MoGua

ecj null.APK 分析报告

APP名称:	ecj
包名:	gjfjj2fh.sang9kgfei.hangtkkg3hiao
域名线索:	38条

URL线索:	29条
邮箱线索:	0条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: ecj.apk
文件大小: 78.58MB
MD5值: 6df59843a57659f05c3a990f80eb17ce
SHA1值: 8465e4263b6fcc7af07bb628c7b5396d5ecf312d
SHA256值: 43a0a477c71cf66395fdccb78ca8a34d4b1d9757b1c7ba84c9d77251652630c6

APP 信息

App名称: ecj
包名: gjfjj2fh.sang9kgfei.hangtkkg3hiao
主活动Activity: com.sanfei.hangtian.shell.XYDShellXYDXYDSplashA
安卓版本名称: null

安卓版本:

域名线索

域名	服务器信息
render.alipay.com	**IP**: 124.95.153.221 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
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**: 120.161583
www.5.com	没有服务器地理信息.
mobilegw.stable.alipay.net	没有服务器地理信息.
app.mi.com	**IP**: 221.194.175.44 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
api-push.meizu.com	**IP**: 221.5.93.66 **所属国家**: China **地区**: Guangdong **城市**: Foshan **纬度**: 23.026770 **经度**: 113.131477
www.geetest.com	**IP**: 60.28.220.193 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181

	经度: 117.176102
3.112.32.142	**IP**: 3.112.32.142 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
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
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
www.3.com	没有服务器地理信息.
mclient.alipay.com	**IP**: 124.95.172.71 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
schemas.microsoft.com	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
open.weixin.qq.com	**IP**: 116.128.169.212 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948

push.statics	没有服务器地理信息.
bjuser.jpush.cn	**IP**: 122.9.5.30 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
api-push.in.meizu.com	**IP**: 206.161.233.191 **所属国家**: United States of America **地区**: Virginia **城市**: Herndon **纬度**: 38.978210 **经度**: -77.386993
netty.io	**IP**: 172.67.130.186 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
94.74.101.54	**IP**: 94.74.101.54 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
wiki.eclipse.org	**IP**: 198.41.30.195 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548
134.175.82.204	**IP**: 134.175.82.204 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.4.com	没有服务器地理信息.

www.1.com	没有服务器地理信息.
d.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
mobilegw.aaa.alipay.net	没有服务器地理信息.
18.176.58.66	**IP**: 18.176.58.66 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
fhwsh.jinxtxws.xyz	**IP**: 101.33.124.228 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
www.downyi.com	**IP**: 61.182.143.64 **所属国家**: China **地区**: Hebei **城市**: Hengshui **纬度**: 37.732220 **经度**: 115.701157
www.eclipse.org	**IP**: 198.41.30.198 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548
ce3e75d5.jpush.cn	**IP**: 120.233.50.37 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108

tsis.jpush.cn	**IP**: 139.9.129.253 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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
wappaygw.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
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.
playready.directtaps.net	**IP**: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
52.195.17.43	**IP**: 52.195.17.43 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
www.2.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://tsis.jpush.cn	cn/jiguang/ao/i.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/ai/b.java
http://182.92.20.189:9099/	cn/jiguang/r/a.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/aj/d.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://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
http://www.geetest.com/first_page	com/geetest/sdk/views/GT3GeetestButton.java

https://push.statics	com/meizu/cloud/pushsdk/networking/http/HttpURLConnectionCall.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/api/PushAPI.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/api/PushAPI.java
http://www.downyi.com/downinfo/173568.html	com/sanfei/hangtian/view/setting/XYDXYDGoogleAuthenticatorActivity.java
http://94.74.101.54:8081	com/sanfei/hangtian/view/friend_info/XYDXYDXYDXYDFriendDetailActivity.java
http://94.74.101.54:8081	com/sanfei/hangtian/view/chat/XYDXYDBaseChatActivityXYD.java
http://app.mi.com/detail/163525?ref=search	com/sanfei/hangtian/presenter/XYDAboutUsPresenter.java
http://fhwsh.jinxtxws.xyz:11101	com/sanfei/hangtian/app/XYDLiteApplication.java
http://134.175.82.204:11101	com/sanfei/hangtian/app/XYDLiteApplication.java
http://52.195.17.43:41000/	com/sanfei/hangtian/app/XYDLiteApplication.java
http://18.176.58.66:41000/	com/sanfei/hangtian/app/XYDLiteApplication.java
http://3.112.32.142:41000/	com/sanfei/hangtian/app/XYDLiteApplication.java
http://www.1.com	com/sanfei/module_base/model/bean/HttpServerConfigEntity.java
http://www.2.com	com/sanfei/module_base/model/bean/HttpServerConfigEntity.java
http://www.3.com	com/sanfei/module_base/model/bean/HttpServerConfigEntity.java
http://www.4.com	com/sanfei/module_base/model/bean/HttpServerConfigEntity.java
http://www.5.com	com/sanfei/module_base/model/bean/HttpServerConfigEntity.java
https://d.alipay.com	com/sanfei/module_base/web/WebViewHelper.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%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
https://tools.ietf.org/html/rfc7540	io/netty/handler/codec/http2/HttpConversionUtil.java

https://wiki.eclipse.org/Jetty/Feature/NPN	io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java
http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html	io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java
https://netty.io/wiki/forked-tomcat-native.html	io/netty/handler/ssl/OpenSsl.java
https://netty.io/wiki/sslcontextbuilder-and-private-key.html	io/netty/handler/ssl/PemReader.java
https://www.openssl.org/docs/man1.0.2/apps/verify.html.	io/netty/handler/ssl/OpenSslCertificateException.java
https://netty.io/wiki/reference-counted-objects.html	io/netty/util/ResourceLeakDetector.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java

邮箱线索

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=ljuccppkcmprr, ST=hwzfwkkxmnoze, L=fhkyclkxcpwie, O=pun1745915562937, OU=jnx1745915562937, CN=TG@apkfangdujiagu
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-29 08:32:42+00:00
有效期至: 2075-04-17 08:32:42+00:00
发行人: C=ljuccppkcmprr, ST=hwzfwkkxmnoze, L=fhkyclkxcpwie, O=pun1745915562937, OU=jnx1745915562937, CN=TG@apkfangdujiagu

序列号: 0x748c8da
哈希算法: sha1
md5值: 984d5ccfb25c505845c9f0dc2f88e288
sha1值: 59aa016d3fdeb074facb22f1b4c8cae875c838ac
sha256值: a25a73a4fd191dc65495c1e1387e3bf6aca8d8e3bb3683c80a8254b28b871138
sha512值: 39fb10a6a139bdb1f578263da0bc832d55204cd53c0dc5de46e1ce2e9dd2e9cbc0abdbb2abf58a865dae81114395626f2ed0b37e831b76d81dff44eab7408f72
公钥算法: rsa
密钥长度: 1024
指纹: bc96fd592dcd4aa2de415d25962de41d0e7e4ddc8a17c4d2b8bad651872abd33

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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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
gjfjj2fh.sang9kgfei.hangtkkg3hiao_com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
gjfjj2fh.sang9kgfei.hangtkkg3hiao_com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
gjfjj2fh.sang9kgfei.hangtkkg3hiao_com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危	录音	允许应用程序访问音频记录路径

	险		
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.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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
gjfjj2fh.sang9kgfei.hangtkkg3hiao.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
gjfjj2fh.sang9kgfei.hangtkkg3hiao_com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
gjfjj2fh.sang9kgfei.hangtkkg3hiao.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
gjfjj2fh.sang9kgfei.hangtkkg3hiao_com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
gjfjj2fh.sang9kgfei.hangtkkg3hiao.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
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
gjfjj2fh.sang9kgfei.hangtkkg3hiao.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
gjfjj2fh.sang9kgfei.hangtkkg3hiao.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
gjfjj2fh.sang9kgfei.hangtkkg3hiao.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.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.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_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.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.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。

gjfjj2fh.sang9kgfei.hangtkkg3hiao_com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信