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

**暑假工（ 3.0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 | 暑假工 |
| 版本 | 3.0 |
| 包名 | dl9wu.burz3.xmc24 |
| 域名线索 | 20条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2025年8月10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 | 安卓专用.apk |
| 文件大小 | 37.31MB |
| MD5值 | dfaadd75fa9857b8960daf2376cd54c1 |
| SHA1值 | 3d255a88f3b33719dd7bf83906b76adf80468e5d |
| SHA256值 | a022f07a000fa43109850d22a30194529efd6a47f3c5de788b388f3c2f6e5c46 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 暑假工 |
| 包名 | dl9wu.burz3.xmc24 |
| 主活动Activity | dl9wu.burz3.xmc24.ui.activity.login.AppLaunch1Activity |
| 安卓版本名称 | 3.0 |
| 安卓版本 | 3 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| nosup-hz1.127.net | IP: 116.196.140.67 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| check-ipv6.netease.im | 没有服务器地理信息.  |
| s3.amazonaws.com | IP: 54.231.172.96 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| ns.adobe.com | 没有服务器地理信息.  |
| abt-online.netease.im | IP: 220.197.34.90 所属国家: China 地区: Sichuan 城市: Leshan  |
| change-api.netease.im | IP: 220.197.34.84 所属国家: China 地区: Sichuan 城市: Leshan  |
| statistic-overseas.yunxinfw.com | IP: 8.219.207.113 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| s3-us-west-1.amazonaws.com | IP: 52.219.216.136 所属国家: United States of America 地区: California 城市: San Jose  |
| schemas.android.com | 没有服务器地理信息.  |
| wannos.127.net | IP: 125.38.11.59 所属国家: China 地区: Tianjin 城市: Tianjin  |
| check-ipv4.netease.im | IP: 220.197.34.90 所属国家: China 地区: Sichuan 城市: Leshan  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| acs.amazonaws.com | 没有服务器地理信息.  |
| 103.216.155.92 | IP: 103.216.155.92 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| 10.0.2.2 | IP: 10.0.2.2 所属国家: - 地区: - 城市: -  |
| yiyong-qa.netease.im | IP: 111.124.202.71 所属国家: China 地区: Guizhou 城市: Zunyi  |
| www.ngs.ac.uk | IP: 130.246.140.235 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Appleton  |
| lbs.netease.im | IP: 220.197.34.89 所属国家: China 地区: Sichuan 城市: Leshan  |
| statistic.live.126.net | IP: 220.197.34.75 所属国家: China 地区: Sichuan 城市: Leshan  |
| yiyong.netease.im | IP: 220.197.34.92 所属国家: China 地区: Sichuan 城市: Leshan  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | C/b.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | Y/g.java  |
| https://statistic.live.126.net  | com/netease/nimlib/c.java  |
| https://statistic-overseas.yunxinfw.com  | com/netease/nimlib/c.java  |
| https://s3-us-west-1.amazonaws.com  | com/netease/nimlib/amazonaws/services/s3/AmazonS3Client.java  |
| http://10.0.2.2:20005  | com/netease/nimlib/amazonaws/services/s3/internal/Constants.java  |
| http://s3.amazonaws.com/doc/2006-03-01/  | com/netease/nimlib/amazonaws/services/s3/internal/Constants.java  |
| http://www.ngs.ac.uk/tools/jcepolicyfiles  | com/netease/nimlib/amazonaws/services/s3/internal/crypto/EncryptionUtils.java  |
| http://acs.amazonaws.com/groups/global/AllUsers  | com/netease/nimlib/amazonaws/services/s3/model/GroupGrantee.java  |
| http://acs.amazonaws.com/groups/global/AuthenticatedUsers  | com/netease/nimlib/amazonaws/services/s3/model/GroupGrantee.java  |
| http://acs.amazonaws.com/groups/s3/LogDelivery  | com/netease/nimlib/amazonaws/services/s3/model/GroupGrantee.java  |
| https://abt-online.netease.im/v1/api/abt/client/getExperimentInfo  | com/netease/nimlib/abtest/c.java  |
| https://statistic.live.126.net  | com/netease/nimlib/net/a/d/a.java  |
| https://statistic-overseas.yunxinfw.com  | com/netease/nimlib/net/a/d/a.java  |
| https://wannos.127.net/lbs  | com/netease/nimlib/v2/u/b/a.java  |
| https://nosup-hz1.127.net  | com/netease/nimlib/v2/u/b/a.java  |
| https://lbs.netease.im/lbs/conf.jsp  | com/netease/nimlib/e/e.java  |
| https://check-ipv4.netease.im/  | com/netease/nimlib/e/e.java  |
| https://check-ipv6.netease.im/  | com/netease/nimlib/e/e.java  |
| https://wannos.127.net/lbs  | com/netease/nimlib/e/g.java  |
| https://nosup-hz1.127.net  | com/netease/nimlib/e/g.java  |
| http://103.216.155.92:9421/api/add\_friend?accid=  | com/netease/yunxin/kit/contactkit/ui/userinfo/BaseUserInfoActivity.java  |
| https://statistic.live.126.net/statics/report/xkit/action  | com/netease/yunxin/kit/corekit/report/ReportConstantsKt.java  |
| https://statistic.live.126.net/statics/report/common/form  | com/netease/yunxin/kit/corekit/report/ReportConstantsKt.java  |
| https://yiyong.netease.im/report\_conf  | com/netease/yunxin/kit/corekit/report/ReportStrategy.java  |
| https://yiyong-qa.netease.im/report\_conf  | com/netease/yunxin/kit/corekit/report/ReportStrategy.java  |
| https://change-api.netease.im/change-api/sdk/task/action/batch  | com/netease/yunxin/artemis/ArtemisTask/YXArtemisPullTask.java  |
| http://103.216.155.92:9421/  | dl9wu/burz3/xmc24/bean/NetUrl.java  |

### **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: True 找到 1 个唯一证书 主题: C=c761d505, ST=c761d505, L=c761d505, O=c761d505, OU=c761d505, CN=c761d505 签名算法: rsassa\_pkcs1v15 有效期自: 2025-07-16 08:58:48+00:00 有效期至: 2125-06-22 08:58:48+00:00 发行人: C=c761d505, ST=c761d505, L=c761d505, O=c761d505, OU=c761d505, CN=c761d505 序列号: 0x3fa3352e 哈希算法: sha256 md5值: 1b24dc7e8f4e8ded8672defd68178b9b sha1值: fb15467e1409360fb61b718f6138e56307438851 sha256值: 6f04a0fda536a7facf499c951567880bce5a7b8c0e21a4f03b077e0917c0b0d5 sha512值: fb0f54da82b44ad495cbf1e1ed329362bf718d2083fd352df0fcccd68e2d4253c46c554786fcbc62ecb5a7194a5b6cff42bbe4b98b82d6ca8c1e6fe447896935 公钥算法: rsa 密钥长度: 1024 指纹: 800d68d9cb1286aae5e3a7128a81e045fd47d0304da3091109f854012af764ee**

## **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.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.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.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.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.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.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.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\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.READ\_MEDIA\_IMAGES | 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.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| dl9wu.burz3.xmc24.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**