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

**SmBoke（ 1.0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 | SmBoke |
| 版本 | 1.0 |
| 包名 | ffcecedc.fhdhdbed.dfaeihbe |
| 域名线索 | 19条 |
| URL线索 | 33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 | SmBoke.apk |
| 文件大小 | 16.92MB |
| MD5值 | 80fedca4b87d9ef2e33272178c6404f9 |
| SHA1值 | b09275c42fe64154e9a4e3d35d3cf94e10bd3415 |
| SHA256值 | 4f42c123c2a7a0a08ed6b7b8c516eda4d4883f38a3215a0c0701f89f2e52b0d8 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | SmBoke |
| 包名 | ffcecedc.fhdhdbed.dfaeihbe |
| 主活动Activity | ffcecedc.fhdhdbed.dfaeihbe.MainActivity |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| dualstack-arestapi.amap.com | IP: 39.98.22.142 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.baidu.com | IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding  |
| wb.amap.com | IP: 59.82.31.104 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| cgicol.amap.com | IP: 123.125.216.213 所属国家: China 地区: Beijing 城市: Beijing  |
| mpsapi.amap.com | IP: 59.82.113.71 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| restsdk.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dualstack.apilocate.amap.com | IP: 106.11.40.50 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m5.amap.com | IP: 106.11.43.74 所属国家: China 地区: Beijing 城市: Beijing  |
| adiu.amap.com | IP: 203.119.204.194 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.smboke.cyou | IP: 154.23.188.137 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| lbs.amap.com | IP: 59.82.121.95 所属国家: China 地区: Beijing 城市: Beijing  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mst01.is.autonavi.com | IP: 59.82.132.243 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apiinit.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003nsl/dc.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/amap/api/col/p0003nsl/db.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003nsl/db.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003nsl/co.java  |
| http://restsdk.amap.com/v3/place/text?  | com/amap/api/col/p0003nsl/a.java  |
| http://restsdk.amap.com/v3/place/around?  | com/amap/api/col/p0003nsl/a.java  |
| http://restsdk.amap.com/v3/config/district?  | com/amap/api/col/p0003nsl/a.java  |
| http://restsdk.amap.com/v3/batch?key=  | com/amap/api/col/p0003nsl/fn.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003nsl/hd.java  |
| http://restsdk.amap.com/v3  | com/amap/api/col/p0003nsl/is.java  |
| https://restsdk.amap.com/v3  | com/amap/api/col/p0003nsl/is.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003nsl/is.java  |
| https://restsdk.amap.com/v4  | com/amap/api/col/p0003nsl/is.java  |
| http://yuntuapi.amap.com  | com/amap/api/col/p0003nsl/is.java  |
| https://yuntuapi.amap.com  | com/amap/api/col/p0003nsl/is.java  |
| http://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/p0003nsl/is.java  |
| https://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/p0003nsl/is.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/p0003nsl/is.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/p0003nsl/is.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/col/p0003nsl/ld.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003nsl/lm.java  |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003nsl/kq.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003nsl/kq.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/p0003nsl/kq.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003nsl/kq.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003nsl/mm.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003nsl/mm.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/p0003nsl/ni.java  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/amap/api/col/p0003nsl/kw.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/amap/api/col/p0003nsl/pd.java  |
| http://apilocate.amap.com/mobile/binary  | com/amap/api/col/p0003nsl/rc.java  |
| http://dualstack.apilocate.amap.com/mobile/binary  | com/amap/api/col/p0003nsl/rc.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/p0003nsl/lc.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/p0003nsl/lc.java  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\  | com/amap/api/col/p0003nsl/k.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://restsdk.amap.com/v4/stats/alitts  | com/amap/api/navi/core/network/h.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/autonavi/amap/mapcore/Inner\_3dMap\_location.java  |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo  | com/autonavi/aps/amapapi/trans/c.java  |
| http://restsdk.amap.com/v3/geocode/regeo  | com/autonavi/aps/amapapi/trans/c.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/trans/a.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/g.java  |
| http://restsdk.amap.com/rest/lbs/dem/dataservice?z=%d&x=%d&y=%d&type=2  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh\_cn&size=1&scale=1&style=6  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://m5.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/PermissionUtils.java  |
| http://www.baidu.com/  | ffcecedc/fhdhdbed/dfaeihbe/WebActivity2.java  |
| https://www.smboke.cyou/  | ffcecedc/fhdhdbed/dfaeihbe/app/Constant.java  |
| http://www.baidu.com/  | ffcecedc/fhdhdbed/dfaeihbe/app/Constant.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |

### **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=eecedfbj, L=dicieegi, O=dagebech, OU=dafjddeg, CN=hbeddehf 签名算法: rsassa\_pkcs1v15 有效期自: 2024-06-07 18:18:34+00:00 有效期至: 2124-05-14 18:18:34+00:00 发行人: C=cn, ST=eecedfbj, L=dicieegi, O=dagebech, OU=dafjddeg, CN=hbeddehf 序列号: 0x2839a7d5 哈希算法: sha256 md5值: ca6efec11282239db37915bdb2838ebd sha1值: 37eb2a2f5cf4c8e48fba9d38efccdd32049c4767 sha256值: 6742fa3833597c0c0b25c9a4f73a5a44f6ba1b789f434d9528711c79edf78289 sha512值: 8276688526ba4663c714b4ac7f1484da94d715afc8e766cb8d43026e5fe20b7c962a4d71a5c70f5acb13bd6e661d9de2b58d2f4eb878d5c6df3e8181014a3393 公钥算法: rsa 密钥长度: 1024 指纹: 601240422c355cdf68bfb4ff5759680848610c6dde1841f8618c2087cf7ae78c**

## **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.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\_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\_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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| 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\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| 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\_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.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.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.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.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.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.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.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。 |
| 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 |

## **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。**