# AI-driven bad bots now account for over half of global web traffic, reveals Thales report



Thales, a leading global provider of technology and security solutions, has unveiled the 2025 Imperva Bad Bot Report, its 12th annual comprehensive study analysing automated bot traffic on the internet. The latest findings highlight the transformative impact of generative artificial intelligence (AI) on the development and deployment of bots, signalling a new era in cyber threat dynamics driven by AI-enhanced actors.

The report reveals a historic milestone in internet traffic patterns: automated bot traffic has surpassed human-generated web traffic for the first time in over a decade, constituting 51% of all web activity during 2024. The proliferation of AI technologies, especially large language models (LLMs), has made bot creation and scaling more accessible, enabling virtually anyone with malicious intent to launch attacks at an unprecedented scale.

Significantly, bad bots—malicious automated programmes—now account for 37% of global internet traffic, up from 32% in 2023, marking six consecutive years of growth in such activity. These bots are increasingly powered by AI tools, which facilitate not only volume but also the refinement of attack strategies through real-time analysis of failed attempts. This evolving ecosystem is fuelled by a growing Bots-As-A-Service (BaaS) marketplace that commercialises bot capabilities to a broader range of threat actors.

Industries like travel and retail are among the hardest hit, with bad bots making up 41% and 59% of their online traffic respectively. The travel sector, in particular, has become the most targeted industry, suffering 27% of all bot attacks in 2024—a rise from 21% the previous year. The nature of these attacks is shifting: advanced bot attacks in travel have declined from 61% to 41%, while simpler bot attacks have surged to 52%, up from 34% in 2023. This indicates that AI-driven automation tools are lowering entry barriers, enabling less technically sophisticated attackers to conduct high volumes of basic bot intrusions, overwhelming travel websites with frequency and scale.

The use of advanced AI tools—such as ChatGPT, ByteSpider Bot, ClaudeBot, Google Gemini, Perplexity AI, and Cohere AI—is reshaping both legitimate user interactions and the methodologies for orchestrating cyberattacks. Within this spectrum, ByteSpider Bot accounts for 54% of AI-powered attacks alone, followed by AppleBot (26%), ClaudeBot (13%), and ChatGPT User Bot (6%).

Tim Chang, General Manager of Application Security at Thales, emphasised the gravity of this trend: “The surge in AI-driven bot creation has serious implications for businesses worldwide. As automated traffic accounts for more than half of all web activity, organisations face heightened risks from bad bots, which are becoming more prolific every day.” He also noted that the tactics once considered advanced evasion methods have now become the standard for many malicious bots, challenging detection and prevention efforts.

A notable development identified in the report is the sharp increase in API-targeted attacks. APIs—application programming interfaces—are critical for modern digital operations, powering payment systems, data exchanges, and AI analytics. The report reveals that 44% of advanced bot traffic is directed at exploiting APIs. Rather than merely causing service disruptions, attackers are targeting the underlying business logic of APIs to conduct automated payment fraud, account hijacking, and data exfiltration. This presents particular risks for sectors heavily reliant on APIs, such as financial services, healthcare, and e-commerce.

Chang highlighted: “The business logic inherent to APIs is powerful, but it also creates unique vulnerabilities that malicious actors are eager to exploit. As organisations embrace cloud-based services and microservices architectures, it’s vital to understand that the very features that make APIs essential can also leave them susceptible to risk of fraud and data breaches.”

Within these targeted sectors, the financial services industry was identified as the most impacted by account takeover (ATO) attacks, accounting for 22% of all such incidents, followed by telecommunications and internet service providers at 18%, and computing and IT sectors at 17%. The financial sector’s significant exposure is linked to the valuable personal identifiable information (PII) held in bank accounts, credit cards, and fintech platforms, making compromised data highly lucrative on illicit markets. The widespread use of APIs in finance further enlarges the attack surface, exposing vulnerabilities in authentication and authorisation that attackers exploit.

The 2025 Imperva Bad Bot Report is grounded in data drawn from Thales’ extensive global telemetry gathered throughout 2024—covering 13 trillion blocked bot requests across a wide array of domains and industries. These insights provide a detailed view of emerging bot threat trends and are intended to assist organisations in understanding and mitigating the risks posed by increasingly sophisticated automated threats.

The report underscores the ongoing evolution of bot tactics and the expanding role of AI in cybercrime, as well as the pressing need for adaptive, sophisticated cybersecurity strategies to address the challenges posed by the growing bot ecosystem.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://cpl.thalesgroup.com/about-us/newsroom/2025-imperva-bad-bot-report-ai-internet-traffic> - This Thales news release confirms the 2025 Imperva Bad Bot Report findings that AI-driven bots now generate over half (51%) of global internet traffic in 2024, marking a historic milestone surpassing human web traffic.
* <https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/> - Imperva's official resource library contains the 2025 Bad Bot Report which details that bad bots make up 37% of all internet traffic, highlighting the six consecutive years of growth in malicious bot activity.
* <https://www.imperva.com/blog/2025-imperva-bad-bot-report-how-ai-is-supercharging-the-bot-threat/> - This blog explains how generative AI and large language models are enabling a surge in both the volume and sophistication of bot attacks, including real-time refinement of attack techniques by AI-powered bad bots.
* <https://techxmedia.com/en/ai-surge-drives-rise-in-bad-bot-attacks-says-thales-report/> - TechXMedia covers how industries such as travel and retail are heavily impacted by bad bots, with travel facing 27% of all bot attacks, and how simpler bot attacks have surged due to AI-driven lowered technical barriers.
* <https://www.afp.com/de/node/3776821> - AFP’s coverage discusses the rise of AI-fueled bots in the 2025 Imperva Bad Bot Report, emphasizing the expansion of Bots-As-A-Service (BaaS), the growing bot threat, and the increasing targeting of APIs for automated fraud and data breaches.