# Malicious bots now generate over half of mobile and e-commerce traffic, Radware finds



Mobile applications and e-commerce platforms are experiencing a significant surge in malicious bot activity, according to Radware's 2025 E-commerce Bot Threat Report. The findings reveal a dramatic shift in online traffic dynamics, with automated programs now accounting for more web activity than human users.

The report indicates that during the 2024 holiday season, approximately 57% of all traffic to online stores originated from bots, marking a substantial increase from prior years. Such automated traffic is noted to have increased by 160% on mobile platforms between the 2023 and 2024 holiday seasons. This rise is attributed to the sophistication of these bots, which employ advanced strategies to mimic genuine user behaviour effectively.

Ron Meyran, Vice President of Cyber Threat Intelligence at Radware, remarked, “Bad bots are no longer just based on simple scripts - they’re sophisticated, AI-enhanced agents capable of outsmarting traditional defenses.” He stressed that businesses relying on conventional security measures would find themselves increasingly vulnerable not just during peak shopping periods but throughout the year.

The research highlights the strategies employed by these malicious bots, with nearly 60% of them utilising behavioural tactics designed to evade detection. Many of these bots take advantage of rotating IP addresses and identities, employ CAPTCHA farms, and mimic human browsing patterns, complicating the identification process for traditional security systems.

The report also addresses the challenges posed by mobile-targeted bot activity, noting that attackers are utilising mobile emulators and headless browsers to replicate legitimate app behaviour. Furthermore, there has been a 32% uptick in attack traffic from residential proxy networks, further complicating the enforcement of traditional security measures such as rate-limiting and geo-fencing.

A concerning trend identified in the report is the rise of multi-vector campaigns that integrate bot activities with traditional exploits and API-targeted attacks. These campaigns go beyond merely scraping prices or testing stolen credentials; their more malicious objective is to take websites offline completely.

As online retailers and e-commerce providers navigate this evolving landscape, the report emphasises the urgent need for enhanced security protocols. To combat these sophisticated threats, businesses must upgrade their security frameworks to incorporate advanced DDoS protection and intelligent traffic monitoring systems. The report suggests that solutions adopting AI-powered detection capabilities are essential to counter the increasingly complex tactics employed by these bots.

In summary, the landscape of online commerce faces unprecedented challenges as malicious bot activity escalates and becomes more sophisticated. The report serves as a clarion call for businesses to reassess their security measures and adapt to the evolving threat landscape, ensuring their operations remain secure in an age dominated by automated traffic.

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

## Bibliography

1. <https://www.radware.com/blog/application-protection/protecting-e-commerce-businesses-against-ai-driven-bot-threats/> - This Radware blog post discusses the increasing sophistication of AI-driven bot attacks targeting e-commerce businesses, highlighting the need for advanced security measures to combat these threats.
2. <https://www.radware.com/blog/application-protection/role-of-machine-learning-in-thwarting-automated-bot-attacks-on-applications/> - This article explores how machine learning is being utilized to detect and mitigate automated bot attacks, emphasizing the importance of adaptive and dynamic security solutions.
3. <https://www.radware.com/blog/application-protection/radware-enhances-its-industry-leading-bot-manager-solution-to-deliver-a-more-secure-mobile-experience/> - This Radware blog post details enhancements to Radware's Bot Manager, focusing on improved security measures for mobile applications against sophisticated bot attacks.
4. <https://www.radware.com/press-release/radware-prevents-bad-bots-from-gaining-unlawful-access-to-native-android-and-ios/> - This press release announces Radware's advancements in bot management, specifically targeting the prevention of bot attacks on native Android and iOS mobile applications.
5. <https://www.cpomagazine.com/cyber-security/62-of-security-incidents-on-ecommerce-retailers-originate-from-bots-including-account-takeover-ddos-and-api-attacks/> - This article reports on a study revealing that 62% of security incidents on e-commerce retailers originate from bots, including account takeovers, DDoS attacks, and API abuses.
6. <https://www.nasdaq.com/press-release/bots-now-make-up-nearly-half-of-all-internet-traffic-globally-2024-04-16> - This Nasdaq press release highlights a report indicating that bots now account for nearly half of all internet traffic globally, with significant impacts on various industries, including e-commerce.
7. <https://www.techradar.com/pro/its-official-the-majority-of-visitors-to-online-shops-and-retailers-are-now-bots-not-humans-heres-why-it-matters-to-you-and-me> - Please view link - unable to able to access data