



MoGua

口袋写作 3.0.5.APK 分析报告



APP名称:

口袋写作

包名:	com.hmz.koudaiwriting
域名线索:	26条
URL线索:	4条
邮箱线索:	0条
分析日期:	2025年9月8日
分析平台:	摸瓜APK反编译平台

文件名: kdwrite_v3.0.5.apk
文件大小: 65.05MB
MD5值: 8c9d6ba74ebaff0afdb85733bc3adfe8
SHA1值: 65b5921d0c317482bcd785b682a6527a0daa4354
SHA256值: c5b5c5f6407036b31dfbdca163dd3f2e08b229630f4ca627dd8051268b13259f

i APP 信息

App名称: 口袋写作
包名: com.hmz.koudaiwriting
主活动Activity: com.hmz.koudaiwriting.MainActivity
安卓版本名称: 3.0.5
安卓版本: 313

🔍 域名线索

域名	服务器信息
adsmind.ugdting.com	IP: 218.60.45.167 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
c2.gdt.qq.com	IP: 220.194.116.33 所属国家: China 地区: Tianjin

	城市: Tianjin 纬度: 39.142181 经度: 117.176102
46a79741.fyeds3.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
sg.ylhglobal.com	IP: 43.159.108.154 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
snowflake.qq.com	IP: 116.130.220.107 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
sketch.com	IP: 108.156.144.90 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
i.gtimg.cn	IP: 123.6.25.75 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613

qzs.qq.com	IP: 221.204.14.52 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
qzs.gdting.com	IP: 119.167.249.58 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
mi.gdt.qq.com	IP: 220.194.116.121 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
100000189777.retail.n.weimob.com	IP: 212.64.63.139 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
xx.xx.xx.xx	没有服务器地理信息.
qzonestyle.gting.cn	IP: 221.204.14.50 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
	IP: 220.194.116.80 所属国家: China 地区: Tianjin

win.gdt.qq.com	城市: Tianjin 纬度: 39.142181 经度: 117.176102
sdk.e.qq.com	IP: 220.194.116.72 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
test.snowflake.qq.com	IP: 221.198.69.15 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
e.qq.com	IP: 220.194.116.85 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
sf3-fe-tos.pglstatp-toutiao.com	IP: 218.11.15.211 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
union.eff.qq.com	IP: 157.255.219.214 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108

v2.gdt.qq.com	IP: 220.194.116.38 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
www.jsdelivr.com	IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
pgdt.ugdtimg.com	IP: 220.194.72.89 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
c.appjiagu.com	IP: 106.63.25.12 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
tdid.m.qq.com	IP: 60.29.239.156 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
android.googlesource.com	IP: 74.125.142.82 所属国家: United States of America 地区: California 城市: Mountain View

纬度: 37.405991
经度: -122.078514

URL线索

URL信息	Url所在文件
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/shake.webp	摸瓜V2引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/shake_text.png	摸瓜V2引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/swipe_right.webp	摸瓜V2引擎
https://qzonestyle.gting.cn/qzone/biz/gdt/mob/sdk/v2/android01/download.html	摸瓜V3引擎
https://sg.ylhglobal.com	摸瓜V3引擎
https://tdid.m.qq.com?mc=2	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_gray_transparent.png	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_dark.png	摸瓜V3引擎
https://sdk.e.qq.com/activate	摸瓜V3引擎
https://infinitedata-pa.googleapis.com	摸瓜V3引擎

http://c.appjiagu.com/apk/cr.html	摸瓜V3引擎
https://xx.xx.xx.xx	摸瓜V3引擎
play.googleapis.com	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_dark_fb.png	摸瓜V3引擎
https://union.eff.qq.com/v2/query/gdtmview	摸瓜V3引擎
https://win.gdt.qq.com/win_notice.fcg?viewid=1	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V3引擎
https://pgdt.ugdtimg.com	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
https://i.gting.cn/ams-web/page-performance/page-performance.min.js?v=1	摸瓜V3引擎
https://mi.gdt.qq.com/gdt_mview.fcg	摸瓜V3引擎
https://sdk.e.qq.com/mediation?version=1	摸瓜V3引擎
https://sketch.com	摸瓜V3引擎
https://v2.gdt.qq.com/	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/webview-cover.png	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://test.snowflake.qq.com/ola/v2	摸瓜V3引擎

https://test.snowflake.qq.com/ola/v2	摸瓜V3引擎
https://c2.gdt.qq.com/	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_light_fw.png	摸瓜V3引擎
https://sdk.e.qq.com/launch	摸瓜V3引擎
https://qzs.qq.com/union/res/union_cdn/page/images/loading_2x.gif	摸瓜V3引擎
https://mi.gdt.qq.com/	摸瓜V3引擎
https://snowflake.qq.com/ola/v2	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_white_transparent_fw.png	摸瓜V3引擎
https://sdk.e.qq.com/mediation?version=2	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_white_transparent_fb.png	摸瓜V3引擎
https://e.qq.com/dev/index.html	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_light_1.png	摸瓜V3引擎
https://46a79741.fyeds3.com/	摸瓜V3引擎
https://adsmind.ugdting.com	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_light_fb.png	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_white_transparent.png	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_dark_fw.png	摸瓜V3引擎

https://github.com/apvarun/toastify-js	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_gray_transparent_fb.png	摸瓜V3引擎
https://100000189777.retail.n.weimob.com/saas/retail/100000189777/21036777/goods/detail	摸瓜V3引擎
https://sdk.e.qq.com/open/v1.1/dns/resolve	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/ams_logo_gray_transparent_fw.png	摸瓜V3引擎

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=CN, ST=广东, L=深圳, O=hmz, OU=hmz, CN=hmz
签名算法: rsassa_pkcs1v15
有效期自: 2016-01-05 14:09:13+00:00
有效期至: 2115-12-12 14:09:13+00:00
发行人: C=CN, ST=广东, L=深圳, O=hmz, OU=hmz, CN=hmz
序列号: 0x709f453
哈希算法: sha256
md5值: 5f99c5f7e2c460104df737e0c469eaad
sha1值: b9b3fe81c9b3dc932452f2cdb176d106d3a9bb10
sha256值: 8e9a48234e369a164f4522480207a0a57144a6b31785e4152027b72668819b4f
sha512值: b60fd499d3469f926bea53854d31548d301e1553db115d492fe813d92235d9e12d45d88083a2d1a4bcd74da94024581e9f1f0c8305d981b397f155915bd6005f
公钥算法: rsa

密钥长度: 2048
指纹: 063213f1c3e259e7bc24cc8e66321273aa9f24b3f121c2d2bbe921c0870a3b45

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.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.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。
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
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
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
oplus.permission.settings.LAUNCH_FOR_EXPORT	未知	Unknown permission	Unknown permission from android reference
com.vivo.identifier.permission.OAID_STATE_DIALOG	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。
com.hmz.koudaiwriting.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
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.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
com.hmz.koudaiwriting.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1105092590://,

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。