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

**KTBB Connect（ 1.06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 | KTBB Connect |
| 版本 | 1.06 |
| 包名 | com.ble.beaconconfig |
| 域名线索 | 11条 |
| URL线索 | 10条 |
| APP图标 |  |
| 分析日期 | 2025年5月5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 | KTBB Connect V1.06(3).apk |
| 文件大小 | 9.22MB |
| MD5值 | b90df3a67ef05f70cf612157de877150 |
| SHA1值 | c669b844c7ceb9cc4180da2d6de1b859a6ca79fd |
| SHA256值 | 777415ef0f92eb375956eca03c0894cd758bf9e8d55cf3d24559de953aa5b9a3 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | KTBB Connect |
| 包名 | com.ble.beaconconfig |
| 主活动Activity | com.ble.activity.MainActivity |
| 安卓版本名称 | 1.06 |
| 安卓版本 | 6 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 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.  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| grs.dbankcloud.cn | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics.dt.dbankcloud.ru | IP: 159.138.204.140 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  |
| grs.dbankcloud.asia | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://)([\\s\\S]+)  | com/huawei/hms/scankit/p/Ab.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/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| 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  |
| https://metrics1.data.hicloud.com:6447  | 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://metrics.dt.dbankcloud.ru  | 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: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=50, ST=50, L=shenzhen, O=guangdong, OU=20, CN=zeng 签名算法: rsassa\_pkcs1v15 有效期自: 2022-08-02 01:46:23+00:00 有效期至: 2047-07-27 01:46:23+00:00 发行人: C=50, ST=50, L=shenzhen, O=guangdong, OU=20, CN=zeng 序列号: 0x2e33f425 哈希算法: sha256 md5值: 50ab688a39c8c6e090c7c490e4fb4a4f sha1值: f4b81810d58ea772fefd9c15ec4f8efc466875f5 sha256值: 5703a06cc9f7951b2be89c16274b28e6d81ff72ba50d17219fd01b85db88c25f sha512值: c5dd30cedc2bf15e9e46c270a9a1e782ad3a1c5edac3708646a2808f4c427cd50081dd70423c7669704c411eee4572920b6c17db1fb135168a98c537fbb175d0 公钥算法: rsa 密钥长度: 2048 指纹: eb7840ec47d9cd0899b83b7d3b8f5b50e4d4f11e04f584b03d0bdd3dd362af84**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "check\_password" : "Enter Password"  |
| "enter\_password" : "Enter Password"  |
| "tip\_password" : "Please enter a password of at least 4 characters"  |
| "check\_password" : "密码验证"  |
| "enter\_password" : "输入密码"  |
| "tip\_password" : "请输入不小于4位密码"  |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **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。**