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

**圣亨新渠道（ 218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 | 圣亨新渠道 |
| 版本 | 218 |
| 包名 | uni.UNID4CD49D |
| 域名线索 | 15条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2025年5月23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 | sht2018\_sign.apk |
| 文件大小 | 37.14MB |
| MD5值 | e98bc8111d5f110d91652c2b1d00290c |
| SHA1值 | a8f345d25be2ad4a5fb9ed85b97924ecc3419c6c |
| SHA256值 | c13c7b0315e487ceefd9abf4c9daa577f4ff412c88cc79861aff6fa21a77c45a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 圣亨新渠道 |
| 包名 | uni.UNID4CD49D |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 218 |
| 安卓版本 | 2018 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| quilljs.com | IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.laiyu.vip | 没有服务器地理信息.  |
| www.google.com | IP: 199.16.158.8 所属国家: United States of America 地区: California 城市: San Francisco  |
| kf.hszps.cn | IP: 39.103.232.70 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| shtluck.syshsy.cn | IP: 39.103.232.70 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| at.alicdn.com | IP: 221.195.63.237 所属国家: China 地区: Hebei 城市: Cangzhou  |
| apis.map.qq.com | IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing  |
| www.baidu.com | IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| hsrh.jz0418.cn | IP: 8.142.104.236 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.thorui.cn | IP: 119.91.210.224 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  |
| 192.168.1.118 | IP: 192.168.1.118 所属国家: - 地区: - 城市: -  |
| 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: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ask.dcloud.net.cn/article/36199  | Mogua Engine V1  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133858920.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133300938.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133278681.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133651548.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133943375.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133506942.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133540794.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133438109.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133176496.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133958474.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133244079.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133119964.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133113295.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818133551942.jpg  | Mogua Engine V2  |
| https://api.laiyu.vip//ue\_upload/img/20190514/1557818134437184.jpg  | Mogua Engine V2  |
| https://www.baidu.com  | Mogua Engine V2  |
| http://192.168.1.118:8081/order/ali\_order?order\_id=  | Mogua Engine V2  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | Mogua Engine V2  |
| https://shtluck.syshsy.cn/user/get\_upapp  | Mogua Engine V2  |
| https://hsrh.jz0418.cn/sytpic/  | Mogua Engine V2  |
| https://kf.hszps.cn/index/index/home?theme=05202d&business\_id=1&visiter\_id=  | Mogua Engine V2  |
| https://shtluck.syshsy.cn/  | Mogua Engine V2  |
| https://domain/pull\_stream  | Mogua Engine V2  |
| https://shtluck.syshsy.cn/uploads/share/gift.jpg')  | Mogua Engine V2  |
| https://www.thorui.cn/)\r\n  | Mogua Engine V2  |
| https://at.alicdn.com/t/font\_1078604\_w4kpxh0rafi.ttf)  | Mogua Engine V2  |
| https://hsrh.jz0418.cn/sytpic/3.jpg);background-size:cover;background-repeat:no-repeat;background-position:50%  | Mogua Engine V2  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | Mogua Engine V2  |
| http://www.w3.org/1999/xlink  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| http://www.w3.org/1998/Math/MathML  | Mogua Engine V2  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=  | Mogua Engine V2  |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=  | Mogua Engine V2  |
| https://www.google.com/maps/?daddr=  | Mogua Engine V2  |
| https://www.google.com/maps/  | Mogua Engine V2  |
| https://quilljs.com/  | Mogua Engine V2  |
| https://quilljs.com  | Mogua Engine V2  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15519997119  | Mogua Engine V2  |
| 18208627757  | Mogua Engine V2  |
| 18540300935  | Mogua Engine V2  |

## **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=辽宁省, L=沈阳, O=辽宁圣亨太生物科技有限公司, OU=辽宁圣亨太生物科技有限公司, CN=sht.keystore 签名算法: rsassa\_pkcs1v15 有效期自: 2022-12-26 15:43:43+00:00 有效期至: 2050-05-13 15:43:43+00:00 发行人: C=CN, ST=辽宁省, L=沈阳, O=辽宁圣亨太生物科技有限公司, OU=辽宁圣亨太生物科技有限公司, CN=sht.keystore 序列号: 0xa9a61b 哈希算法: sha256 md5值: d173fe936b41f94a1c88c7964400a50f sha1值: e35fb9ef3a711bf106742bc1767d53694677a4d4 sha256值: 116ce4a580be646868e851cc5921fbc113e46fe3f4fca222cc1112066f6676fd sha512值: 9782d667434c8f409f4a308deac393ef08412fcac60dd970d9bddf9bfd1fcd507c4b190e0269230f8f2bbb947feecb064bafd33e1198452a5a6de8227568c028 公钥算法: rsa 密钥长度: 1024 指纹: e40e4b9063a7fc115d365b0fe3db4b3d67a972a3f7c6ed39c493887f6eab5b7a**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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.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\_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\_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 |
| 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 |

## **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。**