin/getuiext/service/i.java
http://sdk.open.amp.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.lbs.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
https://api.weibo.com/oauth2/default.html	com/ssjj/fnsdk/share/weibo/WeiboConfig.java
https://cdn.h5wan.4399sj.com/mobile-issue/user_agreement.html	com/ssjj/fnsdk/core/EnvConfigRes.java
https://cdn.h5wan.4399sj.com/mobile-issue/privacy.html	com/ssjj/fnsdk/core/EnvConfigRes.java
http://fnapi.4399sy.com/sdk/api/children_protect.php	com/ssjj/fnsdk/core/EnvConfigRes.java
http://fnapi.4399sy.com/sdk/api/user_agreement.php	com/ssjj/fnsdk/core/EnvConfigRes.java
http://fnapi.4399sy.com/sdk/api/privacy.php	com/ssjj/fnsdk/core/EnvConfigRes.java
http://fnsdk.demo.4399sy.com/sdk/api/fncfg.php	com/ssjj/fnsdk/core/bx.java

http://fnsdk.4399sy.com/sdk/api/inlinepage.php	com/ssjj/fnsdk/core/commonweb/popweb/PopGetPopPageConfigTask.java
http://fnsdk.4399sy.com/sdk/api/inlinepage.php	com/ssjj/fnsdk/tool/fnpopweb/FNPopPage.java
http://fnapi.4399sy.com/sdk/api/privacy.php	com/ssjj/fnsdk/tool/fnpopweb/FNToolConfig.java
http://fnapi.4399sy.com/sdk/api/user_agreement.php	com/ssjj/fnsdk/tool/fnpopweb/FNToolConfig.java
https://api.23x32y.com/pZi6CJdhuBko.html	com/ssjj/fnsdk/platform/FNConfig4399.java
https://api.23x32y.com/0dFXTAnKHU83.html	com/ssjj/fnsdk/platform/FNConfig4399.java
http://www.4399.cn/app-wap-qd-login4399.html?p=24f7b8a7-65e7-4c64-807e-b7a13fa778d5_1444815695415_737eb21d	com/ssjj/fnsdk/platform/FNTestDialog4399.java
http://wlc.4399sy.com/wlc_heartbeat_collection.php	com/ssjj/fn/common/realname/a/b.java
http://mobile.unionpay.com/getclient?platform=android&type=securepayplugin	com/unionpay/UPPayAssistEx.java
https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\	com/unionpay/UPPayAssistEx.java
https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\	com/unionpay/mobile/android/utils/c.java
http://openapi.openspeech.cn/webapi/wfr.do	com/iflytek/cloud/d/a/a.java
http://dev.voicecloud.cn/msc/help.html\	com/iflytek/cloud/resource/c.java
http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/c.java
http://dev.voicecloud.cn/msc/help.html\	com/iflytek/cloud/resource/a.java
http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/a.java
http://dev.voicecloud.cn/msc/help.html\	com/iflytek/cloud/resource/b.java

http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/b.java
http://www.xfyun.cn/s?	com/iflytek/speech/UtilityConfig.java
http://hxqd.openspeech.cn/launchconfig	com/iflytek/common/a/d.java
https://cdn.4399sj.com	cn/m4399/login/union/main/a.java
https://open.e.189.cn/openapi/special/getTimeStamp.do	cn/com/chinatelecom/account/api/c/a.java
https://e.189.cn/sdk/agreement/detail.do?hidetop=true&appKey=	cn/com/chinatelecom/account/sdk/a/b.java
https://wap.cmpassport.com/resources/html/contract.html	cn/com/chinatelecom/account/sdk/a/b.java
https://ms.zzx9.cn/html/oauth/protocol.html	cn/com/chinatelecom/account/sdk/a/b.java
https://collect.ux.21cn.com/collect/custom/accountMsg	cn/com/chinatelecom/account/a/c.java
https://wap.cmpassport.com/resources/html/contract.html	摸瓜V1引擎
https://e.189.cn/sdk/agreement/detail.do?hidetop=true	摸瓜V1引擎
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	摸瓜V1引擎
http://4399sy.com/hd/sypt/notice/privacy/202006/24-45186.html	摸瓜V1引擎
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libuptsmaddonmi.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libuptsmaddon.so
https://appcashier256.95516.com/gateway/mobile/json	lib/armeabi-v7a/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/conf	lib/armeabi-v7a/libentryexpro.so
https://appcashier256.95516.com/app/mobile/conf	lib/armeabi-v7a/libentryexpro.so

https://appcashier.test.95516.com/app/mobile/hft	lib/armeabi-v7a/libentryexpro.so
https://appcashier256.95516.com/app/mobile/hft	lib/armeabi-v7a/libentryexpro.so
https://appcashier.test.95516.com/app/mobile/json	lib/armeabi-v7a/libentryexpro.so
https://appcashier256.95516.com/app/mobile/json	lib/armeabi-v7a/libentryexpro.so
https://appcashier.test.95516.com/gateway/mobile/json	lib/armeabi-v7a/libentryexpro.so
https://config.uca.cloud.unity3d.com	lib/armeabi-v7a/libunity.so
https://cdp.cloud.unity3d.com/v1/events	lib/armeabi-v7a/libunity.so
https://api.uca.cloud.unity3d.com/v1/events	lib/armeabi-v7a/libunity.so
http://www.openssl.org/support/faq.html	lib/x86/libuptsmaddonmi.so
http://www.openssl.org/support/faq.html	lib/x86/libuptsmaddon.so
http://www.go-mono.com/delegate.html	lib/x86/libmono.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
https://config.uca.cloud.unity3d.com	lib/x86/libunity.so
https://cdp.cloud.unity3d.com/v1/events	lib/x86/libunity.so
https://api.uca.cloud.unity3d.com/v1/events	lib/x86/libunity.so

邮箱线索

邮箱地址	所在文件
ftp@example.com	lib/armeabi-v7a/libtersafe2.so

手机线索

手机号	所在文件
17369024377	com/ssjj/fnsdk/core/fnd/b.java
15060355040	com/unionpay/UPPayAssistEx.java

签名证书

APK已签名
v1 签名: True

v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=Guangdong, L=Guangzhou, O=4399sy.com, OU=4399sy.com, CN=4399
签名算法: rsassa_pkcs1v15
有效期自: 2015-04-29 06:46:16+00:00
有效期至: 2124-11-03 06:46:16+00:00
发行人: C=CN, ST=Guangdong, L=Guangzhou, O=4399sy.com, OU=4399sy.com, CN=4399
序列号: 0x19fb5c3c
哈希算法: sha256
md5值: 494ecf3907c3dd5ca1a9cc48e22a65f7
sha1值: 8333fd31f421da2da601522e378e88190abeb3af
sha256值: 6391d216eb9b572495143eaf815534de23cfee94a1bc4d451b846ddb0a7a7478
sha512值: 5119f6dfd93e2142fb313598a05df753e24be93640028ea37cbbec9526d5329ee2febea59dbdd80b6bd9b55c3763bb759d33aa5eccf52c915c3c4366c14e3ddf

硬编码敏感信息

可能的敏感信息
"fnsdk_tkey" : "966ed280e0e827bfd299bc18c3af7baa"

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.RESTART_PACKAGES	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.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
getui.permission.GetuiService.com.sy4399.zjqz	未知	Unknown permission	Unknown permission from android reference
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.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。
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
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.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
org.simalliance.openmobileai.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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。

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.fnsdk.unity.FnSdkUnityActivity	Schemes: fnzjqz://, fnzjqz1://,
com.tencent.tauth.AuthActivity	Schemes: tencent1105683229://,

---

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。