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

**NLService（ 44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 | NLService |
| 版本 | 44 |
| 包名 | com.newlink.service |
| 域名线索 | 3条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2025年6月9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 | NLService\_V44\_Lenovo.apk |
| 文件大小 | 2.42MB |
| MD5值 | 0b7e0c9b05965ed710a1ea09d9c8baeb |
| SHA1值 | eba1bab4191b280648df8bc1280097f6802b107e |
| SHA256值 | 356154c42ccddf95b782e83293380531195c00cca18c7e21ca23eba787894b56 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | NLService |
| 包名 | com.newlink.service |
| 主活动Activity |  |
| 安卓版本名称 | 44 |
| 安卓版本 | 44 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| whois.pconline.com.cn | IP: 221.15.69.47  所属国家: China  地区: Henan  城市: Luoyang |
| www.baidu.com | IP: 110.242.70.57  所属国家: China  地区: Hebei  城市: Baoding |
| www.newlinksz.com | IP: 47.91.240.48  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://whois.pconline.com.cn/ip.jsp | com/newlink/service/MyServices.java |
| http://www.newlinksz.com/product/update | com/newlink/service/MyServices.java |
| http://www.newlinksz.com/product/verification | com/newlink/service/MyServices.java |
| http://www.newlinksz.com/product/usetime | com/newlink/service/MyServices.java |
| https://www.baidu.com | com/newlink/service/util/Util.java |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14961550929 | 摸瓜V2引擎 |
| 14961550927 | 摸瓜V2引擎 |
| 14961550928 | 摸瓜V2引擎 |
| 14961550926 | 摸瓜V2引擎 |
| 14961550925 | 摸瓜V2引擎 |
| 14961550900 | 摸瓜V2引擎 |
| 14961550901 | 摸瓜V2引擎 |
| 14961550902 | 摸瓜V2引擎 |
| 14961550903 | 摸瓜V2引擎 |
| 14961550904 | 摸瓜V2引擎 |
| 14961550905 | 摸瓜V2引擎 |
| 14961550906 | 摸瓜V2引擎 |
| 14961550907 | 摸瓜V2引擎 |
| 14961550908 | 摸瓜V2引擎 |
| 14961550909 | 摸瓜V2引擎 |
| 14961550910 | 摸瓜V2引擎 |
| 14961550911 | 摸瓜V2引擎 |
| 14961550912 | 摸瓜V2引擎 |
| 14961550913 | 摸瓜V2引擎 |
| 14961550914 | 摸瓜V2引擎 |
| 14961550915 | 摸瓜V2引擎 |
| 14961550916 | 摸瓜V2引擎 |
| 14961550917 | 摸瓜V2引擎 |
| 14961550918 | 摸瓜V2引擎 |
| 14961550919 | 摸瓜V2引擎 |
| 14961550920 | 摸瓜V2引擎 |
| 14961550921 | 摸瓜V2引擎 |
| 14961550922 | 摸瓜V2引擎 |
| 14961550923 | 摸瓜V2引擎 |
| 14961550933 | 摸瓜V2引擎 |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, ST=BeiJing, L=HaiDian View, O=Lenovo, OU=STV, CN=lran, E=fansn1@lenovo.com 签名算法: rsassa\_pkcs1v15 有效期自: 2018-07-03 06:52:35+00:00 有效期至: 2045-11-18 06:52:35+00:00 发行人: C=CN, ST=BeiJing, L=HaiDian View, O=Lenovo, OU=STV, CN=lran, E=fansn1@lenovo.com 序列号: 0xd279887ae1681f68 哈希算法: sha1 md5值: 7b4a9928c0b24aa8b5ed217f53769586 sha1值: 510c84d32f8be3f32d54ea004f899c9da28c1878 sha256值: ab3ffe34c012b615d5ef7643d45505cd4926b708bb0aaabe6ff4108443b26b77 sha512值: 2056bced174248326ff0b49f9de238195896157302fa935d394f12cd3263e5451b2f5255f0e6d10515f8c5ebefe5f8c28972e398bdb04ce36124370356f4ccf2 公钥算法: rsa 密钥长度: 2048 指纹: e4507605b9f047a516a5dd5903351709d99cb2bd31a255baa254ac05de4b20e6**

## **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.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\_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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| 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.RECOVERY | 未知 | Unknown permission | Unknown permission from android reference |
| com.mstar.android.permissionn.ACCESS\_TV\_DATA | 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.WRITE\_SECURE\_SETTINGS | 系统需要 | 修改安全系统设置 | 允许应用程序修改系统固定好设置数据。不供普通应用程序使用 |
| android.permission.SHUTDOWN | 合法 | 部分关闭 | 将活动管理器置于关闭状态。不执行完全关闭 |
| android.permission.INTERACT\_ACROSS\_USERS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.CONNECTIVITY\_INTERNAL | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.GET\_PACKAGE\_SIZE | 正常 | 测量应用程序存储空间 | 允许应用程序找出任何包使用的空间 |
| 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.MASTER\_CLEAR | 系统需要 | 将系统重置为出厂默认值 | 允许应用程序将系统完全重置为其出厂设置,擦除所有数据,配置和已安装的应用程序 |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| android.permission.SET\_WALLPAPER\_HINTS | 正常 | 设置壁纸大小提示 | 允许应用程序设置系统壁纸大小提示 |
| 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 |

## **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。**