Key insights of the report

Web scraping is not just a fraud or security problem, it is also a business problem. Scraper bots have a negative effect on many facets of the organization, including revenue, competitive edge, brand identity, customer experience, infrastructure costs, and digital experience, just to name a few.

According to an Akamai research case study, 42.1% of overall traffic activity was from bots, with 65.3% of that bot traffic from malicious bots. And a total of 63.1% of the bad bots traffic used advanced techniques.

Headless browser technology has changed the scraper landscape, requiring an approach to managing this type of bot activity that is more sophisticated than other JavaScript-based mitigations.

Technical impacts that organizations face as a result of being scraped, whether the scraping was done with malicious or beneficial intentions, include website performance degradation, site metric pollution, compromised credentials attacks from phishing sites, increased compute costs, and more.

It is important to observe and understand the different traffic patterns to identify whether a website is incurring human, basic bot, or sophisticated bot traffic. These patterns can range from circadian to intermittent to continuous.