imperva

REPORT

The State of Security Within eCommerce in 2022

Table of Contents

About the report

The Imperva State of Security Within eCommerce 2022 Report analyzes the latest trends in the retail eCommerce industry and the cybersecurity threats affecting it.

The eCommerce market is facing new challenges in the wake of the global pandemic — from growth rates slowing down after the boom brought by the stay-at-home orders to difficulties in customer acquisition due to recent privacy updates, and most recently, inflation. However, this slowdown is most likely a correction, a return to pre-pandemic levels of growth. The industry is projected to retain its overall growth and is estimated to account for a quarter of all retail sales worldwide by 2025[1]. Aiding it are new technologies that are constantly being introduced as well as flexible financing options now available for consumers like Buy Now, Pay Later (BNPL). With these new technologies, the risk to an already highly targeted industry grows bigger than ever.

In this report, we'll cite a wide range of data obtained by the Imperva Threat Research team, to help illustrate the cybersecurity risks we've monitored over the past 12 months. Our goal is to help retailers prepare for a holiday shopping season that's predicted to be record-breaking — both in terms of web traffic and cyber threats.

BY 2025, ONLINE SALES ARE PREDICTED TO MAKE UP ALMOST A QUARTER (24.5%) OF TOTAL GLOBAL RETAIL SALES

1 https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/

Executive Summary

Cyber criminals shop months in advance for holiday steals

As online shopping patterns return to pre-pandemic levels, online retailers are poised for steadier growth — and with it, a steady increase in cyber threats and online fraud, which trend higher for retail websites than others.

The high risk for eCommerce is more noticeable during the holiday shopping season, which now begins as early as October. Bad actors have gotten wise to consumer shopping patterns, which start weeks before significant events like Black Friday due to shipping delays and item availability concerns, as well as marketing tactics such as shops offering unbeatable deals weeks before Black Friday.

The laser focus that criminals have on eCommerce during the holiday season means retailers must strategize to ensure the security of their sites, customers, and data; and protect against multiple types of attacks. Automated threats are a top concern - **62% of attacks on online retailers were automated attacks.** The **Americas, Europe, and the Asia Pacific** were among the top regions for bad bot attacks on retail websites.

Bad bots aren't the end of the story: attacks on retailers increased in sophistication, as more of them masked their origin, going from **3.5% to 33% in just one year**. Attacks exploiting vulnerabilities such as Log4j in 2021 affected retailers during and after the holidays, API attacks on retailers increased starting in October, and DDoS attacks on retailers are bigger and stronger than in previous years. Online retailers should be vigilant against these cyber threats and more throughout the year, especially during the months leading up to major shopping events around the holidays.

HIGHLIGHTS

Online Retailers By The Numbers

13 HRS
potential DDoS downtime during the week of Black Friday

62%
of attacks were automated threats

33%
of attacks mask their origin (up from 3.5%)

20%
of login attempts are malicious account takeover attempts

42%
of all traffic is **API traffic**

Attack Spotlight

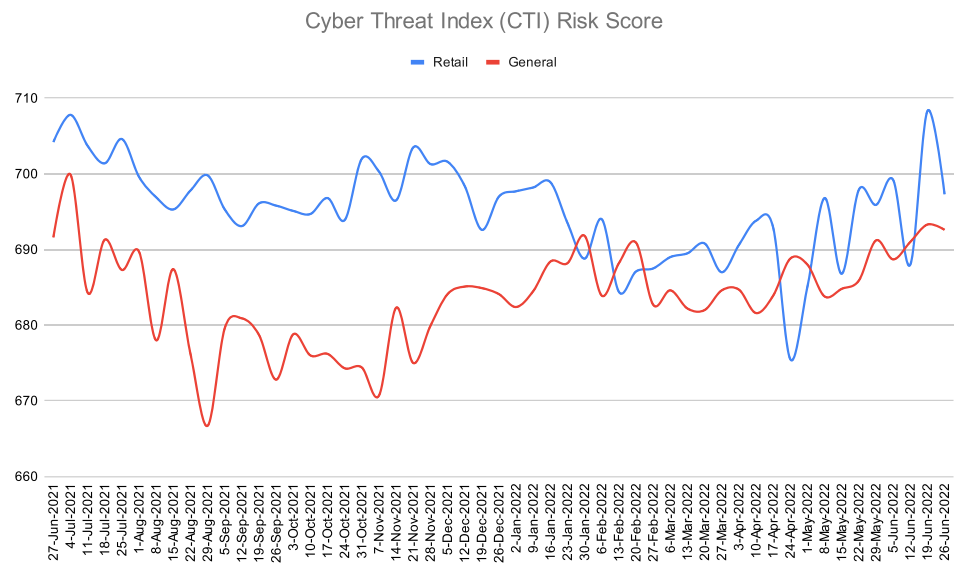
During the week of Black Friday 2021, Imperva mitigated a bot attack of 9 million requests in 15 mins., and 162+ million bot requests targeting the retailer overall during the last 2 weeks of November

eCommerce Risk Overview

Online retailers are at a higher risk

Before we dive deep into the individual threats, we take a bird's-eye view of the landscape using Imperva's Cyber Threat Index (CTI). The CTI provides an easy-to-understand score to track cyber threat levels consistently over time and observe trends. The score is calculated using data gathered from all Imperva sensors across the globe and is based on several ingredients: network traffic, attack traffic, and vulnerabilities.

The chart below represents the risk score over this past year, week over week. We can see that the cyber threat risk score on retail websites (blue line) averaged 695. This is slightly higher than the general trend (red line), averaging 684. Overall, the cyber threat risk score was lower than it was in the past 2 years, perhaps signaling a return to normal levels of internet traffic. Despite that, cyber threats and online fraud remain a top concern for online retailers that, among various other challenges, must first ensure the security and privacy of consumers and their data.



A key trend to look out for is early holiday shopping. Over the past two years, people began holiday shopping before Black Friday due to concerns about shipping delays and out-of-stock items. And it's not just the customers — oftentimes, retailers will offer their best deals before Black Friday, as soon as late October or early November. Bad actors have quickly figured this out, as clearly seen by the spike in the retail trend line at the end of October. We predict that we will see a similar trend this year, of an increase in attacks around mid to late October.

The chart below represents the daily traffic on retail websites throughout the holiday shopping season. Despite the increased popularity of early holiday shopping, staple shopping events remain the highlight of this period of the year. The first is an addition of

TERMS TO KNOW

Account Takeover:
A form of identity theft in which bad actors gain illegal access to user accounts belonging to someone else.

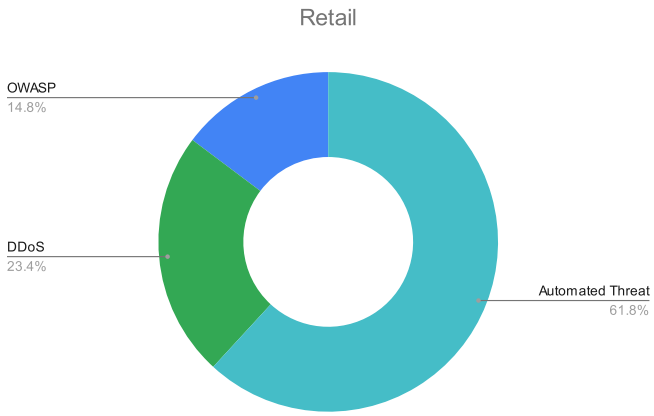
Account Creation:
This type of fraud occurs when fraudsters use stolen personal information from data breaches to create fake accounts utilizing someone else's data.

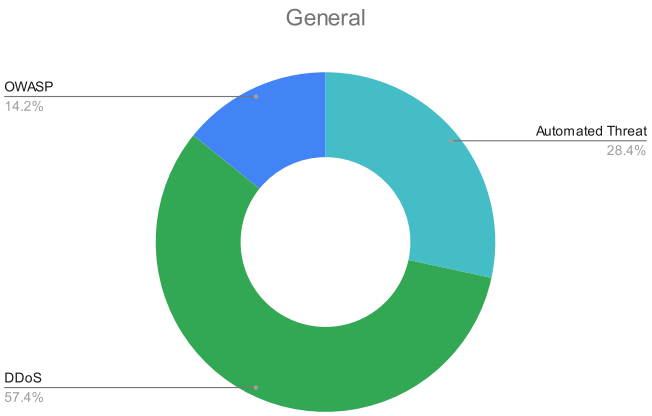
Magecart:
A collective name for online skimming techniques used for stealing personal data from websites—most commonly credit card information, customer details and credentials.

recent years, Singles Day, marked by the peak on November 11th. The second (and most well-known one) is Black Friday, clearly indicated by the 10% spike seen on November 26th. Albeit less popular, Cyber Monday too has generated a small peak in traffic on November 29th.

Automated threats reign supreme

Over the past year, almost two-thirds (61.8%) of attacks that targeted online retailers were classified as automated threats[2], also known as bad bots. That is in stark contrast to the general trend in other industries, where less than a third (28.4%) of attacks were classified as automated threats. Retail eCommerce has proven to be a highly profitable target for bad bot operators time and time again — whether it be price scraping to beat the competition in the SEO for pricing, scalping of limited availability items for their resale value, or account takeover fraud for the various forms of cash behind user accounts.

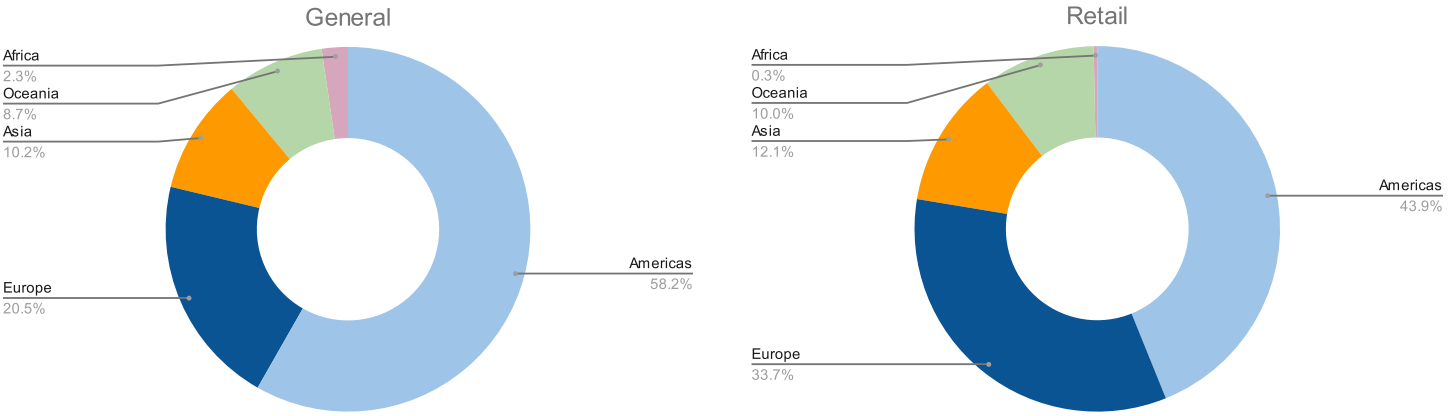




2 https://owasp.org/www-project-automated-threats-to-web-applications/

Most targeted regions

The following charts represent the distribution of attacks targeting websites by their regions. Attacks targeting retailers are more evenly distributed globally. The Americas accounted for 43.9% of attacks, Europe accounted for a third, and Asia Pacific accounted for 22.1%.



Industry Trends

Buy Now, Pay Later Fraud is on the rise

According to Allied Market Research[3], the global Buy Now, Pay Later (BNPL) market size was valued at $90.69 billion in 2020 and is projected to reach $3.98 trillion by 2030, growing at a CAGR of 45.7% from 2021 to 2030. Adjacent to that popularity is the increased risk of online fraud, especially identity fraud. The most common form of such fraud is account takeover, where a bad actor takes over an existing BNPL account and uses it to make unauthorized purchases. The risk is even greater for BNPL, due to the flexibility at which one can perform a fraudulent purchase — either by taking over the BNPL account directly or by taking over a user account with a retailer that is authorized to charge the BNPL account. Imperva's Threat Research team has recorded an alarming increase in account takeover attacks targeting financial services over the past year, with a significant 58% month-over-month growth in May 2022. We predict that this trend will persist as BNPL gains popularity. Another type of account-based fraud is account creation, where bad actors set up mule accounts through which they can utilize stolen identities and credit card information.

PCI DSS 4.0 addresses Magecart

Magecart attacks have been wreaking havoc online for a couple of years now, seeking to steal credit card details through compromised JavaScript code. And what better target for that than eCommerce? Due to their scalability, vulnerabilities in the website

3 https://www.alliedmarketresearch.com/buy-now-pay-later-market-A12528

supply chain are ideal for attackers: a single compromise of a widely used component allows them to hit multiple users on multiple sites, all by exploiting the same vulnerability. A single, well-chosen attack on a widely used application gives attackers access to thousands of sites around the world simultaneously. The newly released PCI DSS 4.0 acknowledges the threat, addressing it in requirement 6.4.3, which provides guidance on how payment page scripts that are loaded and executed in the consumer's browser should be managed.[4]

Hyped product launches galore

From sneakers to gaming consoles and limited-edition collector's items, hyped product launches are a popular way for online retailers to introduce goods of extremely limited stock that are in high demand. A hyped product launch is usually a very well-coordinated campaign effort run by the marketing and eCommerce teams, designed to generate "hype" around a certain product launch, attracting as many consumers as possible. Think of a pair of Air Jordans or Yeezys, for example, or a collector's edition for an upcoming video game. It could also be highly anticipated concert tickets.

In recent years, we have seen an increasing amount of these hyped product launches, or "online drops,'' happening on or around Black Friday. Such hyped product launches are highly susceptible to bad bot operators trying to scoop up as much inventory as possible to later resell for a significant profit — a phenomenon also known as scalping. This is a simple equation: products in high demand that have limited stock equal to inflated resale values. And because some people are willing to pay preposterous prices, the scalping industry is very much alive, well, and thriving.

During the week of Black Friday 2021, Imperva recorded and mitigated a massive scalping attack on a global retailer's drop of a limited-edition collector's item. The attack consisted of 9 million bot requests to the product page in just 15 minutes! To put things into perspective, that's 2,500% more than the average web traffic on the retailer's site. Overall, during the last two weeks of November, Imperva has mitigated over 162 million bot requests targeting the retailer.

A rock-solid bot management strategy must be thoughtfully crafted when preparing for this type of product launch. In addition, a waiting room queueing system is highly recommended to ensure site performance and maintain a positive customer experience (CX). Even the most reliable infrastructure can get overwhelmed by a surge of shoppers attempting to purchase the latest hot items. Furthermore, a queuing system allows for an even playing field for all consumers, leaving no one feeling cheated, thus reducing the risk of damage to the retailer's reputation.

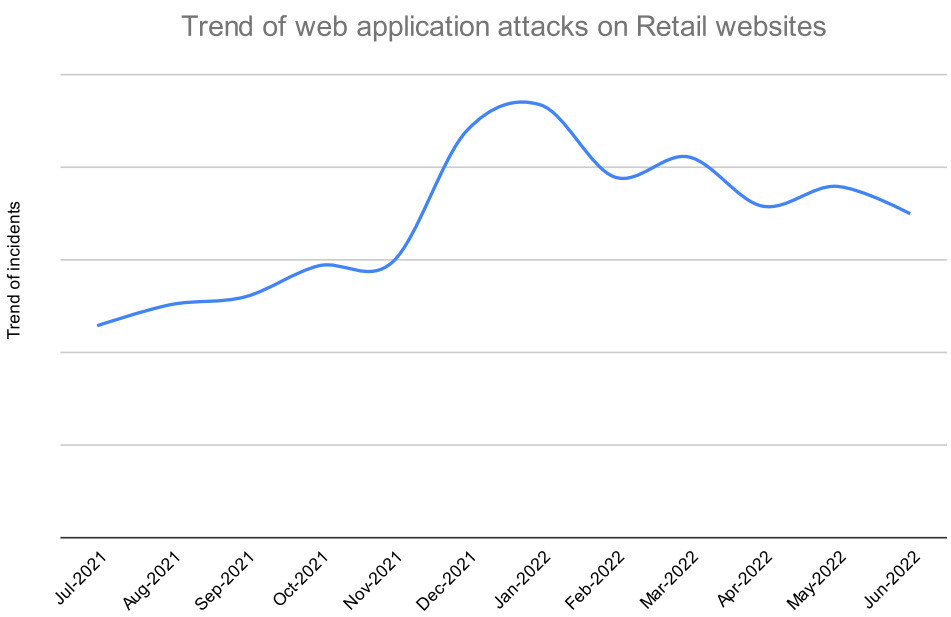
4 https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf

Website attack trends

This section of the report focuses on the more traditional type of web application attacks, as well as web application vulnerabilities. The insights are informed by data analyzed by the Imperva Cloud Web Application Firewall, and the more than 30 million web application attacks and a trillion HTTP requests the product analyzes monthly.

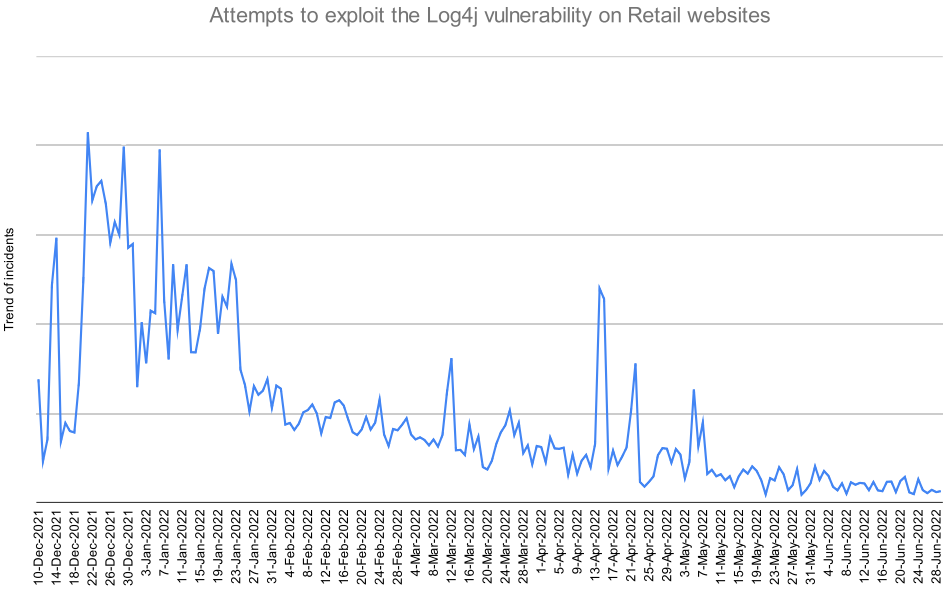
The impact of the Log4j vulnerability

The following graph represents the trend of web application attacks against online retailers throughout the past 12 months in the form of incidents per month.



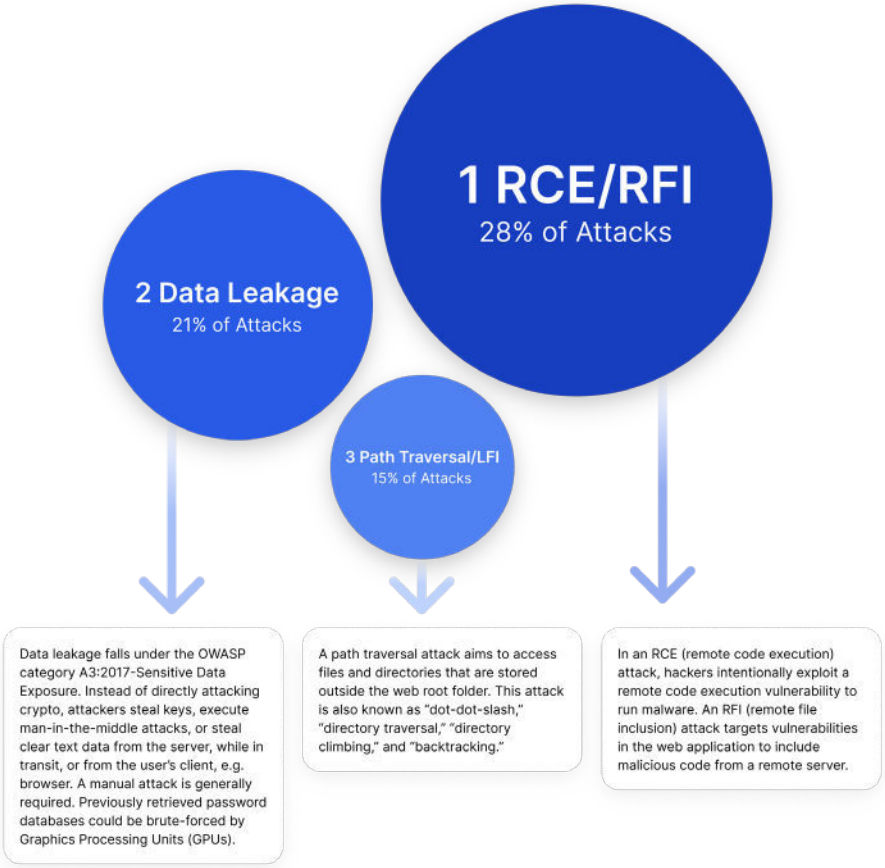
The 2021 holiday shopping season was characterized by a steady increase in attacks between July, peaking in late October and early November. This peak may be an example of attackers adapting to the trend of early holiday shopping. What came as a complete surprise this year, serving as a reminder of the unexpected nature of web application security, was the disclosure of the Log4j vulnerability (CVE-2021-44228) on Friday, December 11. Being a high-profile vulnerability that impacted multiple versions of a widely distributed Java software component, Apache Log4j 2, this specific vulnerability allowed for unauthenticated remote code execution. The discovery of the vulnerability led to a 48% increase in web application attacks month-over-month, clearly seen in the chart above.

The following chart represents the attempts at exploiting the vulnerability as uncovered and blocked by the Imperva Threat Research team. It can clearly be seen spiking right around the time it was initially disclosed, and slowly subsiding following its patching.



Log4j leads to an increase in remote code execution attacks

Going into greater detail, the top three attacks in the online retail sector, by volume, over the past 12 months were RCE/RFI, Data Leakage, and Path Traversal/LFI.



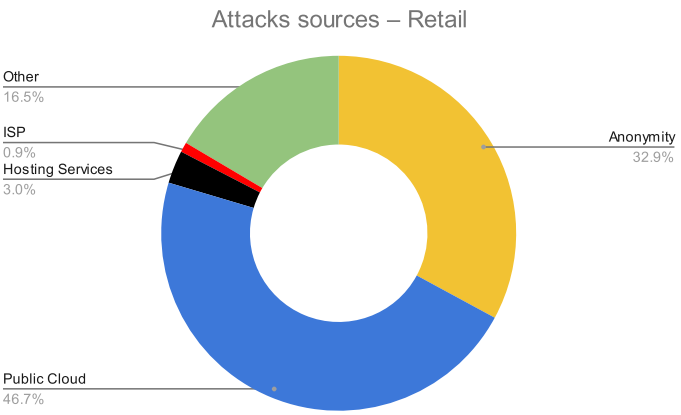
The discovery of the Log4j vulnerability, which can be used to perform unauthenticated remote code execution, has contributed to the increased popularity of RCE/RFI attacks, which accounted for 28% of attacks targeting both online retailers and other industries alike. Some of the malicious activities attackers can do when they are able to run code on a vulnerable eCommerce website server include installing malware to collect all payment information or other sensitive information, bring down the server, redirect traffic to other websites etc.

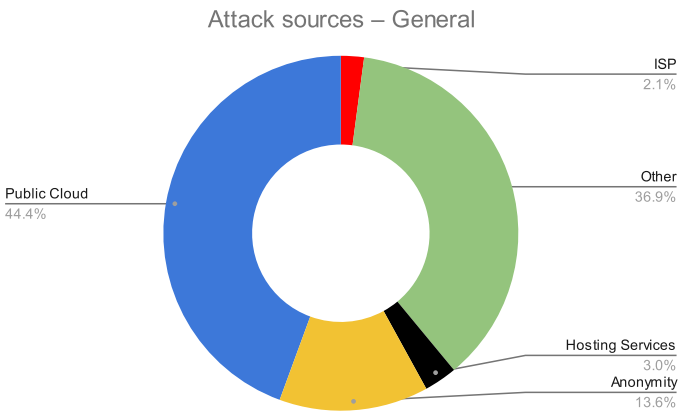
Similar to last year, the volume of attacks that targeted online retailers based on the type of attack was generally aligned with trends seen across all industries, with the top three attacks being the same.

Attackers go to great lengths to cover their tracks

One of the trends shaping the threat landscape is the rise in attack sophistication and intensity. Uncovering the source of attacks reveals another layer of this increasing sophistication.

The following charts represent the source of attacks as uncovered by the Imperva Threat Research team, comparing Retail and the general trend. While the public cloud remains the leading origin of attacks, it is impossible to miss the striking rise in popularity of attacks originating from anonymity frameworks (any frameworks that allow attackers to hide their true source; for example, anonymous proxies, TOR, and more). Attacks originating from anonymity frameworks targeting online retailers jumped from 3.5% last year to a whopping 32.9% this year, while attacks targeting other industries jumped from 1.6% to 13.6% from one year to the next. Anonymity frameworks enable attackers to cover their tracks while executing more elaborate types of attacks. Generally, attacks originating from the public cloud accounted for 44.4%, almost identical to attacks that targeted online retailers (46.7%).

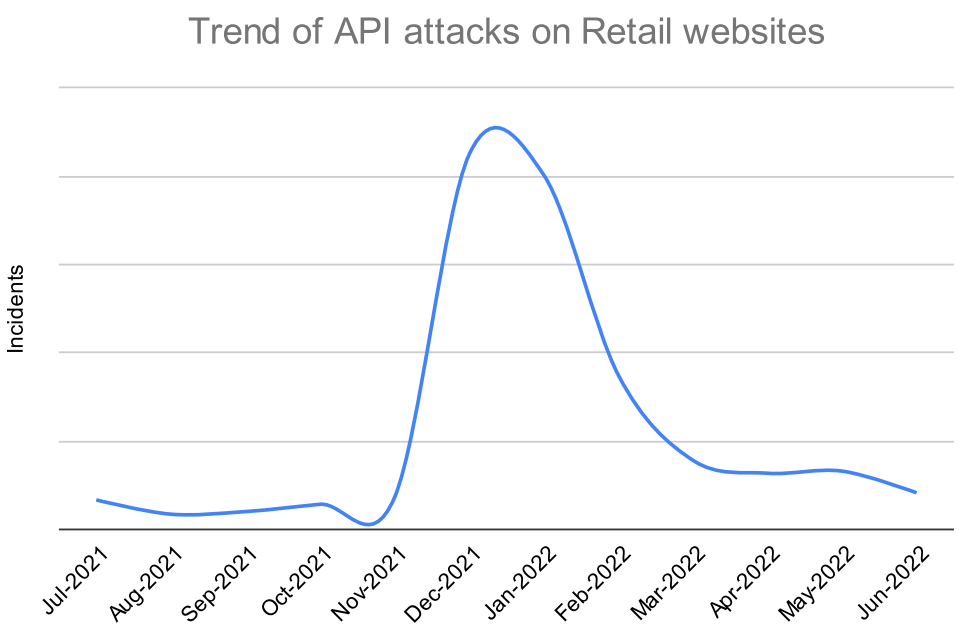




API attack trends

API Security is a key component of Imperva's Web Application and API Protection (WAAP) solution. WAAP monitors and mitigates attacks on our customers' many API endpoints. Analyzing the data collected by its sensors across those endpoints allows for a deeper look and enables a different perspective into the attacks carried out against online retailers over the past 12 months.

The graph below shows the monthly trend of attacks targeting APIs in the online retail industry. During the peak holiday shopping season, attacks increased by 35% between September and October, and another 22% in November, further exemplifying how attackers are targeting early holiday shopping.



It is hard to ignore the massive 92% spike in attacks seen in December and lasting through January of 2022. This is no coincidence — the increase in attacks is right in line with the discovery of the Log4j vulnerability. And although this vulnerability doesn't directly target APIs, the Log4j logging library is commonly used in Java-based APIs. During their scouring of the web for vulnerable websites, attackers will go through all possible endpoints, leading to an increase in the number of attacks on APIs too.

APIs account for a significant portion of traffic

Customers today engage with online retailers in various ways. In the past it was most common to use a computer with a web browser to shop online; today consumers have a vast array of devices capable of making purchases online. It could be anything from a mobile device to a refrigerator, a car, or a smart home assistant. To make all of this possible, a new architecture is required: Headless Commerce. Headless Commerce is a separation of the front-end and back-end of an eCommerce application[5]. It ensures websites work seamlessly and as intended between all devices and viewing formats.

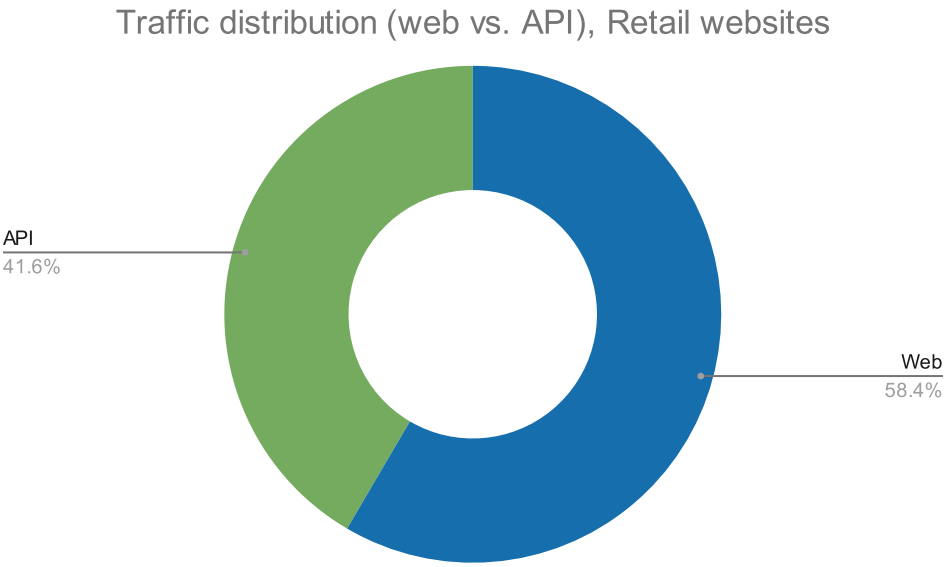
5 https://www.salesforce.com/blog/define-headless-commerce/

APIs are an essential component of this architecture.

This increase in usage of other platforms to make online purchases leads to an almost even split in traffic between the web and APIs, as API traffic accounts for 41.6% of all traffic to online retailers.

Of that API traffic, 12% of is to endpoints which hold sensitive data (credentials, license numbers, credit card numbers, social security numbers etc.) and 3-5% is directed to undocumented, or, Shadow APIs. Those are APIs that exist and are exposed publicly, but that the organization does not have inventoried or actively know about. These are some common use cases where this can occur:

- The API endpoint was deprecated but never removed
- A developer releases a new API endpoint, but does not document or inventory it
- A developer inadvertently makes a change which exposes non-public API endpoints to the public internet



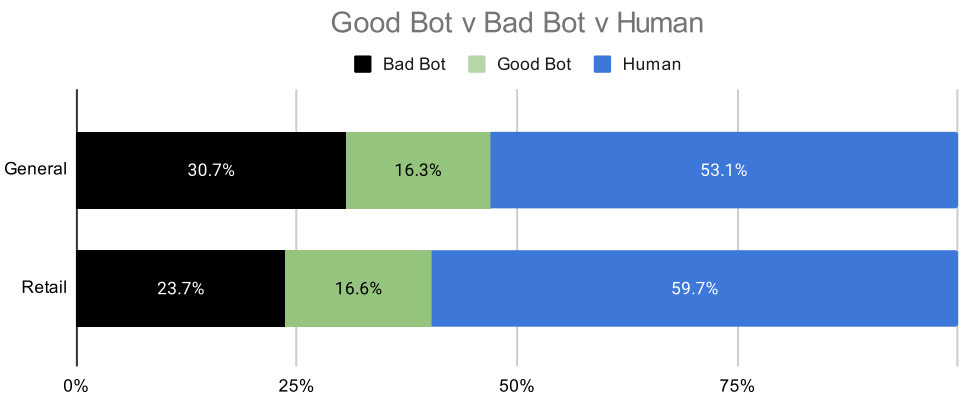
Bot attack trends

Imperva's market-leading Advanced Bot Protection allows businesses to dive deep into the most significant menace to online retailers: automated threats, also known as bad bots. As outlined in the 2022 Imperva Bad Bot Report, there are unique types of automated threats affecting the online retail industry. These include price scraping by competitors and third parties, content scraping, inventory fraud and scalping (Grinchbots, Sneakerbots, etc.), account takeovers, credit card fraud, and gift card abuse — to name just a few.

Advanced Bot Protection collects and analyzes data about bot behavior across websites, APIs, and mobile applications. This data allows Imperva to see how bad bots are used to attack online retailers in particular, and block the attacks accordingly.

Bots account for over 40% of traffic to retailers

While the ratio of bad bot traffic on retail websites has stayed relatively similar to last year, at 23.7%, legitimate user traffic has gone down (59.7%). Good bot traffic levels increased (16.6%), bringing the total bot traffic on retail websites to 40.3%. Despite their name, even good bots can be bad news for businesses. Good bots can skew web analytics reports, making some pages appear more popular than they actually are. In addition to that, they can also hamper conversion rates. Being able to intelligently separate traffic generated by legitimate users, good bots, and bad bots is essential for making informed business decisions. And although the ratio of bad bots on retail websites is lower than the general average (30.7%), it is also important to understand that a lower ratio of bad bot traffic doesn't mean they pose a lesser risk. The volume of bad bots doesn't necessarily align with their level of sophistication. For example, advanced bots are often able to achieve their goal while performing fewer requests than simpler bad bots.



Bot attacks are becoming more complex

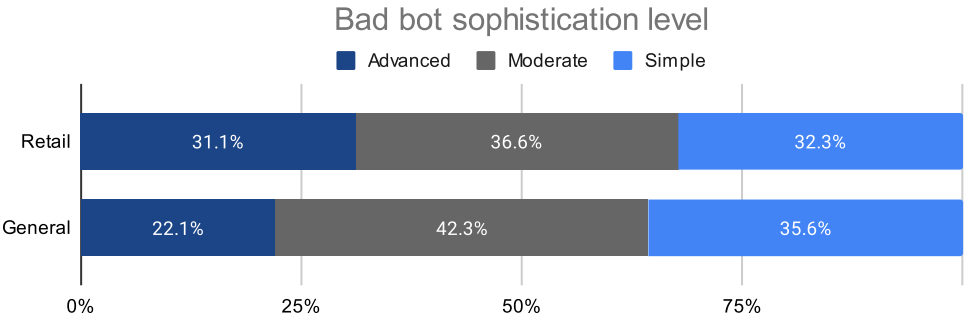
While bad bot traffic levels were higher in other industries compared to online retailers, the level of their sophistication is significantly higher in retail. Compared to last year, the sophistication level of bad bots targeting retail websites is on the rise. To better understand bot sophistication, Imperva created a classification system. Here's the best way to understand each class of bot:

EVASIVE BAD BOTS

A grouping of both moderate and advanced bad bots. They tend to cycle through random IP addresses, enter through anonymous proxies and peer-to-peer networks, and can change their user agents. They use a mix of technologies and methods to evade detection while maintaining persistence on target sites. They often choose "low and slow" tactics, which enable them to carry out significant attacks using fewer requests and even delay requests, allowing them to not stand out from the normal traffic patterns and avoid triggering rate-based security detection thresholds. This method reduces the "noise," or big traffic spikes generated by many bad bot campaigns.

- **Simple:** Bots that connect from a single, ISP-assigned IP address. They connect to sites using automated scripts, not browsers, and don't self-report (masquerade) as being a browser.
- **Moderate:** A more complex type of bot that uses a "headless browser" software, enabling them to emulate browser technology, including the ability to execute JavaScript.
- **Advanced:** These bad bots are capable of producing mouse movements and clicks that fool even advanced detection methods. These bad bots mimic human behavior and are the most evasive. They use browser automation software, or malware installed within real browsers, to connect to sites.

The fact that moderate and advanced bad bots are associated with more evasive attacks and that combined, they make up two thirds of bad bot traffic is a cause for concern. These bots are harder to detect and deter, and will wreak havoc without a proper bot management solution. Particularly alarming was the increase in advanced bad bot traffic, which accounted for 31.3% of all bad bot traffic to online retail websites, compared to 22.1% in all other industries. This is also a significant increase from 23.4% last year, implying to increasing sophistication of bot attacks targeting online retailers.



Bot attacks increased in November

During the 2021 holiday shopping season, advanced bot attacks increased 10% in October and another 34% in November. Amongst the many threats that bots pose to eCommerce, like account takeover and price scraping, inventory hoarding bots are highly prevalent during the holiday shopping season, earning themselves the infamous nickname – Grinchbots. From sneakers to gaming consoles and limited edition collector's items, these bots are sure to ruin holiday shopping for consumers unless stopped.

TERMS DEFINED

Scalping:

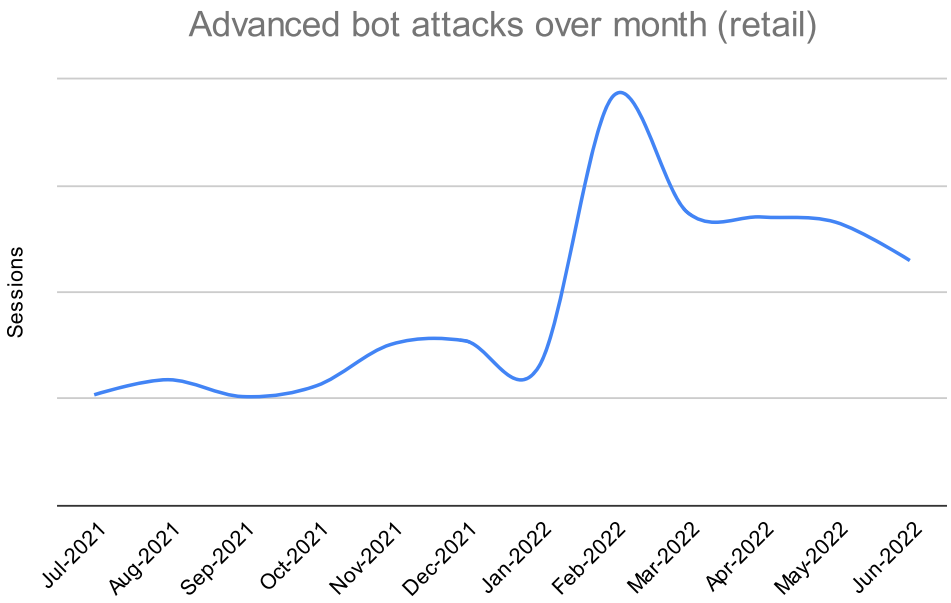
The use of bots to obtain limited-availability and/or preferred goods/services.

Grinchbots:

Variations of scalping bots designed to specially target limited availability, highly coveted holiday season

Bot activity following the events in Ukraine

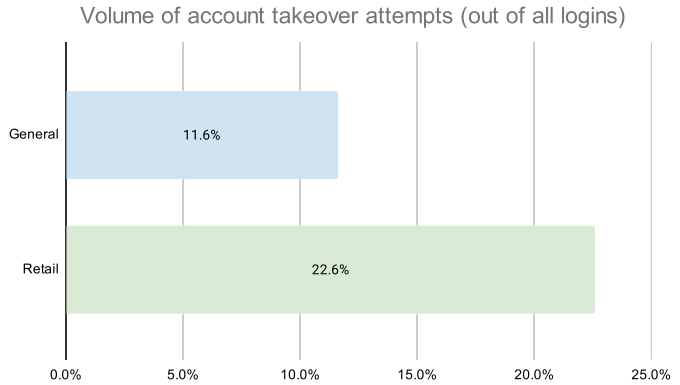
The war in Ukraine has sparked a new wave of attacks globally, which resulted in a 194% spike during February this year. In Ukraine specifically, the Imperva Threat Research team observed a 145% spike in automated attacks targeting web applications between February 24 and March 1, likely intended to disrupt services.

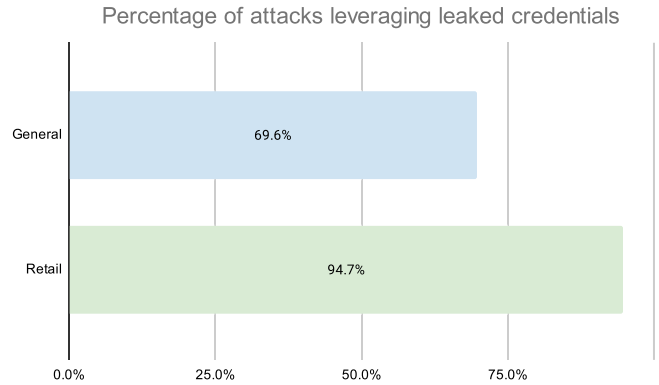


Account takeover fraud: a major risk for eCommerce

An account takeover (ATO) is an attempt by cybercriminals to take over users' accounts for malicious purposes. User accounts on online retail websites hold lucrative incentives for bad actors and fraudsters: saved credit card information, gift card balances, loyalty points, and other customer benefits.

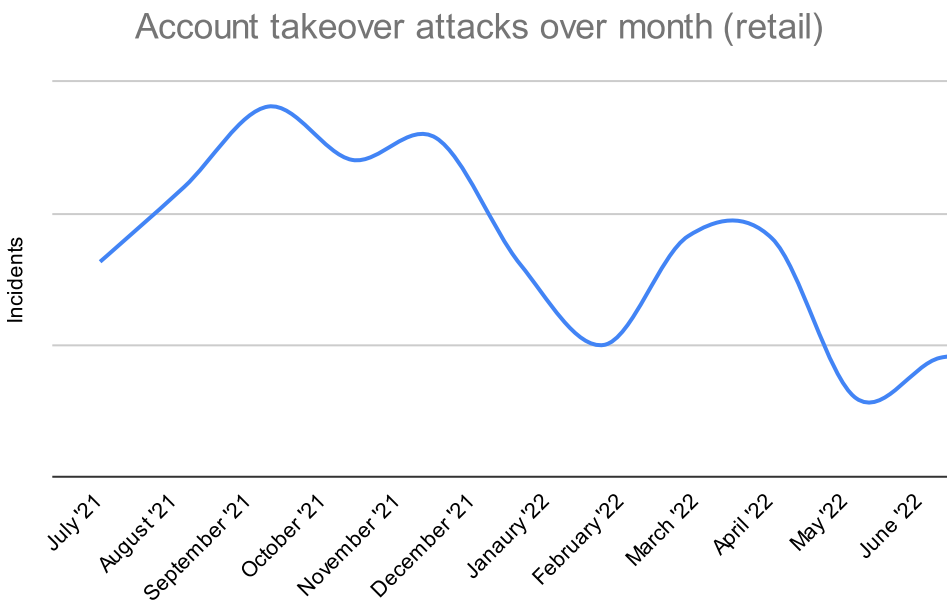
Compared to other sectors, online retailers experience a higher volume of account takeover attempts out of all logins. Almost a quarter (22.6%) of all logins on retail websites are malicious account takeover attempts compared to just over a tenth (11.6%) in all other industries. Of these, hackers performing credential stuffing techniques have used considerably more leaked credentials in ATO attacks targeting online retailers (94.7%) than they did in general (69.6%)





Account takeover attacks target early holiday shopping

In synchronization with early holiday shopping, account takeover attacks increased by 27% as early as August only to further increase in September by another 23%. Despite a slight decrease of 12% in October, threat levels remained high, as attacks increased again in November, this time by 6%. A 57% peak in attacks was recorded in February following the war in Ukraine, lasting throughout March.



DDoS attacks

The goal of an application layer DDoS attack, also known as a layer 7 DDoS attack, is to bring down a server by exhausting its processing resources using a high number of requests. It is measured in requests per second (RPS) — the number of processing tasks initiated each second. Such attacks are executed by DDoS botnets that can establish a TCP handshake and interact with a targeted application. These attacks are different from volumetric DDoS attacks, which manipulate lower-level network protocols. DDoS attacks cripple infrastructure, and may cause downtime leading to losses of hundreds of thousands of dollars per hour.

AVERAGE DOWNTIME PREVENTED PER RETAILER DURING HOLIDAY SHOPPING SEASON:

70 HRS

AVERAGE DOWNTIME PREVENTED PER RETAILER DURING BLACK FRIDAY WEEK:

13 HRS

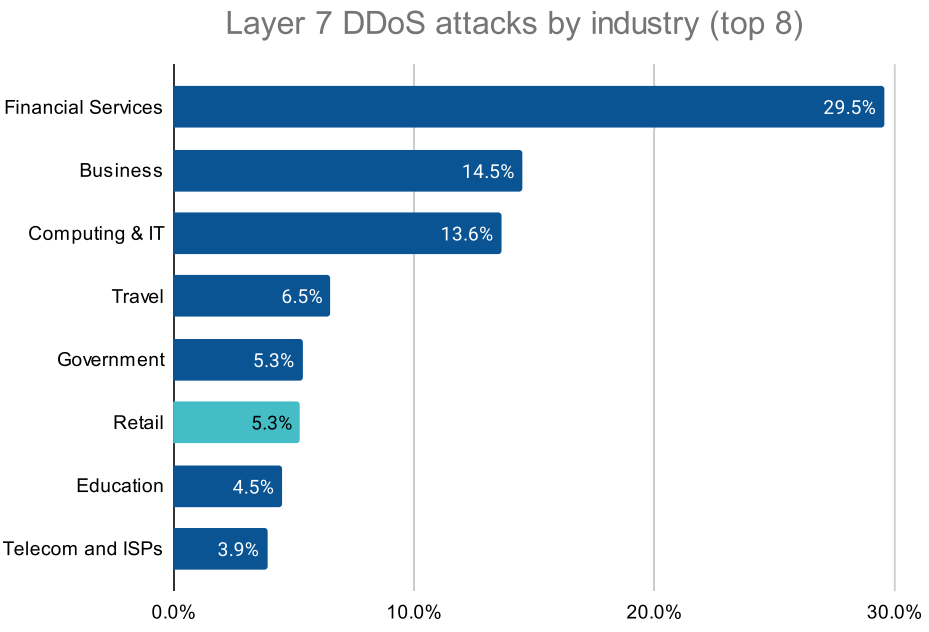
DDoS attacks are reaching new records in rate, frequency, and complexity

This year, a new trend is emerging in which DDoS attacks reach and maintain extremely high rates for several hours, as opposed to only a few minutes at most. Using sophisticated techniques including HTTP pipelining and multiplexing, attackers broke Imperva records at a rate of 3.9M rps with 25.3 billion requests in 5 hours in a single attack, which was launched from a massive botnet of 48,480 different IPs. In a separate attack in the same Spring quarter of 2022, the highest rate was detected at 10M rps using only 12K IPs!

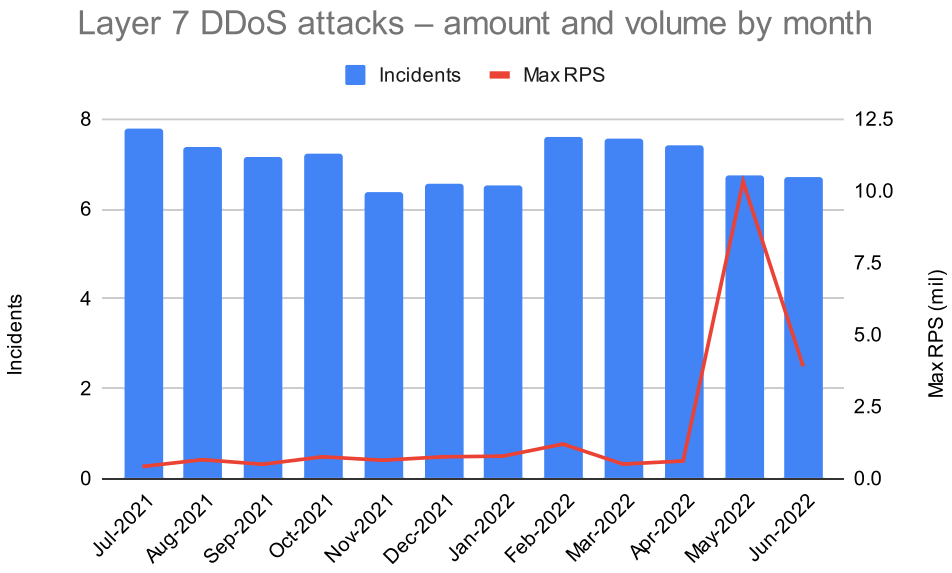
Websites should also prepare for repeat attacks, as in 2022 55% of websites hit by an application-layer DDoS and 80% hit by a network-layer DDoS were attacked again. In most cases, websites were attacked again within 24 hours.

Finally, online retailers should expect to see bigger and stronger DDoS attacks than before. The number of attacks larger than 100 Gbps doubled from Q1 to Q2 2022, and attacks larger than 500 Gbps/0.5 Tbps increased by as much as 287%.

Breaking down the distribution of application layer DDoS attacks by industries, we can see that online retailers were targeted by 5.3% of all attacks recorded and mitigated by Imperva over the past year.



The chart below represents the average number of layer 7 DDoS attacks an online retailer faces per month (blue bars), as well as the average of maximum requests per second recorded on each attack (Max RPS). This past year, the number of monthly attacks has been steady, averaging 7 per month. However, the trend of DDoS attacks breaking new records didn't skip online retailers, as can clearly be seen by the spike in Max RPS during May. This is a case of quality over quantity — all it takes is one well-timed overwhelming attack to cause devastating results for businesses.



Client-side attacks

Last, but certainly not least, client-side attacks continue to wreak havoc across websites in all industries, with specific focus on eCommerce. Similar to other threats, client-side attacks too have evolved. This evolution brings about a new era of highly stealthy attacks that are harder to uncover and are devastating in their results. Online retailers should pay close attention to this threat, as it is one of the biggest risks to the industry for the following reasons:

1. The abundance of JavaScript-based services that are practically used in 98% of websites today[6]. Examples of such services could be anything from a Live-Chat for customer service, eCommerce platforms, payment gateways, and more. This profusion is a fertile ground for attackers looking for exploits in third-party code.
2. The amount of personal data that is either stored in them or transferred through them. eCommerce sites rely heavily on online forms. They usually have a login page, as well as a checkout form. This makes them a perfect victim for attacks designed to steal data from these website forms.

Client-side attacks, often referred to as Magecart or Formjacking attacks, are online skimming techniques. This type of attack involves injecting malicious JavaScript into first-party code or the code of third-party services (the software supply chain) used on legitimate websites. Because JavaScript executes on the client-side, it enables an attacker to collect sensitive personal information directly from the client each time a customer enters their information into a form, similar to how a skimming device would steal data on an ATM or gas pump.

TERMS DEFINED

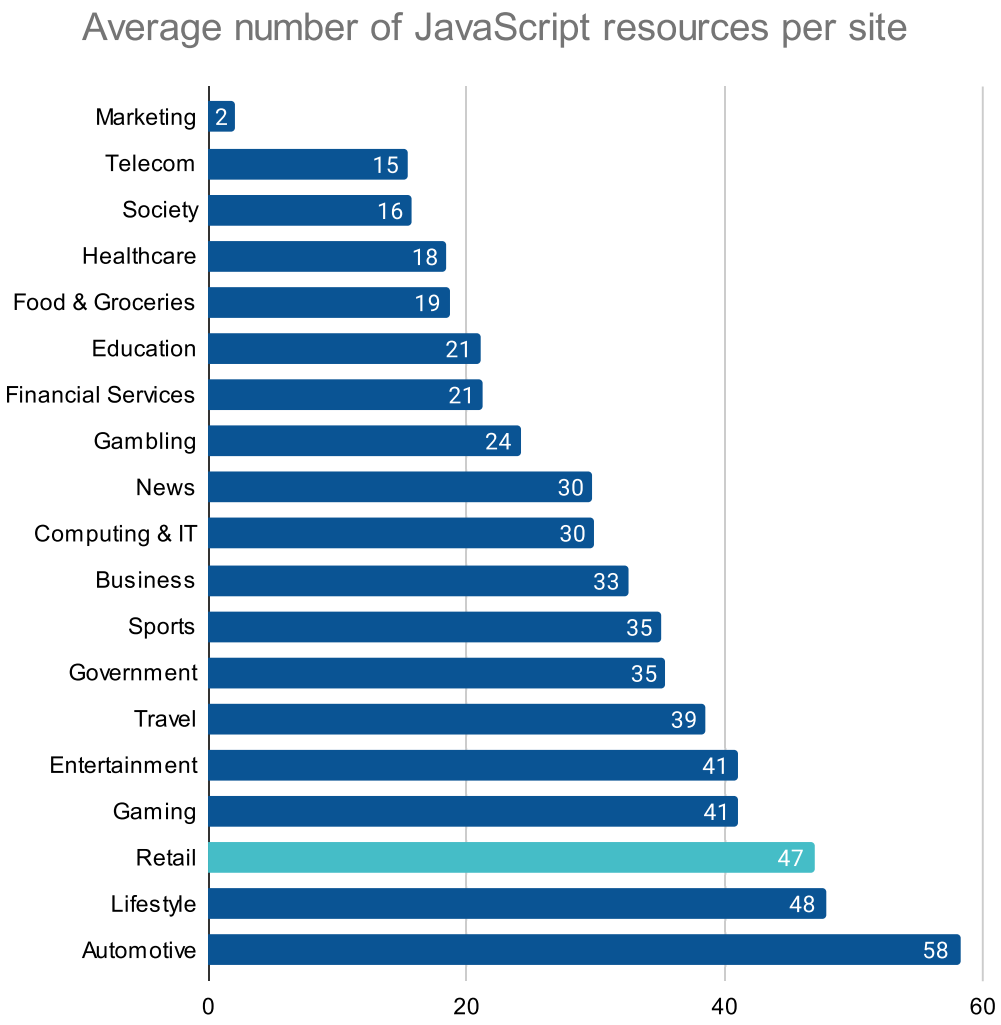
Formjacking:

The use of malicious JavaScript code to hack a website and take over its form pages to collect sensitive user data. By doing so, hackers can steal credit card details and other information from payment forms and checkout pages. It can also be used to steal login credentials from login

6 https://w3techs.com/technologies/details/cp-javascript

Online retailers are at high risk of being targeted by client-side attacks

Java Script is everywhere. Even more so on retail websites. On average, there are 47 JavaScript based resources executing on the client-side at any given moment, putting the industry at a very high risk of Magecart attacks that threaten to steal customers' most sensitive data.



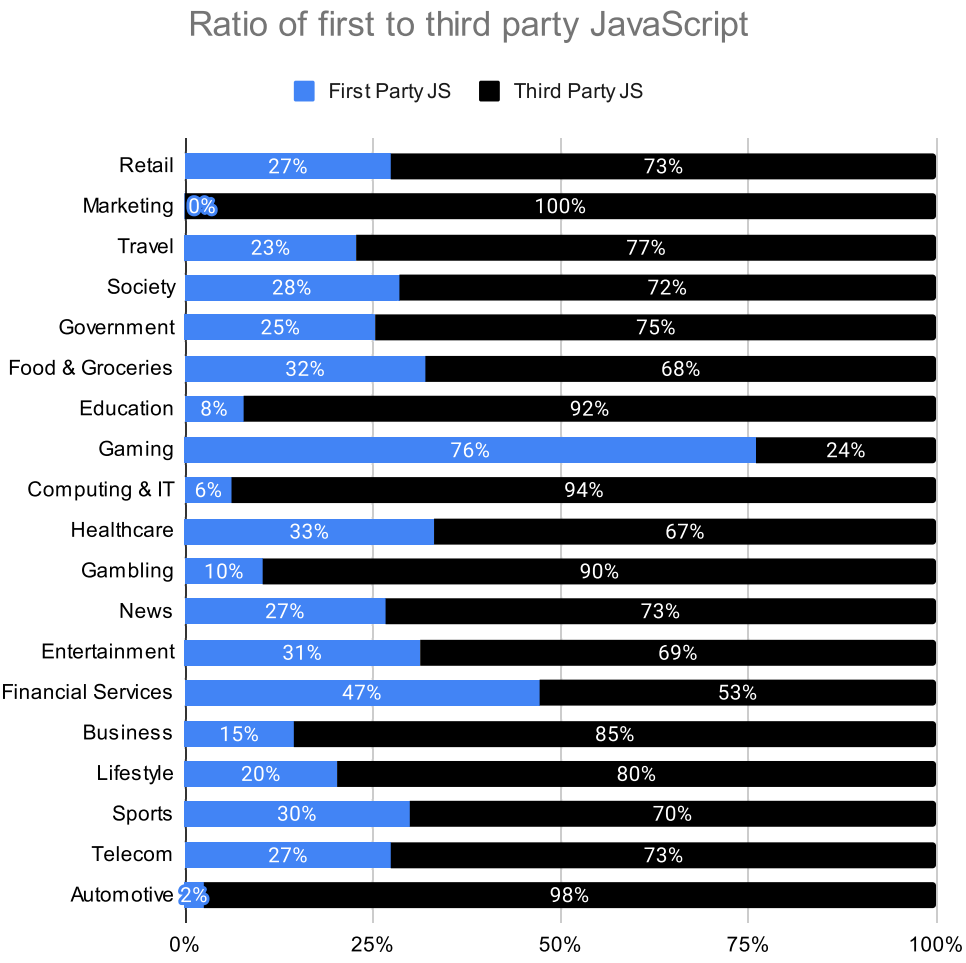
Most eCommerce JavaScript is third-party based

The most sophisticated attackers today understand that websites are based on a supply chain of code, many of it originates from third parties. These attackers continue to seek ways to steal sensitive information like credit card numbers and login credentials by exploiting vulnerable code to plant online skimmers.

The chart below offers an insight into the ratio of first vs. third party JavaScript based services per industry. We can see that 73% of JavaScript-based services on eCommerce websites are third-party services. That means that the majority of JavaScript based services on retail websites are at risk of being compromised by attackers to steal data.

First-party services are scripts that are included in separate (.js) files, yet are located on the same domain name as the HTML page. For example, when browsing example.com, all the scripts under example.com domain are first-party scripts.

Third-party services are scripts that are included in separate (.js) files, yet are located on another domain. For example, if you are browsing example.com, all the scripts under any domain other than example.com are third-party.



Recommendations ahead of the holiday shopping season

While a lot of advice could (and should) be given to consumers ahead of the biggest shopping event of the year, this report focuses on the other side of the (digital) coin: retailers. Just as shoppers are required to be aware of the risks associated with online shopping, retailers must remain vigilant as well. They must stay ahead of cyber risks that are threatening the integrity and continuity of their business, as well as the safety of their customers and their most 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 favorite times for attackers to launch DDoS attacks aimed at online retailers. And with the recent trend of DDoS attacks lasting much longer than in years before, attacks are expected to reach record-breaking volumes while maintaining extremely high rates. It is recommended that you stress-test your infrastructure regularly, and even more frequently before times of anticipated high traffic. It is extremely important to make sure you are properly protecting against DDoS attacks across all web resources, including DNS. Consider implementing a waiting room queueing system that will help ensure site performance and maintain a positive customer experience.
2. **Marketing and eCommerce campaigns are highly likely to become targeted by bots.** For example, bad actors may employ bots to immediately buy up almost all stock for a highly anticipated product launch 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 angry at the retailer, which has a potential to damage brand reputation. Make sure that you are prepared to handle the increased volume of traffic that is going to include a high ratio of evasive bots. These will be trying to scoop up the inventory, denying it from legitimate customers, all while hampering website performance, skewing analytics, and causing severe brand damage.
3. **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 capitals, numbers, symbols, etc. While forcing users to change their passwords on a regular basis could be a bit too much, it is still a good idea to at least suggest they do so. Implementing Multi-factor authentication (MFA) and encouraging use of it by customers is highly recommended. Additionally, be aware of big data breaches that occur from time to time and communicate to your users that it is recommended they change their passwords after a breach has occurred. Account takeover attacks tend to increase by up to three times after a big data breach has occurred, so you should also expect an increase in bot traffic to your login pages. Make sure you have a bot mitigation solution with enhanced account takeover prevention capabilities. Such capabilities include detection and mitigation of credential stuffing attacks, detection of malicious intent from successful logins, and the ability to discover which of your users' credentials have been compromised online.
4. **Protect your existing website functionalities and make sure newly added ones are safe, too.** Some website functionalities are highly exploitable by bad bots. For example, the login functionality opens up the possibility of Credential Stuffing and Credential Cracking attacks to occur. Adding a checkout form increases the chances

of credit card fraud (Carding/Card Cracking). Adding gift card functionality invites bots to commit fraud. Make sure that these pages are properly protected by a bot mitigation solution and have a more strict ruleset.

5. **Take inventory of all your client and server-side JavaScript-based services.** 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. Targeting eCommerce sites with a lot of transactions, especially during times of high traffic, is an ideal strategy for attackers. Consider using a specialized tool that can help in identifying and assessing the risks of each JavaScript-based service, as well as enabling you to block unauthorized ones from executing.
6. **Stay ahead of the scammers.** The holiday shopping season is a perfect time for scammers to launch phishing attacks where they might by masquerading as your brand, sending fake emails that offer coupons and gift cards. Keep abreast of any phishing campaigns and make sure to alert your customers of any suspicious campaign making use of your brand. Additionally, you should be on the alert for possible phishing attacks targeting your employees, as they are the way for an attacker into your organization.

About Imperva

Imperva is the cybersecurity leader whose mission is to help organizations protect their data and all paths to it. Customers around the world trust Imperva to protect their applications, data, and websites from cyber attacks. With an integrated approach combining edge, application security, and data security, Imperva protects companies through all stages of their digital journey. The Imperva Threat Research team and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy and compliance expertise into our solutions.

Imperva for Retail:

With more consumers relying on online shopping, cyber security challenges are increasing. Imperva protects your customers' data and all paths to it so retailers can focus on growing their business rather than recovering their reputation due to breaches or downtime.

- Imperva offers best-in-class cybersecurity solutions from the edge to the database to protect your most valuable assets and is positioned as a leader in the 2022 Gartner Magic Quadrant for Web Application & API Protection.
- Having a robust Web Application Firewall is a specification of the PCI-DSS regulation. Imperva WAF directly addresses this requirement by accurately detecting threats and protecting web based transactions. Additionally, Imperva Client-Side Protection blocks any unauthorized JavaScript services or changes to a web page to prevent account takeover and the theft of payment data – without impacting the customer experience.
- Imperva Cloud Security solutions secure your cloud environment with a complete solution stack that protects your applications, APIs, and databases, helping you stay protected without the risk of a breach or disruption to service.
- Imperva Advanced Bot Protection protects your websites, mobile applications, and APIs from automated threats without affecting the flow of business-critical traffic.

Contact Imperva to see how we can help you secure your web apps and data.