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

**苍南外国语消费机（ 1.1.0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 | 苍南外国语消费机 |
| 版本 | 1.1.0 |
| 包名 | com.becypress.zyjk.cnwgy |
| 域名线索 | 11条 |
| URL线索 | 30条 |
| APP图标 |  |
| 分析日期 | 2025年8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 | JKD2mini\_cnwgy\_1.1.0(1).apk |
| 文件大小 | 9.44MB |
| MD5值 | d00d380b67dc1f0ee64ff101f1ae736f |
| SHA1值 | eecdce18c638d85a934487e0d95720ebc7bc43ca |
| SHA256值 | 1ae22e2b8c3b6050860236f897b5f1355cc53bd15cb183323a3126b80ea5ba02 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 苍南外国语消费机 |
| 包名 | com.becypress.zyjk.cnwgy |
| 主活动Activity | com.becypress.consumer.bcui.splash.SplashActivity |
| 安卓版本名称 | 1.1.0 |
| 安卓版本 | 10 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| logback.qos.ch | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| www.slf4j.org | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.rabbitmq.com | IP: 172.67.32.161 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.android.com | 没有服务器地理信息.  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| groups.google.com | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| projectlombok.org | IP: 104.21.32.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| issuetracker.google.com | IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| 192.168.0.211 | IP: 192.168.0.211 所属国家: - 地区: - 城市: -  |
| www.baidu.com | IP: 110.242.70.57 所属国家: China 地区: Hebei 城市: Baoding  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://issuetracker.google.com/issues/116541301  | android/databinding/ViewDataBinding.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/j.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/pattern/parser/f.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/joran/action/e.java  |
| http://schemas.android.com/apk/res/android  | com/afollestad/materialdialogs/prefs/PrefUtil.java  |
| http://192.168.0.211:8090/bc/gateway/emgt  | com/becypress/consumer/bcui/base/server/d.java  |
| https://www.rabbitmq.com/ssl.html  | com/rabbitmq/client/Fb.java  |
| https://www.rabbitmq.com/  | com/rabbitmq/client/impl/C.java  |
| http://192.168.0.211:8090  | defpackage/C0732wc.java  |
| http://192.168.0.211:8090/bc/gateway/om/  | defpackage/C0732wc.java  |
| http://xml.org/sax/features/validation  | defpackage/Ua.java  |
| http://xml.org/sax/features/namespaces  | defpackage/Ua.java  |
| http://logback.qos.ch/codes.html  | defpackage/Cb.java  |
| http://logback.qos.ch/codes.html  | defpackage/gp.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/AbstractC0341a.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/J.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/AbstractC0432q.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/A.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/AbstractC0425j.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://projectlombok.org/LICENSE  | lombok/core/Main.java  |
| https://projectlombok.org/not/calculated  | lombok/eclipse/EclipseAST.java  |
| https://projectlombok.org  | lombok/eclipse/agent/PatchFixesShadowLoaded.java  |
| https://projectlombok.org/  | lombok/eclipse/agent/PatchFixesShadowLoaded.java  |
| https://projectlombok.org/features/experimental/FieldNameConstants  | lombok/eclipse/handlers/HandleFieldNameConstants.java  |
| https://projectlombok.org/features/experimental/FieldNameConstants  | lombok/javac/handlers/HandleFieldNameConstants.java  |
| https://projectlombok.org  | lombok/installer/Installer.java  |
| http://groups.google.com/group/project-lombok  | lombok/installer/eclipse/EclipseProductLocation.java  |
| http://www.baidu.com  | me/goldze/mvvmhabit/http/b.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/f.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/d.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | lombok/javac/handlers/JavacHandlerUtil.java  |
| 17179869184  | lombok/javac/handlers/HandleDelegate.java  |
| 17179869184  | lombok/delombok/PrettyPrinter.java  |

## **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=zyjk 签名算法: rsassa\_pkcs1v15 有效期自: 2021-07-09 06:32:11+00:00 有效期至: 2121-06-15 06:32:11+00:00 发行人: CN=zyjk 序列号: 0x66b82315 哈希算法: sha256 md5值: f7be90169fd5ccecb50b464d8a530663 sha1值: ea9b069ae2d04298aa281ffe70e63a43b0cbbcae sha256值: 1204551214779cd724e6dfe90f70b5cdf5412aa3f6f2fabcecc11243cc4d2319 sha512值: 18c16ad8430e4d1ddb49eec1dd34c521cebf71c99758c5018b1ec4066a03a7557564306044bb8878f9501a3bd04daa08ca9faef6ef0aaa087f4103ea54e57f51 公钥算法: rsa 密钥长度: 2048 指纹: 5accfa221bbf8812fe31e464e44b048f8035b18460ecd2b33646088b40addfe3**

## **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.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.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.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\_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.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.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.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| 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\_PRIVILEGED\_PHONE\_STATE | 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。**