



MoGua

DeepSeek 1.2.6.APK 分析报告



APP名称:

DeepSeek

包名:	com.deepseek.chat
域名线索:	34条
URL线索:	39条
邮箱线索:	5条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件名: com.deepseek.chat_1.2.6.apk
文件大小: 11.14MB
MD5值: 9285afadd706a2b22c81d7c5a65b174a
SHA1值: 025edc8837c3a6c4af6cc837b51552eca41c8649
SHA256值: c50878af9ddc98c11b035e9c0714ec590a804e32566a01313ec7dea2230bbca3

i APP 信息

App名称: DeepSeek
包名: com.deepseek.chat
主活动Activity: com.deepseek.chat.MainActivity
安卓版本名称: 1.2.6
安卓版本: 85

🔍 域名线索

域名	服务器信息
goo.gle	IP: 67.199.248.12 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.750134 经度: -73.997009
www.slf4j.org	IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
ns.adobe.com	没有服务器地理信息.
	IP: 120.232.169.168

wap.cmpassport.com	所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
fp-it-tracker.fengkongcloud.com	IP: 60.28.204.181 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
accounts.google.com	IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
long.open.weixin.qq.com	IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
ktor.io	IP: 18.238.192.40 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
gator.volces.com	IP: 60.223.217.242 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508

download.deepseek.com	IP: 101.73.66.114 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
config2.cmpassport.com	IP: 112.33.111.251 所属国家: China 地区: Anhui 城市: Hefei 纬度: 31.863815 经度: 117.280830
schemas.android.com	没有服务器地理信息.
toblog.volceapplog.com	IP: 116.136.186.203 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
chat.deepseek.com	IP: 60.204.2.4 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
log2.cmpassport.com	IP: 36.140.86.18 所属国家: China 地区: Gansu 城市: Lanzhou 纬度: 36.056690 经度: 103.792221
	IP: 221.204.15.89

castatic.fengkongcloud.com	所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
apmplus.volces.com	IP: 116.136.186.204 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
castatic-dev.fengkongcloud.com	IP: 81.70.118.179 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mp.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
abtest.volceapplog.com	IP: 221.194.162.226 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
ms.zzx9.cn	IP: 124.64.196.27 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
tobapplog.volceapplog.com	IP: 221.194.162.224 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
cdn.deepseek.com	IP: 111.202.6.31 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
databyterangers.com.cn	没有服务器地理信息.
klink.volceapplog.com	IP: 221.194.162.225 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
auth.wosms.cn	IP: 124.64.196.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
captcha.fengkongcloud.cn	IP: 123.117.133.135 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

rcs.cmpassport.com	IP: 120.232.169.172 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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
js.hcaptcha.com	IP: 104.19.229.21 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mon.snssdk.com	IP: 123.6.122.247 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
youtrack.jetbrains.com	IP: 63.33.88.220 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
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
tab.volces.com	IP: 60.223.217.235 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508

 URL线索

URL信息	Url所在文件
https://chat.deepseek.com/feedback	E8/C0149d.java
https://klink.volceapplog.com/service/2/device_register/	L6/c.java
https://klink.volceapplog.com/service/2/device_update	L6/c.java
https://klink.volceapplog.com/service/2/app_alert_check/	L6/c.java
https://toblog.volceapplog.com/service/2/app_log/	L6/c.java
https://tobapplog.volceapplog.com/service/2/app_log/	L6/c.java
https://toblog.volceapplog.com/service/2/log_settings/	L6/c.java
https://abtest.volceapplog.com/service/2/abtest_config/	L6/c.java
https://toblog.volceapplog.com/service/2/profile/	L6/c.java
https://apmplus.volces.com/apm/device_register	L2/j.java

https://apmplus.volces.com/monitor/collect/c/session	L2/j.java
https://js.hcaptcha.com/1/api.js'\n	Pa/r.java
https://gator.volces.com/service/2/device_register/	A8/C0036g.java
https://gator.volces.com/service/2/device_update	A8/C0036g.java
https://gator.volces.com/service/2/app_alert_check/	A8/C0036g.java
https://gator.volces.com	A8/C0036g.java
https://gator.volces.com/service/2/log_settings/	A8/C0036g.java
https://gator.volces.com/service/2/profile/	A8/C0036g.java
https://tab.volces.com/service/2/abtest_config/	A8/C0036g.java
https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html	R6/C0684g.java
https://cdn.deepseek.com/policies/zh-CN/deepseek-privacy-policy.html	R6/C0684g.java
https://cdn.deepseek.com/policies/en-US/deepseek-terms-of-use.html	R6/C0684g.java
https://cdn.deepseek.com/policies/zh-CN/deepseek-terms-of-use.html	R6/C0684g.java
https://www.slf4j.org/codes.html	Sd/d.java
https://chat.deepseek.com/feedback	Xc/d.java
https://chat.deepseek.com/feedback)	Xc/d.java
http://ns.adobe.com/xap/1.0/\u0000	a2/C0797g.java
https://auth.wosms.cn/dro/netm/v1.0/qc	cn/fly/verify/es.java

https://config2.cmpassport.com/client/uniConfig	cn/fly/verify/eh.java
https://log2.cmpassport.com:9443/log/logReport	cn/fly/verify/eh.java
https://rcs.cmpassport.com/unisdk/rs/scripAndTokenForHttps	cn/fly/verify/eh.java
https://wap.cmpassport.com/resources/html/contract.html	cn/fly/verify/pure/entity/a.java
https://e.189.cn/sdk/agreement/detail.do	cn/fly/verify/pure/entity/a.java
https://ms.zzx9.cn/html/oauth/protocol2.html	cn/fly/verify/pure/entity/a.java
https://youtrack.jetbrains.com/issue/KT-55980	ac/AbstractC0851q.java
https://goo.gle/compose-feedback	f0/AbstractC1259p.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=	com/tencent/mm/opensdk/diffdev/a/c.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=	com/tencent/mm/opensdk/diffdev/a/b.java
https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=	com/tencent/mm/opensdk/openapi/WXAPISecurityHelper.java
https://castatic-dev.fengkongcloud.com/pr/v1.0.3/index.html\	com/ishumei/sdk/captcha/O0000O000000oO.java
https://castatic.fengkongcloud.com/pr/v1.0.4/index.html	com/ishumei/sdk/captcha/SmCaptchaWebView.java
https://captcha.fengkongcloud.cn/ca/v1/log	com/ishumei/sdk/captcha/O000O00000oO/O000O00000OoO.java
https://fp-it-tracker.fengkongcloud.com/v3/tracker	com/ishumei/sdk/captcha/O000O00000oO/O000O00000oO.java
http://fp-it-tracker.fengkongcloud.com/v3/tracker	com/ishumei/sdk/captcha/O000O00000oO/O000O00000oO.java
https://apmplus.volces.com/monitor/collect/c/cloudcontrol/file	com/apm/insight/runtime/ConfigManager.java

https://apmplus.volces.com/monitor/collect/c/native_bin_crash	com/apm/insight/runtime/ConfigManager.java
https://apmplus.volces.com/settings/get	com/apm/insight/runtime/ConfigManager.java
https://apmplus.volces.com/monitor/collect/c/core_dump_collect	com/apm/insight/runtime/ConfigManager.java
https://apmplus.volces.com/monitor/collect/c/crash_portrait	com/apm/insight/runtime/ConfigManager.java
https://apmplus.volces.com/monitor/collect/c/exception	com/apm/insight/runtime/ConfigManager.java
https://apmplus.volces.com/monitor/collect/c/logcollect	com/apm/insight/runtime/ConfigManager.java
https://apmplus.volces.com/monitor/collect/c/crash	com/apm/insight/runtime/ConfigManager.java
https://apmplus.volces.com/monitor/collect/c/exception/dump_collection	com/apm/insight/runtime/ConfigManager.java
https://apmplus.volces.com/monitor/collect/c/rapheal_file_collect	com/apm/insight/runtime/ConfigManager.java
https://js.hcaptcha.com/1/api.js	com/hcaptcha/sdk/HcaptchaConfig.java
https://databyterangers.com.cn	gb/c.java
https://chat.deepseek.com/feedback	g9/d.java
https://cdn.deepseek.com/policies/zh-CN/third-party-info-sharing-list.html	g9/d.java
https://cdn.deepseek.com/policies/zh-CN/collected-personal-information.html	g9/d.java
https://cdn.deepseek.com/policies/zh-CN/app-permissions.html	g9/d.java
http://schemas.android.com/apk/res/android	x1/AbstractC2958b.java
https://apmplus.volces.com/monitor/collect/c/cloudcontrol/get	s5/AbstractC2430a.java
https://apmplus.volces.com/monitor/collect/c/cloudcontrol/file	s5/AbstractC2430a.java

https://apmplus.volces.com/monitor/collect/c/logcollect	s5/AbstractC2430a.java
https://cdn.deepseek.com/policies/en-US/deepseek-terms-of-use.html	I0/c.java
https://cdn.deepseek.com/policies/zh-CN/deepseek-terms-of-use.html	I0/c.java
https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html	I0/c.java
https://cdn.deepseek.com/policies/zh-CN/deepseek-privacy-policy.html	I0/c.java
https://databyterangers.com.cn/simulator/mobile/log	Lb/m.java
https://ktor.io/docs/http-client-engines.html	Za/f.java
https://accounts.google.com/o/oauth2/revoke?token=	pa/RunnableC2293c.java
http://castatic.fengkongcloud.com/pr/v1.0.4/assets/GT-Walsheim-Pro-Bold.ttf\	y8/AbstractC3106j.java
https://chat.deepseek.com	F7/e.java
https://chat.deepseek.com/feedback	I9/l.java
https://ktor.io/docs/faq.html	ab/C0827d.java
https://download.deepseek.com/app?utm_source=android_app	V7/c.java
https://chat.deepseek.com/feedback	M8/e.java
https://mon.snssdk.com/monitor/collect/c/cloudcontrol/file	p5/AbstractC2279a.java

 邮箱线索

邮箱地址	所在文件
abjccbaidcg4bgcdcacj@dybhbbbg.ad	cn/fly/verify/ab.java
fk5gj@hm9ed2figevfkcgjff8f.fgel	cn/fly/verify/bv.java
015ybhbibjddebge@babjcd.ebfbbbibh	cn/fly/verify/bs.java
didkce@dlfedkfcdi.didk	cn/fly/verify/dh.java
u0013android@android.com0 u0013android@android.com	qa/j.java

手机线索

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=zhejiang, L=hangzhou, O=DeepSeek, OU=DeepSeek, CN=DeepSeek
签名算法: rsassa_pkcs1v15
有效期自: 2024-11-04 02:29:09+00:00
有效期至: 2052-03-22 02:29:09+00:00
发行人: C=cn, ST=zhejiang, L=hangzhou, O=DeepSeek, OU=DeepSeek, CN=DeepSeek
序列号: 0x478ea09c194ed805
哈希算法: sha256
md5值: 1e1d1800a35927e71b85f5dbd35536e7
sha1值: ca2378d73740d0010d2c4bce7eef948b32fef14b
sha256值: c6893c5368f7b5122fecdafc6c4ecf49e0b3dc4e42bd166cdb646907788c7ffa
sha512值: 1f1b5f60e77021476f2af5c8e580c8ad55d7416181e0a80eeaea9d9c797ba388cfbafd631ebded3b19c525ee107e642b6aca75fe91f3fd33ab2ce0f3011496b2
公钥算法: rsa
密钥长度: 2048

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.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.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.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
com.deepseek.chat.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.deepseek.chat.MainActivity	Schemes: com.deepseek.chat://, Hosts: authorized_android,