imperva

REPORT

# The State of Security Within eCommerce 2021

# Contents

# Introduction

**The Imperva State of Security Within eCommerce 2021 Report analyzes the latest cybersecurity threats affecting the eCommerce industry.**

The ongoing global pandemic has accelerated eCommerce growth by four to six years according to Adobe[1], pushing more consumers online. And even with physical stores slowly re-opening and more people getting vaccinated, growth is still predicted, albeit at a steadier rate. Following a 25.7% surge during 2020, to $4.213 trillion, eCommerce sales worldwide are expected to climb a further 16.8% this year, to $4.921 trillion[2]. That growth puts an already highly targeted sector by cyber threats at an even greater risk.

In this report, we'll cite a wide range of data mined by Imperva Research Labs, 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.

SURGE IN ECOMMERCE SALES WORLDWIDE IN 2020

**25.7%**

EXPECTED INCREASE IN ECOMMERCE SALES WORLDWIDE FOR 2021

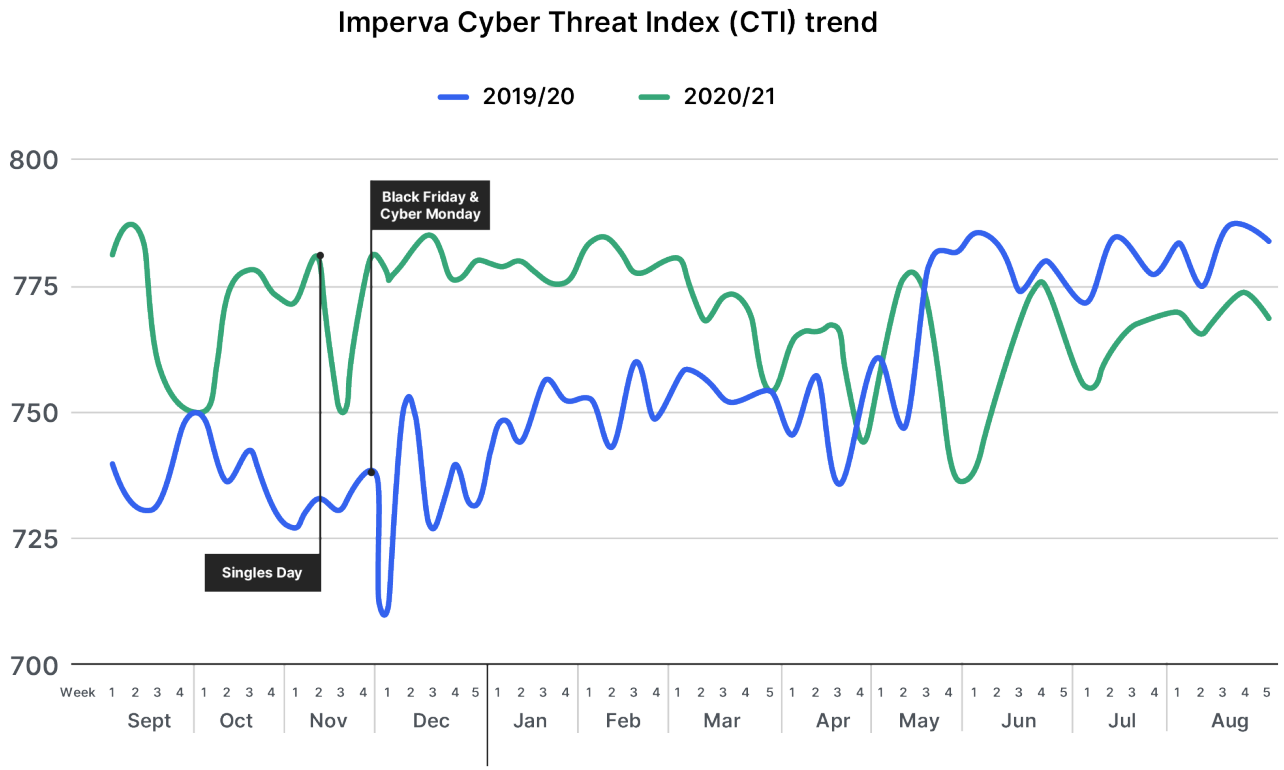
**16.8%**

[1] https://www.forbes.com/sites/johnkoetsier/2020/06/12/covid-19-accelerated-e-commerce-growth-4-to-6-years/?sh=f2b9700600f
[2]https://www.emarketer.com/content/global-ecommerce-forecast-2021

# Executive Summary

## Cyber threat levels remain high

Cyber threats remain a significant challenge for the retail industry, months after the global pandemic served to accelerate its digital transformation. Based on a 12-month analysis by Imperva Research Labs, threat levels remain elevated compared to previous years. As seen in the chart below, threat levels from August 2020 to March 2021 have been significantly higher than those of the previous year (blue line). The lines converge around April, when in 2020 the impact of the global pandemic has began to take effect. While attacks during the second half of 2020 are elevated over the current 2021 levels, there is still reason for caution and for organizations to be on alert.



It is interesting to see the peak in attacks during the week leading to Singles Day on November 11 - a major shopping day throughout Asia. Threat levels then peaked again during Black Friday identifying the start of the holiday shopping season in the US.

The 2021 holiday shopping season is fast approaching. Looking at all the security concerns detailed in this report, and the events of previous years, we predict that security threats will rise again in November 2021 as shoppers flock online for a variety of online shopping events, from Singles Day to Black Friday and Cyber Monday.

**TERMS DEFINED**

## Account Takeover:

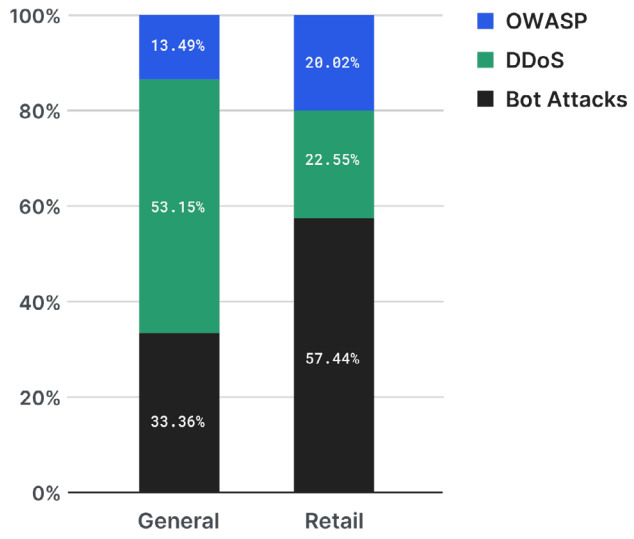
Account Takeover is a form of identity theft in which bad actors gain illegal access to user accounts belonging to someone else. This is usually achieved using brute force login techniques such as Credential Stuffing, Credential Cracking or Dictionary attack.

## Bots are the most common threat to eCommerce

Over a half (57%) of all attacks recorded on retail websites were carried out by bots in 2021, a notable difference in comparison to all industries (33%). Bots are a common presence on retail websites, due to their many use cases -- like user account takeover, price and content scraping by competitors and third-parties, inventory abuse by scalpers, credit card fraud, and more. The global pandemic created a perfect condition for bad bots: more people shopping online than ever before. This resulted in more user accounts being created, and more funds attached to them - a strong incentive for bad actors looking to execute account takeover. Alarmingly, a third of all login attempts on eCommerce websites have been account takeover attempts.

One particular disruption that's had a ripple effect across the retail industry is the ongoing global chip shortage. Essentially, the shortage in semiconductor chips is slowing production rates for many highly coveted electronics. Enter scalpers and their inventory hoarding Grinchbots. As demonstrated last holiday season, bots took advantage of scant supplies and created frustration for consumers globally. Imperva Research Labs recorded a massive 788% increase in bad bot traffic to retail websites globally between September and October 2020, just as pre-orders for next generation gaming consoles were launched. As more people rely on online shopping, and the demand for limited-quantity items remains high, bad bots will be a disruptive force again during the holiday shopping season.

**Attack distribution by type**




**TERMS DEFINED**

### Account Takeover:

Account Takeover is a form of identity theft in which bad actors gain illegal access to user accounts belonging to someone else. This is usually achieved using brute force login techniques such as Credential Stuffing, Credential Cracking or Dictionary attack.

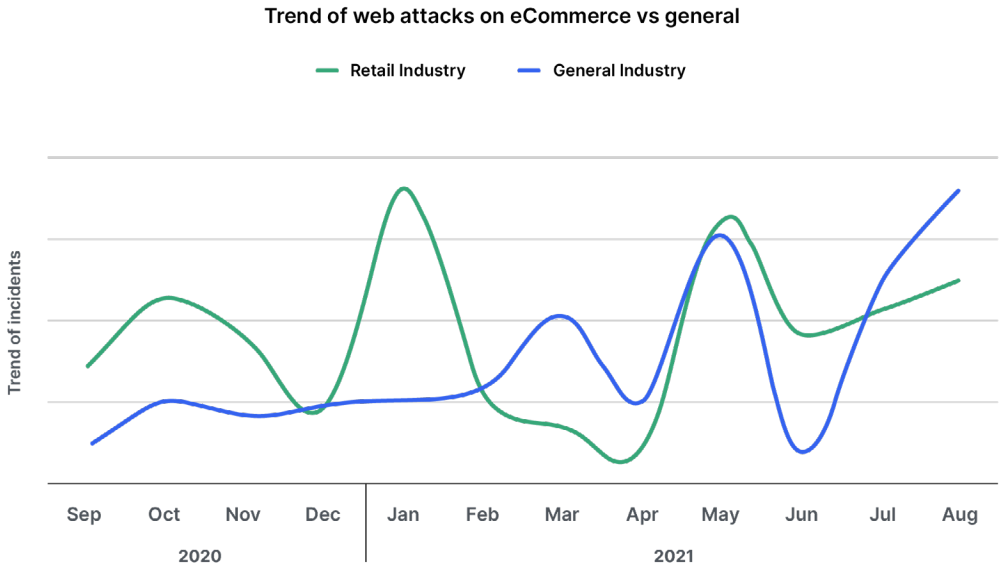
# Website attack trends

This section of the report focuses on web application attacks as defined by the Open Web Application Security Project (OWASP). The insights are informed by data analyzed by the Imperva Cloud Web Application Firewall, and the more than 30 million web application attacks and trillion HTTP requests the product analyzes monthly.

## The trend of web attacks didn't follow previous years

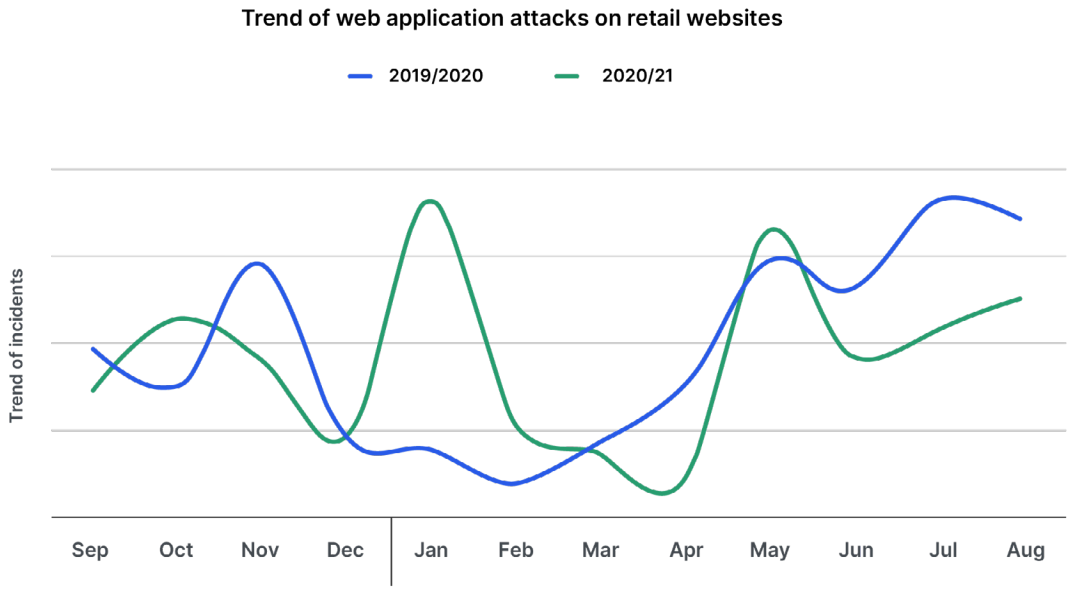
The following graph compares the trend of web application attacks against online retailers to the overall number of attacks in the form of incidents per month.

While the trends are mostly similar, the profile of attack traffic on eCommerce websites is characterized by unique spikes, like the one in January, possibly due to end of year or New Year promotional sales. Additionally, attacks on eCommerce greatly surpass the general trend line throughout the end of the calendar year. One of the causes for the early peak in attacks during October instead of November is that some of the most sought-after holiday presents were available for online purchase starting in October. The spike around May coincides with an overall increase in global shopping around that time[3], illustrating that bad actors target key periods when shoppers are most active.




[3] https://www.salecycle.com/blog/stats/when-are-people-most-likely-to-buy-online/

When comparing the trend of attacks to that of the previous year, we learn that 2021 is characterized by more sporadic peaks in attacks, rather than following a somewhat predictable trend like the ones we've seen in past years. 2020 saw a unique (and large) rise in attacks, but they mostly remained elevated and the peaks were less noticeable compared to 2021.

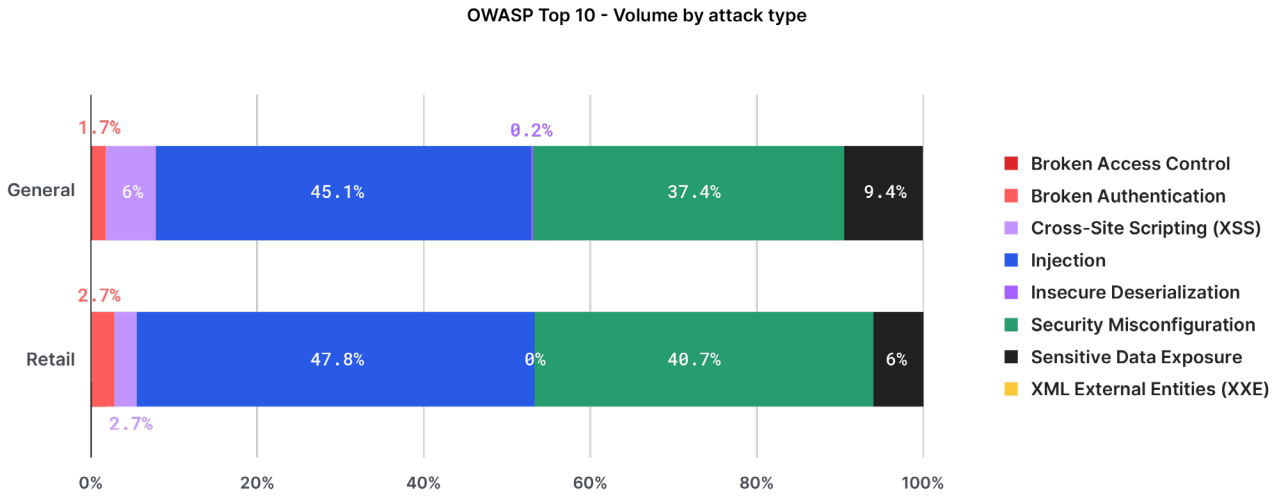


## Top three web application attacks

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

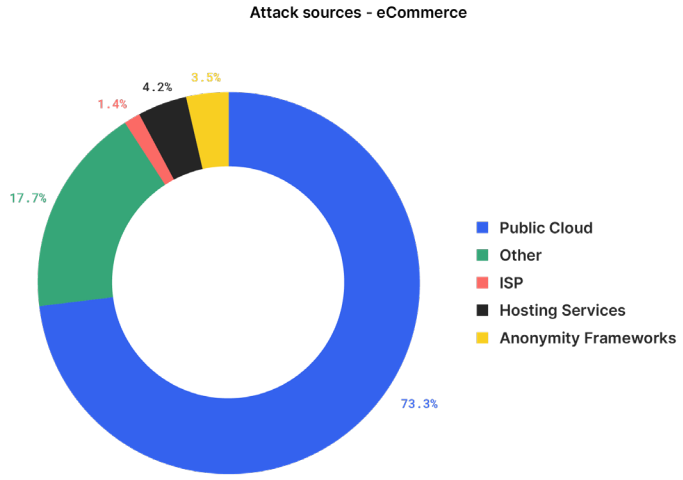
| | ATTACK NAME | % OF ATTACKS | DESCRIPTION |
|---|---|---|---|
| 1 | Data Leakage | **31.3%** | Data leakage falls under the OWASP category A3:2017-Sensitive Data Exposure. Instead of directly attacking crypto, attackers steal keys, execute man-in-the-middle attacks, or steal clear text data from the server, while in transit, or from the user's client, e.g. browser. A manual attack is generally required. Previously retrieved password databases could be brute-forced by Graphics Processing Units (GPUs). |
| 2 | RCE/RFI | **19.3%** | In an RCE (remote code execution) attack, hackers intentionally exploit a remote code execution vulnerability to run malware. An RFI (remote file inclusion) attack targets vulnerabilities in the web application to include malicious code from a remote server. |
| 3 | Path Traversal/LFI | **13.4%** | A path traversal attack aims to access files and directories that are stored outside the web root folder. This attack is also known as "dot-dot-slash", "directory traversal", "directory climbing" and "backtracking". |

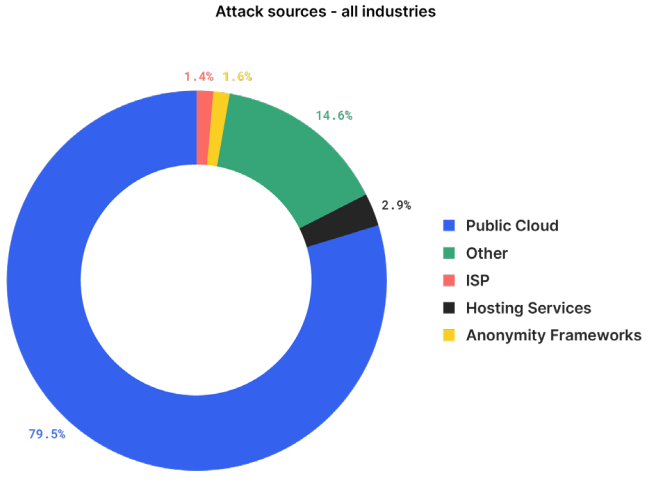
Taking a closer look at the volume of attacks on eCommerce based on the type of attack, it is aligned with trends seen across all industries. However, retail sites experienced slightly higher volumes of Data Leakage attacks - 31.3% compared to 26.9% in all industries, as these sites usually have access to a host of valuable data. RCE/RFI (19.3%) and Path Traversal (13.4%) were slightly less common compared to all industries (21.6% and 14.7%, respectively).



## Public cloud is the main source of attack traffic to eCommerce

In addition to understanding the specific attack vectors, Imperva Research Labs also uncovered the source of the attacks - comparing the retail industry to all other industries. Of the identifiable sources, a public cloud service is used for the majority of requests in attacks across all industries (79.5%). A similar picture could be seen in attacks made specifically in eCommerce, where public cloud is the source of the majority of attacks (73.3%). Hosting services (4.2%) and anonymity frameworks (3.5%), while less common, are still more popular in eCommerce than in all industries. The reason for this may be due to this enabling attackers to cover their tracks while executing more elaborate types of attacks.



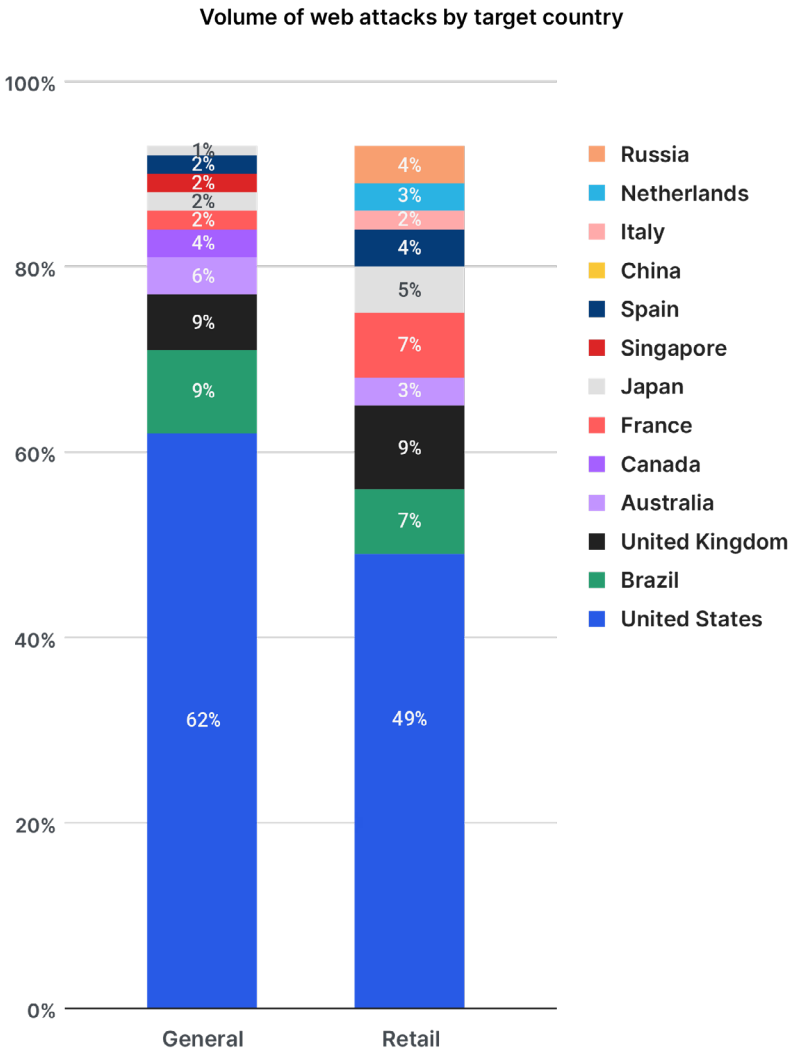



## The United States is the top targeted country by web attacks

The majority of web attacks in the last 12 months targeted websites based in the US (49%). The next three most popular targets—UK, France, and Brazil, respectively—lag statistically behind. These figures are largely consistent with attacks across all industries, with the US. experiencing the highest number of overall attacks (62%).

TARGETED WEB ATTACKS TOWARDS WEBSITES BASED IN THE US IN THE LAST 12 MONTHS

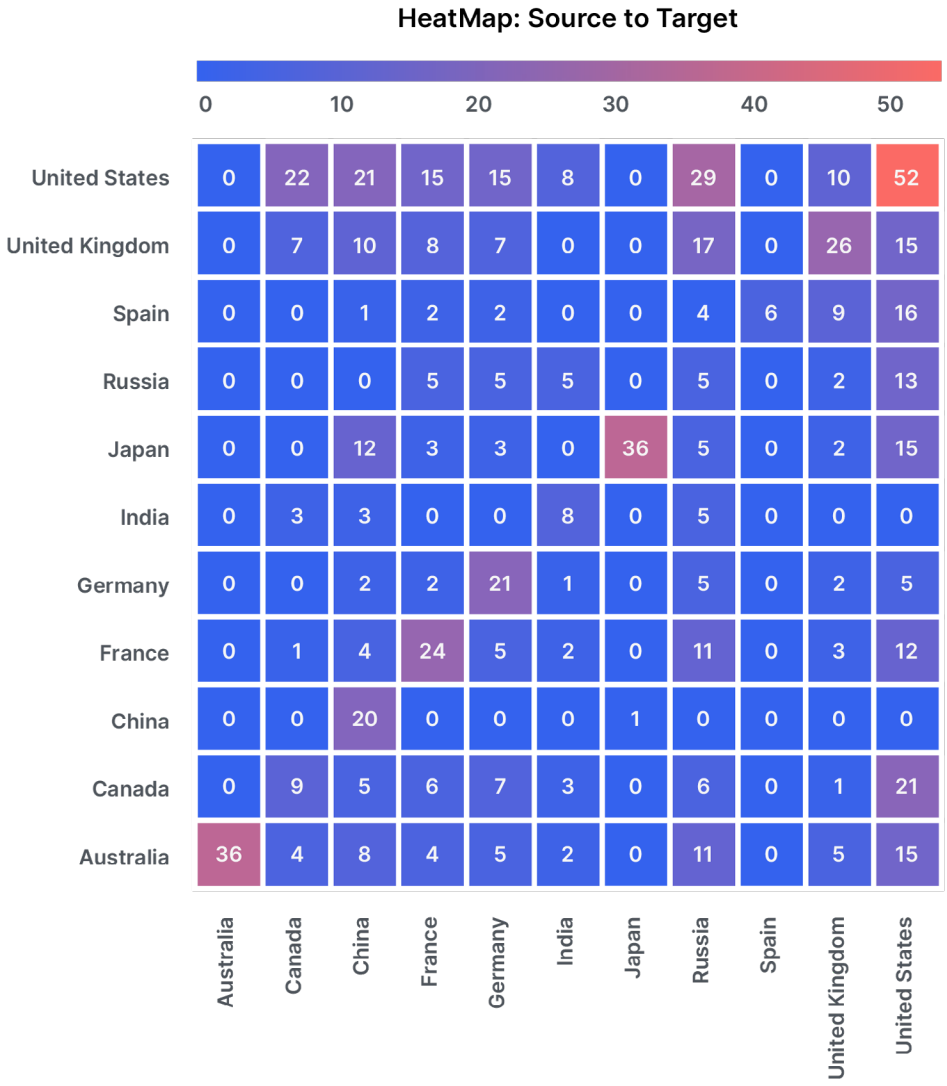
**49%**



The heatmap below uses a comparative score that is based on millions of incidents recorded monthly by the Imperva Web Application Firewall, to make it easier to compare and analyze. Looking at it, we can see, in most cases the majority of the attacks carried out on a particular country's online retailers were carried out from within that same country. For example, almost a third of the attacks experienced by targets in the US were launched from the US (29.5%).

Contrary to this, Russian-based attacks were more likely aimed at US targets than on targets in their own country. The majority of these attacks were RCE/RFI (41.6%) and Data Leakage (32.7%). This is also the case for China and even Canada. Meanwhile, threat actors in Australia, Japan, and the UK appeared to mostly target their own respective country's online retailers.

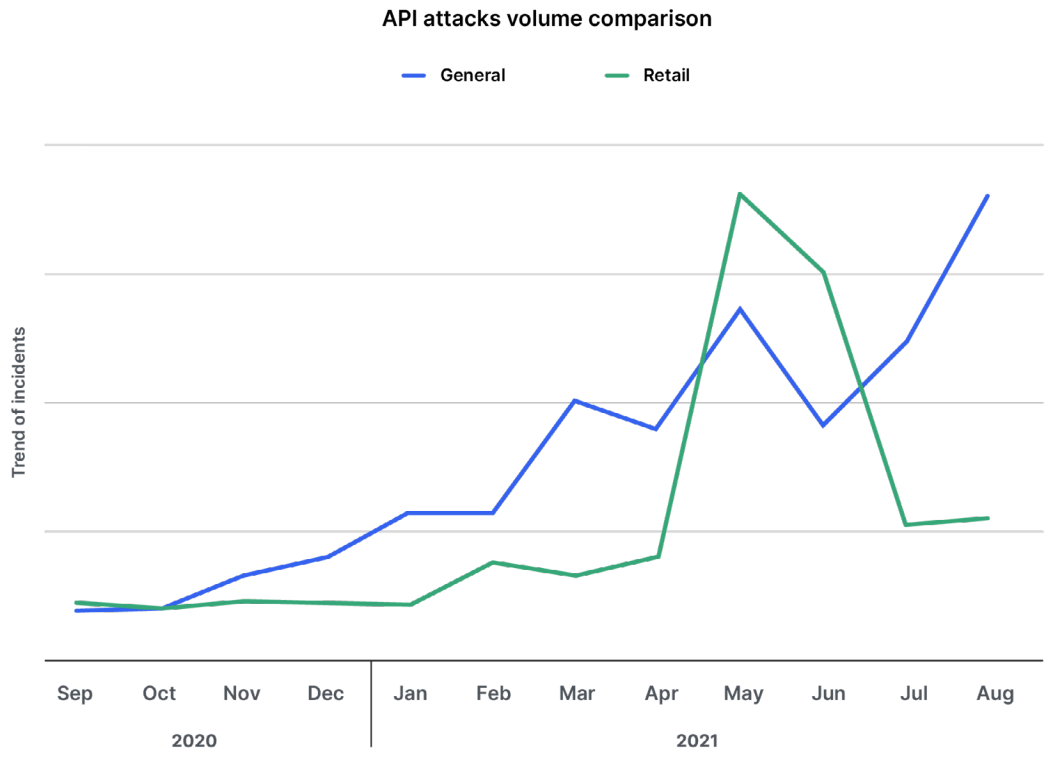
It's important to note that the data indicates only the location from which the attack was launched, and not necessarily the location of the attacker.



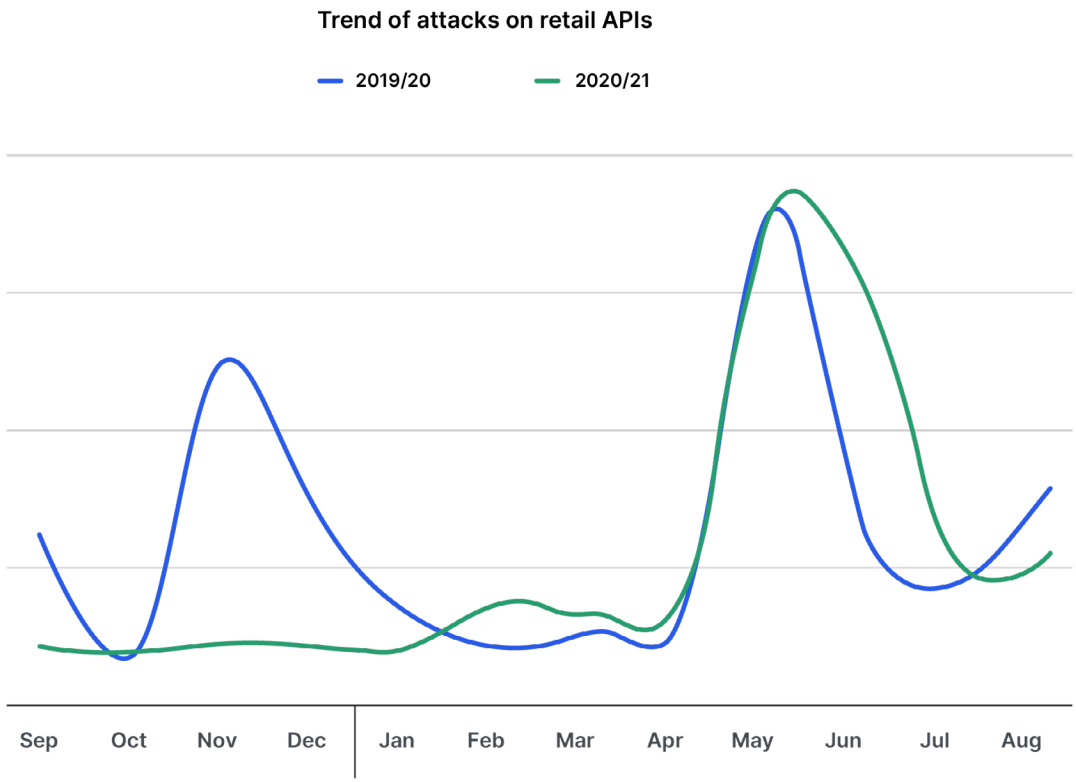
# API attack trends

Imperva Cloud WAF isn't the only source of data that can provide valuable insights into the past year's attacks. A key component of our application security suite, Imperva API Security, monitors and mitigates attacks on our customers' many API endpoints. Taking a deeper look at the data, it helps us paint another detailed – yet very different – picture of the attacks carried out against online retailers over the last 12 months.

The graph below shows the trend of attacks targeting APIs in the retail industry (green trend line), compared to all industries (blue trend line). API attacks on the retail sector have been slightly less common this year than on other industries, surpassing the general trend line during the late April - June period. As mentioned previously, there is an overall increase in global shopping around that time, possibly due to multiple shopping events taking place around the globe.

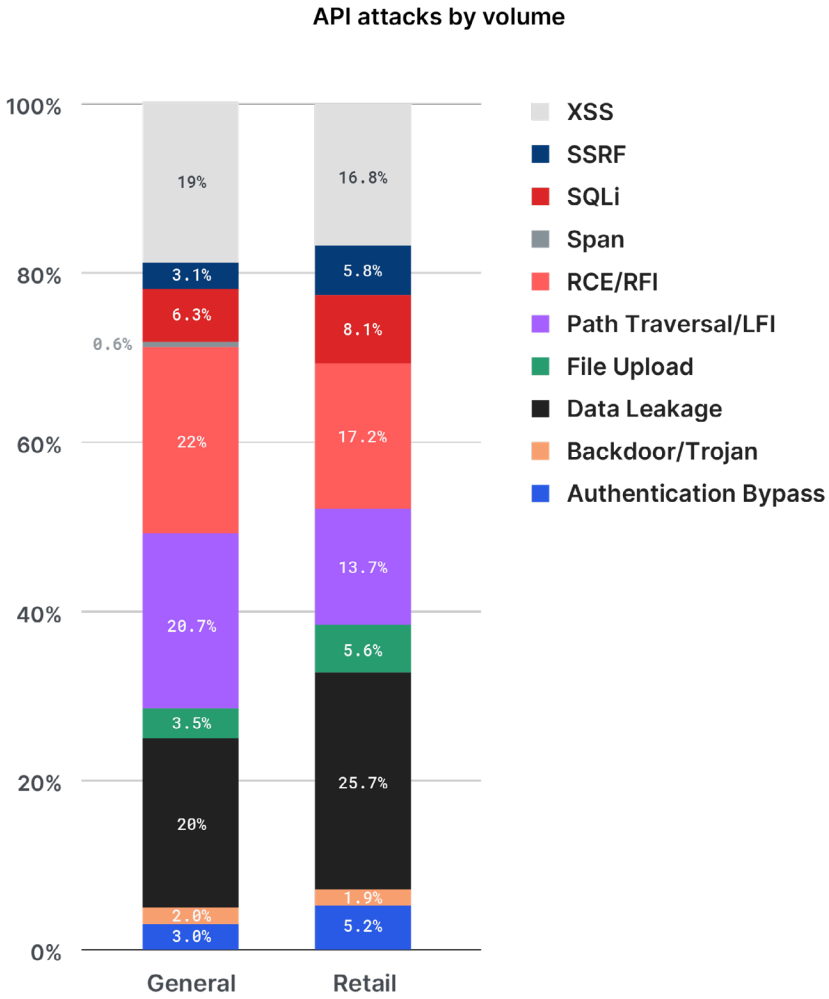


When we compare the trend of API attacks in eCommerce to last year, we can see a different trend. Interestingly, there was no peak during the 2020 holiday shopping season compared to 2019. This could be because the pandemic has changed shopping patterns, making them less predictable.



## Data Leakage tops API attacks on retail

The following graph illustrates the distribution of attacks that were targeting APIs specifically. The picture here varies from attacks targeting web applications, as the most common attacks targeting retail APIs differ slightly from those targeting all other industries. The top three attack types targeting retail APIs were Data Leakage (25.7%), RCE/RFI (17.2%), and Cross-Site Scripting (XSS) (16.8%).




**TERMS DEFINED**

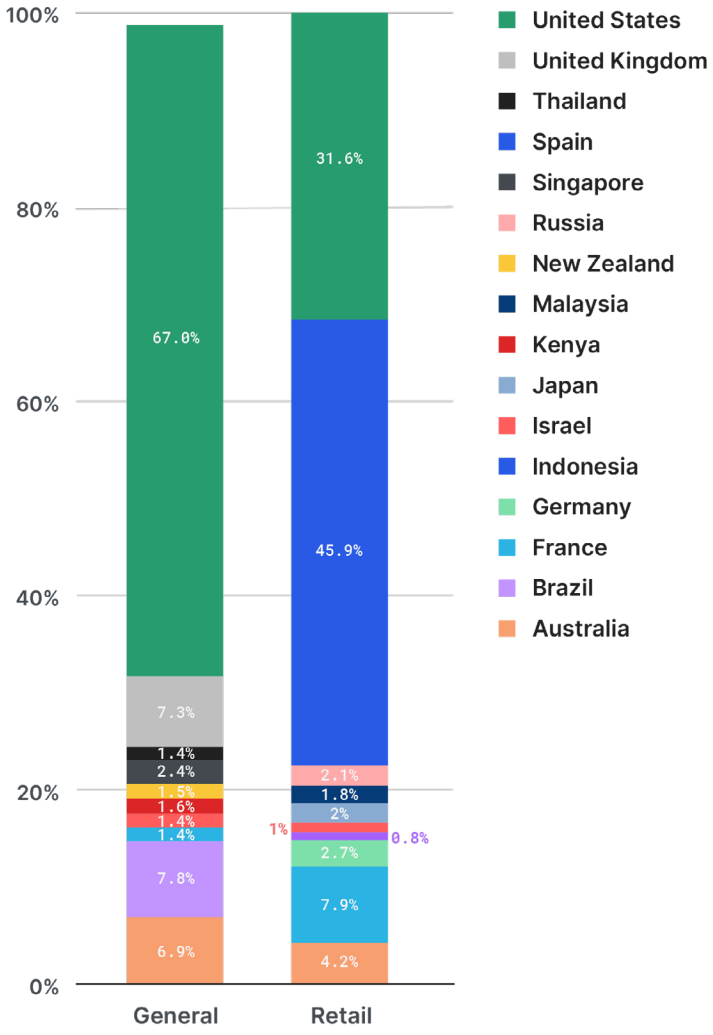
### Cross-Site Scripting (XSS):

Injection of malicious code into a vulnerable web application. Unlike other web attack vectors, XSS doesn't directly target the application itself, but rather the users of the web application. User accounts may be compromised, Trojan horse programs activated, and page content modified, misleading users into willingly surrendering their private data.

## Spain tops the list of source countries for API attacks

Spain leads other countries (45.9%) when it comes to launching API attacks targeting the retail industry. While not the majority here, the US was still a source of almost a third of API attacks on online retailers, with 31.6% originating from it. As noted previously, the data indicates only the location from which the attack was launched, and not necessarily the location of the attacker.

**Volume of API attacks by source country**



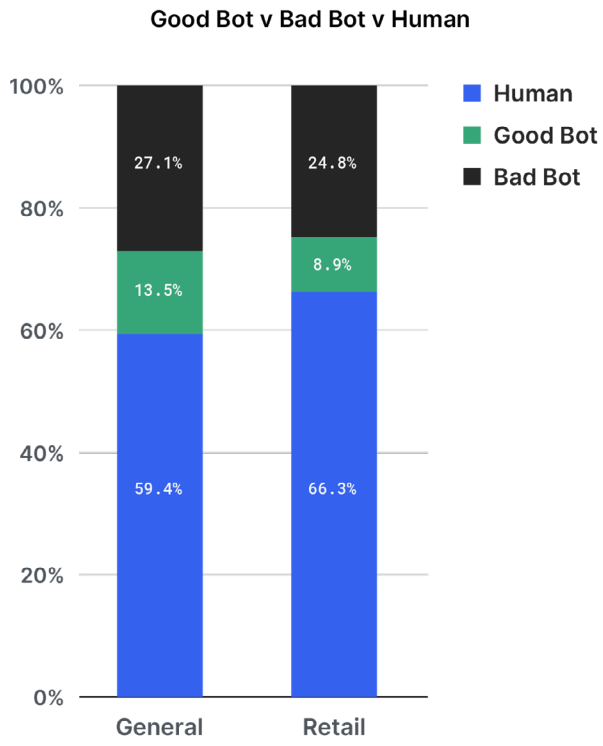
# Bot attack trends

Imperva Advanced Bot Protection provides a valuable source of data with a perspective on the automated threats that affect online retailers, also known as bad bots. As outlined in the 2021 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.

By collecting and analyzing data about the behavior of bots used to perform automated attacks on websites, APIs, and mobile applications, the platform can block them. It's this data that allows us to see how bad bots are used to attack online retailers in particular.

## A quarter of online retail traffic is bad bots

Despite the increase in human traffic as more people adapted to online shopping during the pandemic, automated traffic to retail websites comprised a third of requests, and bad bots were responsible for a quarter of those. That is slightly lower than the general picture in all industries combined. However, it is important to note that the volume of bad bots doesn't necessarily align with the level of their sophistication. For example, an advanced bad bot may be able to achieve its goals while performing fewer requests than simpler bad bots.




**TERMS DEFINED**

### Scalping:

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

### Grinchbots / Sneakerbots:

Variations of scalping bots designed to specially target limited edition sneakers (Sneakerbots) or highly coveted holiday season gifts (grinchbots).

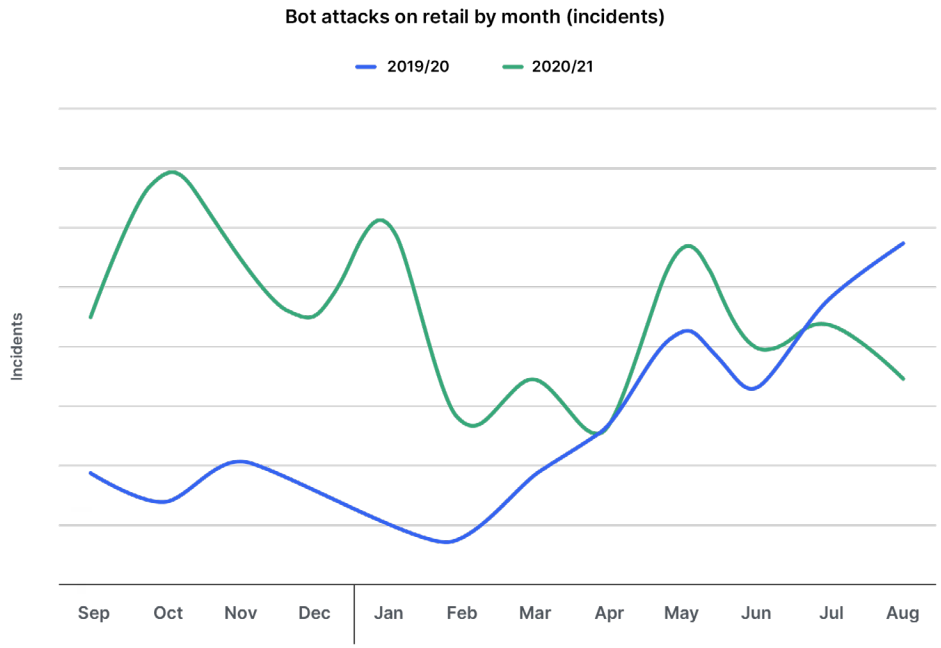
## Bots continue to thrive throughout the ongoing pandemic

INCREASE IN MONTHLY BOT ATTACKS FROM 2020 TO 2021

**13%**

Compared to last year, 2021 has seen a 13% increase in monthly bot attacks. Amongst the many threats that bots pose to eCommerce, like account takeover and price scraping, the pandemic has put inventory hoarding bots under the spotlight. During the early days of the pandemic, we noticed that bots were being used to hoard large inventories of certain commodities. Face masks, sanitizers, detergents, and home workout equipment are just a few examples. They all had a common theme: they were in high demand due to the panic caused by the pandemic. Scalping isn't a new phenomenon by any means. Bots have been used for years to gain the competitive edge on limited edition designer sneakers like Air Jordans and Yeezys as well as in-demand event tickets. The pandemic just had them setting their sights on new targets.

In actuality, the ongoing chip shortage actually made scalping bots more "popular" during the pandemic. It brewed the perfect storm for bots to thrive in. The supply of semiconductor chips is struggling to meet demand, affecting over 169 industries and has led to major shortages and queues amongst consumers for graphics cards, video game consoles, cars, and other electrical devices. This, combined with other factors, made bad bots aggressively target the gaming hardware market in the second half of 2020 and throughout the holiday season, with a peak in attacks clearly seen in October 2020, making it the month with the highest number of bad bot incidents in online retail websites. The bad news for retailers and consumers alike is that this shortage is predicted to last well into 2022. That means getting a new gaming console or a GPU this holiday season is once again predicted to be an almost impossible task made harder by the increase in bad bot attacks. For retailers, this means that a bot management strategy is essential to reducing the risk of malicious bot traffic.

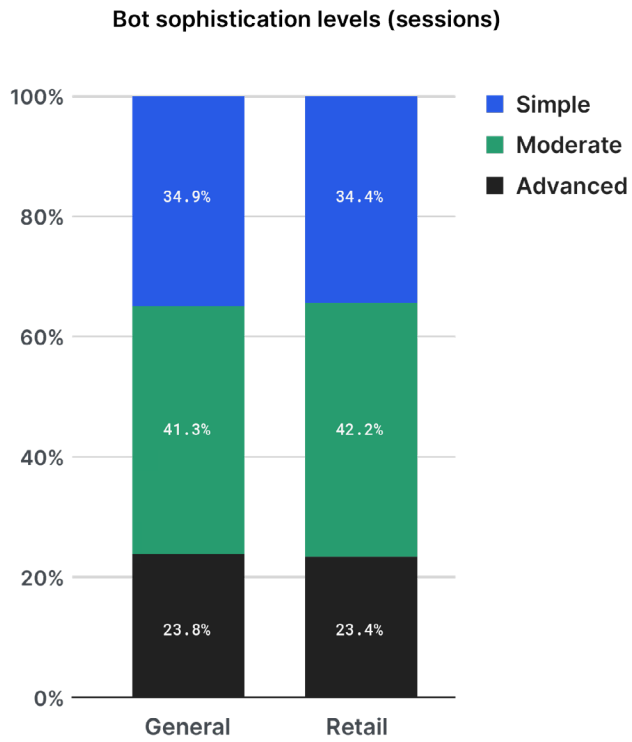


## Bot sophistication levels reflect the general picture

The majority of bad bot traffic to eCommerce is classified as moderate bad bots (42.2%), followed by simple bad bots (34.3%), and advanced bad bots (23.4%). The increase in moderate and advanced bots could be tied to the rise of scalping bots. Here's the best way to understand each breed of bot:

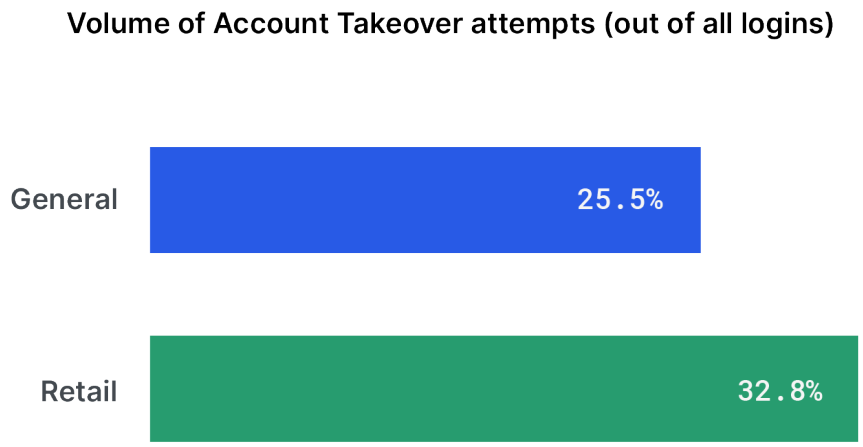
- **Simple:** Bots that connect from a single, ISP-assigned IP address. They connect to sites using automated scripts, not browsers, and don't self-report (masquerade) as being a browser.
- **Moderate:** A more complex type of bot that uses a "headless browser" software, enabling them to emulate browser 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.

Moderate and Advanced bad bots are trickier to detect and handle. These usually tend to cycle through random IP addresses, access 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.



## Account Takeover: a third of all login attempts on eCommerce sites

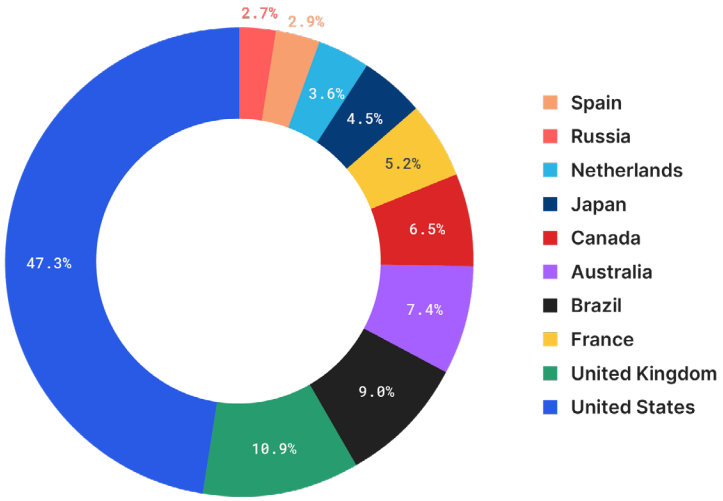
Perhaps the most damaging threat of all bot attacks, account takeover (ATO) is a malevolent attempt by bad actors to take over user accounts for malicious purposes. Put simply, account takeover is identity theft. Retail websites are an extremely lucrative target for these bad actors: saved credit card information, gift card balances, loyalty points, and other customer benefits are the main incentives. Compared to other sectors, retailers experience a higher volume of account takeover logins than all total login attempts. Almost a third of all login attempts to online retail websites have been ATO attempts (32.8%), compared to a quarter (25.5%) in all other sectors.



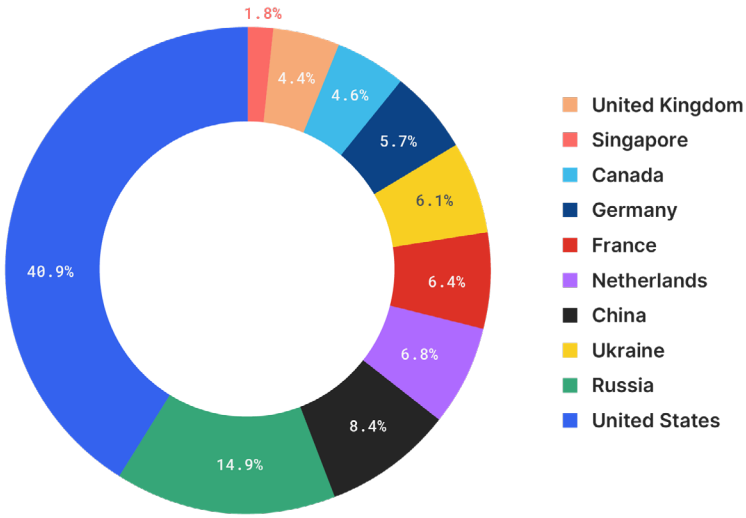
## The US is the main source of bot attacks and the top target

A common theme of bad bot attacks is that on many occasions, bad bots are launched from the same country they are targeting. As noted earlier, the data indicates only the location from which the attack was launched, and not necessarily the location of the attacker.

**Top targeted countries by bot attacks**




**Top source countries of bot attacks**



# 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 upwards of hundreds of thousands of dollars per hour.

At the time of writing this report, a new botnet named 'Meris' (the Latvian word for 'plague') is making the rounds, breaking records and potentially generating some of the biggest DDoS attacks in history. It is spreading across the internet – and according to new research[4], it might have already infected 200,000 devices. This activity is reflected in the charts below, and is absolutely a threat to look out for, especially during the holiday shopping season. In addition to monitoring the activity, Imperva DDoS Protection has successfully helped customers mitigate the activity from this enormous botnet.

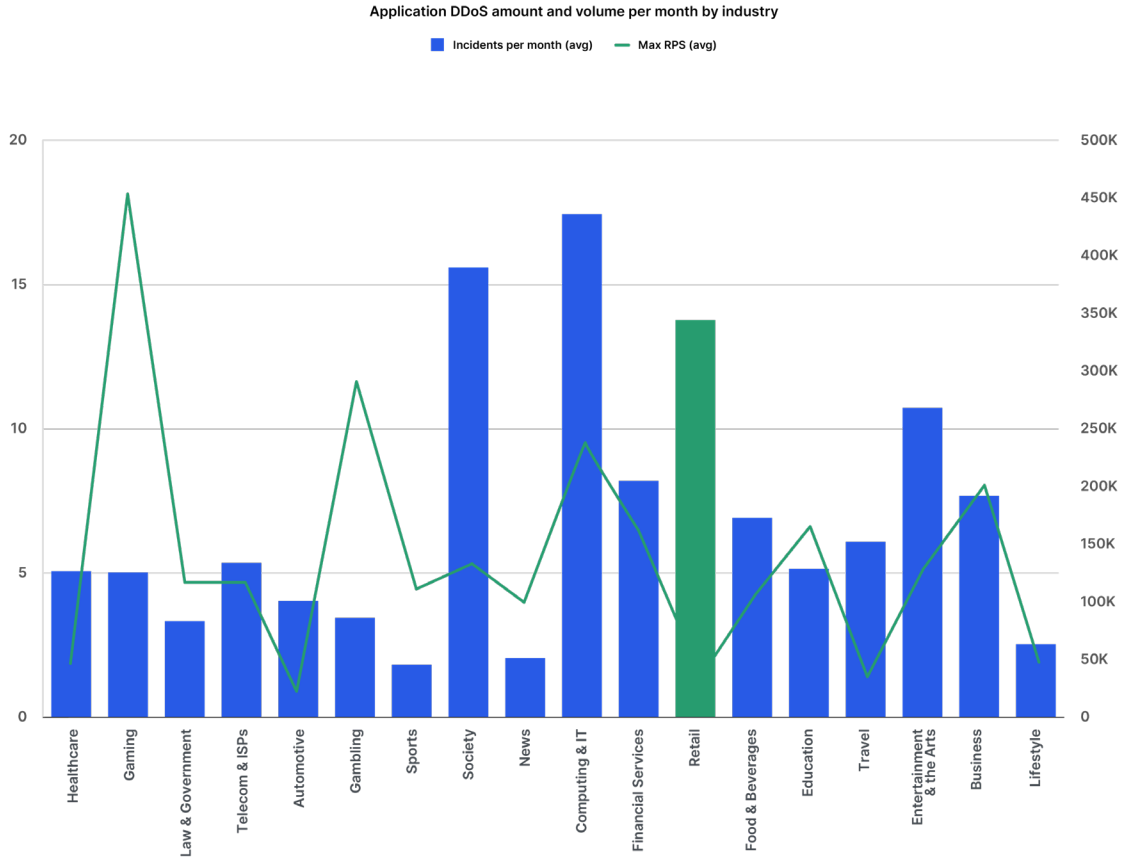
## DDoS incidents were frequent, but of a lower intensity than other industries

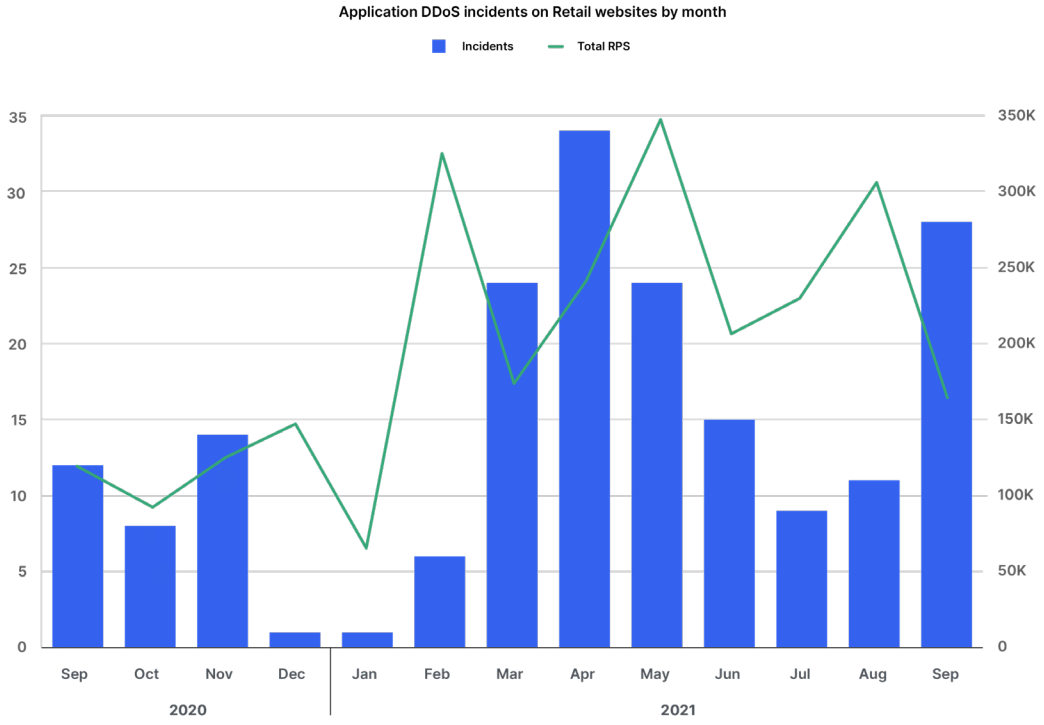
Throughout the year, on average, the retail industry has seen the third highest amount of application-layer DDoS incidents per month, at around 14. Interestingly, that does not correlate with the intensity of said attacks in terms of max requests per second (RPS), which was quite low, averaging a maximum of 35K. However, DDoS incidents have increased considerably in September 2021, presumably as a result of the new 'Meris' botnet, just ahead of the holiday season. If this trend was to persist, online retailers should expect an increase in DDoS attacks.

### 'Meris' Botnet

The new 'Meris' botnet is currently breaking records and potentially generating some of the biggest DDoS attacks in history. It is absolutely a threat to look out for, especially during the holiday shopping season. In fact, Imperva is already seeing, and successfully mitigating, the activity of this enormous botnet.

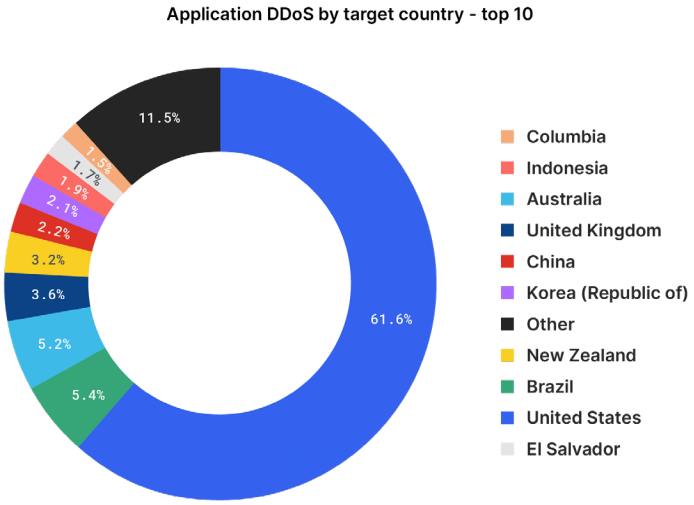
[4] https://threatpost.com/yandex-meris-botnet/169368/


Application DDoS amount and volume per month by industry
Incidents per month (avg)
Max RPS (avg)
20
15
10
5
0
500K
450K
400K
350K
300K
250K
200K
150K
100K
50K
0
Healthcare
Gaming
Law & Government
Telecom & ISPs
Automotive
Gambling
Sports
Society
News
Computing & IT
Financial Services
Retail
Food & Beverages
Education
Travel
Entertainment & the Arts
Business
Lifestyle


Application DDoS incidents on Retail websites by month
Incidents
Total RPS
35
30
25
20
15
10
5
0
350K
300K
250K
200K
150K
100K
50K
0
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
2020
2021

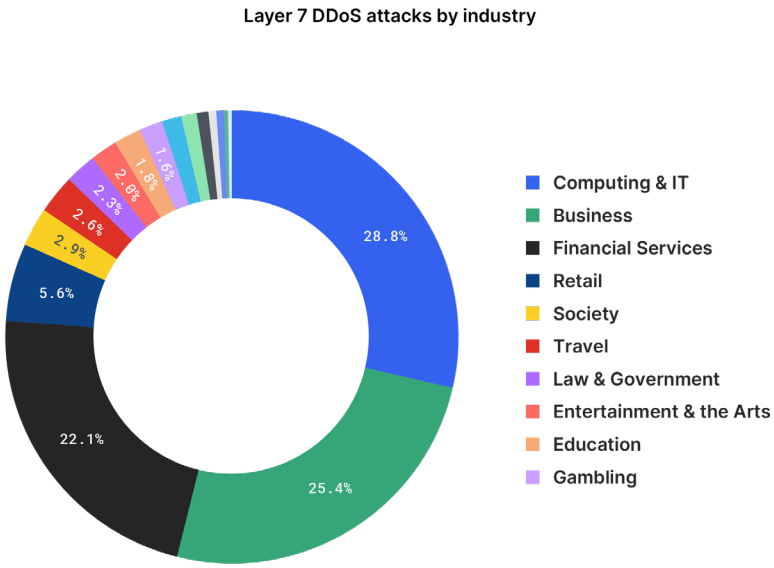
## The US was targeted by almost two-thirds of all attacks

In the past year, the US has become significantly more targeted by application-layer DDoS attacks compared to the previous year. It was targeted by 61.6% of all attacks, followed by a significant margin by Brazil, which was targeted by 5.4% of attacks, and Australia, targeted by 5.2% of attacks.




## The impact of DDoS attacks on e-commerce

As detailed in the **Imperva Global DDoS Threat Landscape Report**, the retail industry was the fourth most targeted by application layer DDoS attacks in the past year, accounting for 5.6% of all attacks recorded.



# Client-side attacks

Client-side attacks have become significantly more prominent in recent years for two reasons:

1. The abundance of JavaScript-based services. These can be anything from a Live-Chat for customer service, eCommerce platforms, payment gateways, and more. This creates a fertile ground for attacks using exploits in third-party code.
2. The amount of personal data passing 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.

These attacks are commonly referred to as Magecart attacks, named after the notorious hacker collective that pioneered the method as an online skimming technique. 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.

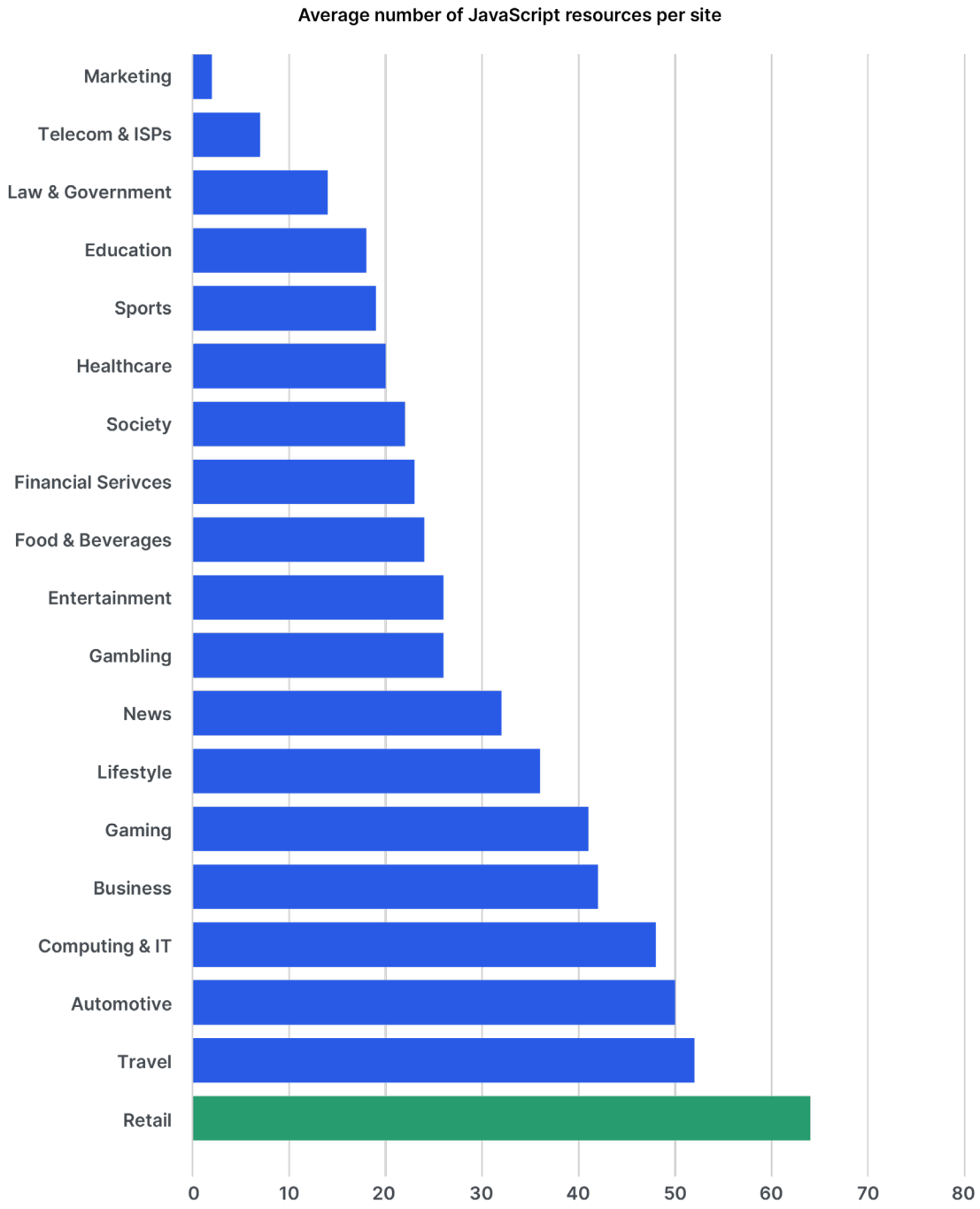
**TERMS DEFINED**

### Magecart:

Magecart is a collective of malicious hacker groups that target online shopping cart systems to steal customer payment card information. This is also known as a supply chain type of attack.

## Retail sites have the highest average number of JavaScript-based services

On average, websites in the retail industry have 64 JavaScript-based services executing on the client-side.



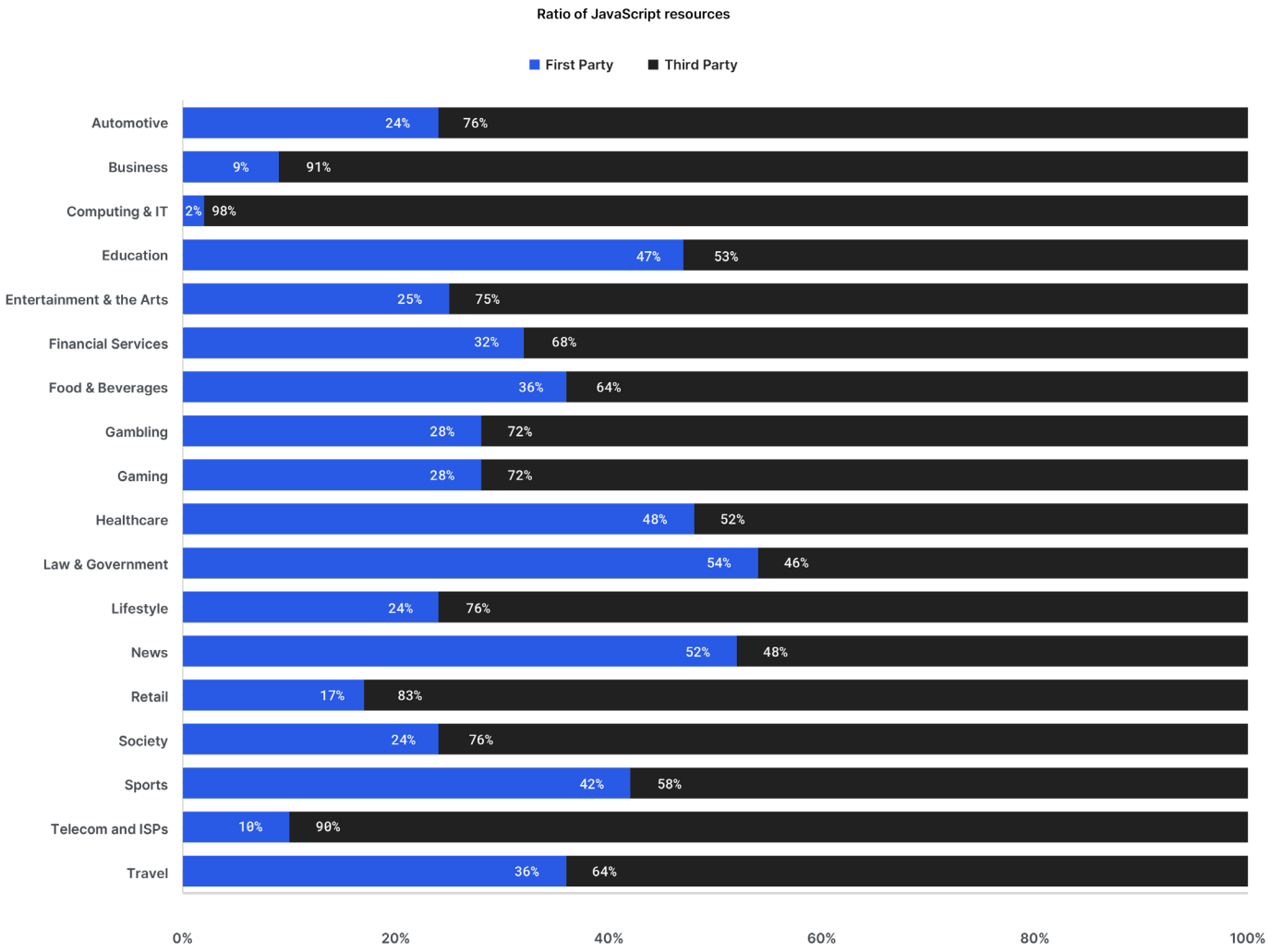
## The majority of eCommerce JavaScript services are third-party

The chart below dives deeper into the number of JavaScript-based services on websites, dissecting the data into first vs. third-party services. The majority (83%) of JavaScript-based services on eCommerce websites are third-party services.

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.

According to the OWASP, the single greatest risk is a compromise of the third-party JavaScript-server, and the injection of malicious JavaScript into the original tag JavaScript.



## An ad-blocker that injects ads?

Stealing sensitive information isn't the only thing the client-side attack surface allows for. There are numerous ways for hackers and scammers to manipulate it for their own benefit. A recent example of this is an ad-injection campaign uncovered by the Imperva Research Labs, where very ironically, a certain ad-blocking extension available for both Chrome and Opera browsers was actually injecting ads. Ad injection is the process of inserting unauthorized advertisements into a publisher's web page to entice the user to click on them. Ad injection can originate from various sources like malicious browser extensions, malware, and even through stored cross-site scripting (XSS). How does it benefit the perpetrator? Here are just a few examples:

1. Competing brands can advertise on rivals' websites, potentially stealing customers away.
2. Price comparison ads can be used to distract customers' attention from making a purchase.
3. Affiliate codes or links can be injected as well, allowing scammers to cash in on purchases without ever helping a single customer.
4. Scammers can cash in on application downloads using affiliate links.

What we can learn from this is that the client-side attack surface is constantly evolving, allowing for very elaborate attacks and new types of fraudulent activity that sneak past traditional security tools.

**TERMS DEFINED**

### Ad-injection:

Ad-injection is the process of inserting unauthorized advertisements into a publisher's web page with the intention of enticing the user to click on them.

# Recommendations ahead of the peak 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 'Meris' botnet, attacks are expected to reach record-breaking volumes. It is recommended that you stress-test your infrastructure regularly, and even more frequently prior to 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, especially in light of the recent 'Meris' botnet attacks.

2. Good marketing campaigns don't just attract customers, they attract bots, too. Take for example last year's launch of the new generation of gaming consoles and GPUs. Almost all stock was immediately purchased by bots, leaving consumers disappointed and angry at the retailer. Unfortunately, these are still very sought after with low and unpredictable restocks. The bottom line is, if you announce a date and time for a coveted product launch or a limited availability item, expect bots to be there and get their hands on it first. Make sure that you are prepared to handle the high volume of traffic and that you have a bot management solution in place only allowing legitimate customers into your website. Otherwise, the makeup of traffic will include a high ratio of advanced bots trying to scoop up the products. They will be denying legitimate users, all while hampering website performance, skewing analytics, and no less importantly causing severe brand damage.

3. Encourage good credential habits 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. Imperva Research Labs 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 **2021 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 customer experience.
- 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.