

## 全球网络流量近半数来自机器人

- 自动化和恶意流量连续第五年上升
- 恶意机器人占有所有网络流量的 32%
- 44%的帐户接管攻击针对 API 端点



©Thales

当地时间 4 月 16 日，全球领先的网络安全领导者泰雷兹（Thales）宣布发布《[2024 年 Imperva 恶意机器人报告](#)》（[2024 Imperva Bad Bot Report](#)），对全球互联网上的自动化机器人流量进行了全面分析。2023 年，近一半（49.6%）的网络流量来自机器人，比上一年增长了 2%，这是 Imperva 自 2013 年开始监测自动化流量以来报告的最高水平。

与恶意机器人相关的网络流量占比连续第五年呈现增长趋势，从 2022 年的 30.2% 增长至 2023 年的 32%，而来自人类用户的流量则持续下降至 50.4%。每年，自动化流量对网站、API 和应用程序的攻击给企业造成数十亿美元的损失。

泰雷兹旗下的 Imperva 应用安全总经理 Nanhi Singh 表示：“机器人是每个行业面临最普遍且增长最快的威胁之一。从简单的网络爬取到恶意帐户接管、垃圾邮件和拒绝服务，机器人通过降低在线服务质量，并要求在基础设施和客户支持方面进行更多投资，从而对企业的利润造成负面影响。由于攻击者将注意力集中在可能导致帐户被盗用或数据泄漏的 API 相关滥用行为上，企业必须积极应对恶意机器人的威胁。”

《2024年 Imperva 恶意机器人报告》中提及的主要趋势包括：

- **全球平均恶意机器人流量达到 32%：**爱尔兰（71%）、德国（67.5%）和墨西哥（42.8%）是 2023 年恶意机器人流量最高的国家。与 2022 年（32.1%）相比，美国的恶意机器人流量比例也略高，达到 35.4%。
- **生成式 AI 的使用越来越多，这与简单机器人的兴起有关：**生成式 AI 和大语言模型（LLM）的快速崛起，导致简单机器人的比例从 2022 年的 33.4% 增加至 2023 年的 39.6%。该技术使用网络爬虫机器人和自动化爬虫来训练模型，同时让非技术用户能够自行编写自动化脚本。
- **帐户接管是持续存在的业务风险：**与上一年同期相比，2023 年的帐户接管（ATO）攻击增加了 10%。值得注意的是，44% 的 ATO 攻击均针对 API 端点，而 2022 年这一比例为 35%。在互联网上的所有登录尝试中，有 11% 与帐户接管相关。2023 年，遭受 ATO 攻击最多的行业分别是金融服务业（36.8%）、旅游业（11.5%）和商业服务（8%）。
- **API 是攻击的流行途径：**2023 年，自动化威胁导致的 API 攻击占比高达 30%。其中，17% 是恶意机器人利用业务逻辑漏洞，即 API 设计和实施中的缺陷，使攻击者能够操纵合法功能并访问敏感数据或用户的帐户。网络罪犯使用自动化机器人查找并利用 API，把它当作访问敏感数据的直接途径，使其成为业务逻辑漏洞的主要目标。
- **所有行业都面临机器人问题：**游戏产业（57.2%）的恶意机器人流量连续第二年占比最大。与此同时，零售业（24.4%）、旅游业（20.7%）和金融服务业（15.7%）遭受的机器人攻击数量最高。在法律与政府（75.8%）、娱乐（70.8%）和金融服务业（67.1%）网站上，高级恶意机器人（即那些极力模仿人类行为并逃避防御的机器人）占比最高。
- **来自住宅网络服务提供商的恶意机器人流量增至 25.8%：**早期的恶意机器人规避技术依赖于伪装成合法人类用户常用的用户代理（浏览器）。在过去一年，伪装成移动用户代理的恶意机器人占有所有恶意机器人流量的 44.8%，高于五年前的 28.1%。进阶行动者将移动用户代理与住宅或移动 ISP 的使用相结合。住宅代理允许机器人运营商通过伪装成流量来源是由 ISP 分配的合法住宅 IP 地址来逃避检测。

Singh 补充道：“自动化机器人将很快超越来自人类的网络流量比例，从而改变企业构建和保护其网站、应用程序的方式。随着更多人工智能工具的推出，机器人将变得无处不在。企业是时候投资机器人管理和 API 安全工具，以管理来自恶意自动化流量的威胁。”

#### 其他信息：

- [点击下载](#)《2024 年 Imperva 恶意机器人报告》以获取更多见解。
- 查看 Imperva [高级机器人保护](#)、[API 安全](#)与[客户端保护](#)，了解如何保护网站、移动应用程序和 API 免受自动化攻击和欺诈，避免对关键业务流量造成影响。
- 阅读 [Imperva 博客](#)，了解最新的产品和解决方案新闻，以及来自 Imperva 威胁研究 (Imperva Threat Research) 的相关情报。

#### 关于泰雷兹

作为全球先进科技的领导者之一，泰雷兹（泛欧证券交易所代码：HO）专注于航空、航天、数字身份与安全等领域，为构建一个更安全、更环保、更包容的世界开发产品及解决方案。

集团每年投入约 40 亿欧元研发资金用于关键科技，如量子技术、边缘计算、6G 和网络安全等。

泰雷兹全球 81000\*名员工遍布 68 个国家和地区，2023 年集团销售收入 184 亿欧元。

\*数据不包括正在剥离的轨道交通业务。

#### 新闻联系人

泰雷兹媒体关系部  
安全与网络安全  
Marion Bonnet  
+33 (0)6 60 38 48 92  
[marion.bonnet@thalesgroup.com](mailto:marion.bonnet@thalesgroup.com)

#### 请访问

[泰雷兹集团](#)

[云保护和软件授权解决方案 | 泰雷兹集团](#)

[网络安全解决方案 | 泰雷兹集团](#)

微信公众号：泰雷兹创新说

