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

**STO（ 2.1.9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 | STO |
| 版本 | 2.1.9 |
| 包名 | uni.UNIEF91F25 |
| 域名线索 | 16条 |
| URL线索 | 24条 |
| APP图标 |  |
| 分析日期 | 2025年2月6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 | sto.apk |
| 文件大小 | 39.39MB |
| MD5值 | 82ec5a7cfb81c28d2c7eeeab7b887777 |
| SHA1值 | e9c5ff77e37d34543f8f08a1a941ac9c2cbab1e8 |
| SHA256值 | 8b6272a5495d3589f1658f841f0ecfd6983044e2d3c40c1378ab7339155bea9f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | STO |
| 包名 | uni.UNIEF91F25 |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 2.1.9 |
| 安卓版本 | 219 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| schemas.android.com | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.google.com | IP: 31.13.94.49  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| quilljs.com | IP: 172.66.43.93  所属国家: United States of America  地区: California  城市: San Francisco |
| 47.238.4.119 | IP: 47.238.4.119  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| service.dcloud.net.cn | IP: 111.229.199.57  所属国家: China  地区: Beijing  城市: Beijing |
| m3w.cn | IP: 221.204.73.192  所属国家: China  地区: Shanxi  城市: Taiyuan |
| er.dcloud.io | 没有服务器地理信息. |
| files.cdn.coreshop.cn | IP: 42.56.93.203  所属国家: China  地区: Liaoning  城市: Shenyang |
| apis.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| api.sstoss.com | IP: 18.166.83.193  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| oss.colorui.org | IP: 162.210.199.65  所属国家: United States of America  地区: District of Columbia  城市: Washington |
| ns.adobe.com | 没有服务器地理信息. |
| er.dcloud.net.cn | IP: 43.142.57.168  所属国家: China  地区: Beijing  城市: Beijing |
| ask.dcloud.net.cn | IP: 115.56.90.192  所属国家: China  地区: Henan  城市: Jiaozuo |

### **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://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/283 | io/dcloud/feature/utsplugin/ProxyModule.java |
| https://ask.dcloud.net.cn/article/35627 | io/dcloud/e/b/a.java |
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/e/b/a.java |
| https://er.dcloud.io/rv | io/dcloud/e/c/h/c.java |
| https://er.dcloud.net.cn/rv | io/dcloud/e/c/h/c.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/g/b.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 |
| https://files.cdn.coreshop.cn/corekf/logo.png | 摸瓜V2引擎 |
| https://oss.colorui.org/cos/img/4put2.png | 摸瓜V2引擎 |
| https://github.com/facebook/regenerator/blob/main/LICENSE | 摸瓜V2引擎 |
| https://oss.colorui.org/cos/img/8v2yr.png | 摸瓜V2引擎 |
| https://oss.colorui.org/cos/img/qhgtb.png | 摸瓜V2引擎 |
| https://api.sstoss.com | 摸瓜V2引擎 |
| http://47.238.4.119:2070/api/Common/UploadImages | 摸瓜V2引擎 |
| https://oss.colorui.org/cos/img/pa1m9.png | 摸瓜V2引擎 |
| https://service.dcloud.net.cn/uniapp/feedback.html | 摸瓜V2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: False 找到 1 个唯一证书 主题: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug 签名算法: rsassa\_pkcs1v15 有效期自: 2021-04-12 08:27:53+00:00 有效期至: 2121-03-19 08:27:53+00:00 发行人: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug 序列号: 0x363bc393 哈希算法: sha256 md5值: 06838cc840093b9d4689fc419ba1a3f3 sha1值: 97c84101b9141c130dd75d7428a2922518c36dcd sha256值: b01d06180d003e79c7b9088993b8e5ae7a19b0da1161aa097c7f398a6f514fa7 sha512值: 67720eb20639d1f5f9c8b7b201b185ea4364f6a89bedd35aa1d273002c16d65a7739f59679510d3b96c1f2c3dd3136d9a34451cb679251a86ff4cafdc18314bf 公钥算法: rsa 密钥长度: 2048 指纹: b27ac6d7a4586417c251be6e44179616262379e57da2d1e19db0995be0ddf509**

## **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" |
| "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\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| 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 |
| 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 |
| 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.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.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。 |
| 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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.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 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |

## **10. 应用内通信**

**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。**