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

**数字宝盒（ 1.0.1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 | 数字宝盒 |
| 版本 | 1.0.1 |
| 包名 | com.digital.box.android |
| 域名线索 | 1条 |
| URL线索 | 1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 | shuzibaohe-1.0.1.apk |
| 文件大小 | 102.91MB |
| MD5值 | cbe38e65f092c6131825fd5b9bddf3b5 |
| SHA1值 | b7efc389ce6ecbc5c3d7f284e16c8a56ff5d181b |
| SHA256值 | 96ef2201bfa0870c944c7b48ece3d77ed1b83c87d496368c2b74f5e6b8ce536e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 数字宝盒 |
| 包名 | com.digital.box.android |
| 主活动Activity | com.digital.box.android.ui.activity.SplashActivity |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 2 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| render.alipay.com | IP: 221.211.234.79 所属国家: China 地区: Heilongjiang 城市: Jiamusi  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html  | 摸瓜V1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: CN=WeiJiaQi, OU=IT Department, O=Beijing, L=Beijing, ST=Beijing, C=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2025-02-24 09:30:06+00:00 有效期至: 2050-02-18 09:30:06+00:00 发行人: CN=WeiJiaQi, OU=IT Department, O=Beijing, L=Beijing, ST=Beijing, C=CN 序列号: 0x1 哈希算法: sha256 md5值: f2ef5d7d942871bf8bed4db8c3db0d89 sha1值: 192ef46a66db184a6435a733befa0d7c548c0cad sha256值: ce18a1dd5295992a023f316019174c879e88c39c437b29520cbe5da4a64363b6 sha512值: e6ca53abdedc856c8242ac029828bbfb475543b23c846467df80a1f7e0065dccc23218a056e5cce0e23c2af0fe48f6a66cf40af19ca3a8115206fdd27b565716 公钥算法: rsa 密钥长度: 2048 指纹: 745b753b1bb6ff3c8c4213f737e7be1aed160ba4f5db5a429235e05db410255e**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "login\_pwd" : "登录密码"  |
| "mq\_auth\_code" : "验证码"  |
| "pay\_password" : "设置支付密码"  |
| "payment\_password" : "支付密码"  |
| "please\_again\_password" : "请再次输入密码"  |
| "please\_again\_set\_pay\_password" : "请再次设置支付密码"  |
| "please\_complete\_auth" : "请先完成实名认证"  |
| "please\_password" : "请输入六位纯数字密码"  |
| "please\_set\_pay\_password" : "请设置6位纯数字支付密码"  |
| "please\_write\_password" : "请输入密码"  |
| "please\_write\_pay\_password" : "请输入支付密码"  |
| "pwd\_login" : "密码登录"  |
| "set\_max\_pwd" : "请设置6–15位密码"  |
| "set\_payment\_password" : "设置支付密码"  |
| "set\_pwd" : "设置密码"  |
| "setting\_pwd" : "暂无支付密码，请设置支付密码"  |
| "verify\_payment\_password" : "验证支付密码"  |
| "mq\_auth\_code" : "Kode verifikaso"  |
| "mq\_auth\_code" : "Kod pengesahan"  |
| "mq\_auth\_code" : "驗證碼"  |
| "login\_pwd" : "登录密码"  |
| "pay\_password" : "设置支付密码"  |
| "payment\_password" : "支付密码"  |
| "please\_again\_password" : "请再次输入密码"  |
| "please\_again\_set\_pay\_password" : "请再次设置支付密码"  |
| "please\_complete\_auth" : "请先完成实名认证"  |
| "please\_password" : "请输入六位纯数字密码"  |
| "please\_set\_pay\_password" : "请设置6位纯数字支付密码"  |
| "please\_write\_password" : "请输入密码"  |
| "please\_write\_pay\_password" : "请输入支付密码"  |
| "pwd\_login" : "密码登录"  |
| "set\_max\_pwd" : "请设置6–15位密码"  |
| "set\_payment\_password" : "设置支付密码"  |
| "set\_pwd" : "设置密码"  |
| "setting\_pwd" : "暂无支付密码，请设置支付密码"  |
| "verify\_payment\_password" : "验证支付密码"  |
| "mq\_auth\_code" : "CAPTCHA"  |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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\_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.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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 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.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。 |
| 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.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 |
| com.digital.box.android.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| com.digital.box.android.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 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 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **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。**