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

**上交所（ 5.3.5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 | 上交所 |
| 版本 | 5.3.5 |
| 包名 | com.sse.android.ssegwapp |
| 域名线索 | 19条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2025年10月2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 | com.sse.android.ssegwapp\_5.3.5.apk |
| 文件大小 | 50.71MB |
| MD5值 | f1238f6b75ecb7c130beaf3dfcc6764e |
| SHA1值 | 4fec98e9364dee0455b95bba3eefa19398daa3cc |
| SHA256值 | 9b09ea4911f1c922b600ebe790fe7bc8e16fbe6985edc0abe59369e21f1c59d1 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 上交所 |
| 包名 | com.sse.android.ssegwapp |
| 主活动Activity | com.hundsun.application.base.CommonSplashActivity |
| 安卓版本名称 | 5.3.5 |
| 安卓版本 | 6416 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| lame.sf.net | IP: 104.18.21.237 所属国家: United States of America 地区: California 城市: San Francisco  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.dbankcloud.asia | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.zetetic.net | IP: 99.84.133.82 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| grs.dbankcloud.cn | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://www.zetetic.net/sqlcipher/  | 摸瓜V1引擎  |
| https://www.zetetic.net/sqlcipher/license/  | 摸瓜V1引擎  |
| https://github.com/sqlcipher/android-database-sqlcipher  | 摸瓜V1引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| http://www.openssl.org/support/faq.html  | lib/arm64-v8a/libgmssl.so  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libj2v8.so  |
| http://lame.sf.net  | lib/arm64-v8a/libmp3lame.so  |

### **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: O=www.trs.com 签名算法: rsassa\_pkcs1v15 有效期自: 2015-08-31 03:56:45+00:00 有效期至: 2040-08-24 03:56:45+00:00 发行人: O=www.trs.com 序列号: 0x55e3d07d 哈希算法: sha1 md5值: e448c44d928ffdacf1435f3c581f7344 sha1值: 5ea2b0a109916f3b3010936e6e6c6886a642676b sha256值: 30a24cceaa9d33610106ac6f1dda7403189c086f9f6148a14686f3e9d2cad971 sha512值: 7ab6c5a285b25280c6ba1324ca53a8f23eda9e58b8f4972ae1c65bb07bd4d4138fcce057533bc0bf1b377d1c49de2511a661f04db052e8790bd0df0c33c95957 公钥算法: rsa 密钥长度: 1024 指纹: 31d67c568ca2e0175c17f40e0fddd6b0d2264fe9d142d5aff1bd29370b92df6a**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "jsapi\_user" : "com.hundsun.JSAPI.UserJSAPI"  |
| "library\_android\_database\_sqlcipher\_author" : "Zetetic, LLC"  |
| "library\_android\_database\_sqlcipher\_authorWebsite" : "https://www.zetetic.net/sqlcipher/"  |

## **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 |
| --- | --- | --- | --- |
| com.sse.android.ssegwapp.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sse.android.ssegwapp.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| 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.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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| com.sse.android.ssegwapp.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.sse.android.ssegwapp.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.hundsun.application.base.CommonSplashActivity | **Schemes**: growing.58fa9709bbb93878://, um.://,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1104921363://,  |

**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。**