Online Retailers: Five Threats Targeting Your Business This Holiday Shopping Season

By Erez Hasson, Gabi Stapel

As the holiday season approaches, a palpable sense of joy and anticipation fills the air. Twinkling lights adorn homes, the aroma of freshly baked cookies wafts through the kitchen, and the sound of laughter and carolers' melodies resonate on frosty evenings. It's a time when families come together, cherished traditions are upheld, and the spirit of giving is at its zenith.

Amid this festive backdrop, a shadowy concern lurks that can cast a damper on the celebrations: the persistent threat of security risks that target retailers and holiday shoppers. As consumers revel in the season's merriment, cybercriminals are equally eager to exploit the spike in online shopping activity, making it crucial for retailers to stay vigilant.

This blog will cover everything that you need to know to prepare for the year’s busiest shopping period.

Key Takeaways:

- The eCommerce industry remains a lucrative target for cybercriminal activity due to the number of shoppers that interact and share data on retail websites, high transaction volumes, and the growing network of APIs and third-party connections that make up the online retail supply chain.
- The holiday shopping period is a popular time for cybercriminals to target online retailers and cause chaos for legitimate shoppers.
- Expect high levels of malicious activity starting earlier in the shopping season. Attackers will try to keep up with shoppers looking for holiday savings and a better selection of items. As a result, there will likely be an increase in attacks around mid to late October.
- Almost 400 resources, on average, are loaded per retail site, making eCommerce websites highly vulnerable to client-side data breaches.
- Over 50% of bad bot traffic on retail sites comes from advanced bots, those that emulate human behavior and are harder to detect.
- Account takeover (ATO) attacks continue to rise and often spike during the holiday season. Today, 15% of login requests, across all websites, are malicious ATO attempts.

- Distributed denial of service (DDoS) attacks continue to pose a significant threat, especially low-volume, lengthy attacks that can remain undetected and impact online transactions.
- Business logic attacks were the most significant threat to the retail industry in the past 12 months as cybercriminals scraped, abused, and attacked vulnerable APIs and third-party connections to exfiltrate data, create fake user accounts, manipulate pricing, or access restricted products.

Why is the eCommerce industry a target of security attacks?

Financial incentives, a wealth of personal data, a high volume of transactions, and a wide array of attack vectors make eCommerce a high-value target for cybercriminals. In the coming year, retailers are likely to face even more attacks as nearly a quarter of all global retail sales are expected to be made online by 2025.

Despite many shopping and sales events spread throughout the calendar year, Cyber Week – the shopping period that includes Thanksgiving, Black Friday, and Cyber Monday – remains the most popular. Black Friday online sales totaled a record $9.12 billion in 2022 in the US, while Cyber Monday experienced a record-breaking total of $11.3 billion in sales. In total, consumers spent $35.3 billion during Cyber Week 2022. Singles Day (November 11) is another popular shopping event that has seen tremendous growth in recent years, with sales estimated at $157 billion (1.1 trillion yuan) in 2022.

What are the biggest threats targeting the eCommerce industry?

Digital Skimming

As application logic shifts from server-side to client-side, and as more third-party code is incorporated into websites, the risk of client-side attacks grows. Digital skimming attacks like Magecart, formjacking, and other online skimming techniques can result in long-term, devastating data breaches. These attacks involve injecting malicious JavaScript into first-party code or the code of third-party services (the software supply chain) used on legitimate websites. Just a single line of malicious code, such as a JavaScript sniffer, is sufficient. Because this JavaScript executes on the client-side, it enables attackers to collect sensitive personal information directly from the client each time a customer enters their information into an online form.

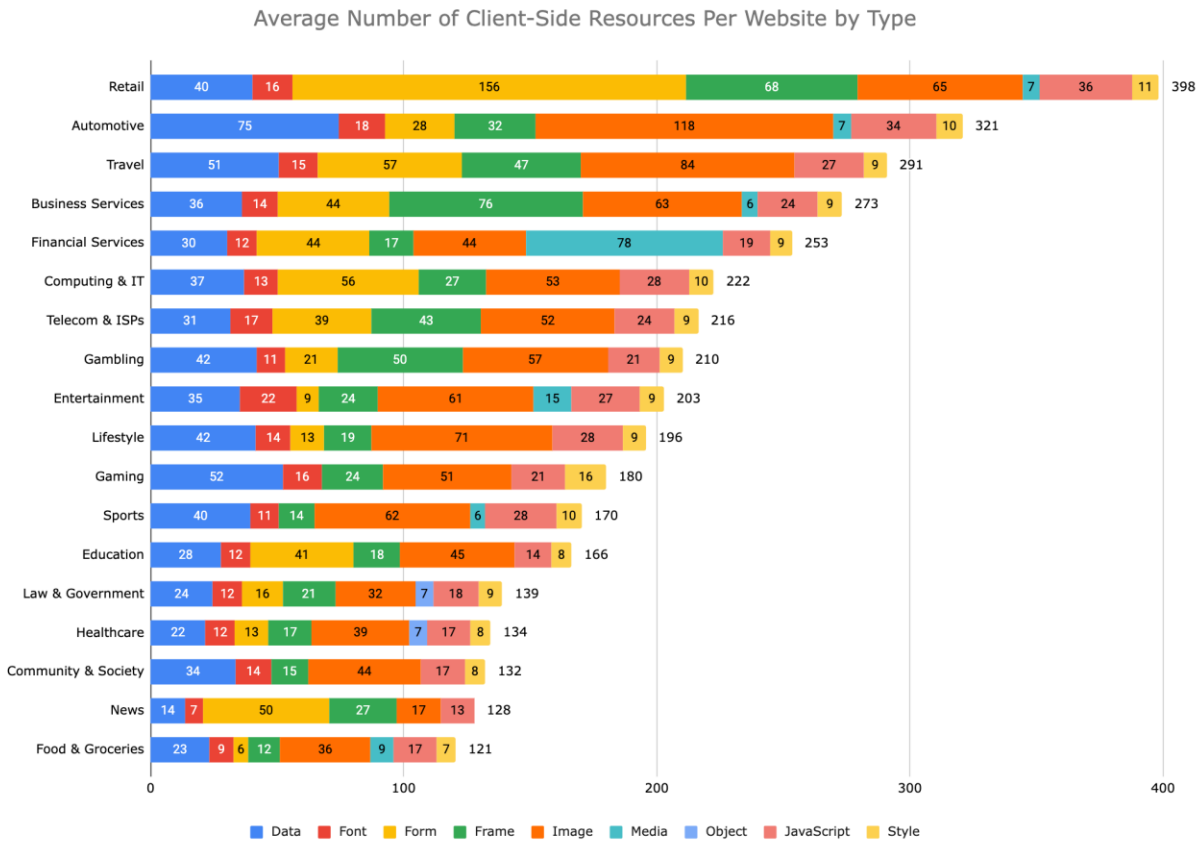
Any business relying on third-party vendors for parts of their website code is at risk of Magecart and other forms of digital skimming attacks. Even if you drop in just a simple

code for analytics, you might inadvertently insert a Magecart payload into your website. These vulnerabilities in the website supply chain are ideal for attackers because a single compromise of a widely used component is enough to enable them to hit multiple users on multiple sites around the world simultaneously.

Client-side, or the web application front-end, refers to the actions that occur on a user's device, rather than on the server-side. When a user interacts with a web application, such as filling out a form or clicking a button, these actions are performed on the client-side. This could involve rendering web pages, executing scripts, or handling user inputs. These activities are conducted on the client's device, independent of the server.

Sophisticated attackers understand that websites heavily leverage a supply chain of code which is a blind spot for organizations. On retail websites, a majority of the code originates from third-party sources. As such, attackers find ways to steal sensitive information by exploiting vulnerable scripts to plant online skimmers.

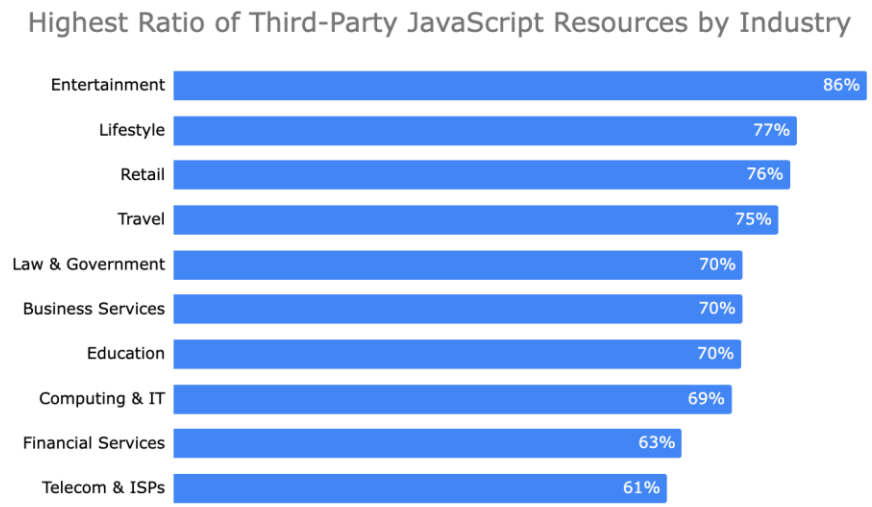
On average, modern web applications load 209 resources on the client-side at any given time. In contrast, the retail industry loads an average of 398 per site.



JavaScript is the most popular choice of client-side resource for attackers to exploit because it's a fundamental building block found in 98.7% of modern web applications. Furthermore, it is an extremely flexible tool that can easily be manipulated in numerous ways, making it an ideal vector for abuse.

Once compromised, embedded JavaScript code can be used for malicious monitoring of mouse movements and keystrokes without a user's knowledge. Attackers can track user behavior while code injection can exploit a user's browser, steal cookies, impersonate users to perform actions on a separate website, and more. These compromises usually occur through a server-side compromise, supply chain attacks, or methods like stored Cross-Site Scripting (XSS).

The following chart represents the top ten industries with the highest ratio of third-party JavaScript code, of which retail is third (76%). The higher the ratio of third-party services, the greater the risk of a compromise through the software supply chain.



If an application's client-side is not protected, an attacker can force load malicious scripts. These injections can originate from server-side compromise, supply chain attacks, or methods like stored Cross-Site Scripting (XSS).

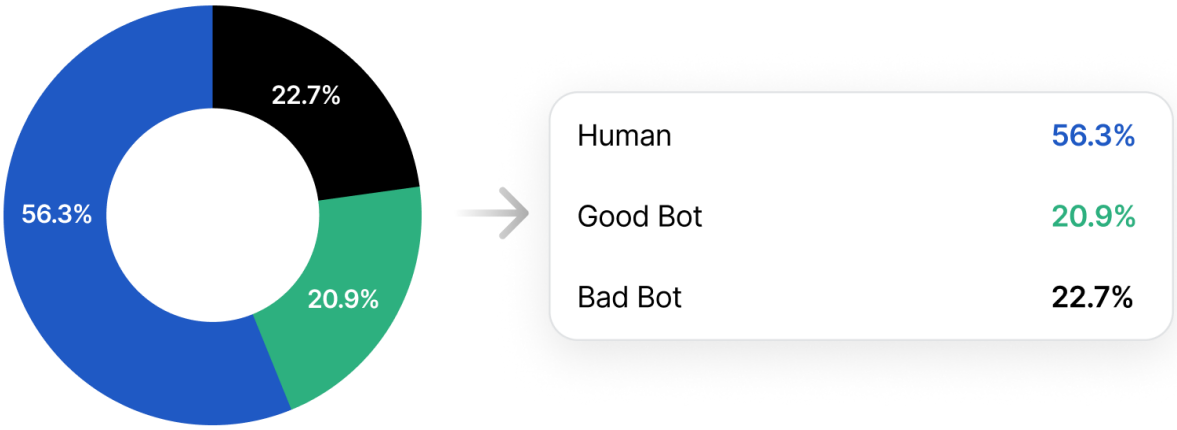
Recognizing the risk, PCI DSS 4.0 includes new requirements about securing payment pages from malicious scripts and unauthorized modification or tampering.

Bad Bots

Bad bots are software applications that run automated tasks on the internet with malicious intent.

Bad bot attacks on retail sites are trending upwards as we go into the holiday season. Since July, automated attacks have risen by 14%, with most attacks occurring on US-based sites, followed by retail sites in France. This trend will likely continue throughout the holiday shopping season.

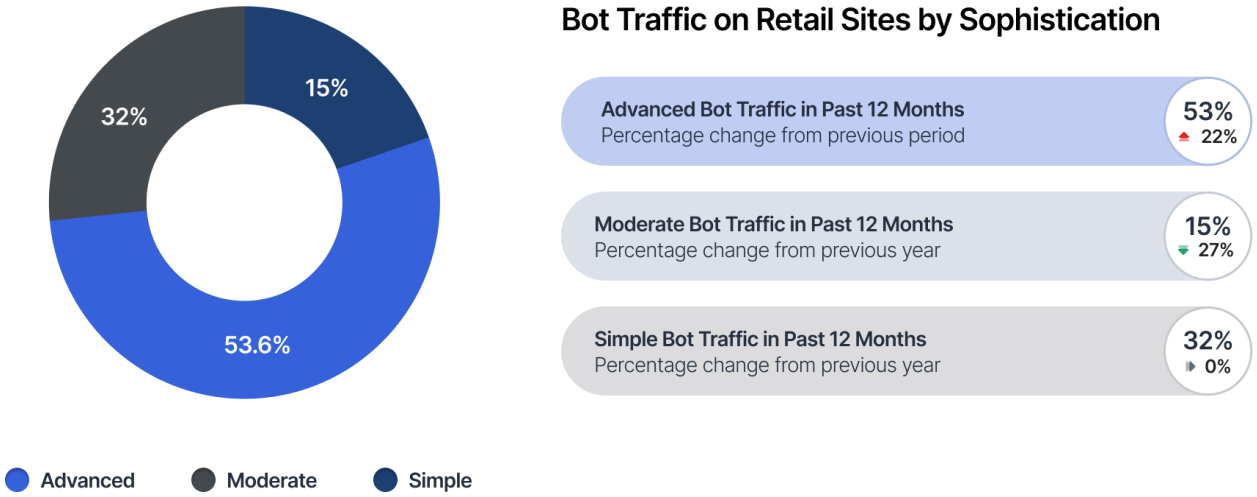
Retail Website Traffic Profile (Human v Good Bot v Bad Bot)



During the last year, 22.7% of traffic on retail sites originated from bad bots, which is lower than previous years. Online retailers experienced a higher volume of good bot traffic (20.9%) due to the prevalence of price scraping by search engines and price comparison websites. There are several factors contributing to the slightly lower rate of bad bot traffic compared to previous years:

- The volume of online transactions decreased: Since its peak in 2020, in-store activity has resumed and now makes up the majority of sales for retailers.
- Fewer cases of high-demand, limited-stock product launches: While the ticketing and live entertainment industry has been plagued with notable bot-related incidents in the past year, retail has largely been spared. However, limited edition sneaker drops or the release of popular video games and consoles still attracts a high volume of automated attacks and is a risk for retailers.

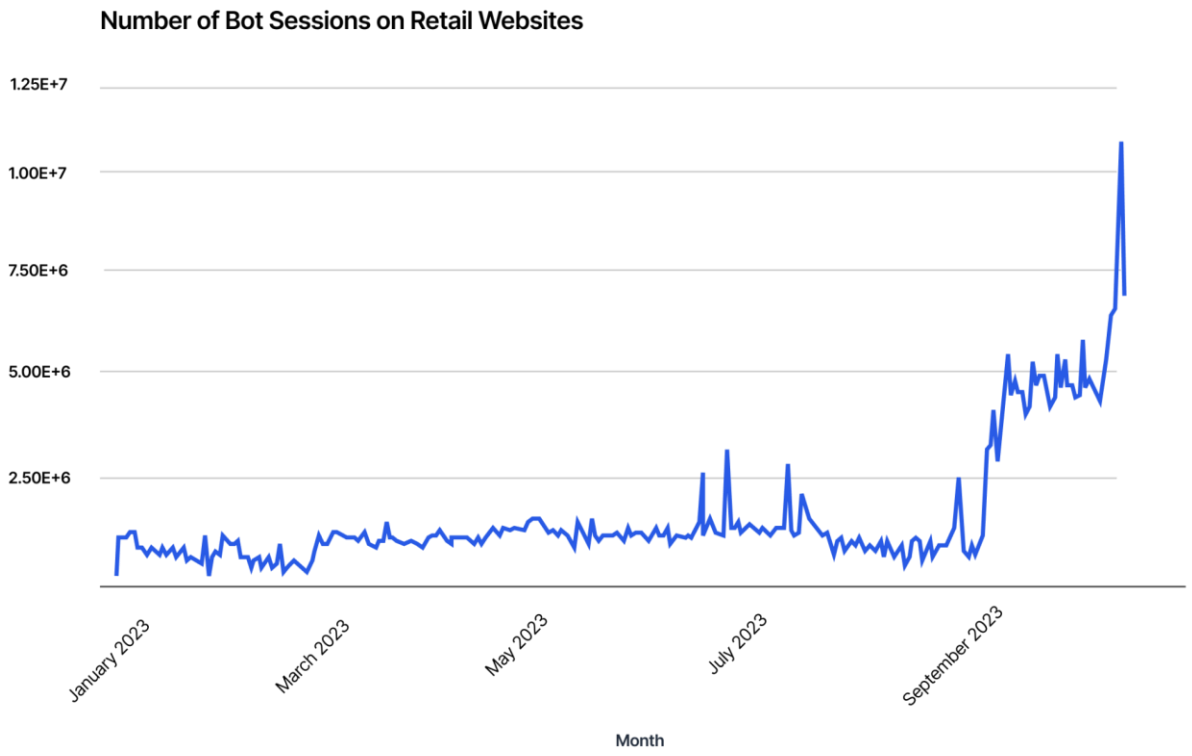
While 22.7% of traffic originating from bad bots might not seem significantly high, it is when considering their sophistication.



Over 50% of bad bot traffic on retail sites globally in the last year came from advanced bots, a sharp increase over the 31.1% recorded in 2022 and 23.4% recorded in 2021. Advanced bots are harder to detect and deter and capable of evading basic defenses. They're also more likely to carry out disruptive attacks and online fraud.

Retailers in Australia (62.99%), France (61.53%), and the United States (66.5%) saw the highest proportion of advanced bots compared to the global average. The considerable level of advanced bad bots on retailers' sites is a cause for concern as the sophistication of bots continues to grow annually.

Bot attacks are rising as we enter the holiday season. Since early September, simple and moderate bot attacks have risen steadily.



Some of the bad bot use cases that are rampant across eCommerce include:

- Competitors that scrape data to gain an edge (e.g. pricing, inventory levels, proprietary content)
- Scalpers that use bots to obtain limited availability items and resell them at a higher price
- Distributed Denial-of-Service (DDoS)
- Criminal activities such as carding or card cracking, gift card cracking, and account takeover.
- Bad bots can also skew analytics data, undermining accurate decision-making by providing false traffic metrics and ultimately impacting marketing and sales strategies.

Grinch bots, a variation of scalping bots designed to target highly coveted holiday season gifts, are particularly common in the holiday shopping season. These sophisticated bots are used to disrupt holiday sales events and limited product launches. They query online inventories and purchase the most sought-after items of the season for the sole purpose of reselling them at a significant markup.

During the 2020 and 2021 holiday shopping seasons, bot operators used Grinch bots to pursue next-generation gaming consoles and GPUs, among other high-demand, limited-

quantity items. Today, the focus has shifted towards collector's items such as trading cards, collector edition video games and branded goods, sneakers, and more.

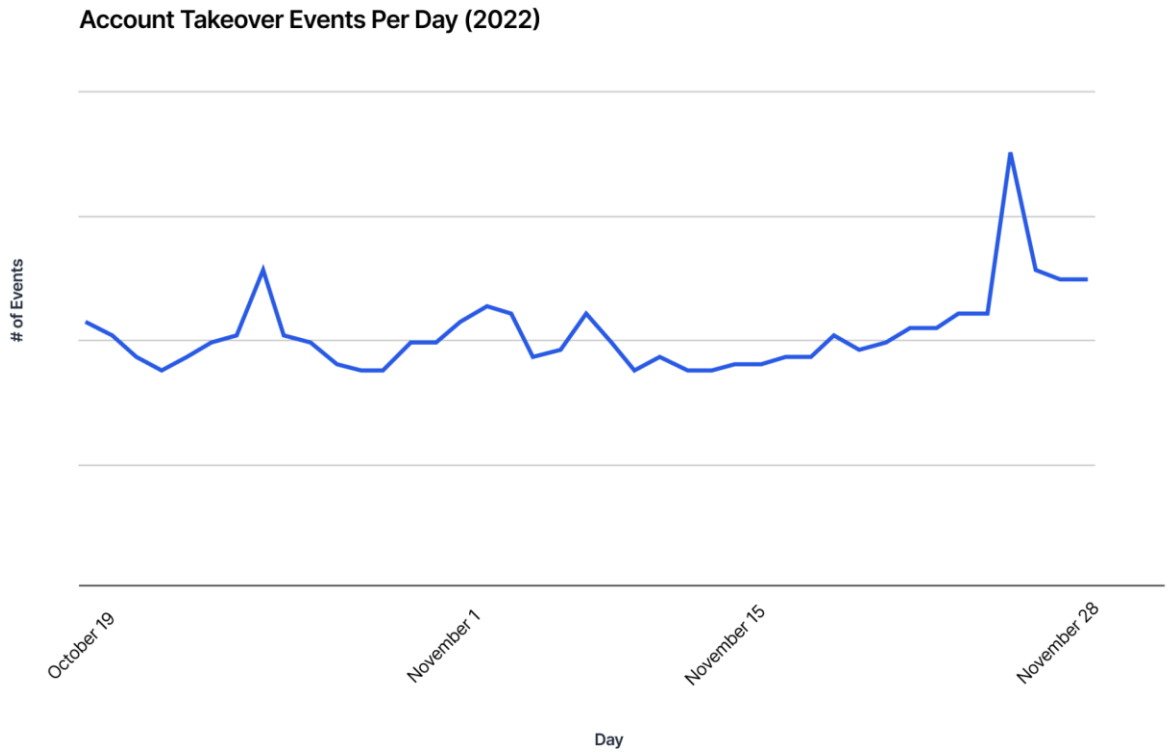
Account Takeover Fraud

Account Takeover (ATO) is a form of identity theft where a malicious actor gains unauthorized access to a user's online account, typically by exploiting weak or stolen credentials. Once inside the account, the attacker can misuse the account in various ways — from making unauthorized purchases to stealing sensitive personal data. Account takeover is common in eCommerce because once attackers gain access to user accounts, it allows them to exploit credit card details, loyalty points, gift card codes, and other forms of payment for their financial gain.

One such payment form that has seen a significant increase in popularity is Buy Now, Pay Later (BNPL). Buy Now Pay Later service revenue rose 88% during the 2022 holiday shopping season. For attackers, this is yet another ripe target, resulting in an increase in account takeover attacks targeting BNPL services. The risk is even greater for BNPL, due to the flexibility at which one can perform a fraudulent purchase — by taking over the BNPL account directly or by taking over the user account on the retailer's side that is authorized to charge the BNPL account.

Throughout the 2022 holiday shopping season, Imperva recorded elevated levels of account takeover events. Attacks rose 12% in October and culminated with a 66% increase in account takeovers on Black Friday (November 25). Another notable increase was recorded on October 26, just a month ahead of Black Friday, as account takeovers

increased by 29%.



Distributed Denial-of-Service (DDoS)

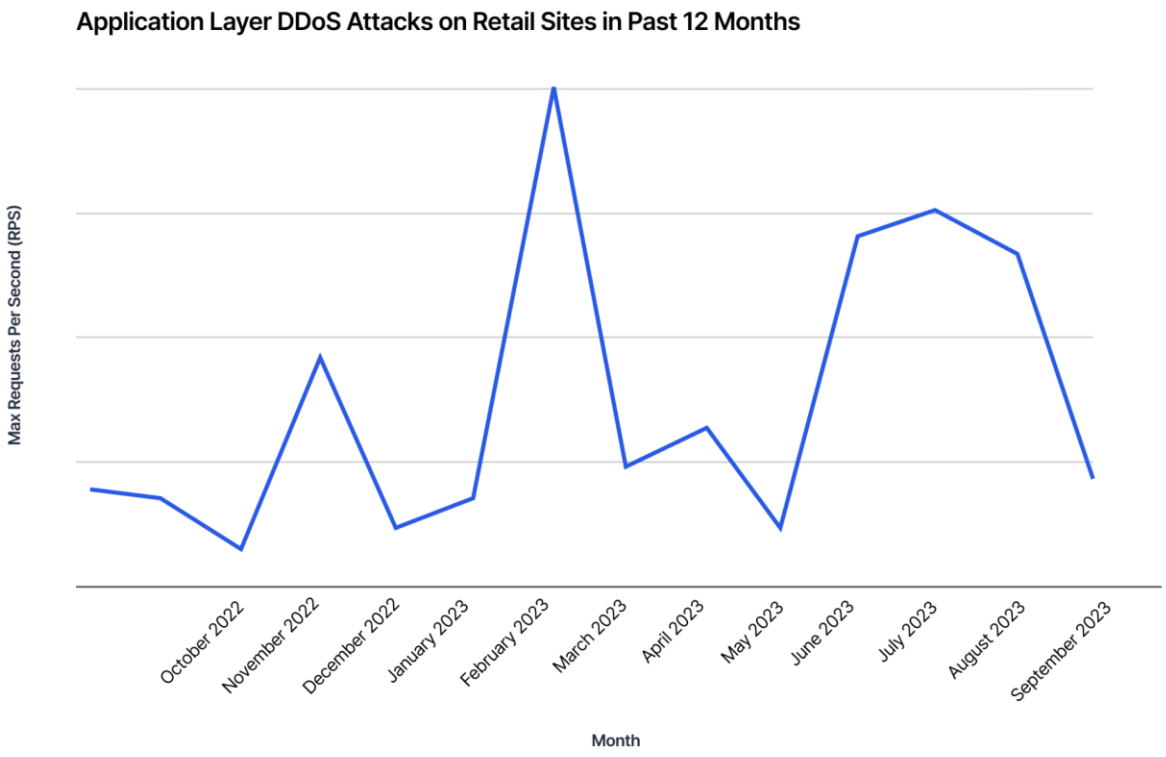
Distributed denial-of-service (DDoS) attacks are a persistent threat to online retailers. Attacks aim to overwhelm a retailer's network or servers with a flood of traffic, making it inaccessible to legitimate shoppers. When an attack happens, the retailer is unable to handle legitimate requests, which leads to disruptions in service. These attacks often come from vast networks of compromised devices, known as botnets.

The retail industry is an attractive target for DDoS attacks for several reasons:

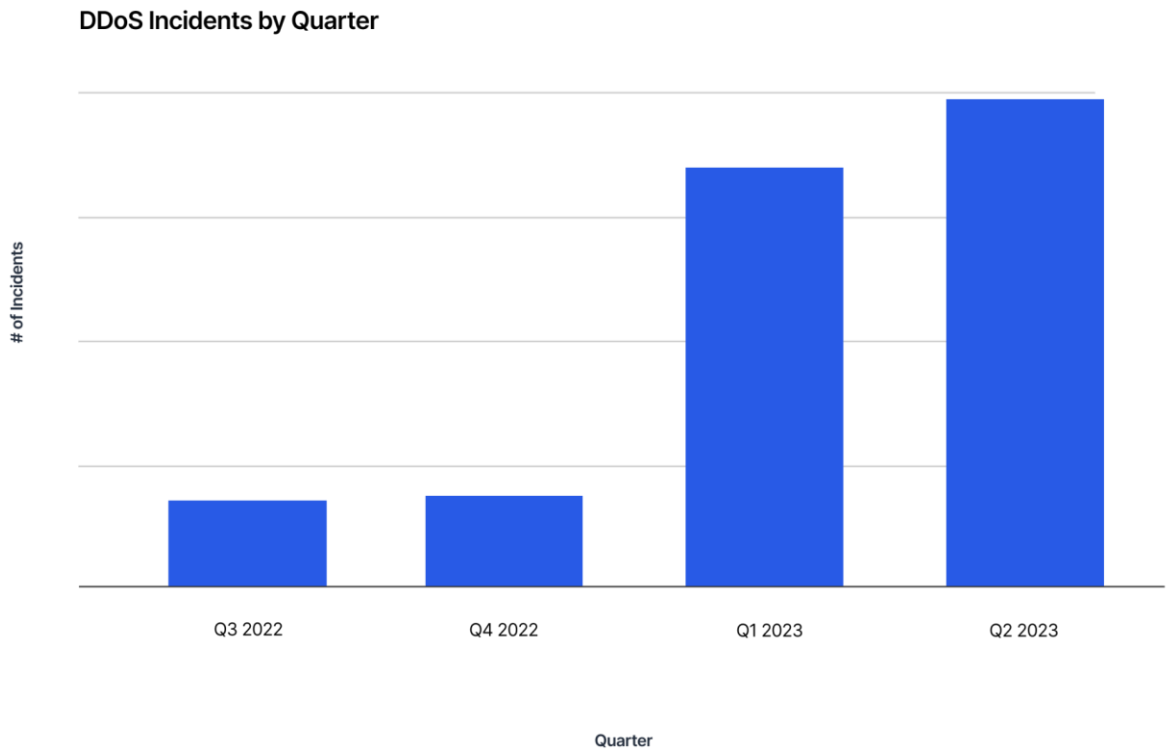
- The industry is expected to see $6.3 trillion in revenue in 2023, so even minutes of downtime, due to DDoS, can cause millions of dollars in lost revenue.
- Slow performance or downtime due to DDoS can impact a company's reputation, especially if the site is targeted during peak shopping periods and/or an important release or product drop.
- A DDoS attack can be used as a sabotage tactic to push shoppers towards a competitor's site.

The largest application layer (layer 7) attack Imperva saw on retail sites was 1.22M requests per second (RPS) in February 2023, due to a targeted attack on a Spanish shopping site. Previously, another spike in traffic in November 2022 correlated with attacks during Cyber Week, particularly around Black Friday and Cyber Monday.

Overall, application layer DDoS attacks averaged 460K requests per second (RPS) over the past 12 months. In comparison to prior years, attacks in the last year have been generally smaller in size, which could be the result of shifting attack tactics or cybercriminals focused on attacking different industries. This doesn't mean that the threat of a DDoS attack should be overlooked. Smaller attacks, such as those recorded in the past 12 months, can still affect performance and revenue, especially if they are sustained over long periods.



DDoS attacks have been exhibiting a growing trend of focusing on the application layer (layer 7) throughout the first half of 2023. This shift to application layer attacks is prevalent across all industries, particularly in retail, with a massive 417% increase in the volume of layer 7 DDoS attacks between the back half of 2022 and the first half 2023. The rise in DDoS attacks has been considerably higher in the United States, Australia, Germany, and France.



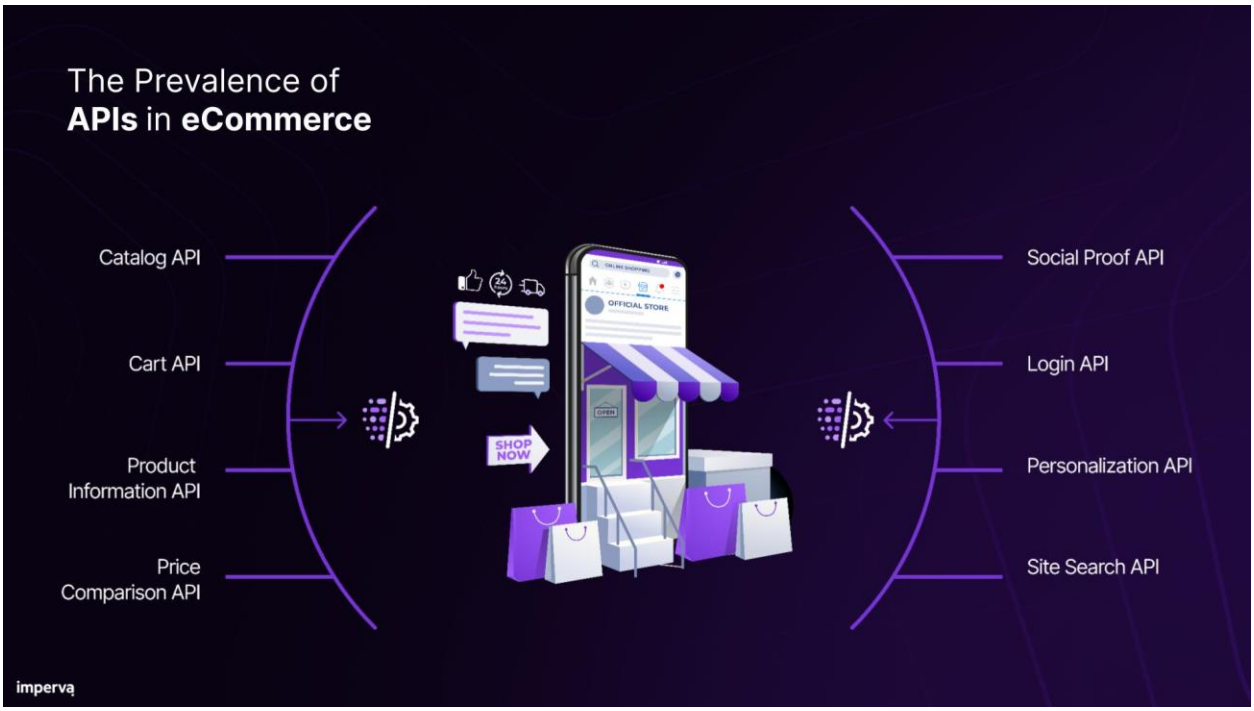
Since September 1, the number of application layer DDoS attacks has been higher in comparison to the same time last year, underscoring the annual trend of cybercriminals increasing attacks as the holiday shopping season begins.

The largest network layer (layer 3 and 4) attack reached 42 Gigabytes per second (GBPS) in September 2022. Similar to what Imperva monitored at the application layer, network layer attacks were small or moderate in size. These attacks can still pack a punch. Even attacks at an average of 10 GBPS can lead to transaction failures or downtime, which can affect sales and a customer's loyalty.

The average amount of downtime global online retailers in 2022, protected by Imperva DDoS Protection, avoided during Cyber Week was 17 hours, an increase of four hours, on average, of downtime in comparison to 2021. During the holiday shopping season (October 1 - December 1), Imperva mitigated 341 hours of downtime, on average, per retailer.

API Attacks

In the world of online shopping, web applications and Application Programming Interfaces (APIs) are the backbone of online business operations.



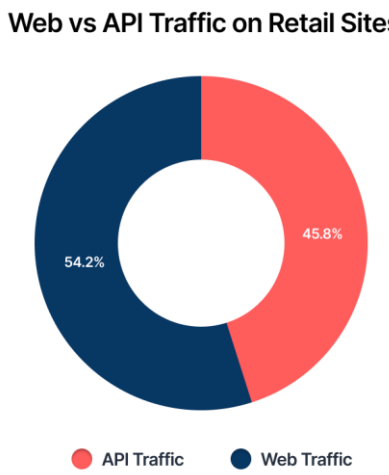
Web applications power the user interfaces of eCommerce platforms, enabling customers to browse products, add them to carts, and make purchases. APIs facilitate seamless integration between different software components and databases, allowing for functionalities like payment processing, inventory management, and third-party integrations.

The industry's reliance on third-party integrations, like payment processing or CRM programs, gives cybercriminals more attack surface and the opportunity to abuse existing APIs. Because retailers store vast amounts of payment and user data, API connections are ripe targets for exfiltrating that data.

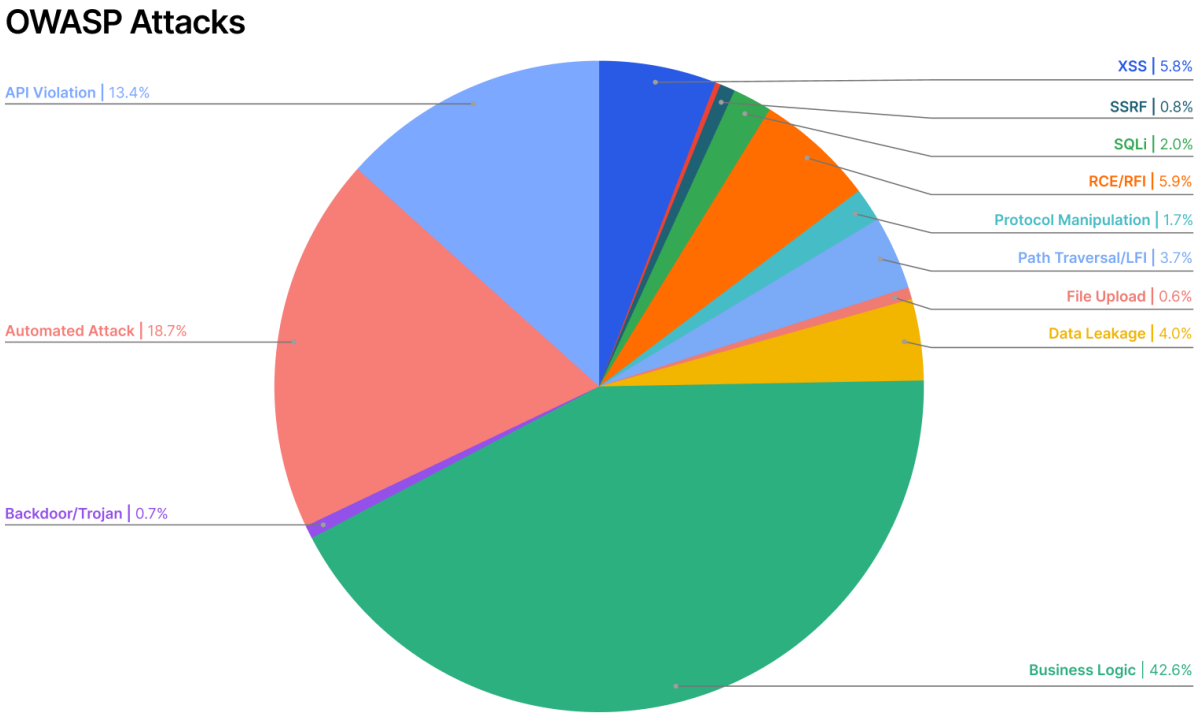
In the retail industry, web applications are often complex. They could be exposed to a business logic attack (BLA), an exploit of an application's intended functionality and processes, rather than its technical vulnerabilities. The BLA manipulates workflows, bypasses traditional security measures, and misuses legitimate features to gain unauthorized access or cause damage without triggering security alerts. In retail, attackers can exploit business logic to manipulate pricing or access restricted products.

In the past, online shopping was primarily done on a computer and web browser. Today, consumers interact and transact across a multitude of devices, ranging from mobile phones to refrigerators, cars, and smart home assistants. This evolution necessitates a fresh architectural approach: headless commerce. This system detaches the front-end from the back-end of an ecommerce platform, ensuring consistent and intended

functionality across all devices and display formats. Central to this structure are APIs. Today, API traffic accounts for 45.8% of all traffic to online retailers, up from 41.6% last year.



In the last year, the most common attack on retail sites was associated with business logic. This shouldn't come as a surprise as business logic vulnerabilities are highly custom and specific to individual applications and APIs. Therefore, a common attack pattern doesn't exist to monitor these endpoints and it's impossible to apply a generic rule and assume all application and API deployments are secure.



On eCommerce API sites, API violations are the most common security incident. API violations occur when the API is used in ways it wasn't intended, such as data scraping, account takeover attacks, or inventory hoarding. Retail sites handle high traffic volumes, manage valuable data, and often integrate with third-party applications through APIs, so this method of attack is attractive to cybercriminals.

Recommendations ahead of the holiday shopping season

Just as shoppers should be aware of the risks associated with online shopping, retailers must remain vigilant as well. They must avoid cyber risks threatening the integrity and continuity of their business, as well as the safety of their customers and their sensitive personal information.

1. **Prepare for a high volume of traffic, as well as distributed denial-of-service (DDoS) attacks.** Black Friday and Cyber Monday are the most popular shopping events of the year. From discounts to limited edition product launches, shoppers flock online to get the best deals and exclusive products. This influx of traffic could potentially bring even the sturdiest of infrastructure to a halt, risking costly downtime. Consider implementing a waiting room queueing system that can help ensure site performance and maintain a positive customer experience. The holiday season is also a time for attackers to launch DDoS attacks aimed at online retailers. It is recommended that you stress-test your infrastructure regularly, especially before periods when high traffic is anticipated. Make sure you are properly protecting against DDoS attacks across all web resources, including DNS.

2. **Prioritize the security of the client-side.** Magecart-style attacks are notorious for making use of compromised first or third-party JavaScript to exfiltrate sensitive information out of website forms such as login and checkout. To mitigate this risk, perform continuous monitoring and inventorying of all services on the client-side, review them, and ensure that only authorized ones can run. You can leverage HTTP Content-Security-Policy headers, but be cautious – these can be difficult to implement and maintain across the organization. PCI DSS 4.0 has added two requirements that directly address client-side attacks, increasing the responsibility for businesses accepting or processing online payments. To ensure maximum security and compliance with these requirements, we recommend employing a specialized tool for client-side protection. Such tools provide continuous inventorying and monitoring, risk assessment, and easy blocking of unwanted services with just a single click.

3. **Marketing and eCommerce campaigns are likely to become targeted by bots.** Bad actors are likely to employ bots to buy up as much inventory from highly anticipated product drops as possible -- such as a new pair of sneakers, a gaming console, or a limited-edition collectors' item. The equation is simple: announce a date and time for a coveted product launch and bots will be there to try and get their hands on it first. If they succeed, consumers are left disappointed and frustrated at the retailer, which has the potential to damage the brand's reputation. Prepare to handle increases in traffic volume that is likely to include a high proportion of bots. Automation will be used to scoop up the inventory, denying it from legitimate customers. At the same time, bot traffic diminishes website performance and skews website analytics.

4. **Protect critical paths and website functionalities from bots seeking to abuse business logic.** Some website functionalities are highly exploitable. For example, login functionality opens up the possibility of credential stuffing and credential cracking attacks. Adding a checkout form increases the chances of carding or card cracking. Gift cards are a popular gift during the holiday season, and adding gift card functionality invites bots as well. Gift card payment processes on websites are often under sustained attack from sophisticated bad bots trying to defraud people from the money loaded onto a card. Ensure these pages are properly protected by a bot mitigation solution and employ a stricter ruleset.

5. **Encourage good account credential hygiene and safety.** The safety of your users' accounts is a major part of the security of your business. Ensure that user passwords require a minimum number of characters, use of capital letters, numbers, symbols, etc. Implementing multi-factor authentication (MFA) and encouraging its use is highly recommended. Additionally, be aware of data breaches as account takeover attacks tend to increase by up to three times following a breach. As such, expect an influx of bot traffic to your login pages after these events, and encourage users to change their passwords. Make sure you have a bot mitigation solution with dedicated account takeover prevention capabilities. Such capabilities include detecting and mitigating credential stuffing attacks, differentiating malicious and authentic login attempts, and discovering which of your users' credentials have been compromised online.

6. **Stay ahead of the scammers.** The holiday shopping season is a perfect time for scammers to launch phishing attacks. Cybercriminals might masquerade as your brand, sending fake emails that offer discounts and gift cards. Stay apprised of any phishing campaigns and make sure to alert your customers of any suspicious campaign(s) making use of your brand. Additionally, be on the alert for insider threats as phishing attacks will also target your employees.