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

**出发（ 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 | 出发 |
| 版本 | 1.0 |
| 包名 | com.wzp.android.rpc |
| 域名线索 | 10条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年6月17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 | 出发.apk |
| 文件大小 | 5.46MB |
| MD5值 | 342b56476e2f17091c991cb5116c3853 |
| SHA1值 | 5ba8e9200999e7bb9fe37533881258d28d25b97e |
| SHA256值 | 6bd47061b535d936c4d511c760e20ce455ad220cef663f6352791d03d3617bac |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 出发 |
| 包名 | com.wzp.android.rpc |
| 主活动Activity | com.wzp.android.rpc.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 |
| --- | --- |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| 139.9.164.5 | IP: 139.9.164.5 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.eclipse.org | IP: 198.41.30.198 所属国家: Canada 地区: Ontario 城市: Brampton  |
| wzp-obs.obs.cn-east-2.myhuaweicloud.com | IP: 122.112.208.161 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| sekiro.virjar.com | IP: 182.92.142.39 所属国家: China 地区: Beijing 城市: Beijing  |
| netty.io | IP: 104.21.3.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://xml.apache.org/xslt  | cn/hutool/core/util/XmlUtil.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | cn/hutool/core/util/XmlUtil.java  |
| http://xml.org/sax/features/external-general-entities  | cn/hutool/core/util/XmlUtil.java  |
| http://xml.org/sax/features/external-parameter-entities  | cn/hutool/core/util/XmlUtil.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | cn/hutool/core/util/XmlUtil.java  |
| https://sekiro.virjar.com  | com/virjar/sekiro/business/api/util/Constants.java  |
| https://www.openssl.org/docs/manmaster/apps/verify.html  | com/virjar/sekiro/business/netty/handler/ssl/OpenSslCertificateException.java  |
| http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html  | com/virjar/sekiro/business/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java  |
| http://www.eclipse.org/jetty/documentation/current/npn-chapter.html  | com/virjar/sekiro/business/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java  |
| http://netty.io/wiki/sslcontextbuilder-and-private-key.html  | com/virjar/sekiro/business/netty/handler/ssl/PemReader.java  |
| http://netty.io/wiki/forked-tomcat-native.html  | com/virjar/sekiro/business/netty/handler/ssl/OpenSsl.java  |
| http://netty.io/wiki/reference-counted-objects.html  | com/virjar/sekiro/business/netty/util/ResourceLeakDetector.java  |
| https://wzp-obs.obs.cn-east-2.myhuaweicloud.com/serverurl.txt  | com/wzp/android/rpc/Main.java  |
| http://139.9.164.5:1234/ppmt/receiveEvent  | com/wzp/android/rpc/Main.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| auth-agent@openssh.com  | cn/hutool/extra/ssh/ChannelType.java  |

### **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=Android Debug, O=Android, C=US 签名算法: rsassa\_pkcs1v15 有效期自: 2022-06-30 17:24:50+00:00 有效期至: 2052-06-22 17:24:50+00:00 发行人: CN=Android Debug, O=Android, C=US 序列号: 0x1 哈希算法: sha1 md5值: a791f38d7878c1e3ad44421645bfbc62 sha1值: 8c09b3d31c2336686a3f7de7979ee4e7f56b7caa sha256值: 1b31f2da171bc3685389a345b8290b9b08377302de002abd16bbf839e8ac72f0 sha512值: 218fa80efd861c631ad9e10242e5f4f4eb6482ca63f8ba4cdb02c8ba3a3aa966e1aa845aeb77ded497869e0ace2e1a5b6e63e486aee7c02dc74b14e9136398c0 公钥算法: rsa 密钥长度: 2048 指纹: 4e4c867905e6278cfc01b4f8ad2eed608051818d77b886cbf5e05f80575d1fb3**

## **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**

## **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。**