imperva

# The Biggest Threats to Online Retailers This Holiday Season

Amidst holiday joy, cyber threats deploy: 'tis the season for cybercriminals to target festive shoppers. Here are five threats retailers should prepare for this holiday season:

## Digital Skimming

The online equivalent of physical credit card skimmers (commonly referred to as Magecart). This type of attack leverages exploitable client-side resources, such as JavaScript code, to exfiltrate sensitive information directly from users' web browsers. Almost 400 resources, on average, are loaded per retail site, making eCommerce websites highly vulnerable to client-side data breaches. This combination of a broadened attack surface and a high volume of digital transactions puts online retailers at a high risk. Learn more about the importance of securing the client-side.

## Bad Bots

**Over half of bad bot traffic on retail sites comes from advanced bots** emulating human behavior, complicating detection. Scalpers use bots to snap up scarce, high-demand items, causing frustration amongst consumers and harming brand reputation. Competitors and third parties employ bots for scraping pricing, inventory, and proprietary content, leading to revenue loss. Fraudsters use bots for credit card and gift card fraud and to exploit promotions with fake user accounts. All this bad bot activity distorts analytics data, impacting marketing and sales strategies with inaccurate traffic metrics. Learn more about bad bots.

## Account Takeover (ATO)

A type of attack where cybercriminals gain illegal access to online user accounts, mainly by leveraging stolen credentials obtained through data breaches and leaks. Today, **15% of login requests are malicious ATO attempts**. These attacks continue to rise and often spike during the holiday season. User accounts on eCommerce sites make for a lucrative target due to the numerous financial incentives – saved payment information, store credit, gift card balances, loyalty points, and more.

## API Attacks

**API traffic accounts for 45.8% of all traffic to online retailers.** These APIs are integral to eCommerce, powering everything from product displays to shipping logistics. However, this increased reliance on APIs also makes them attractive targets for cybercriminals, providing them with more points of entry. APIs are also more susceptible to business logic abuse and fraud, making them an ideal target for automated attacks. This targeting of APIs can result in significant damage, including reputational harm, consumer trust erosion, and financial losses.

## Distributed Denial of Service (DDoS) Attacks

DDoS attacks have been exhibiting a growing trend of focusing on the application layer (layer 7) throughout the first half of 2023. Retail in particular, has seen a massive, **417% increase in application layer DDoS attacks** between H2 2022 to H1 2023. DDoS attacks have been notorious for causing chaos and disruptions for online retailers over the years. This is especially true during peak shopping periods when even minutes of downtime, due to DDoS, can cause millions of dollars in lost revenue. Learn more about DDoS.