imperva

2020 REPORT

# The State of Security within eCommerce

# Contents

# Introduction

## The impact of the COVID-19 pandemic on eCommerce

The impact of COVID-19 has made 2020 a year unlike any other. Among the many effects of the global pandemic has been a huge increase in online retail business. With much of the world's population under various degrees of lockdown, and with many people unable to reach their local grocery stores, consumers have increasingly turned to online retailers large and small for safety and convenience.

Online sales in the US alone were up by 30.1 percent year-on-year in the first six months of 2020 — compared to only four percent of overall sales[1]. US consumers spent $497 billion online between January and August 2020, with sales exceeding $2 billion on 130 different days. Compare this to 2019, when sales exceeded $2 billion on just two days[2].

Consumers have increasingly turned to online retailers large and small for **safety and convenience**

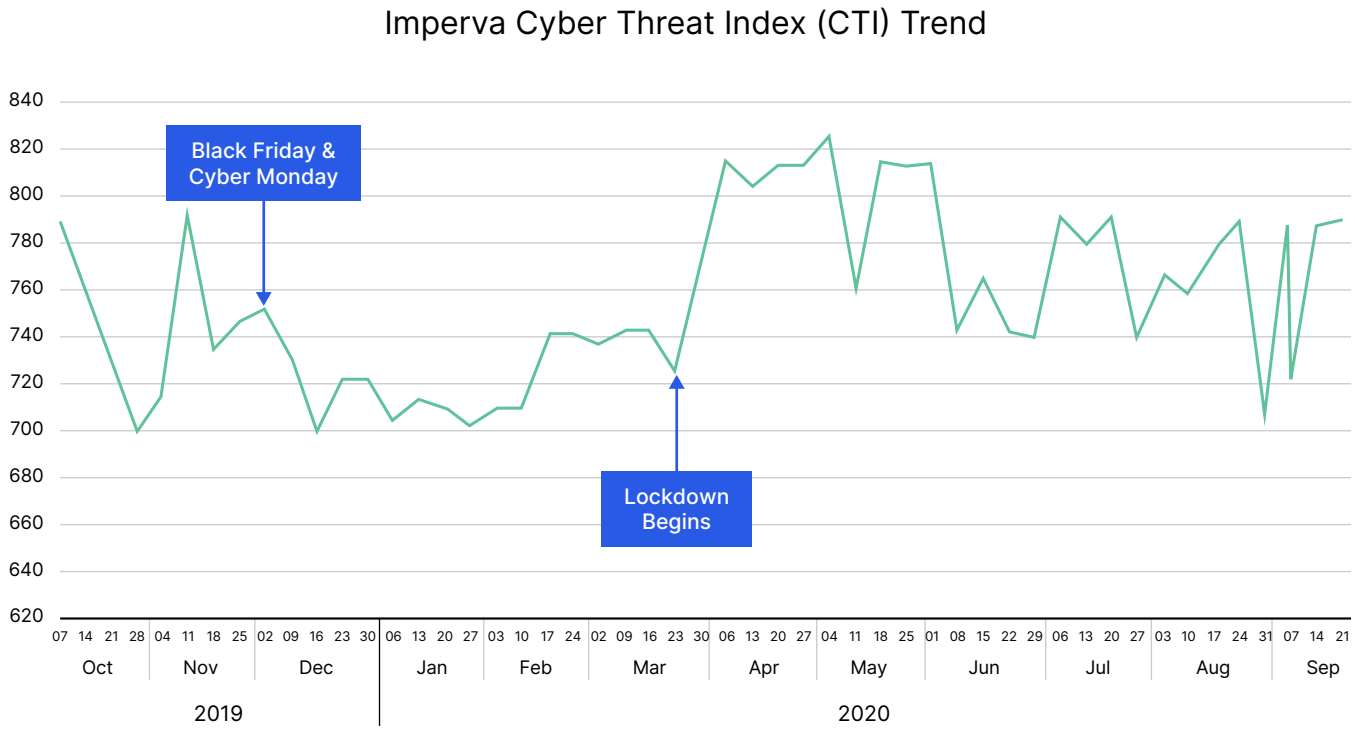
| TIME PERIOD | # OF DAYS THAT DAILY SALES VOLUME EXCEEDED $2B |
|---|---|
| 2019 | **2 days** |
| 2020 (January to August) | **130 days** |

## Rising cyber threat facing eCommerce businesses

However, as the volume of online sales has risen, so too has the volume of cyber-attacks on online retailers. Imperva's Cyber Threat Index (CTI) is a continuous measurement and analysis of the global threat landscape and applications. Calculated using data gathered from all Imperva sensors across the world, it can be broken down by industry. In the overview of the CTI for the retail sector for the year to September 2020, below, you can see how it rises dramatically around the beginning of the global lockdown measures and the accompanying growth in online shopping. In fact, you'll notice how it surpasses even the previous peak around Black Friday and Cyber Monday, 2019.

[1] Digital Commerce 360 analysis of U.S. Department of Commerce data

[2] Adobe Digital Economy Index




This year's holiday season is fast approaching. When we consider that the level of threat facing online retailers already exceeds last year's seasonal peak, it's reasonable to assume that, by the end of November 2020, they'll reach levels never before seen.

In this report, we'll use different sources of Imperva data to look at the types of attack we've seen over the past 12 months, where they've come from, how they've been delivered, and what online retailers can to do to prepare for what's likely to be an unprecedented holiday season — in terms of traffic and in terms of threat.

# Website attack trends

Imperva's Cyber Threat Index (CTI) provides an easy-to-understand score which allows us to track cyber threat levels over time and observe trends. Among the data used to inform the CTI, is the more than 30 billion monthly Web application attacks made across a trillion HTTP requests analyzed by our Web Application Firewall service (Cloud WAF). Looking at this WAF data more closely presents us with a more detailed understanding of the threat landscape faced by retailers over the past 12 months, and gives us a good indication of what lies ahead.

This report focuses on the well understood web attacks encapsulated within the OWASP Top 10 — widely considered to be the most critical security risks to web applications.

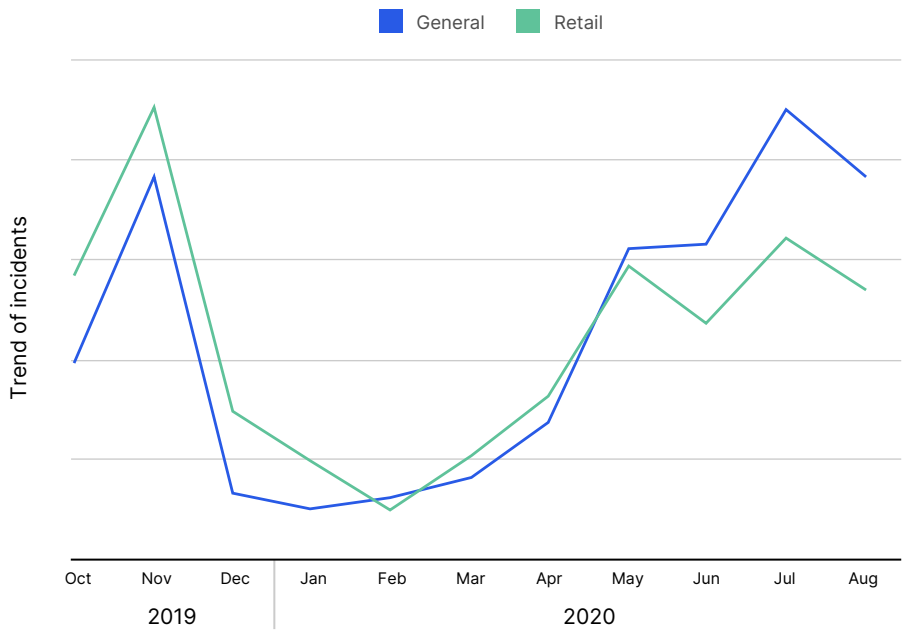
## Web attacks on eCommerce (mostly) mirrors all other industries

The graph below compares the level of OWASP Top 10 attacks on online retailers against the overall number of attacks.

The first thing you'll notice is how closely it mirrors the CTI graph, first peaking around Black Friday and Cyber Monday, and then again as lockdown measures are introduced. But the next thing you'll see is that, although experiencing an unseasonable number of attacks in 2020, the online retail sector hasn't been targeted to the same extent as all other industries. Yet.

Trend of Web Attacks for Retail/eCommerce Versus All Other Industries

(Change over months, based on the number of incidents)

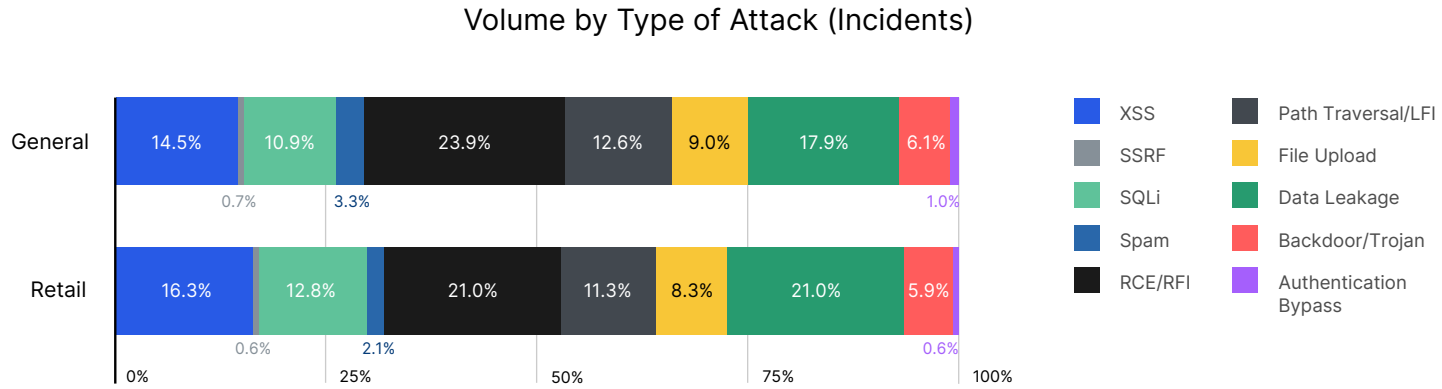


## Top three web attack types

Going into greater detail, the top three attacks on the online retail sector, by volume, over the past 12 months are RCE/RFI, data leakage and cross-site scripting.

| VOLUME BY TYPE OF ATTACK (INCIDENTS) | | | |
|---|---|---|---|
| | ATTACK NAME | PERCENTAGE OF ATTACKS | DESCRIPTION |
| 1 | RCE/RFI | 21.0% | 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. |
| 2 | Data Leakage | 21.0% | Attackers may steal or modify weakly protected sensitive, often financial, data to conduct credit card fraud, identity theft, or other crimes. |
| 3 | Cross-site scripting (XSS) | 16.3% | Cross site scripting (XSS) injects 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. |

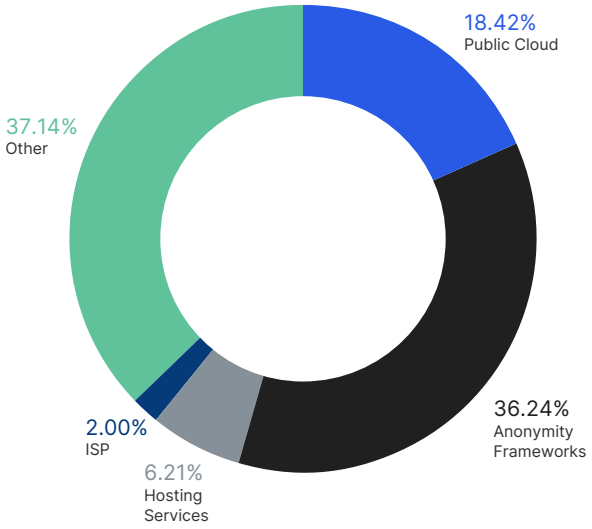
The volume of attacks on online retailers is broadly in line with those seen by all industries taken as a whole. Retail sites, however, experienced more XSS and data leakage due to the valuable payment and credit card information they hold.



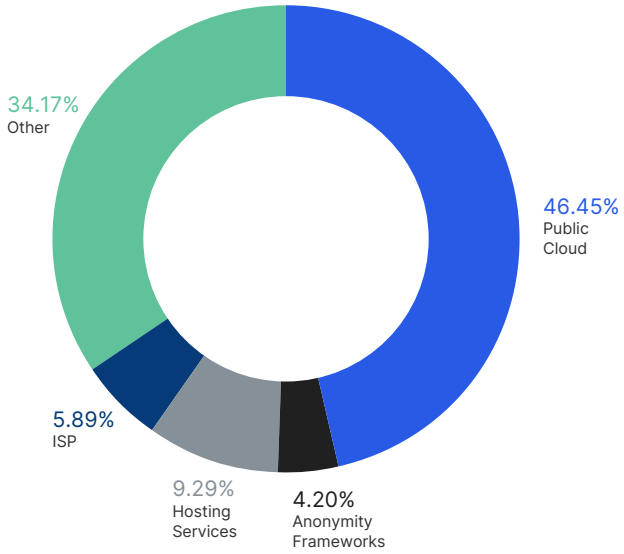
## Most eCommerce web attacks from anonymous sources

In addition to understanding how these attacks were carried out, we're also able to see the source of the requests for most of them. The two graphs below show contrasting approaches. Of the identifiable sources, a public cloud service is used to make the majority of requests for attacks across all industries. For attacks made specifically on online retailers, however, anonymity frameworks are the preferred sources, enabling attackers to cover their tracks, and launch attacks without being identified by their target. Also anonymity frameworks are used to launch many account takeover attacks involving credential stuffing and credential cracking.

### Attack Sources - eCommerce/Retail

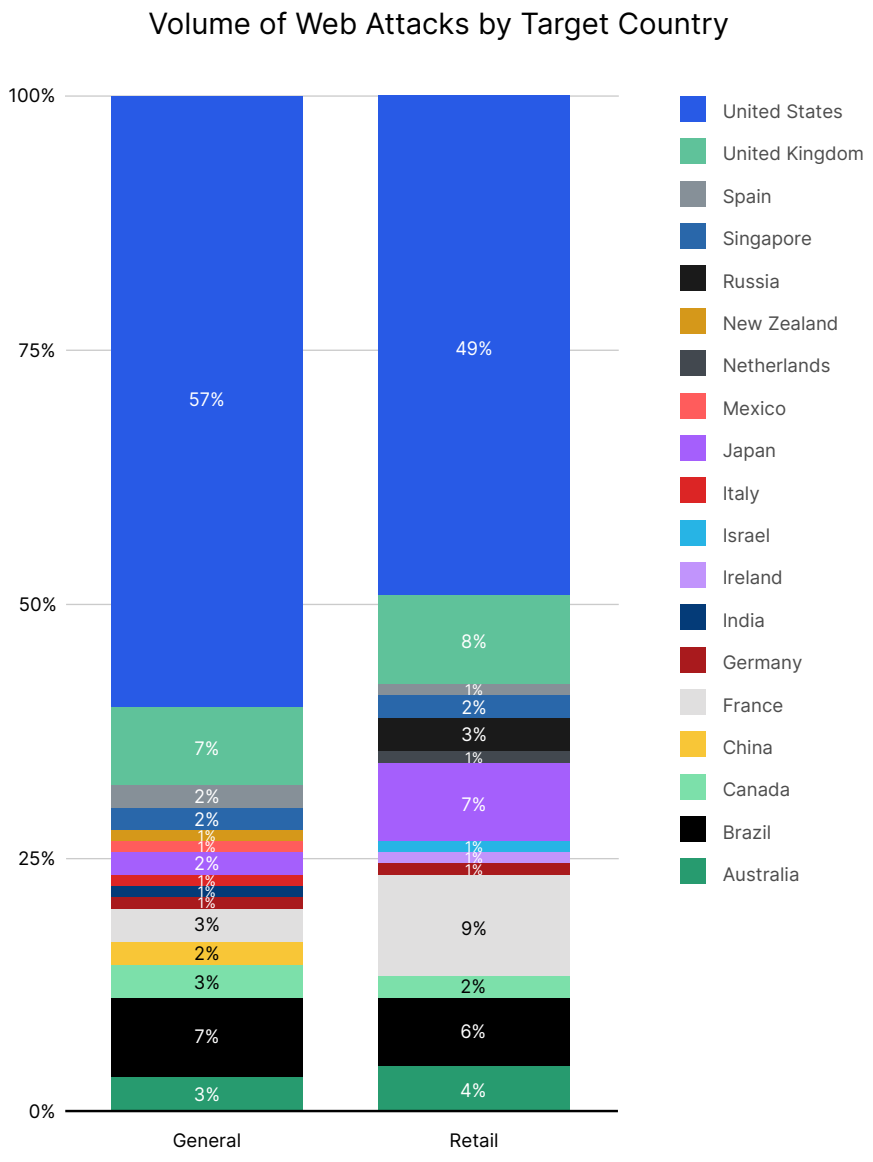



### Attack Sources - All Industries



## US most popular target for web attacks

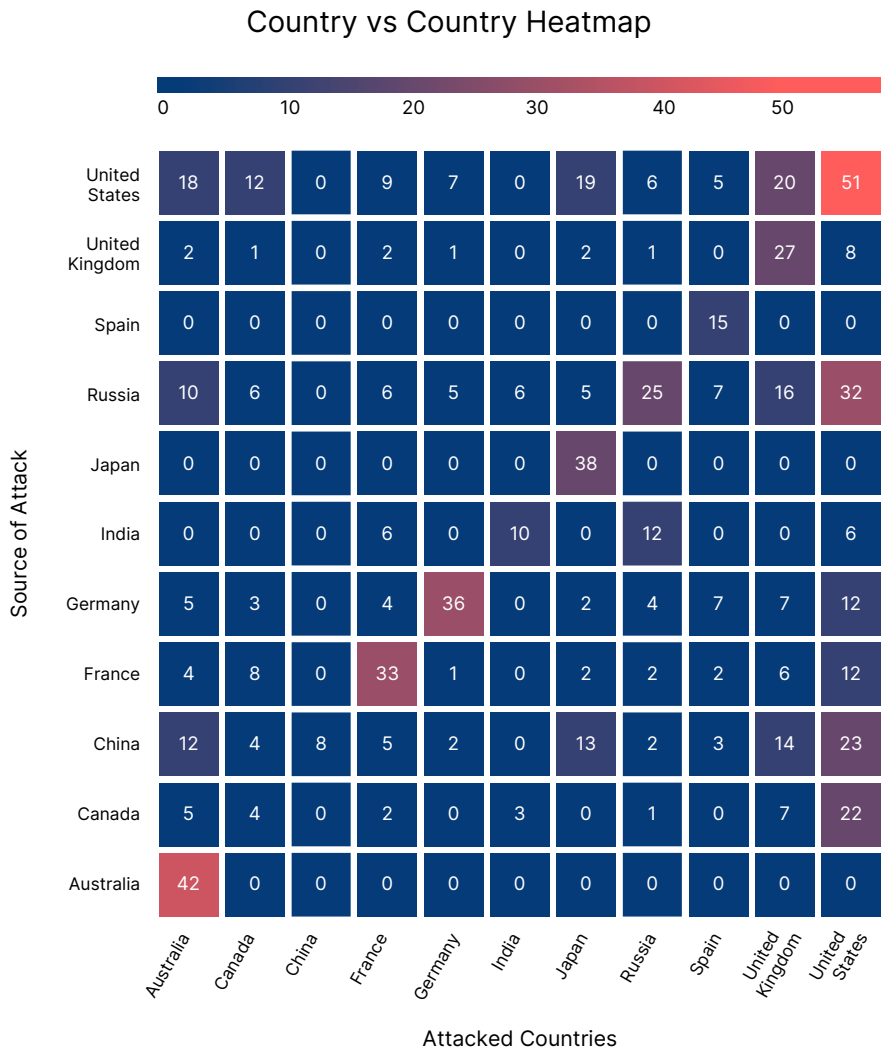
The vast majority of web attacks in the last 12 months (49%) were carried out against sites located in the US. The next two most popular targets, France, and the UK, were a significant distance behind, at 9% and 8% respectively. Again, these figures are largely in line with the general picture, with the US experiencing the highest number of overall attacks at 57%. Interestingly, though, while the UK was in second place here, at 7%, it shared that spot with Brazil.



We can see from the comparative scores in the heatmap below that, in most cases, the majority of the attacks carried out on a particular country's online retailers were actually carried out from within the same country. For example, just over a third of the attacks experienced by targets in the US were performed by threat actors in the US.

There were exceptions, however. Russian sources were responsible for more attacks on US targets than on targets in their own country, as were China and, surprisingly, Canada. Interestingly, threat actors in Australia and Japan appeared to mostly target their own respective country's online retailers.

In most cases, the majority of the attacks carried out on a particular country's online retailers **were actually carried out from within the same country.**

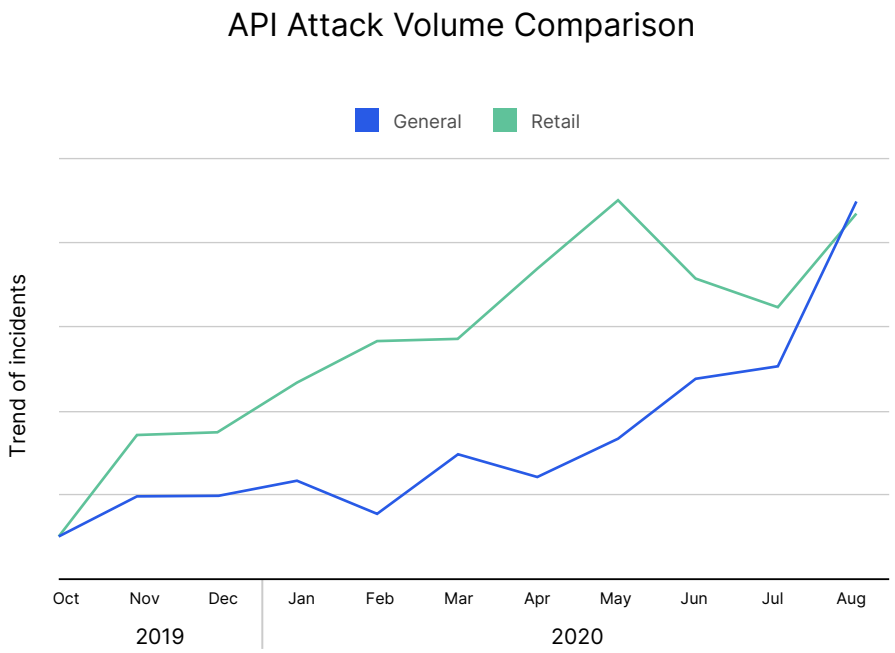


# API attack trends

Imperva Cloud WAF isn't the only source of data we can turn to for insight 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. Looking at the data it provides helps us paint another detailed – and very different – picture of the attacks carried out against online retailers over the last 12 months.

The graph below shows how the volume of attacks on retailers' APIs far exceeded the average overall volume, rising – as expected – during the peak shopping season last year before reaching a huge peak in May, a time when most of the world was on lockdown and, by necessity, shopping online. Indeed, there's little doubt that it was this reliance on online retailers that made them such an attractive target for criminals.

There's little doubt that the **reliance on online retailers during lockdown** made them an attractive target for criminals



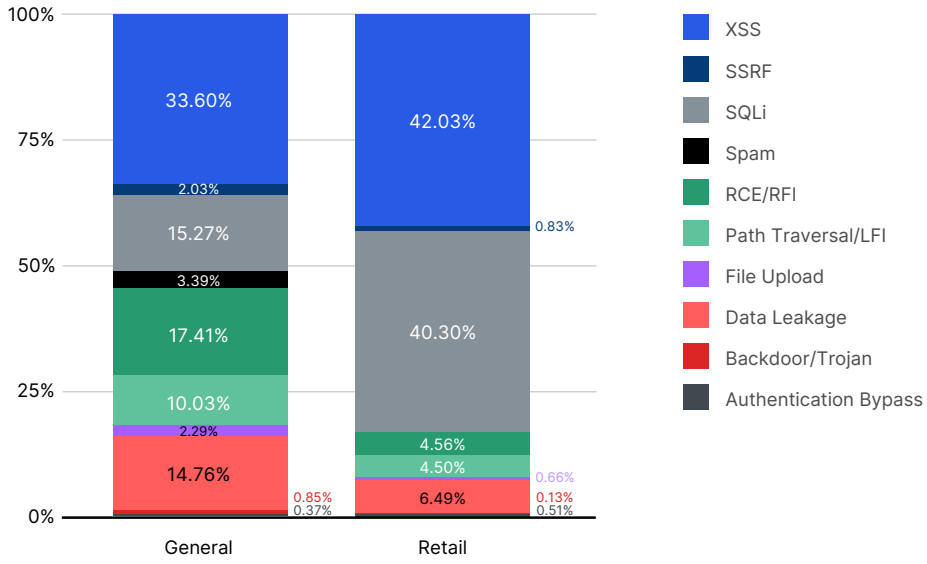

## XSS and SQLi top list of API attacks on eCommerce

As the next graph illustrates, the types of API attacks differed too, with XSS and SQLi accounting for the majority, at 42.03% and 40.3% respectively.

SQL injection, or SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business. In the case of an online retailer, SQLi could be used to obtain the personal and financial details of its customers.

Elsewhere, while XSS – at 33.6% – was also the most commonly used attack vector overall, it was followed by a relatively even split of RCE/RFI (17.41%), SQLi (15.27%), and data leakage (14.76%).

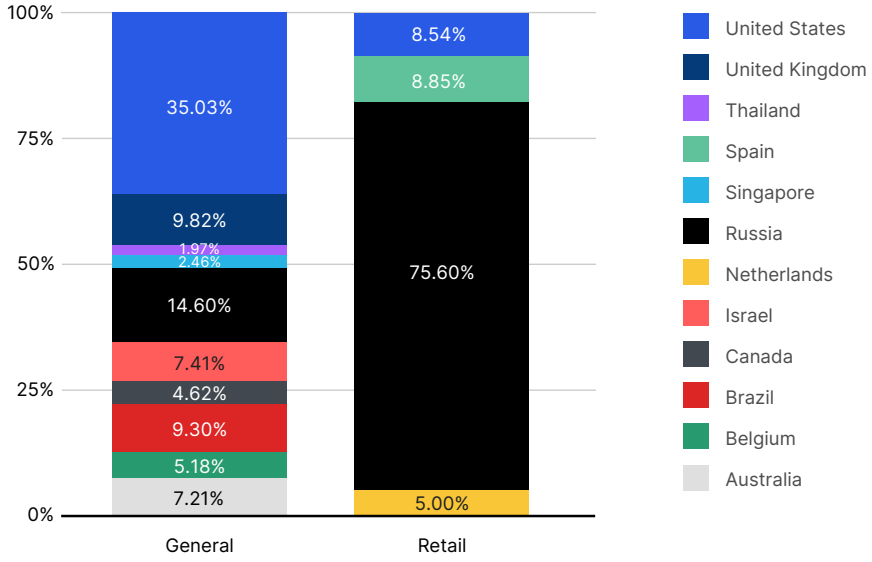
## API Attacks by Volume




## Russia is primary source of API Attacks

When it came to the source of these attacks, one country stood head and shoulders above the others – Russia – the starting point of an incredible three quarters of all attacks on online retailers in the year to September 2020. In stark contrast, only 14.6% of attacks overall originated in Russia. The US was the primary source of more than a third of the attacks on all industries combined.

## Volume of API Attacks by Source Country



# Bot attack trends

Imperva's Cloud WAF and Advanced Bot Protection offer another valuable source of data with which we can measure the types of attacks carried out against the online retail sector which, as outlined in our Bad Bot Report, are unique to the industry. For example, competitors use bad bots to aggressively scrape pricing and inventory information, while Grinchbots and Sneakerbots create denial of inventory problems for customers seeking limited edition items. Criminals also use bad bots to commit fraud by stealing gift card balances, as well as to gain access to user accounts and credit card information.

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

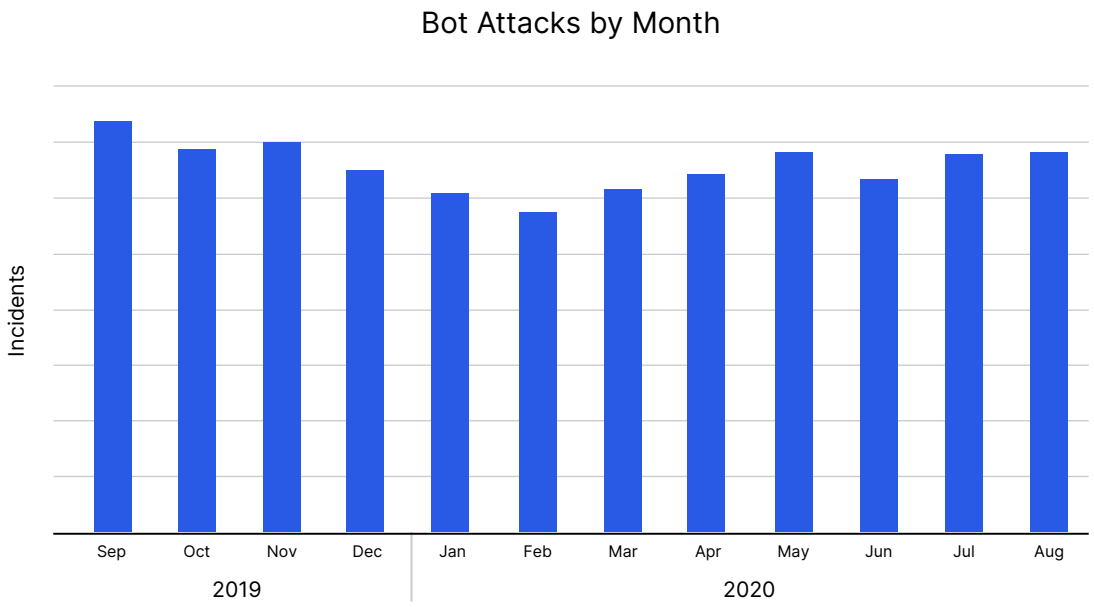
**The majority of attacks (98.04%) on online retailers are carried out by automation, commonly known as bots.**

## Bots perform all attacks

The majority of attacks (98.04%) on online retailers are carried out by automation, commonly known as bots.

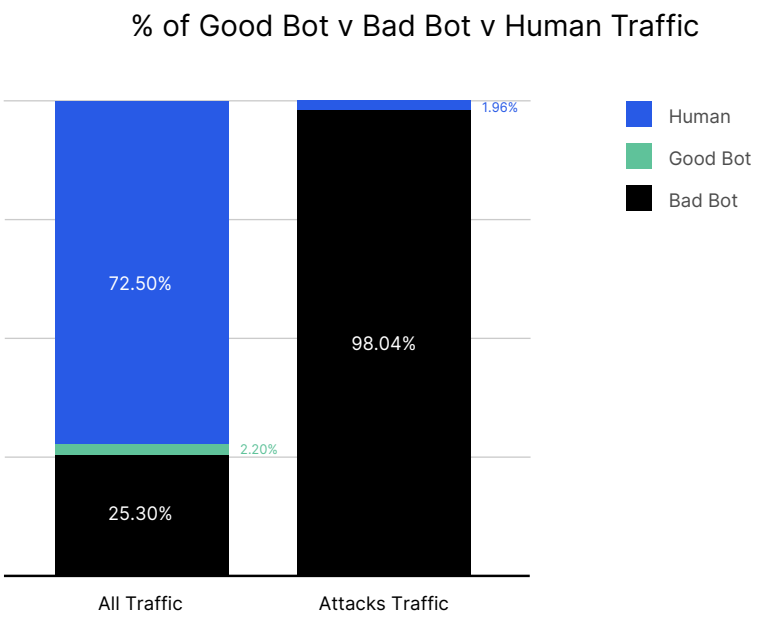
## Bots - an ever-present threat

In common with the Cyber Threat Index (CTI), WAF and API data, there were peaks in bad bot attacks around the 2019 holiday season, and again in April 2020 as lockdown measures were enforced. These peaks aren't as significant as any we've seen elsewhere, however. This suggests that bots are an ever-present threat. Automation never sleeps, meaning bots will typically be active 24/7.



## Bad bots behind most attack traffic to retail

We can see that, although bots only account for 27.5% of normal traffic, they are responsible for the majority of attack traffic experienced by retailers. In fact, less than 2% of attack traffic is generated by human operators.

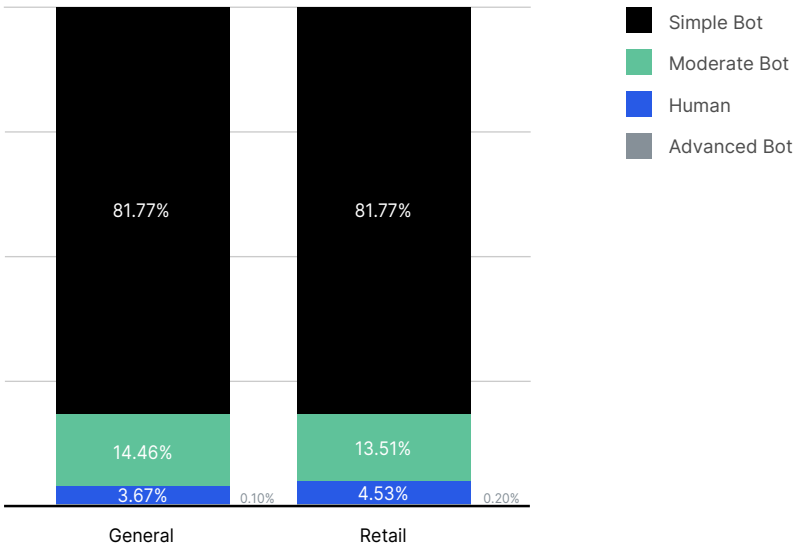



## Simple bots are the most popular

Depending on their purpose, and how they operate, different bots are classified by their levels of sophistication — simple, moderate, and advanced.

As the graph below shows, simple bots are used in the majority of all attacks — both on retail and in general. Connecting from a single, ISP-assigned IP address, this type of bot connects to sites using automated scripts, rather than browsers, and doesn't self-report as being a browser. Moderate bots, used in just over one in ten attacks, are more complex, and use "headless browser" software that simulates browser technology—including the ability to execute JavaScript. Advanced bots, used in a small minority of attacks, are a combination of moderate and sophisticated bad bots. They tend to cycle through random IP addresses, enter through anonymous proxies and peer-to-peer networks, and are able to change their user agents.

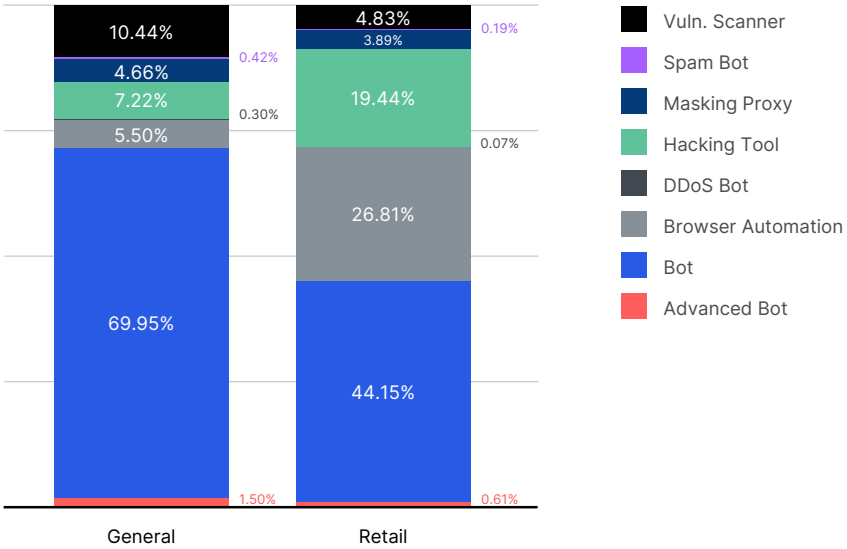
## Bot Sophistication (by Number of Attacks)




## Simple bots top list of attack tools

While simple bots were predominantly used as clients in attacks on retailers (44.15%), we see many more instances of the use of browser automation (26.81%) and hacking tools (19.44%) to connect to sites than we do overall.

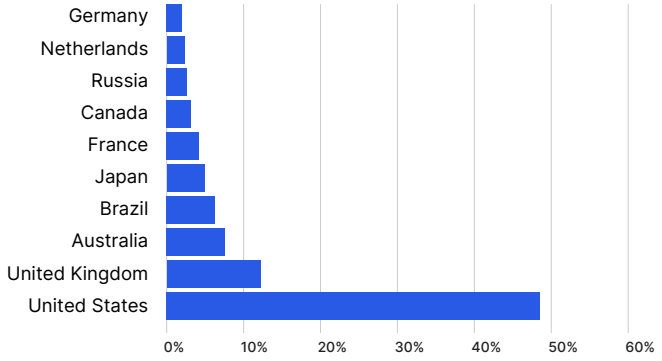
## Top Attack Tool Types



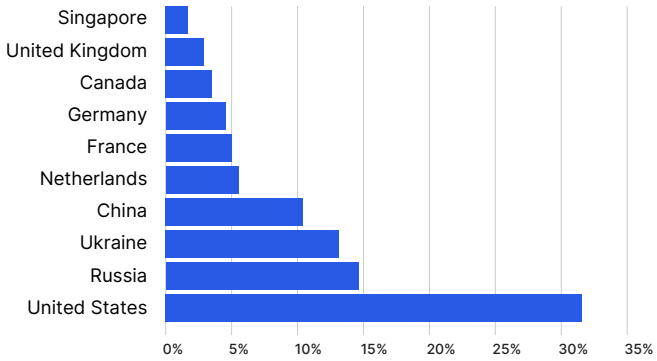
## US both biggest target and source of attacks

Online retail sites in the US were the biggest target for attacks by bad bots, with the primary sources of these attacks being the US itself (30.93%), Russia (14.39%), and Ukraine (12.92%).

### Top 10 Target Countries by Incident



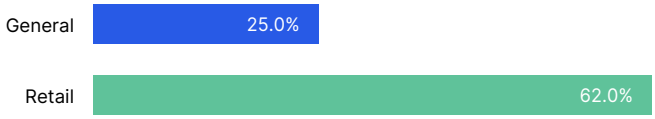

### Top 10 Source Countries by Incident




## Account Takeover bots twice as popular against eCommerce

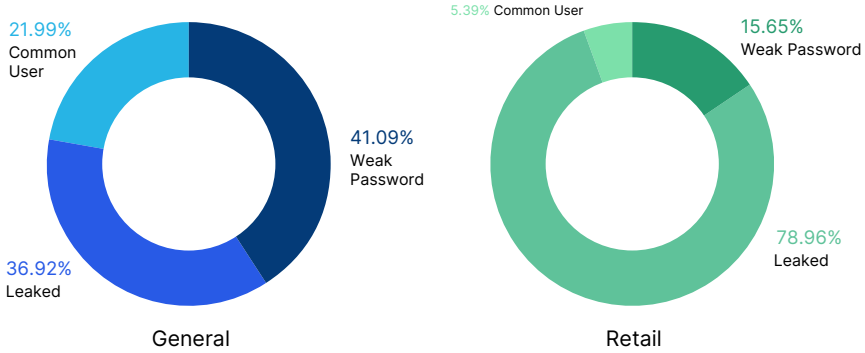
Finally, as its name suggests, an account takeover – or ATO – is an attempt by cybercriminals to take over users' accounts for malicious purposes. Online retailers experienced more than twice as many ATO attempts (62%) than all other sectors (25%).

### Volume of Account Takeover Attempts on Login Pages




Of these, hackers performed credential stuffing techniques and used considerably more leaked credentials in ATO attacks on retail targets (78.96%) than they did in general (36.92%), as they typically guarantee a higher success rate than credential cracking, which uses common or weak passwords paired with the stolen login name.

### Type of Credentials Used on Login Pages



# DDoS attacks

The goal of an application layer, or layer 7, DDoS attack is to bring down a server by exhausting its processing resources with a high number of requests. It's measured in requests per second (RPS)—the number of processing tasks initiated per second. Such attacks are executed by DDoS bots able to establish a TCP handshake to interact with a targeted application.

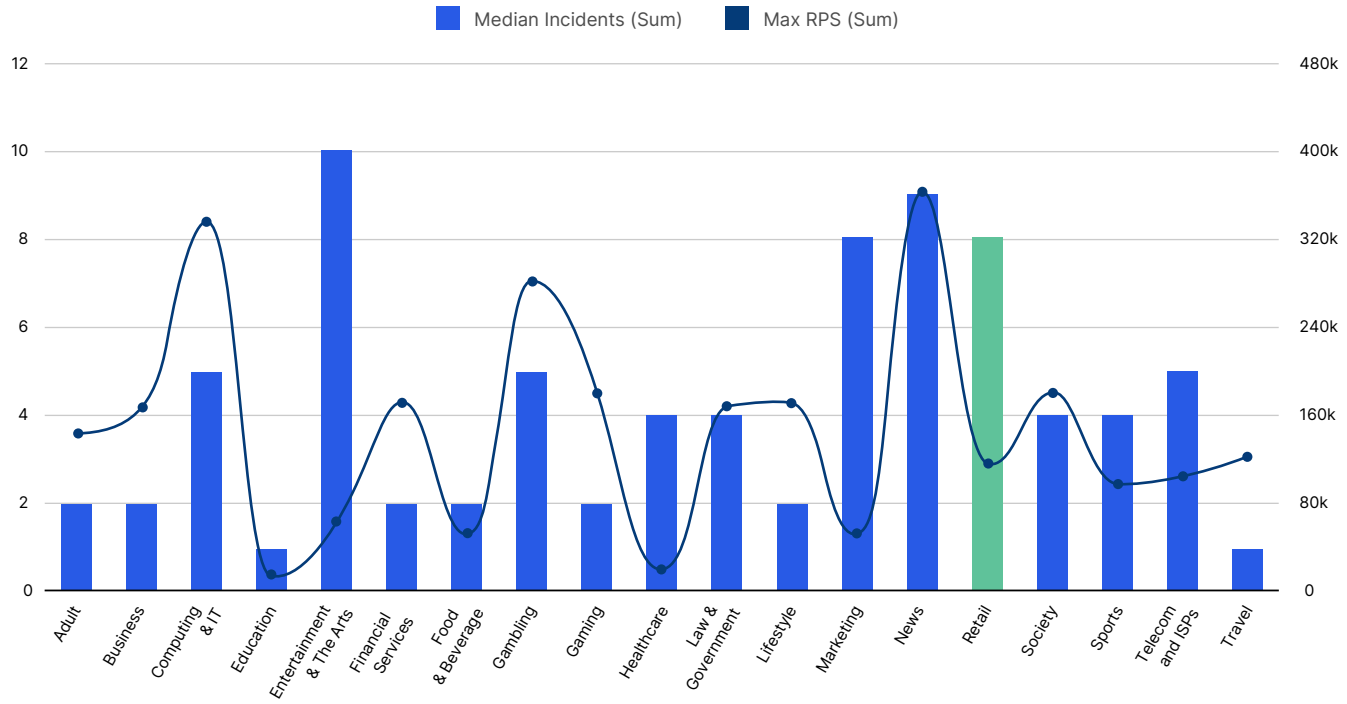
## Rise in number and size of DDoS attacks

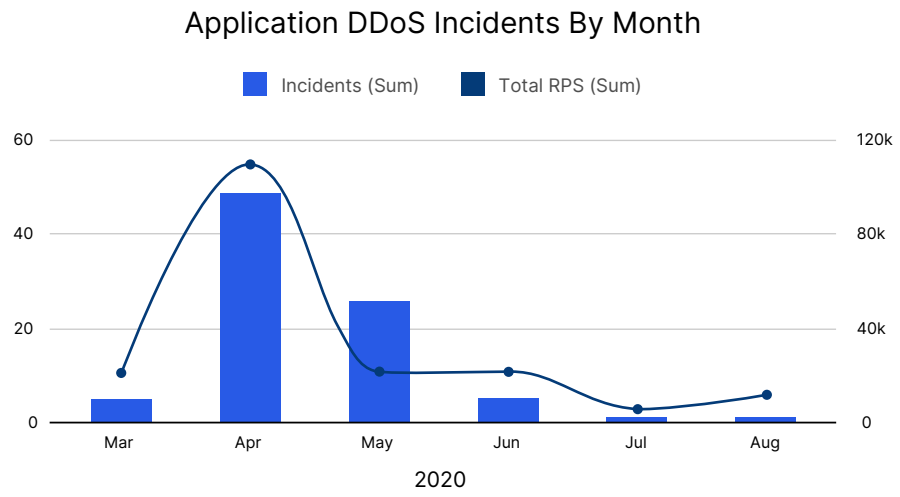
Over the course of the year, the online retail sector experienced an average eight application layer DDoS attacks a month. In April 2020, however, as the demand for online shopping began its rapid ascent, Imperva saw a corresponding peak in application layer DDoS attacks on retailers. Between them, 49 separate incidents accounted for almost 100,000 RPS.

In April 2020, as online shopping began its rapid ascent, Imperva saw a **corresponding peak in application layer DDoS attacks** on retailers

Application DDoS Amount and Volume Per Month by Industry

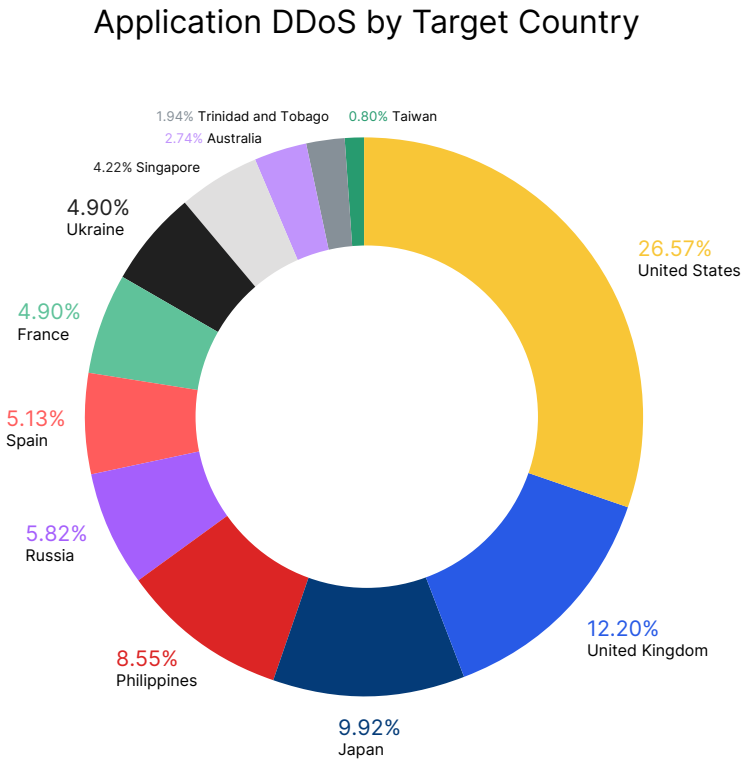
(Incidents Per Site and Max RPS)






## US biggest target for DDoS attacks

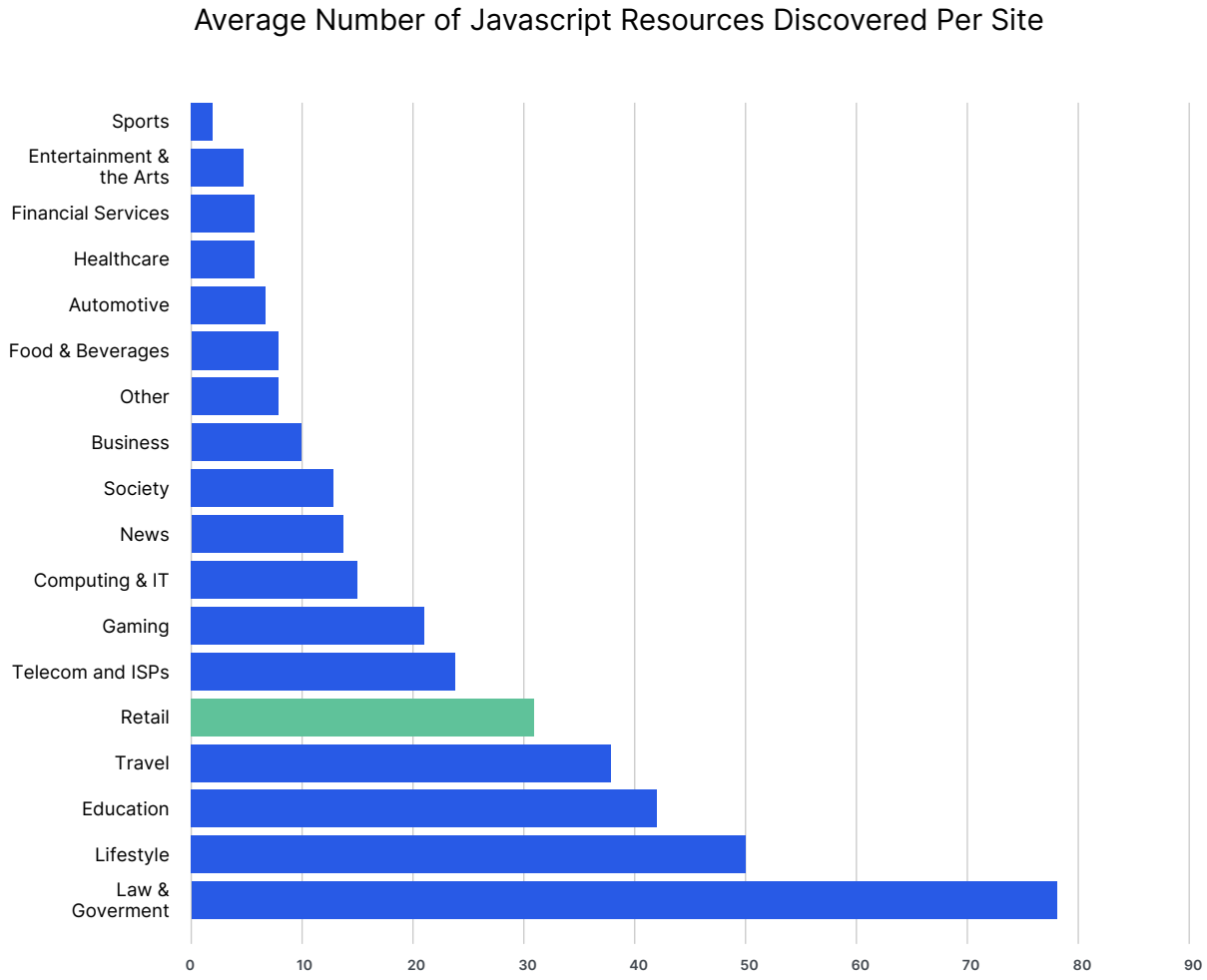
The US was the most popular target for DDoS attacks, experiencing more than a quarter of these attacks (26.57%), with 12.2% targeting the UK, 9.92% targeting Japan, and 8.55% of attacks impacting online retailers in the Philippines.



# Client-side attack surface is real

Finally, with an average 31 JavaScript resources per site, online retailers are vulnerable to forms of theft such as form-jacking, data-skimming, and Magecart attacks, in which criminals target online shopping carts to steal customers' payment information.

**The average number of JavaScript services on retail websites is 31**



# The Covid effect on Black Friday and Cyber Monday

So, what does this mean for online retailers?

Probably the most important thing to take from these findings is that we're about to experience a Black Friday like no other. Since the introduction of global lockdown measures in March and April 2020, traffic to eCommerce sites has, on a number of occasions, exceeded the peaks typically seen in the holiday shopping season. But, while this is obviously great news in terms of revenue, it's hugely concerning when you consider that the volume of cyber-attacks on online retailers is also at an all-time high.

Whether it's committing fraud, stealing your customers' financial information, or damaging your brand, different attackers will use different techniques depending on their objective. And although some regions are more prone to attack than others, retailers can't consider themselves safe simply because their sites aren't based in the US, Russia, or Japan.

With an idea of the scale of security challenge that lies ahead, Imperva can help retailers ensure they enjoy the rewards of their most profitable holiday season yet.

Probably the most important thing to take from these findings is that **we're about to experience a Black Friday like no other**

# About Imperva

Imperva is the cybersecurity leader whose mission is to protect data and all paths to it. Imperva protects the data of over 6,200 customers from cyber attacks through all stages of their digital transformation. Imperva provides application and data security solutions to help organizations implement and sustain security, compliance and privacy initiatives.

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.

We offer best-in-class cyber security solutions from the edge to the database to protect your most valuable assets:

- 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 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.