



MoGua

速汇 1.1.3.APK 分析报告



APP名称:

速汇

包名:	com.hcnzjt.fipl
域名线索:	11条
URL线索:	9条
邮箱线索:	0条
分析日期:	2025年1月8日
分析平台:	摸瓜APK反编译平台

文件名: hcnzjt.apk

文件大小: 5.88MB

MD5值: e76bf19453b26409a6a2b0d2965fe711

SHA1值: 11b1de4121e2f06e4ef669ff31790d8f9cba5d0c

SHA256值: 1c459fe91d223d4379f9a76d337582b02ebd6886bce309289d79395c2fcf3606

i APP 信息

App名称: 速汇

包名: com.hcnzjt.fipl

主活动Activity: com.hcnzjt.fipl.StartActivity

安卓版本名称: 1.1.3

安卓版本: 20220330

🔍 域名线索

域名	服务器信息
lb-4vgarouk-1mthkqe28ai9bluo.clb.ap-guangzhou.tencentclb.com	IP: 106.52.160.228 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ns.adobe.com	没有服务器地理信息.
soft.tbs.imtt.qq.com	IP: 119.167.201.75 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941

cfg.imtt.qq.com	IP: 109.244.173.227 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
mdc.html5.qq.com	IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
debugtbs.qq.com	IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
debugx5.qq.com	IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
pms.mb.qq.com	IP: 109.244.173.227 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
tbsrecovery.imtt.qq.com	IP: 109.244.244.237 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397232
schemas.android.com	没有服务器地理信息.
log.tbs.qq.com	IP: 109.244.244.37 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

URL线索

URL信息	Url所在文件
http://lb-4vgarouk-1mthkqe28ai9bluo.clb.ap-guangzhou.tencentclb.com	c/g/a/a/g.java
http://lb-4vgarouk-1mthkqe28ai9bluo.clb.ap-guangzhou.tencentclb.com/app	c/g/a/b/a.java
http://lb-4vgarouk-1mthkqe28ai9bluo.clb.ap-guangzhou.tencentclb.com/app/index.php/captcha.html?	c/g/a/b/a.java
http://lb-4vgarouk-1mthkqe28ai9bluo.clb.ap-guangzhou.tencentclb.com/app/index.php/home/index/kefu	c/g/a/b/a.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	c/j/a/c/u.java
https://log.tbs.qq.com/ajax?c=pu&tk=	c/j/a/c/u.java
https://log.tbs.qq.com/ajax?c=dl&k=	c/j/a/c/u.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	c/j/a/c/u.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	c/j/a/c/u.java

https://tbsrecovery.imtt.qq.com/getconfig	c/j/a/c/u.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	c/j/a/c/k.java
https://pms.mb.qq.com/rsp204	c/j/a/b/j0.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	c/j/a/b/n0/a.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
http://schemas.android.com/apk/res/android	b/h/e/d/g.java
http://ns.adobe.com/xap/1.0/\u0000	b/l/a/a.java

邮箱线索

手机线索

签名证书

APK已签名

v1 签名: True

v2 签名: True

v3 签名: True

找到 1 个唯一证书

主题: C=chengdu, ST=chengdu, L=chengdu, O=jt1685062340405, OU=jg1685062340405, CN=clca

签名算法: rsassa_pkcs1v15

有效期自: 2023-05-26 00:52:20+00:00

有效期至: 2073-05-13 00:52:20+00:00

发行人: C=chengdu, ST=chengdu, L=chengdu, O=jt1685062340405, OU=jg1685062340405, CN=clca

序列号: 0x2626e640

哈希算法: sha1

md5值: a910e4cd519eaf2dd1cb59223b4a0491

sha1值: 2b5c34dacdb632409e5d66098ce51baf9f154597

sha256值: c23da1d0a6f45551a51f732481b7d680d06a811c7585b67323f63cd2dc5e6c08

sha512值: 08729e435e2fab44b09b5b6a98e969a6658896c90c53d727da2d39c00aa96b19cdc0c4618d645fca124308ab6175474608ed44192b1d3bf05d03c10b098b4b1c

公钥算法: rsa

密钥长度: 1024

指纹: 0b90147ad50e01a8e34485234ba15cbfb7d2096730359e6aa784b83f1162ba55

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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

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。