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

**好办公（ 1.0.6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 | 好办公 |
| 版本 | 1.0.6 |
| 包名 | uni.ktmhfz |
| 域名线索 | 16条 |
| URL线索 | 24条 |
| APP图标 |  |
| 分析日期 | 2025年6月20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 | juguyj-gjhfscxw.apk |
| 文件大小 | 122.57MB |
| MD5值 | c5cee3058390f303f37ecc3c2eae89bc |
| SHA1值 | fc2176fc806d87bb7e673c8905072b4e7241d78a |
| SHA256值 | e83580197408adac727e9062ae064625ab4c7f7b1142a1bea56ea245e26f521f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 好办公 |
| 包名 | uni.ktmhfz |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.6 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ns.adobe.com | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.android.com | 没有服务器地理信息.  |
| at.alicdn.com | IP: 124.95.150.18 所属国家: China 地区: Liaoning 城市: Shenyang  |
| env-00jxto01apte-static.normal.cloudstatic.cn | IP: 116.142.235.233 所属国家: China 地区: Beijing 城市: Beijing  |
| m3w.cn | IP: 221.204.20.165 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| www.google.com | IP: 31.13.68.169 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| er.dcloud.net.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| quilljs.com | IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| ask.dcloud.net.cn | IP: 124.163.195.89 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| apis.map.qq.com | IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing  |
| img-cdn-qiniu.dcloud.net.cn | IP: 119.188.150.101 所属国家: China 地区: Shandong 城市: Jinan  |
| er.dcloud.io | 没有服务器地理信息.  |
| service.dcloud.net.cn | IP: 110.40.181.119 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| https://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/feature/utsplugin/ProxyModule.java  |
| https://er.dcloud.io/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://er.dcloud.net.cn/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://ask.dcloud.net.cn/article/35627  | io/dcloud/p/r.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/p/r.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/p/h1.java  |
| https://er.dcloud.io/rv  | io/dcloud/p/d0.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/p/d0.java  |
| https://ask.dcloud.net.cn/article/287  | io/dcloud/share/IFShareApi.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifViewUtils.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| https://ask.dcloud.net.cn/article/36199  | 摸瓜V1引擎  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=  | 摸瓜V2引擎  |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=  | 摸瓜V2引擎  |
| https://www.google.com/maps/?daddr=  | 摸瓜V2引擎  |
| https://www.google.com/maps/  | 摸瓜V2引擎  |
| https://quilljs.com/  | 摸瓜V2引擎  |
| https://quilljs.com  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| https://github.com/indutny/elliptic/issues  | 摸瓜V2引擎  |
| https://github.com/indutny/elliptic  | 摸瓜V2引擎  |
| https://github.com/crypto-browserify/crypto-browserify  | 摸瓜V2引擎  |
| https://feross.org/opensource>  | 摸瓜V2引擎  |
| https://env-00jxto01apte-static.normal.cloudstatic.cn/domain.json  | 摸瓜V2引擎  |
| https://github.com/emn178/js-md5  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1852921\_9ntd3e3nsl5.eot);src:url(https://at.alicdn.com/t/font\_1852921\_9ntd3e3nsl5.eot  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1852921\_9ntd3e3nsl5.woff2)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1852921\_9ntd3e3nsl5.woff)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1852921\_9ntd3e3nsl5.ttf)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1852921\_9ntd3e3nsl5.svg  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1905649\_xxq6s2ik49s.eot);src:url(https://at.alicdn.com/t/font\_1905649\_xxq6s2ik49s.eot  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1905649\_xxq6s2ik49s.woff2)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1905649\_xxq6s2ik49s.woff)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1905649\_xxq6s2ik49s.ttf)  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_1905649\_xxq6s2ik49s.svg  | 摸瓜V2引擎  |
| https://img-cdn-qiniu.dcloud.net.cn/fonts/uni.ttf)  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| git@github.com fedor@indutny.com emn178@gmail.com  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 19919152923  | 摸瓜V2引擎  |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=Kjhae, ST=Ym3il, L=idLxr, O=sz1750157501902, OU=og1750157501902, CN=jypr 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-17 10:51:44+00:00 有效期至: 2075-06-05 10:51:44+00:00 发行人: C=Kjhae, ST=Ym3il, L=idLxr, O=sz1750157501902, OU=og1750157501902, CN=jypr 序列号: 0x7baead9a 哈希算法: sha512 md5值: 648b1864151297ef6352e1c998430002 sha1值: a6740bde88966fd3043b981352d05c95c68c7b14 sha256值: cefec71388ca7d3a25cf4da69c20f2f5d8175c3f7863076bc0a22e8f1095b0e9 sha512值: 1bcd84dd269ddc267219f6e145ca764b0801021202aa0b11f4ac78ae04cc699a8933af14780325f8dc6fb634e66296c7e8042aeb9abc5d91c1a15a766b720e56 公钥算法: rsa 密钥长度: 4096 指纹: f746743242667c6b2fbdeac24f50db8ff42ac3da3bdd60f446565d7e8a1ad3ea**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API"  |
| "dcloud\_io\_without\_authorization" : "not authorized"  |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service"  |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed"  |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained"  |
| "dcloud\_oauth\_token\_failed" : "failed to get token"  |
| "dcloud\_permissions\_reauthorization" : "reauthorize"  |
| "dcloud\_tips\_certificate" : "certificate"  |
| "log\_number\_private" : "Private"  |
| "rule\_type\_private" : "Private numbers"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_io\_without\_authorization" : "没有获得授权"  |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权"  |
| "dcloud\_oauth\_token\_failed" : "获取token失败"  |
| "dcloud\_permissions\_reauthorization" : "重新授权"  |
| "dcloud\_tips\_certificate" : "证书"  |

## **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.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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MODIFY\_PHONE\_STATE | 系统需要 | 修改电话状态 | 允许应用程序控制设备的电话功能。具有此权限的应用程序可以切换网络,打开和关闭电话收音机等,而无需通知您 |
| android.permission.ANSWER\_PHONE\_CALLS | 危险 |  | 允许应用接听来电。 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PROJECTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: huiyi://,  |

**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。**