Key insights of the report

Web attacks against applications and APIs surged by 49% between Q1 2023 and Q1 2024. The exponential growth in demand for applications and APIs has transformed them into lucrative targets for threats actors who are seeking to exploit security gaps to gain unauthorized access to their intended target's valuable data.

108 billion API attacks were recorded from January 2023 through June 2024. The relentless assaults against this critical digital interface, which serves as an invisible gateway to organizations, can potentially lead to data theft, damages to brand reputation, and regulatory fines, amounting to significant financial losses.

API abuse is a growing concern for businesses that rely on APIs to provide access to their data and services, and it can occur in various forms, including data breaches, unauthorized access, and distributed denial-of-service (DDoS) attacks.

The commerce vertical was victim to the most web application and API attacks, experiencing more than double the amount of attacks than any other industry.

DDoS attacks challenge traffic over all ports and protocols on Layers 3 and 4 and Layer 7. This also includes the Domain Name System (DNS) protocol, which Akamai researchers observed to be a component of 60% of the Layers 3 and 4 DDoS attack events identified in the past 18 months.

Akamai researchers observed high technology, commerce, and social media to be the top three industries in application-layer DDoS attacks, experiencing more than 11 trillion attacks (75% of the attacks) in just 18 months.