Evaluation Warning: The document was created with Spire.Doc for Python.

**口袋写作（ 3.0.5版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 口袋写作 |
| 版本 | 3.0.5 |
| 包名 | com.hmz.koudaiwriting |
| 域名线索 | 26条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年9月8日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | kdwrite\_v3.0.5.apk |
| 文件大小 | 65.05MB |
| MD5值 | 8c9d6ba74ebaff0afdb85733bc3adfe8 |
| SHA1值 | 65b5921d0c317482bcd785b682a6527a0daa4354 |
| SHA256值 | c5b5c5f6407036b31dfbdca163dd3f2e08b229630f4ca627dd8051268b13259f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| adsmind.ugdtimg.com | IP: 218.60.45.167 所属国家: China 地区: Liaoning 城市: Shenyang  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| c2.gdt.qq.com | IP: 220.194.116.33 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 46a79741.fyeds3.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| sg.ylhglobal.com | IP: 43.159.108.154 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| snowflake.qq.com | IP: 116.130.220.107 所属国家: China 地区: Beijing 城市: Beijing  |
| sketch.com | IP: 108.156.144.90 所属国家: United States of America 地区: Washington 城市: Seattle  |
| i.gtimg.cn | IP: 123.6.25.75 所属国家: China 地区: Henan 城市: Zhengzhou  |
| qzs.qq.com | IP: 221.204.14.52 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| qzs.gdtimg.com | IP: 119.167.249.58 所属国家: China 地区: Shandong 城市: Qingdao  |
| mi.gdt.qq.com | IP: 220.194.116.121 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 100000189777.retail.n.weimob.com | IP: 212.64.63.139 所属国家: China 地区: Beijing 城市: Beijing  |
| xx.xx.xx.xx | 没有服务器地理信息.  |
| qzonestyle.gtimg.cn | IP: 221.204.14.50 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| win.gdt.qq.com | IP: 220.194.116.80 所属国家: China 地区: Tianjin 城市: Tianjin  |
| sdk.e.qq.com | IP: 220.194.116.72 所属国家: China 地区: Tianjin 城市: Tianjin  |
| test.snowflake.qq.com | IP: 221.198.69.15 所属国家: China 地区: Tianjin 城市: Tianjin  |
| e.qq.com | IP: 220.194.116.85 所属国家: China 地区: Tianjin 城市: Tianjin  |
| sf3-fe-tos.pglstatp-toutiao.com | IP: 218.11.15.211 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| union.eff.qq.com | IP: 157.255.219.214 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| v2.gdt.qq.com | IP: 220.194.116.38 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.jsdelivr.com | IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco  |
| pgdt.ugdtimg.com | IP: 220.194.72.89 所属国家: China 地区: Tianjin 城市: Tianjin  |
| c.appjiagu.com | IP: 106.63.25.12 所属国家: China 地区: Tianjin 城市: Tianjin  |
| tdid.m.qq.com | IP: 60.29.239.156 所属国家: China 地区: Tianjin 城市: Tianjin  |
| android.googlesource.com | IP: 74.125.142.82 所属国家: United States of America 地区: California 城市: Mountain View  |

### **4.2 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.gtimg.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  |
| 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.gtimg.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://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.ugdtimg.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  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 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**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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 |

## **10. 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**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**