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

**中国国际扶贫中心（ 2033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 | 中国国际扶贫中心 |
| 版本 | 2033 |
| 包名 | butie.com |
| 域名线索 | 4条 |
| URL线索 | 5条 |
| APP图标 |  |
| 分析日期 | 2025年7月6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 | 屠.apk |
| 文件大小 | 5.24MB |
| MD5值 | cce7e87c26a5d50a3b1dcf972f3bbf68 |
| SHA1值 | 95df036b5c8e73fd5f38065ede7f43d85977e83a |
| SHA256值 | 9c3e2d7e2f59edd061e4a4bf7ddc40e4fad49fd8d791d3dc611014c5991ced0d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 中国国际扶贫中心 |
| 包名 | butie.com |
| 主活动Activity | com.iapp.app.run.load |
| 安卓版本名称 | 2033 |
| 安卓版本 | 100001 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| schemas.android.com | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.w3.org/TR/SVG11/feature  | com/caverock/androidsvg/C0200SVGParser.java  |
| http://www.w3.org/2000/svg  | com/caverock/androidsvg/C0200SVGParser.java  |
| http://www.w3.org/1999/xlink  | com/caverock/androidsvg/C0200SVGParser.java  |
| http://xmlpull.org/v1/doc/features.html  | com/caverock/androidsvg/C0200SVGParser.java  |
| http://xml.org/sax/features/external-general-entities  | com/caverock/androidsvg/C0200SVGParser.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/caverock/androidsvg/C0200SVGParser.java  |
| http://xml.org/sax/properties/lexical-handler  | com/caverock/androidsvg/C0200SVGParser.java  |
| http://www.w3.org/2000/svg  | com/mus/utils/C0075.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/f.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| pat@pat.net  | bsh/Interpreter.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179878401  | bsh/ParserTokenManager.java  |
| 17179869184  | bsh/ParserTokenManager.java  |
| 17179869184  | com/caverock/androidsvg/C0114SVG.java  |
| 17179869184  | com/caverock/androidsvg/C0200SVGParser.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=cn, ST=bj, L=bj, O=ipuser, OU=ipuser, CN=ipuser 签名算法: rsassa\_pkcs1v15 有效期自: 2016-07-02 11:43:26+00:00 有效期至: 2098-08-21 11:43:26+00:00 发行人: C=cn, ST=bj, L=bj, O=ipuser, OU=ipuser, CN=ipuser 序列号: 0x3435f5c4 哈希算法: sha256 md5值: c118816b9a0f406ba5ba053c67638185 sha1值: ae773917cc7a7523b41e1eb95bed61cf0aa8e3b0 sha256值: ac0d0777ca24956f8d584c69a7fd5d2e4fb88e276d953aec9e29ceeb9aa78e32 sha512值: 4667da273fe54297d8c90136e189f721a4bf15ba360aac00f095756e2ed09e59edcf69e08cddd20c379bff78f3b4d59c0fcb3ad5ed3c93dc472c8a85a40a21f5**

## **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.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.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| 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.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\_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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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 |

## **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。**