



Entering Through the Gift Shop

Attacks on Commerce

Table of Contents

2	Commerce at the forefront of cyberattacks
3	Key insights of the report
4	Web application and API attacks
10	Third-party JavaScript: A pathway to supply chain attacks
13	The assaults on commerce consumers continue
20	Phishing campaigns during the holiday season
23	Attacks on Commerce: APJ Snapshot
33	Attacks on Commerce: EMEA Snapshot
42	Conclusion: Combating attacks against commerce
43	Methodology
44	Credits

Commerce at the forefront of cyberattacks

Commerce organizations are challenged with a complex and dynamic attack surface that continues to introduce risks, resulting in both server-side and client-side threats. Because of the nature and troves of sensitive data like personally identifiable information and payment account details these organizations possess, the commerce vertical remains one of the most attacked industries and a lucrative target for cybercriminals.

Compared to other industries like financial services and healthcare, commerce is less heavily regulated but needs the same security maturity level. The commerce industry is characterized by a complex ecosystem of infrastructure to secure, such as point-of-sale (PoS) terminals, Internet of Things (IoT) devices, and mobile, and it leverages web applications and APIs to drive business further. Scripts from third-party vendors are often tapped to enhance the overall customer experience and drive conversions on the commerce websites. Doing so introduces another layer of risk, as most third-party scripts use open source libraries, and attackers could exploit vulnerabilities found in them. We see this trend in Magecart-style attacks in which [JavaScript libraries are abused via exploitation](#) of security flaws. Because retailers have a huge volume of sensitive data to protect against, we're also seeing ransomware groups go after them. In our [global ransomware report](#), commerce (retail and hospitality) accounted for 16% of Conti attacks. This is similarly echoed by another [report](#) from Sophos, which observed the surging attack rate in the retail industry.

Although security and IT teams are feeling the pressure of protecting their perimeter and customer information, having [limited security budgets](#) poses challenges for these teams to do more with less. In this latest State of the Internet/Security (SOTI) report, we examine various attack types that commerce organizations and their customers face. We explore our multitude of datasets in areas such as web applications, bots, phishing, and usage of third-party scripts, to get a "pulse" of what's happening in this sector and help cybersecurity leaders and practitioners understand some of the threat trends impacting the commerce industry. Akamai sees an enormous number of attacks across all our security tools, so we can share the shifts we see in malware attacks, customer impacts, regulatory requirements, and emerging threats.



Key insights of the report

- Commerce remains the top vertical for web application and API attacks, with more than 14 billion attacks — largely due to the industry's continued digitalization and the attackers' available selection of web application vulnerabilities to breach their intended targets.
- Local File Inclusion (LFI) attacks increased by 314% between Q3 2021 and Q3 2022, showing an attack trend leaning toward remote code execution (RCE), and attackers leveraging LFI vulnerabilities to gain a foothold and for data exfiltration.
- Server-Side Request Forgery (SSRF), Server-Side Template Injection (SSTI), and Server-Side Code Injection have emerged as critical attack techniques to defend against because of the possible dangers they pose to commerce organizations.
- Half of the JavaScript that the commerce vertical uses comes from third-party vendors, and this introduces the increased threat of client-side attacks like web skimming and Magecart attacks. It is critical to put mechanisms in place that detect these attacks on payment pages to remain compliant with the new requirements in PCI DSS 4.0.
- In addition, attackers could also abuse security gaps in scripts — and as such, can become a pathway to infiltrate bigger, lucrative targets in supply chain attacks.
- Akamai observed malicious bot requests surpassing 5 trillion events in 15 months, with assaults against commerce customers proliferating via credential stuffing attacks that can lead to fraud.

Web application and API attacks

Expanding on the recently released [app and API SOTI report](#), attacks on the commerce vertical have been growing in both complexity and frequency. More organizations are relying on web applications to drive customer experience and online conversions. Adversaries have become aware of this and are taking advantage of vulnerabilities, design flaws, or security gaps, as observed by their attempts to abuse web-facing servers and applications.

Looking back at our 2020 SOTI commerce report, [Loyalty for Sale: Retail and Hospitality Fraud](#), we can compare the attack trends and vulnerabilities we were seeing before the pandemic to trends we are seeing today. Commerce remains the most-targeted web attack vertical, with retail remaining as the leading sub-vertical within commerce. Akamai researchers have also been observing a significant shift in the leading commerce attack vectors, with Local File Inclusion (LFI) having largely surpassed SQL injection (SQLi) and Cross-Site Scripting (XSS). In this section, we will analyze the rise and fall of these vectors and attempt to better understand some of the security impacts that have been occurring in the commerce industry in the past year.

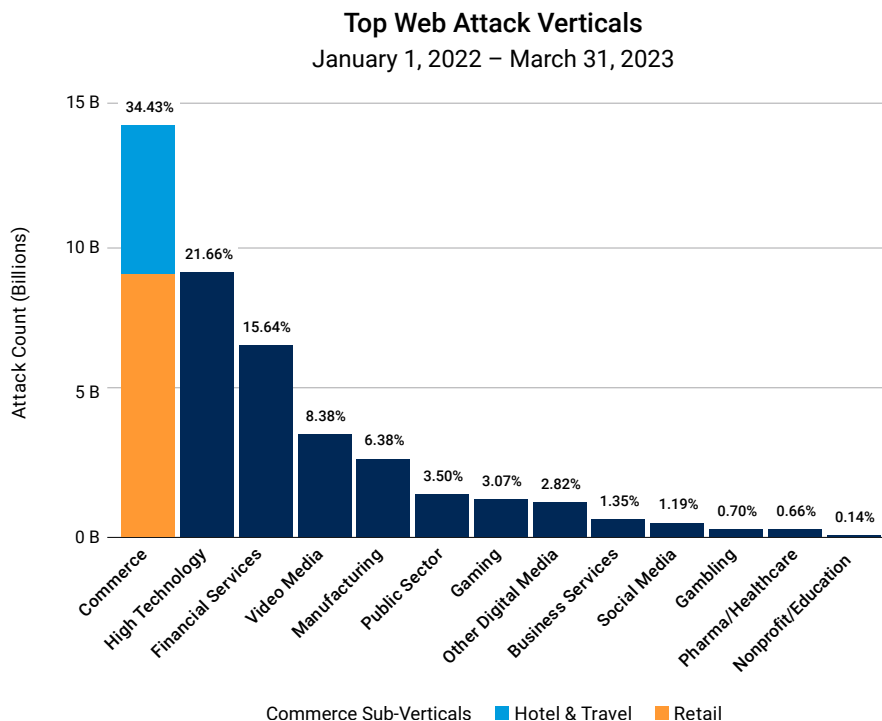


Fig. 1: Commerce remains the most-targeted web attack vertical and accounts for 34% of Akamai's observed attacks (14,530,406,933); retail remains the leading sub-vertical within commerce, accounting for 62% of its attacks



Shift in top injection vectors (from SQLi to LFI)

Akamai data has shown a significant shift in attack vector trends, with LFI attacks leading the way in commerce with 56%, XSS with 24%, and SQLi with 12%. For the two years from 2019 to the beginning of 2021, the top three web app attack vectors were SQLi, LFI, and XSS, respectively. This complete seat change of the top three web attack vectors, as seen in the graphs below (Figures 2 and 3), is echoed accordingly across other industries.

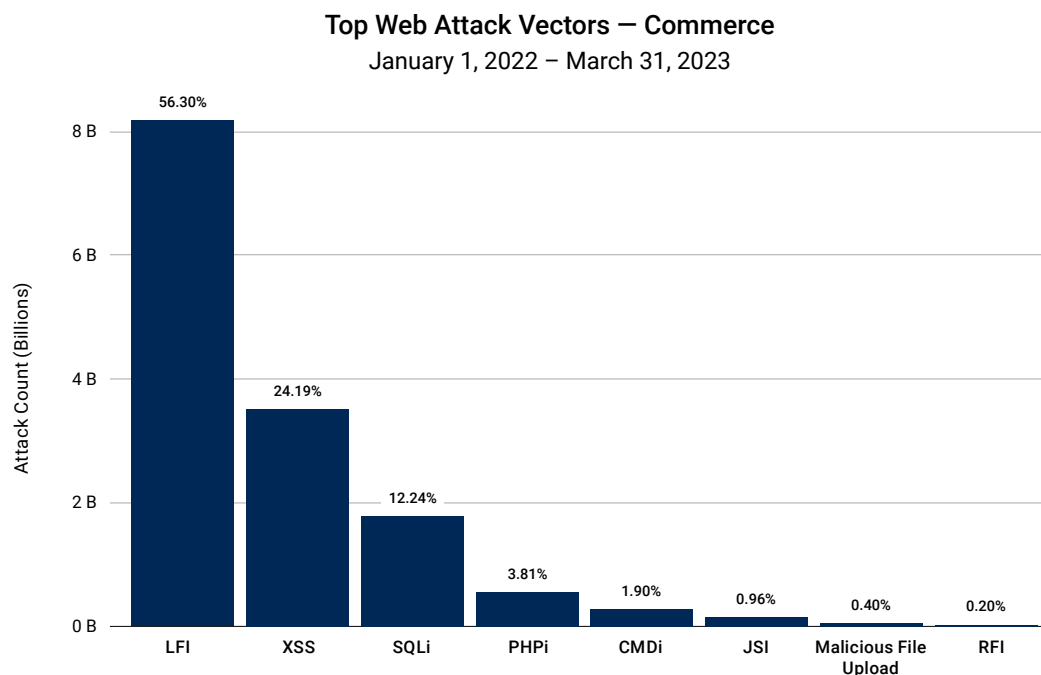


Fig. 2: LFI is currently the top commerce attack vector, more than doubling the amount of XSS attacks

Top 3 Daily Web Application Attack Vectors – Commerce

January 1, 2019 – December 31, 2022

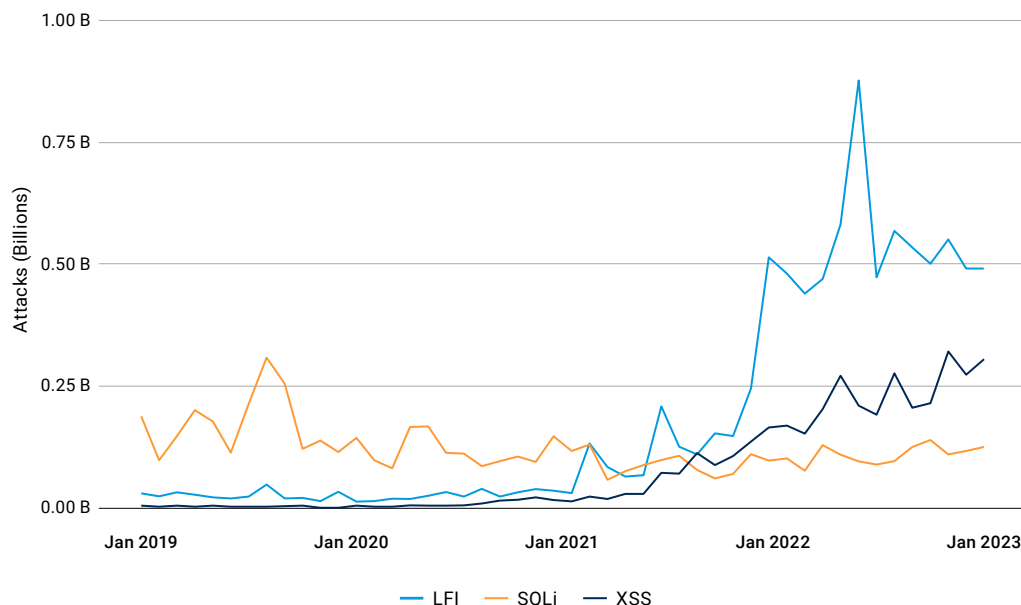


Fig. 3: As reported in our recent [Slipping Through the Security Gaps SOTI report](#), the top commerce attack vector shifted to become LFI attacks in early 2021; LFI attack activity increased by more than 300% between Q3 2021 to Q3 2022

Nowadays, attackers have found the exploitation of LFI vulnerabilities to be more helpful in scanning networks for targets and exposing information leading to directory traversal attacks and deeper breaches. This is as opposed to how it was a few years ago, with the higher volume of SQLi attacks mainly just permitting access to sensitive data. These exploited LFIs may often lead to RCE via attack chaining. Injection attacks are listed as #3 in the [OWASP Top 10](#) Web Application Security Risks. Implementing proper security throughout the development lifecycle would better safeguard against these attacks. Let's take a closer look at the LFI threat.

The main cause for an LFI vulnerability is [improper input validation](#). This means that input being received by a server has not been properly sanitized, and the input may then be permitted to access unauthorized information and receive unauthorized privileges on the server, which can result in a complete compromise of the system. An LFI attack begins with the attacker identifying an application with insufficient filtering or validation of user input, such as with a vulnerable web application's PHP code. The hacker can then modify a URL string with the directive `"../"` or by other means to confirm the ability for directory traversal. Data may then be infiltrated and/or a malicious script may be uploaded by the hacker to the host server.

Even some of the [strongest brands](#) in the commerce world have been victim to LFI vulnerabilities. With the continued [rise of ecommerce](#), it's crucial for these businesses to increase protection against the number one web app attack vector. [Safeguarding techniques](#) include hardcoding the file path so that it is not allowed to be directly modified, confirming proper input validation such as a required concatenation for the dynamic path (e.g., a-z and 0-9 instead of /, /%, etc), and limiting the inclusion from directories to better prevent against directory traversal attacks.

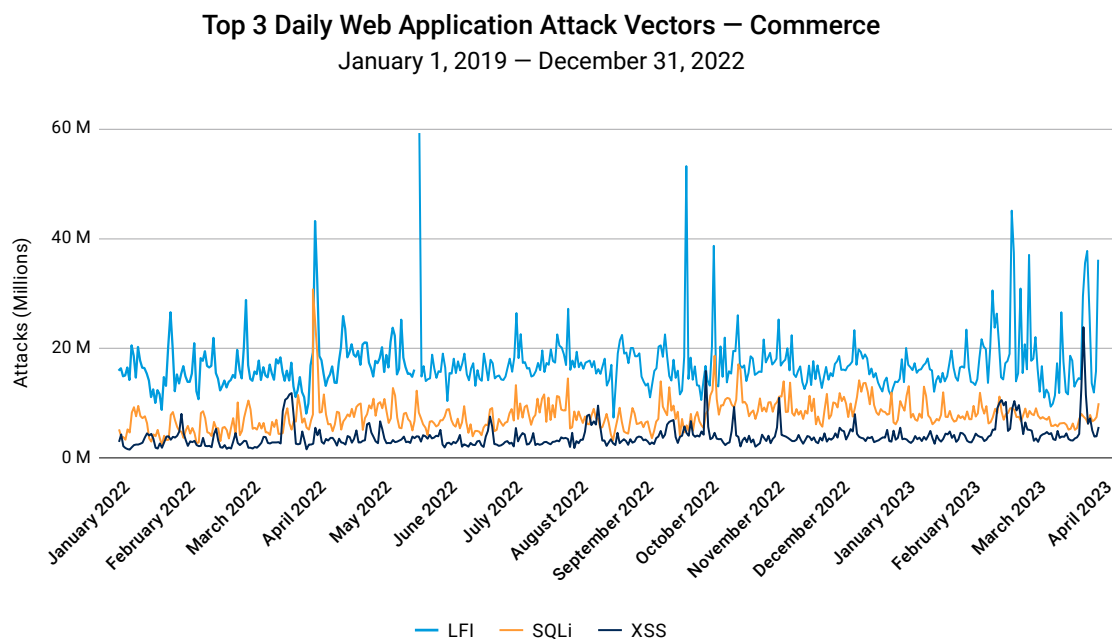


Fig. 4: In the 15-month time span from January 2022 to March 2023, LFI, XSS, and SQLi were the top three attack vectors, and they maintained this trend for the majority of that time

Additionally, this shift in the most active threat technique will drive a change in how companies are validating their security controls. Pen test and red teams should focus on uncovering LFI vulnerabilities. Security programs should ensure that the controls are reporting on both attempts and compromises. By testing the full lifecycle of an attack, we can ensure our security operations center (SOC) processes are able to mitigate them. Finally, leveraging the MITRE ATT&CK framework provides a reason to study the cyber kill chain steps — and the techniques used to execute them.

Other emerging attack vector trends

Attack vectors such as Server-Side Request Forgery (SSRF), Server-Side Template Injection (SSTI), and Server-Side Code Injection have been [gaining popularity](#). They pose a significant threat to commerce organizations and other verticals because of their potential impact and damages caused by them, leading to data exfiltration and RCE. This, in turn, may be playing a role in preventing online sales and damaging a company's reputation. In a [survey by Norton](#), about 63% of consumers said they worry about their data being stolen, and approximately 44% reported they feel more at risk from cybercrime than they did before the pandemic began. Also, in a [survey conducted by Arcserve](#), nearly 60% of consumers said they wouldn't buy from a website that had been breached in the prior 12 months. This poses an additional problem for attacked commerce merchants, especially since their customers would then be likely to switch to market competitors.

SSTI appears to be an attacker's [favored technique for zero-day attacks](#) and represents some of the most significant vulnerabilities in recent years, including Log4j. Akamai researchers observed that when the [Log4j vulnerability](#) was initially disclosed in December 2021, the commerce vertical was affected with approximately 58% of all exploitation attempts. This, along with the increased risks of other vulnerabilities and the expanding online attack surface, may have impacted customers.

It's also important to understand the huge risks and impact that SSRF vulnerabilities have on the commerce industry. SSRFs were initially exploited from Microsoft's Exchange Servers by the Hafnium cybercriminal group and became part of a supply chain cyberattack that impacted an estimated 60,000 organizations, [including commerce](#). Hafnium utilized the SSRF vulnerability to run commands to the web servers. Unfortunately, these widespread Hafnium attacks are [just the beginning](#), as Microsoft Exchange users have been submitting new ransomware attacks that originated from this hack.



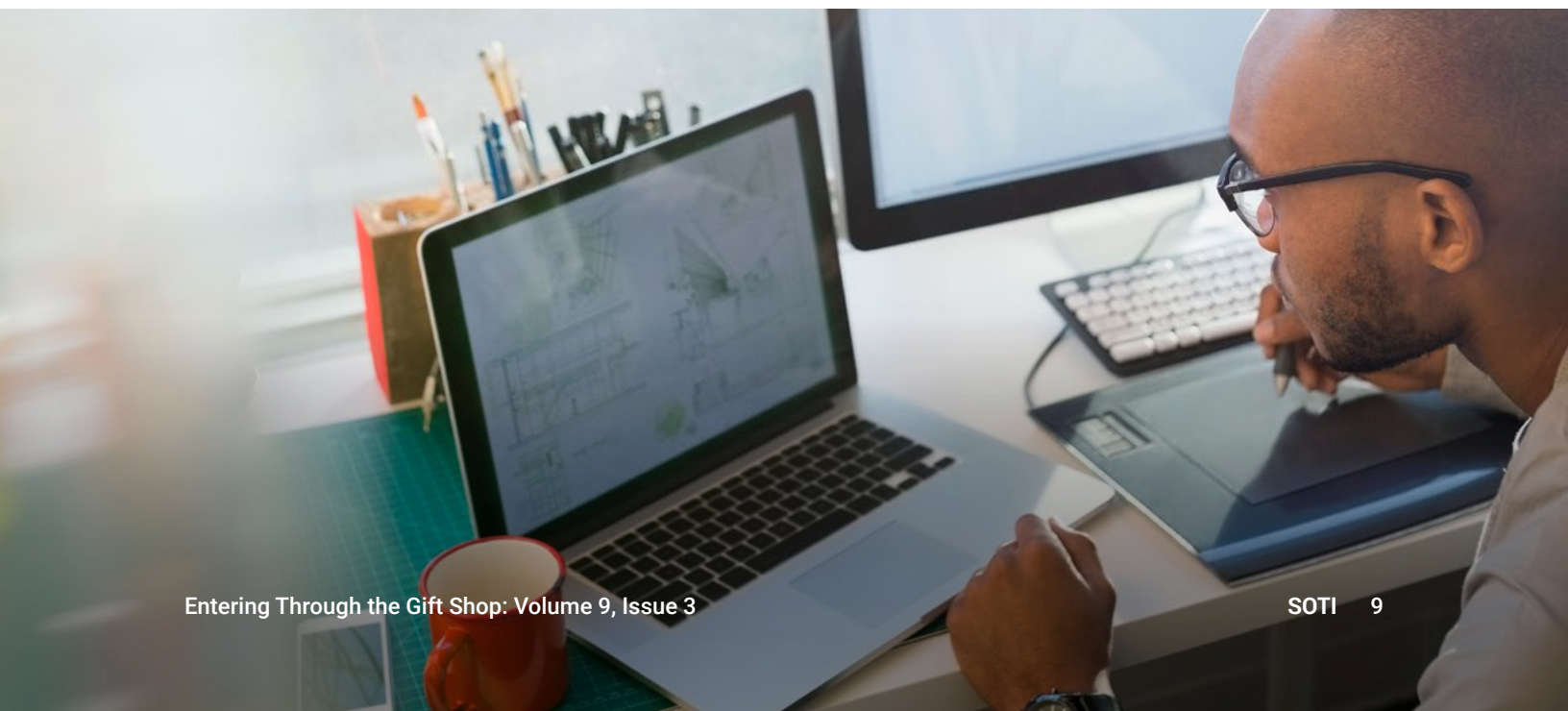


Akamai researchers have observed an [ongoing increase](#) in both authorized vulnerability-scanning traffic and attack attempts searching for SSRF vulnerabilities in other software as well.

So, how exactly do the exploits of SSRF vulnerabilities allow for commerce businesses to be attacked? [SSRF attacks target the server](#) with the goal of privilege escalation for an attacker through bypassing the server's authentication controls. For example, HTTP-to-server requests may be modified by an attacker to specify a URL local to the server itself. This may then allow the attacker to bypass the normal access controls and obtain full administrative privileges. This can occur through various applications, such as in checking to see if a particular item may be in stock [via a shopping application](#).

These kinds of vulnerabilities and techniques exposed from the Hafnium attacks lead to a growing concern for the rise of SSRF attacks in the commerce vertical, among others. SSRF vulnerabilities continue to be significantly exploited and are being utilized for maximum attack by ransomware attackers. From our previous ransomware report in the first half of 2022, we noted retail to be the third-most attacked vertical for ransomware attacks reported by Conti. Given what we've observed, we believe it is safe to assume we will continue to see retail be one of the most attacked verticals within a variety of attack types.

Some basic best practices are to integrate security hooks into the DevSecOps model pipeline (i.e., WAF — App and API protection), turn on blocking and auto-updates for rules (attacks are moving too fast to have a human in the loop), and ensure your solution includes defending against bots and DDoS.



Third-party JavaScript: A pathway to supply chain attacks

Commerce organizations use third-party scripts to quickly add functionality like payment processing, chatbots, and metrics tracking, and to enhance the overall user experience. Although they have many advantages and benefits, third-party scripts can also introduce security risks to your perimeter. Attackers can inject malicious code to a targeted site simply by modifying third-party resources (loaded as part of it), using them in a similar fashion to a backdoor. In addition, they can abuse a vulnerability, and edit the malicious code to one of the third-party vendor scripts loaded as part of the targeted website. In some instances, attackers can scan websites for any client-side vulnerabilities they can leverage as a point of entry. If a particular aspect of the script uses a vulnerable library, each website using it can be at risk of being compromised. And since organizations lack the visibility and control of managing vulnerabilities residing on third-party scripts and other updates, that could potentially become a pathway in breaching their organization.

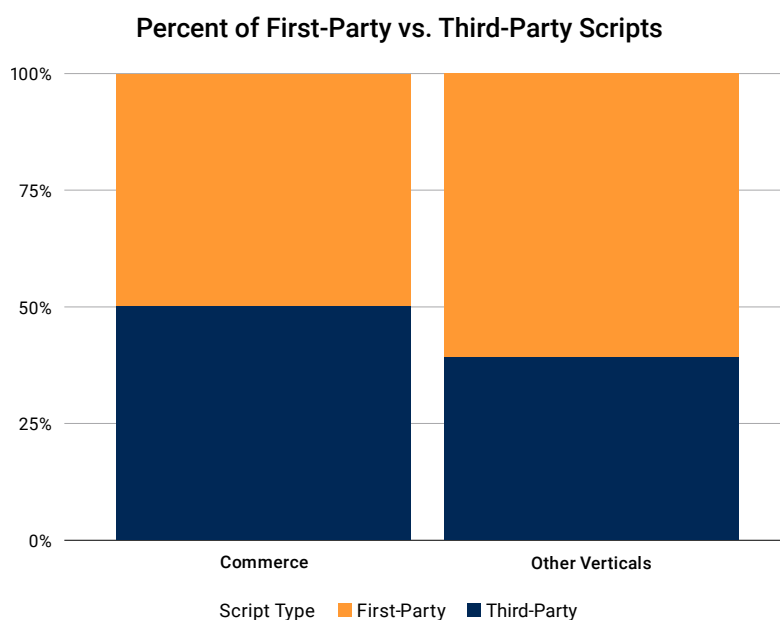


Fig. 5: Half of the JavaScript used for commerce websites is from third-party vendors, compared to all other verticals that only use third-party vendors for 39% of their scripts; this makes commerce companies more prone to security risks associated with using scripts from third-party vendors

Our data shows that 50% of the scripts used in the commerce vertical come from third-party resources (Figure 5). This is relatively higher in comparison to all other verticals (39%). Although using third-party scripts does not necessarily mean that they are less trusted or malicious in nature, it puts organizations at risk of security flaws within these third-party scripts. The security gaps or vulnerabilities could become a pathway for attackers to infiltrate bigger, lucrative targets in supply chain attacks. Attacking organizations via exploitation of third-party resources, which have access to sensitive information and have fewer security protections than the intended targets, could pave the way for attackers to breach other organizations. On the other hand, consumers are also at risk of potentially getting their information stolen or accounts used for unauthorized transactions in Magecart attacks, which we will discuss more in the next section.

The perils of web skimming attacks

Magecart is a specific style of a web skimming attack that leverages ecommerce platform script vulnerabilities. The moniker comes from the popular ecommerce platform Magento. In a Magecart attack, malicious code is injected either in first- or third-party scripts (such as that of the checkout page) via the exploitation of a vulnerability, to gain sensitive information like customer payment details and personal identifiable information.

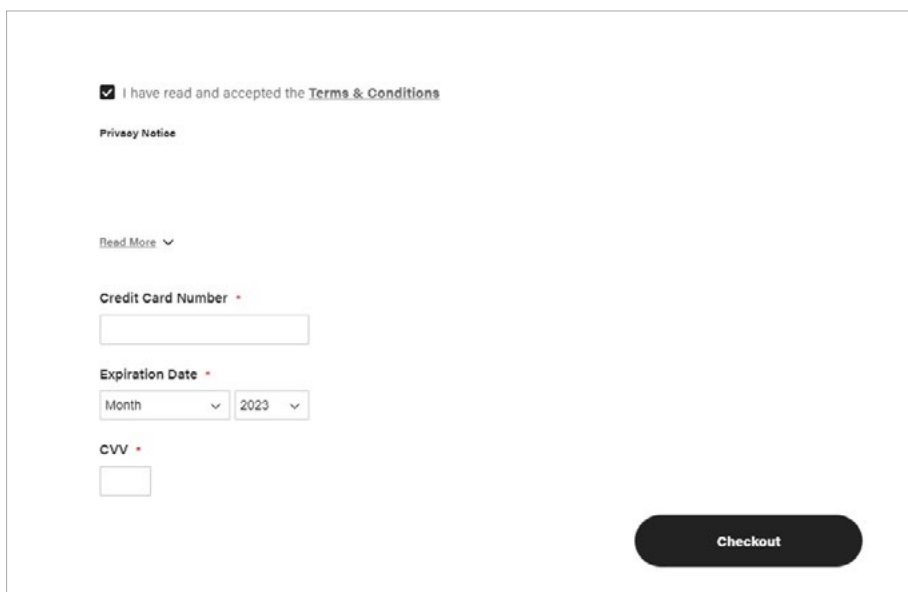
There are three means in which attackers can carry out Magecart attacks:

- Exploit vulnerabilities in the websites to inject malicious code. For example, attackers launched attacks against websites using ecommerce platforms like Magento, WooCommerce, Shopify, and WordPress, which have many known vulnerabilities that can be easily found on the web. Although most of them are patched, some websites may be running outdated versions that put them at risk of exploits.
- Leverage a vulnerability to edit or add the malicious code to one of the third-party vendor scripts that are loaded as part of the targeted website.
- Buy domains of deprecated services/vendors and load the malicious code on the websites where these domains are still running.

Entering Through the Gift Shop: Volume 9, Issue 3

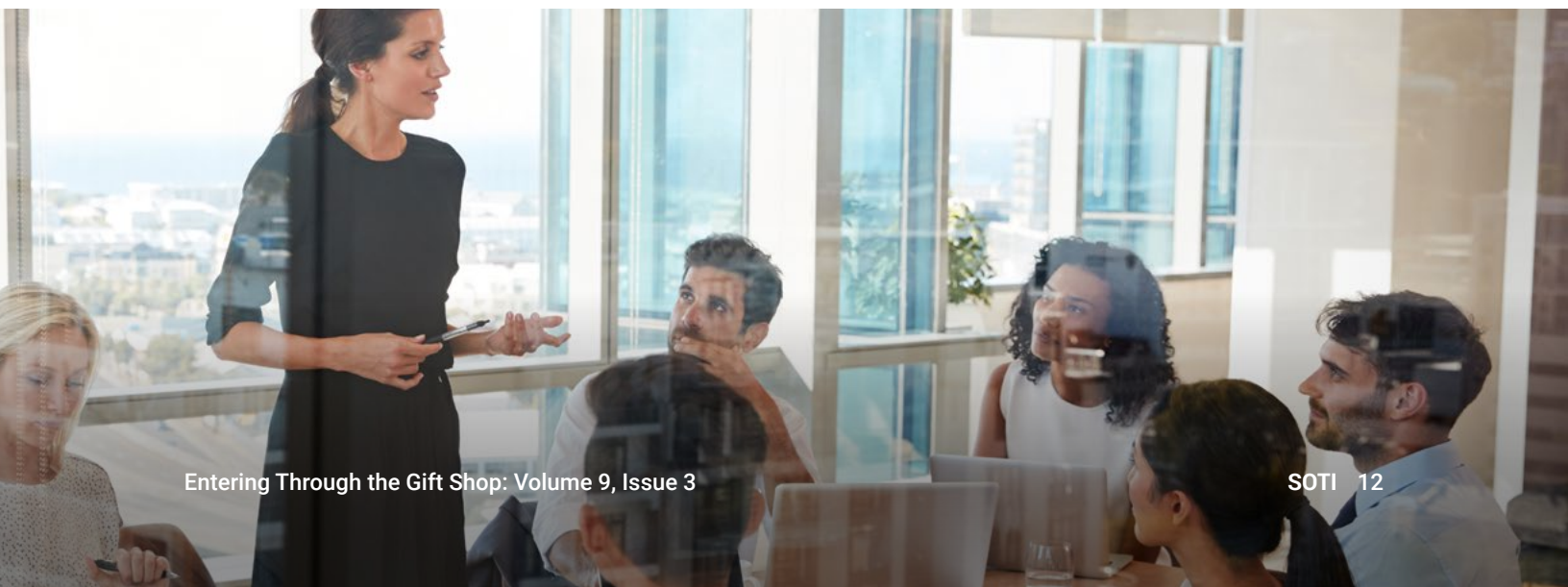
In [one of the attacks](#) we've identified and mitigated, the attacker injected the code in a first-party resource, and users who input and submitted their information in the payment form at the checkout page could have their details (e.g., CVV, credit card number, and name) sent to a C2 server.

Another famous attack from the Magecart group targeted [a major airline](#), abusing third-party scripts in their payment page, which resulted in the theft of users' confidential data such as payment information. This attack reportedly impacted more than 350,000 customers, resulting in a hefty [GDPR fine](#) of £20 million (or nearly US\$25 million as of this writing).



The image shows a payment form with a checkbox labeled "I have read and accepted the Terms & Conditions" and a link to "Privacy Notice". Below this is a "Read More" link. The form includes fields for "Credit Card Number", "Expiration Date" (with a dropdown for "Month" and a "2023" dropdown), and "CVV". A "Checkout" button is at the bottom right. A semi-transparent white box is overlaid on the form, containing the same fields but with a different layout, illustrating a form injection attack.

Fig. 6: The form injection occurs in the targeted site, wherein the skimmer modifies the page and injects a fake form that steals user information before redirecting the user to the legitimate third-party payment vendor





During our analysis of the attack methodologies used in a Magecart attack against one of North America's largest liquor retailers, Akamai researchers saw [similar active attacks](#) that hit more than 100 websites. Attackers used notable tactics like purporting to be Google Tag Manager and developing a fake credit card form (Figure 6) before redirecting users to the legitimate third-party vendor that processes the payment. Once these users click the bogus "Submit Payment" button, it sends the gathered credit card data to its C2 server and points them to the legitimate third-party vendor payment page. It is important to highlight the evolving ways in which skimmers operate. We are seeing web skimmers actively modifying the page — injecting a bogus form to obtain credit card information during the checkout process of an external payment vendor where they do not have any access.

Web skimming attacks are generally challenging to detect because they occur within the browser on the client side, as opposed to common server-side web attacks. However, the ramifications of these attacks could be detrimental to the organization, like damage to its brand and reputation, loss of customer trust, stolen sensitive information, and fines from regulation and compliance issues, amounting to significant financial losses. New script security requirements outlined in the upcoming Payment Card Industry Data Security Standard (PCI DSS 4.0) require organizations to justify all scripts observed on checkout pages, and employ mechanisms to detect as well as alert on script changes, to secure payment card data within the browser against script-based attacks.

Beyond compliance, to combat the hazards that web skimming attacks pose, it is critical that organizations have a comprehensive understanding of what scripts are executing within the browser, and the actions these scripts are taking. Regular scanning to address script vulnerabilities can help stop attacks before they occur. Security solutions like [Page Integrity Manager](#), which analyze script behavior to detect and alert on suspicious anomalies, are instrumental in protecting your customers' information against JavaScript threats.

The assaults on commerce consumers continue

The customers of commerce organizations and websites are also in the crosshairs. Attackers go after the paths of least resistance, and instead of targeting large organizations, they go after their customers with an array of attacks like account takeover and credential stuffing to obtain their information, or use what's in their account to conduct fraudulent transactions. Additionally, stolen personal information or accounts with balances could be sold on the [dark web](#). Attacks against consumers can also have

an impact on commerce organizations; it not only damages their brand and reputation, it puts an additional strain on their security teams and takes up resources and time to address or investigate fraudulent activities conducted without the consumer’s knowledge.

Bot attacks surge, used in scraping and scalping operations

Malicious bot activities targeting the commerce vertical are on the rise, with more than 5 trillion requests observed in 15 months. The ascending number of malicious bots is worth noting (Figure 7), given the many use cases of threat actors leveraging the bots to commit fraud and other malicious attack attempts. Even [benign bots can damage the customer experience](#) by slowing down website performance or conducting price scraping that feeds into audience hijacking tactics designed to lure your customers away to a competing site.

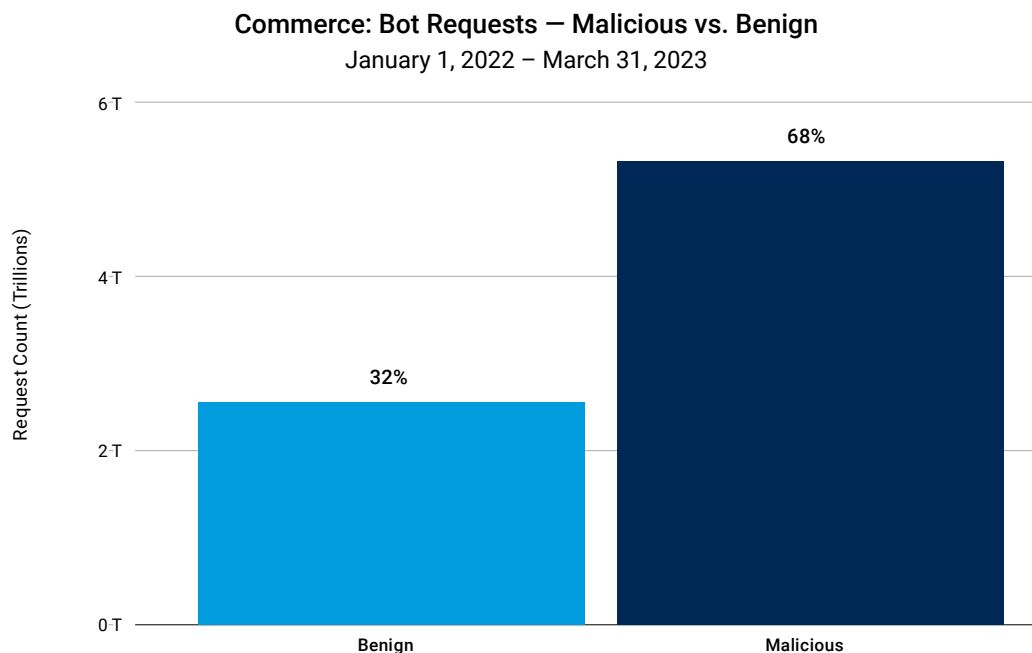


Fig. 7: The overall number of malicious bot requests surpassed 5 trillion between January 2022 and March 2023

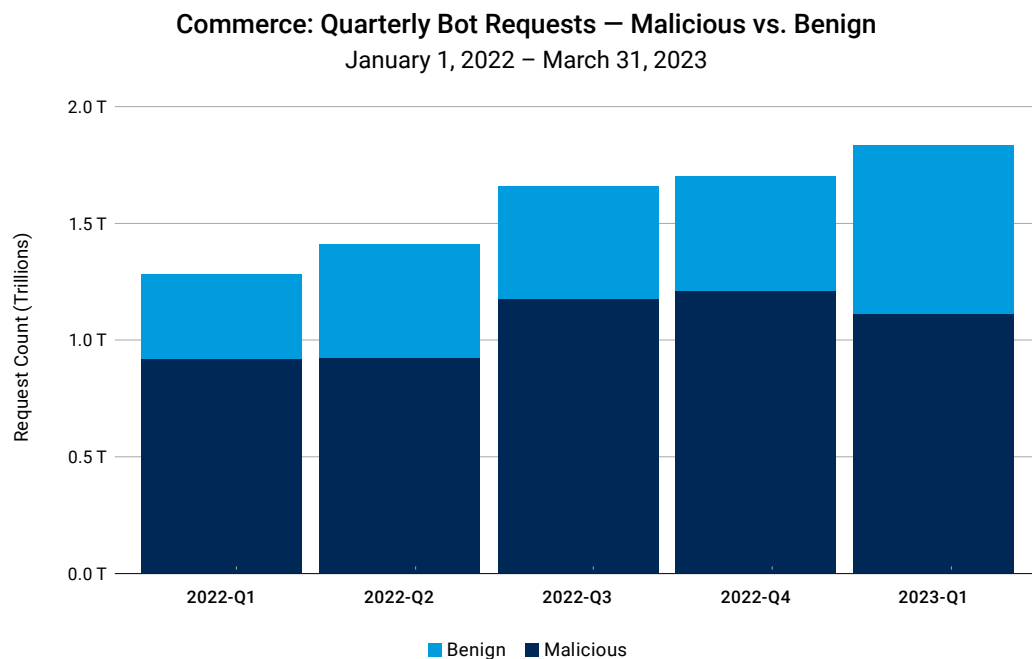


Fig. 8: The increase in the number of malicious bot requests in the later part of the year may be due to holiday online shopping

It is also interesting to see how bot activities tend to spike toward the later part of the year, in time for holiday shopping, then level out the following quarter (Figure 8).

Attackers use bots for nefarious purposes like credential stuffing attacks via automating username and password combinations (stolen through phishing attacks, via data breaches, or sold on the dark web), leading to account takeover. Because password reuse is a common practice, this inadvertently makes it easier for attackers to try out these stolen credentials in multiple accounts via automated tools like bots. Once these login attempts are successful, attackers could potentially drain what's in the user's account and use it for their own purposes.

According to a [report from Okta](#), there were about 10 billion credential stuffing attack attempts in the first quarter of 2022, with retail customers as one of the top targets. Attackers may be after a consumer's loyalty or reward points; in other cases, they can monetize the information in the account. The ramifications of credential stuffing attacks could extend beyond consumers, as this could lead to financial losses for organizations as well. For instance, a [fast-food company](#) in North America suffered from this type of attack, impacting more than 70,000 accounts; as a result, they had to restore rewards and account balances.

Case study: Scalping

The use case of bots against the commerce vertical and their customers is not only limited to credential stuffing attacks. Akamai research observes how botnets are being leveraged in various scalping operations, whether it's to score limited-edition items during major sales events, for high demand/low inventory products (e.g., PlayStation), or for promotion of regular commodities like household items (to be sold at full price).

Harnessing the power of botnets in scalping operations

Major sales events (more colloquially known as “hype” or “high-heat” events) are especially common with online ticketing companies and sneaker retailers. Scalpers may design and develop their own botnets to increase their success while participating in these events, or simply buy a license from one of the bot products available on the market designed for scalpers and hype sales events. Prices may vary based on their known checkout success rate. The following two examples appear on a regular basis and illustrate the products’ sophistication:

- [“Most Advanced Bot”](#) offers various bot solutions for some of the top retail brands on the internet for prices between \$79.99 and \$99,999. Sneaker bots, which require more complex software to defeat the advanced bot management products that protect those sites, usually cost the most. The product is a Google Chrome extension, and the user has to provide a description of the item they are looking for; enter their login, payment, and shipping information; enable the bot; and let it do the work.
- [AIOBot.com](#) offers a \$299/year subscription to its software, which is compatible with many retailer websites. The subscription includes regular software updates to stay effective and keep up with the evolution of bot management products. AIOBot supports proxies to load balance the traffic through multiple IP addresses to reduce the risk that bot management solutions will block the traffic.



Easily available tools, such as bot software, lower the bar and allow cybercriminals without the technical knowledge or infrastructure to get into the game by simply availing “as a service” offerings in the underground markets. From the point of view of the defenders, this shows the extent of the adversarial challenge that bot management product vendors face: Many developers produce easy-to-use software designed to defeat detection and provide the best service to their users.

Bots outpace regular customers during major sales events

Due to the high-profile nature of these events, and the revenue potential for scalpers and “bot vendors,” the incentive is significant – driving a high level of sophistication and persistence of the attack. Figure 9 represents how botnets are used as part of the operation:

1. The scalper configures the botnet before the event to execute the checkout workflow that includes defining a set of credentials to log in to the site, credit card information, and shipping address to complete the checkout process. Bots will “listen” for the announcement that the event has started and immediately grab as many items as possible and check them out. The operation is so fast that regular users cannot compete and will have a harder time successfully checking out one of the items.
2. Once the purchase is completed and confirmed, it will be posted on a marketplace and sold at a premium.
3. A regular consumer who missed out on the sales event or was unable to purchase the item may be willing to pay the premium and buy it.

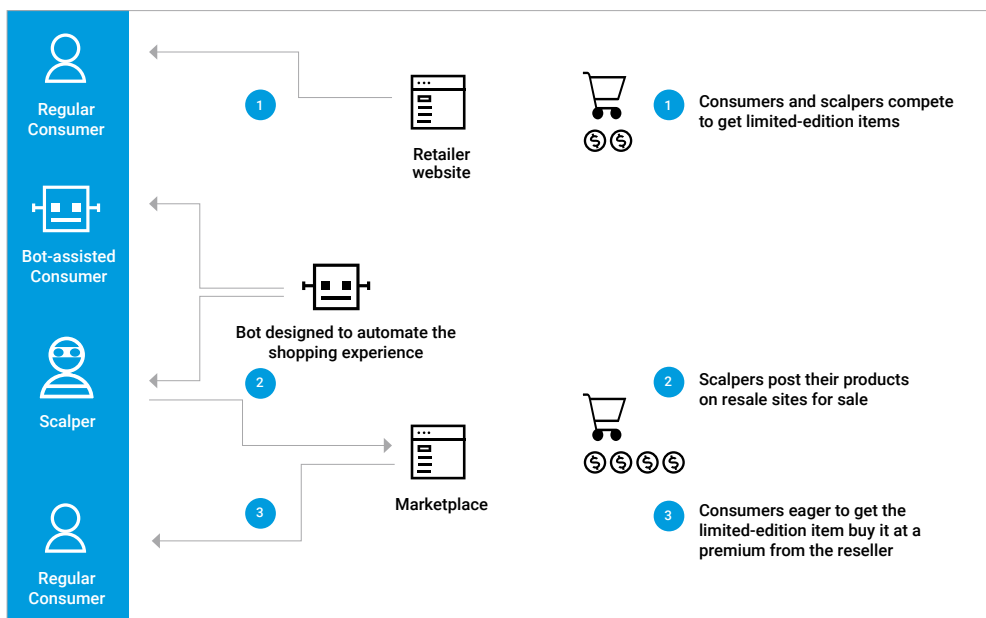


Fig. 9: How scalpers use botnets during major sales events to score limited-edition items
Entering Through the Gift Shop: Volume 9, Issue 3

Scalpers make profit through bargain hunting

Scalpers who are after low inventory or discounted products employ botnets not only to check out these products but also to scrape websites to find the inventory or good deals. Several “scraper as a service” offerings are available for hire, and can be used to analyze data collected and generate a shopping list that fits certain criteria that meets a predefined profit margin. Figure 10 provides an overview of the operation:

1. Once the botnet is deployed and configured, it scrapes targeted websites on a regular basis. Its behavior is similar to any web search engine indexing a site and visiting every possible link to find all the products. If the scalper is only after specific products, the activity may be limited to a small area of the site.
2. The data collected is sent to a database, analyzed based on predefined criteria, and the results on the products and sites found are returned to the operators.
3. The operator reviews the data, refines the “shopping list” if needed, and purchases the targeted products. This step may be automated to speed up the operation. If the scalper is attempting to buy a larger inventory, they will have to use multiple accounts to reduce the risk of being detected by fraud prevention products.
4. Once acquired, the items will be posted for sale for a premium on a consumer marketplace.



Unlike the hype events scenario, the scalper may not make a significant amount of money with each sale — what will make the difference here is the volume of items sold. A US\$15 net profit on 100 units of the same item translates to US\$1,500.

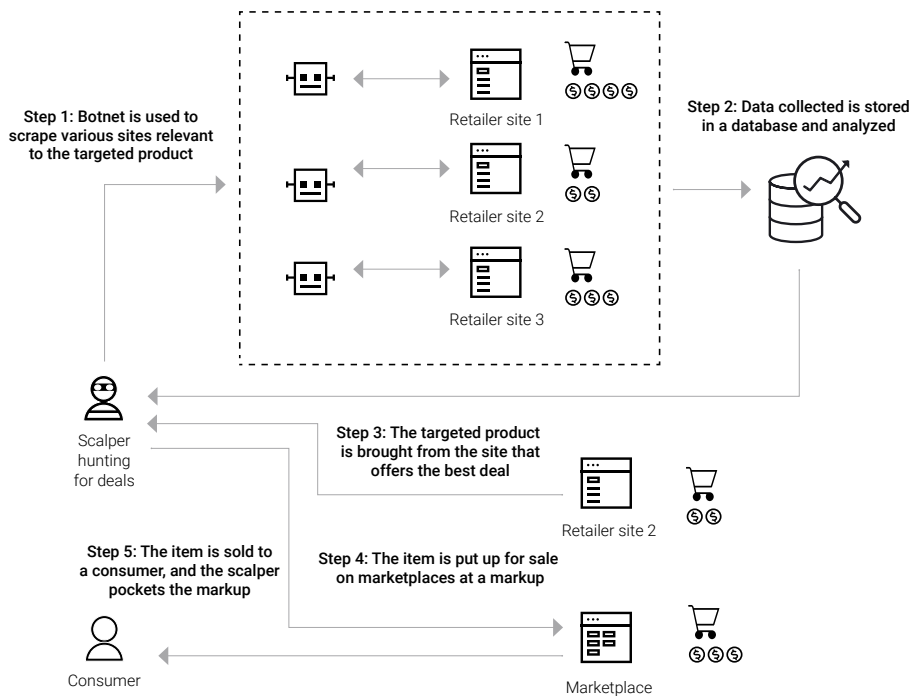


Fig. 10: How scalpers use botnets to scout for products, reselling them at a margin to gain profit

The impact of scalping to retailers and consumers

Scalping impacts retailers and consumers differently. Consumers are the ultimate victims of these schemes, since they are the ones paying a premium for products. They may not compare prices before buying commodities, and such user behavior may have enabled the scalper's business model. For retailers, the impacts are multiple, but ultimately boil down to financial losses. The recurring scraping activity significantly increases the website activity, and subsequently the cost of infrastructure to service these requests; in some cases, this may cause occasional site instability and unavailability issues, which directly translate to loss of revenue.

Additionally, scraping traffic skews site analytics, critical for strategic decisions on product offering and pricing. Lastly, scalping can impact consumer trust and erode brand reputation, especially when it comes to hype events. Consumers who feel that they are not treated fairly may also take their business elsewhere, which again leads to revenue loss for retailers.

Entering Through the Gift Shop: Volume 9, Issue 3

Phishing campaigns during the holiday season

Retailers remain prime targets for fraudsters impersonating their brand and logo to effectively lure unsuspecting customers via phishing attacks. Although retailers and travel/hospitality organizations continue to face threats like phishing year-round, we see more attacks against them during the holiday season. This is similarly echoed in the report [2022 Holiday Season Cyber Threat Trends by Retail and Hospitality ISAC](#), where phishing and credential harvesters are the top threats highlighted by commerce organizations. In Q1 2023, Akamai research observed that more than 30% of phishing campaigns (Figure 11) were activated against commerce customers. Although we saw more campaigns than actual victims, it is also worth noting that attackers are targeting this industry, and users must remain vigilant as cybercriminals may be after their personal or banking information.

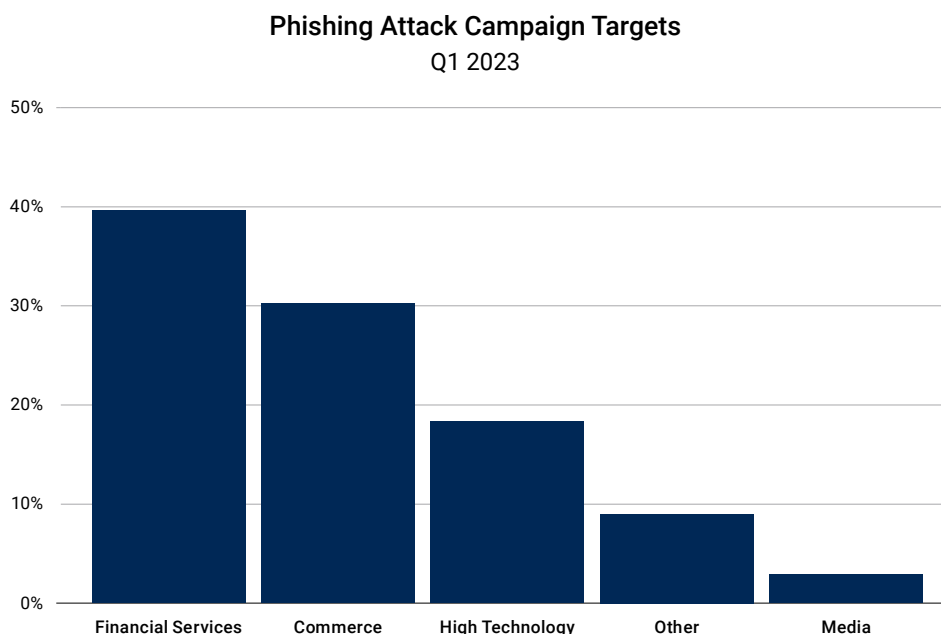


Fig. 11: Over 30% of phishing campaigns targeted ecommerce brands in Q1 2023

While it is no longer surprising to hear about phishing attacks capitalizing on the holiday season, or attackers ramping up their campaigns in one of the busiest times of the year, what is notable is the growing sophistication of both the phishing kits and the attackers behind them. Case in point: Last year, we unearthed a [phishing kit that mimics reputable brands](#), is delivered via email, and is characterized by fake sites that are well crafted, design-wise, to gain the trust of the victims. The social engineering tactics also involve promising a reward (Figure 12) when consumers complete a survey in five minutes (a specific time is indicated, including an actual stopwatch to create that sense of urgency). Users need to input their personal information to obtain their supposed prize and for shipping purposes. However, attackers end up gaining their credit card data.

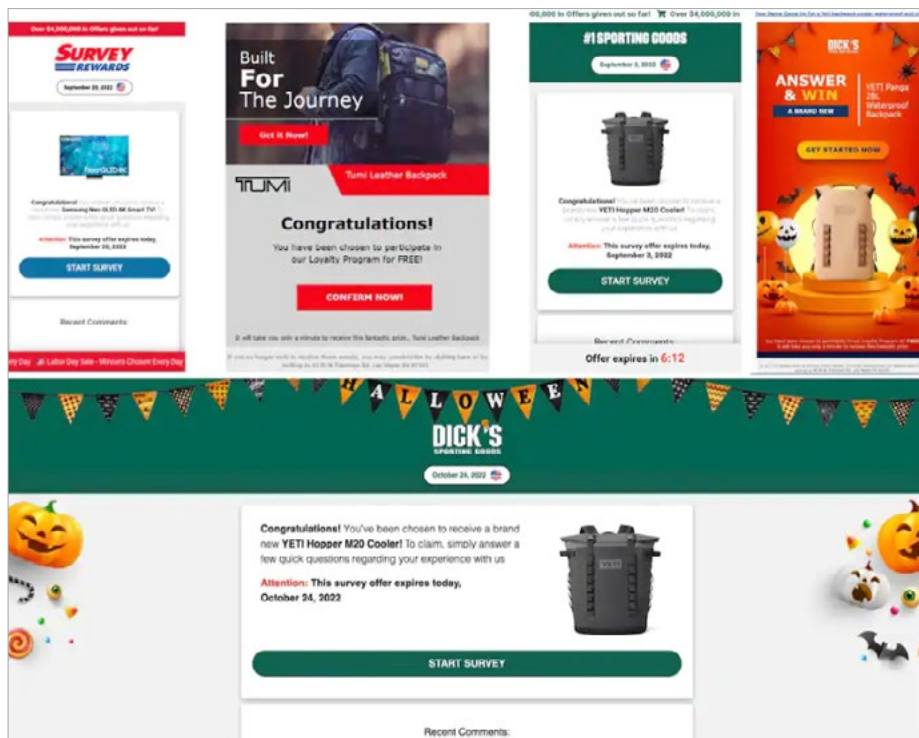
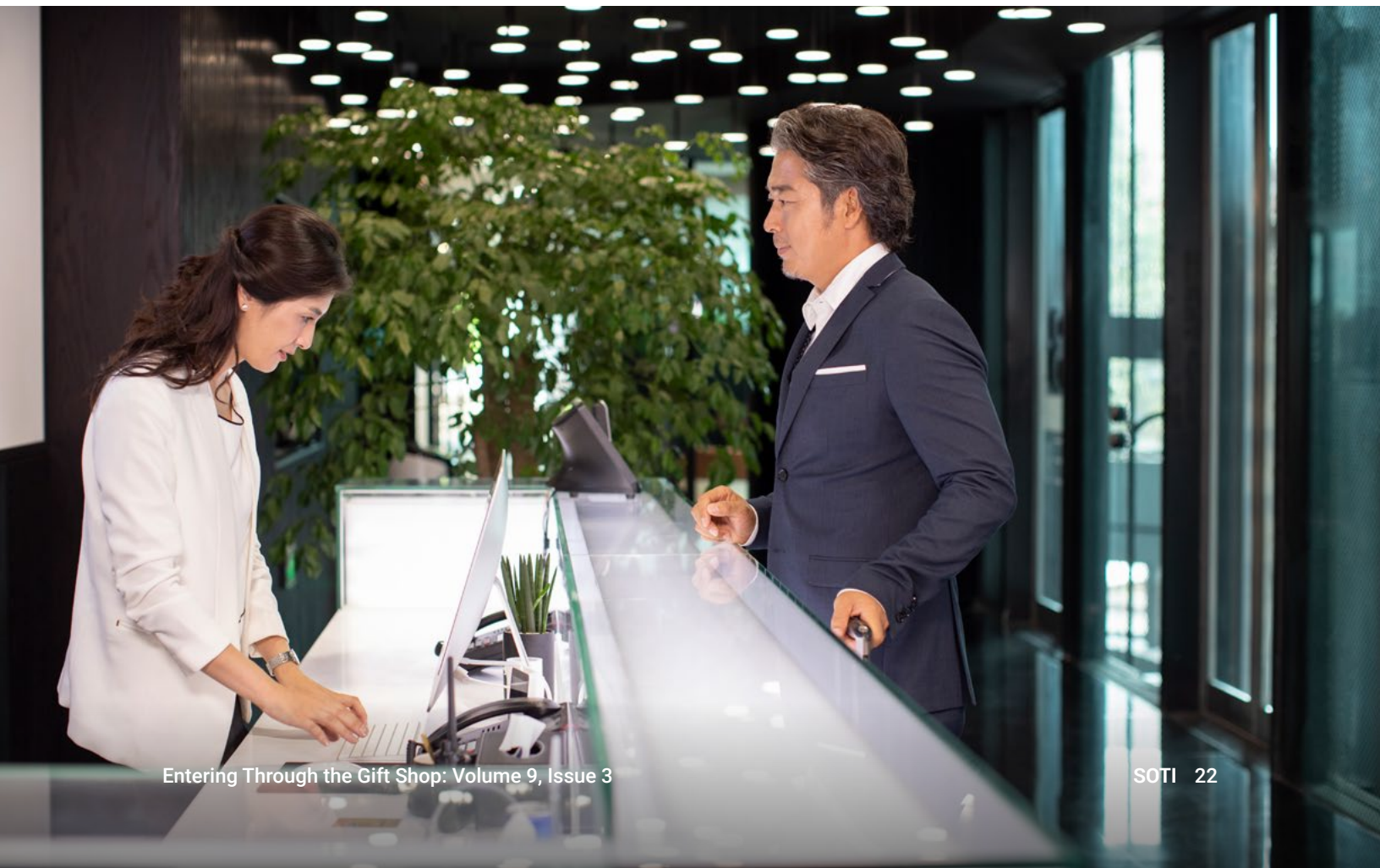


Fig. 12: Phishing campaigns leveraged the holiday spirit to steal user information



What makes this campaign dangerous is the resiliency of the scam's infrastructure, using cloud services to deploy a chain of multilayered redirects including URL shorteners to hide malicious links behind the scam, making them challenging to detect even once some of the redirects are taken down or disabled. Our analysis shows that 89% of affected victims are from the United States and Canada, as cybercriminals created campaigns that target specific geographic locations. This is just one of the many examples of how phishing attacks could impact commerce customers. And of course, these attacks also could harm the brand and reputation of the organizations being impersonated.

For more information on the attack trends in the commerce organizations in the [Asia-Pacific and Japan \(APJ\)](#) and [Europe, Middle East, and Africa \(EMEA\)](#) regions, please refer to the regional sections found in the next section.



Attacks on Commerce:

APJ Snapshot

The APJ Snapshot is a companion piece to our larger commerce SOTI report, *Entering Through the Gift Shop: Attacks on Commerce*. Please refer to that report for detailed descriptions of how adversaries leverage the attack vectors we describe below, recommendations and best practices to safeguard your organization against application and API risks, and our research [methodologies](#).

Web application and API attacks

During the period of January 2022 through March 2023, commerce was the second-most frequently targeted web attack vertical in APJ at 20% (Figure 1). This comes as no surprise given our research conducted for our previous [app and API SOTI report](#), which revealed WAF attacks on financial services in APJ grew 248% from 2021 to 2022 and clearly positioned financial services as the top web attack vertical in the region.

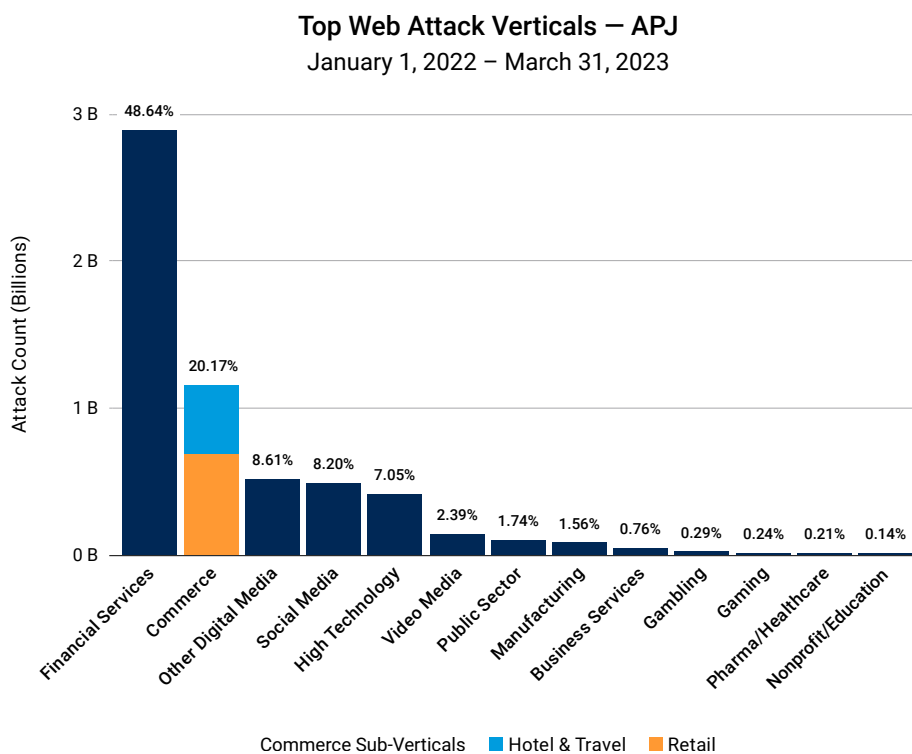


Fig. 1: Commerce (shown as hotel and travel in blue and retail in orange) is the second-most frequently attacked vertical in APJ

However, this does not imply that the impact of these attacks on the commerce vertical is in any way diminished, or that attackers aren't actively targeting this sector. The pandemic-induced rush to quickly release applications to support online conversions has resulted in poor coding, design flaws, and security gaps that attackers take advantage of to abuse web-facing servers and applications.

Looking more closely at our two commerce sub-verticals, we see that retail accounts for 57% of attacks, and hotel and travel 39% of attacks (Figure 2).

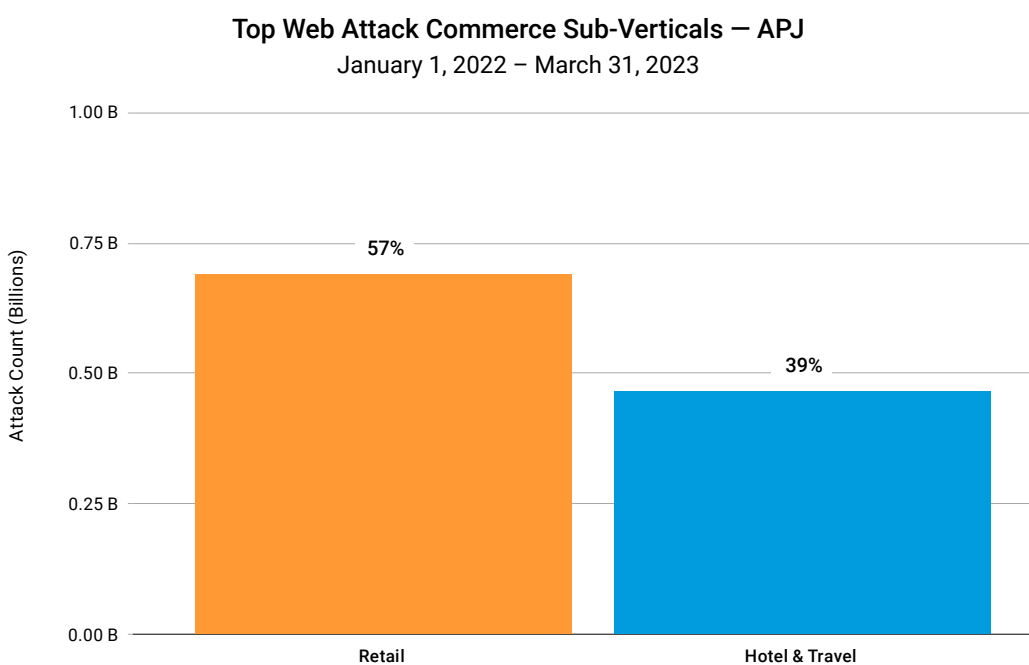


Fig. 2: Attacks on retail versus hotel and travel sub-verticals in APJ

A closer look at sub-verticals

As a region, APJ is second to North America in web attacks on hotel and travel (Figure 3).

Top Web Attack Regions – Hotel & Travel

January 1, 2022 – March 31, 2023

Region	Attack Count	Percentage
N. America	4,660,023,861	86.71%
APJ	464,565,789	8.64%
EMEA	150,905,185	2.81%
LATAM	98,656,861	1.84%

Fig. 3: Top web attack regions for hotel and travel

This is being driven by Australia, in combination with India (Figure 4).

Top 5 Web Attack Target Areas – APJ Hotel & Travel

January 1, 2022 – March 31, 2023

Target Area	Attack Count	Percentage
Australia	296,042,363	63.72%
India	104,251,223	22.44%
Indonesia	30,487,524	6.56%
Singapore	18,235,046	3.93%
Japan	7,183,209	1.55%

Fig. 4: Top web attack target areas in APJ for hotel and travel



The latest cyberthreat report by the Australian Cyber Security Centre (ACSC) cites a [13% jump in cybercrime](#) in the past financial year, with just over half of attacks targeting individuals for fraud and theft. Commerce is a prime battleground, and in our 2020 SOTI commerce report, [Loyalty for Sale](#), Akamai researchers found that cybercriminals target vulnerabilities in the existing workflow and supply chain in the hotel and travel sub-vertical to steal personal information or cash out trade reward and loyalty points. Additionally, [APJ is the fastest-growing market](#) for online travel booking, expected to expand at a CAGR of 9.8% from 2022 to 2030. These factors could be contributing to the jump in cybercrime in the region, and more specifically, attacks on this sub-vertical.

The top web attack target areas in APJ for retail are India and China (Figure 5). Loyalty and rewards programs in combination with a [proliferation of shopping days](#) across these areas, when consumer activity and promotions increase, present attractive opportunities for cybercriminals to ply their trade.

Top 5 Web Attack Target Areas — APJ Retail
January 1, 2022 – March 31, 2023

Target Area	Attack Count	Percentage
India	274,691,549	39.98%
China	160,324,603	23.34%
Japan	97,610,298	14.21%
Indonesia	57,776,552	8.41%
South Korea	52,989,145	7.71%

Fig. 5: Top web attack target areas in APJ for retail

With respect to daily web application attacks, commerce tends to map to all verticals in the region but at a smaller scale, with the exception of a big spike at the end of March 2023 attributed to a different vertical (Figure 6).

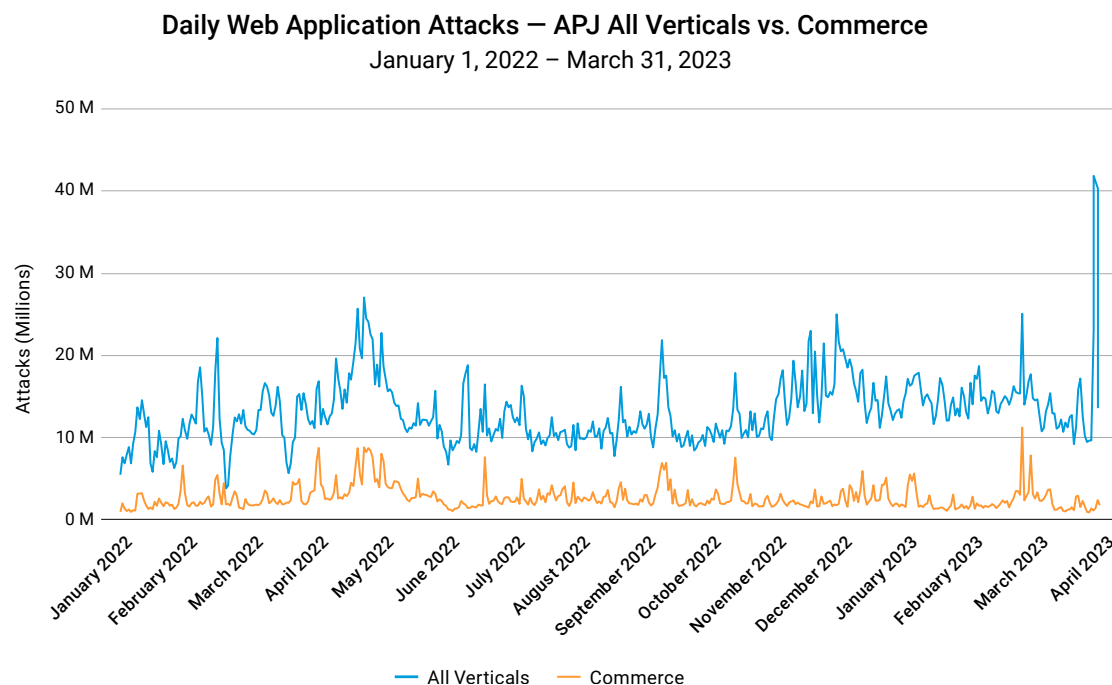


Fig. 6: Daily web application attacks on commerce vs. all verticals

Top injection vectors

APJ commerce and both sub-verticals follow the same global commerce trend in terms of attack vectors, with Local File Inclusion (LFI) being the most popular, followed by Cross-Site Scripting (XSS) and SQL injection (SQLi) (Figure 7).

LFI has risen in popularity over other attack vectors, as attackers have found the exploitation of LFI vulnerabilities to be more helpful in scanning networks for targets and exposing information leading to directory traversal attacks and deeper breaches. Successful exploits may often lead to remote code execution via attack chaining.

It's worth noting that the use of LFI is more prevalent in the APJ hotel and travel sub-vertical (Figures 8 and 9). However, the LFI spike in February 2023 can be attributed to retail. So all commerce companies should focus on uncovering LFI vulnerabilities as well as using tools and best practices to protect against LFI-based attacks.

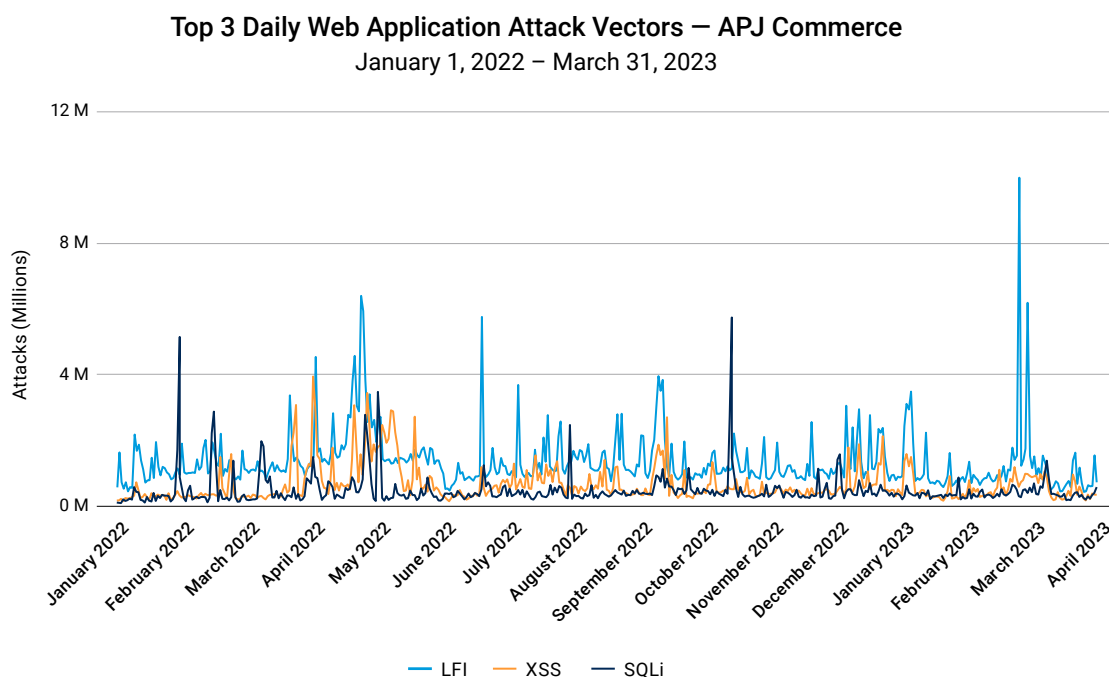


Fig. 7: Daily web application attack vectors for APJ commerce

Top Web Application Attack Vectors – APJ Hotel & Travel

January 1, 2022 – March 31, 2023

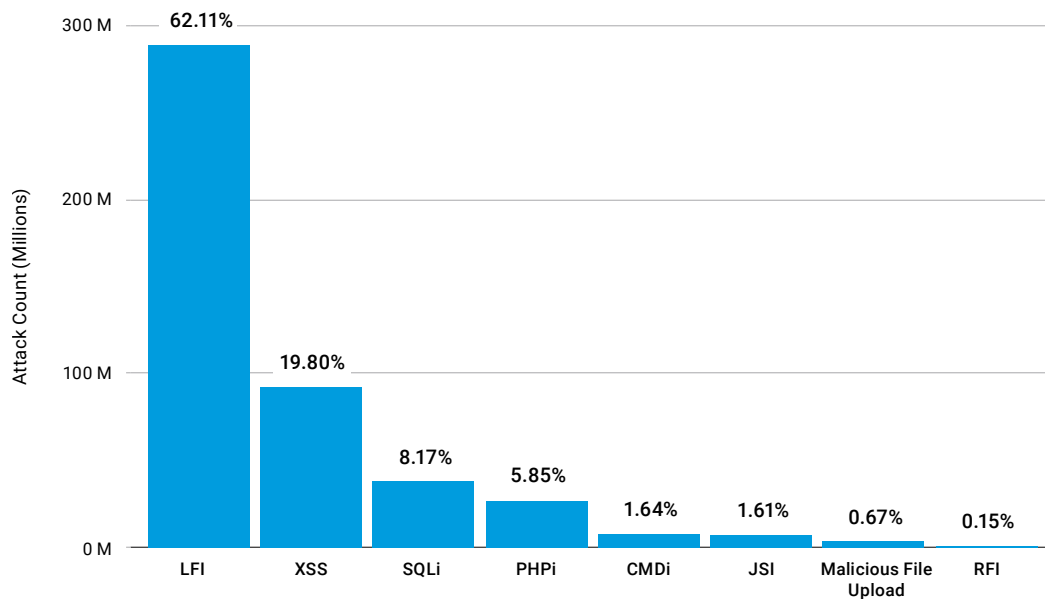


Fig. 8: LFI usage is 3 times higher than the next closest attack vector within APJ hotel and travel

Top Web Attack Vectors – APJ Retail

January 1, 2022 – March 31, 2023

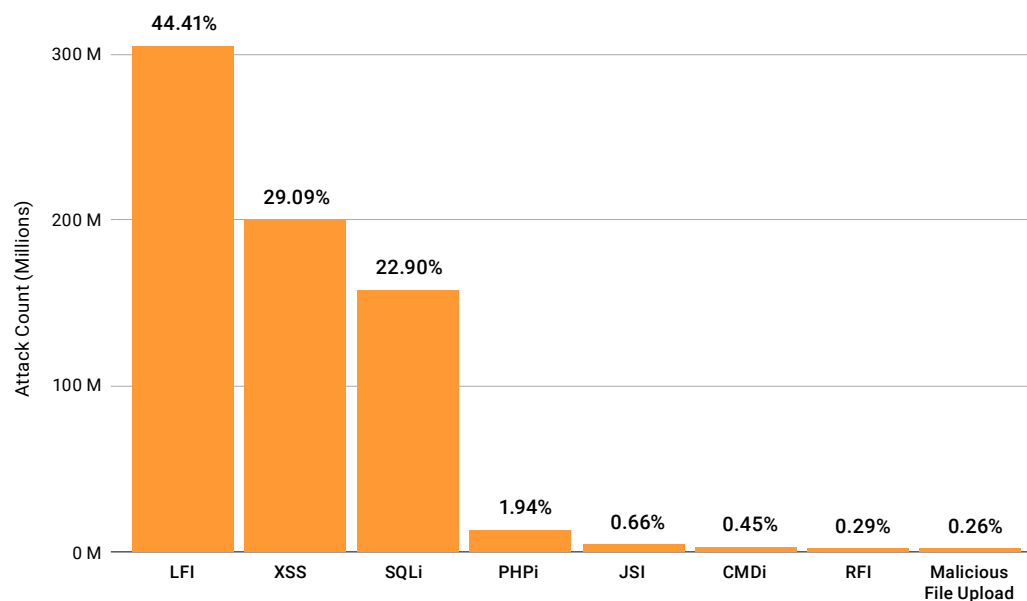


Fig. 9: Top web attack vectors in APJ retail

Third-party scripts: A growing attack surface

Commerce organizations use third-party scripts to quickly add functionality like payment processing, chatbots, and metrics tracking, and to enhance the overall user experience. But because these scripts are out of their control, they have little visibility into the development and testing of the code and potential vulnerabilities. Additionally, third-party scripts may use code from other third parties, which creates more blind spots and pathways for attacks.

Our data shows that 57% of the scripts used by commerce organizations in APJ come from third parties, which is higher in comparison to other verticals (48%) (Figure 10).

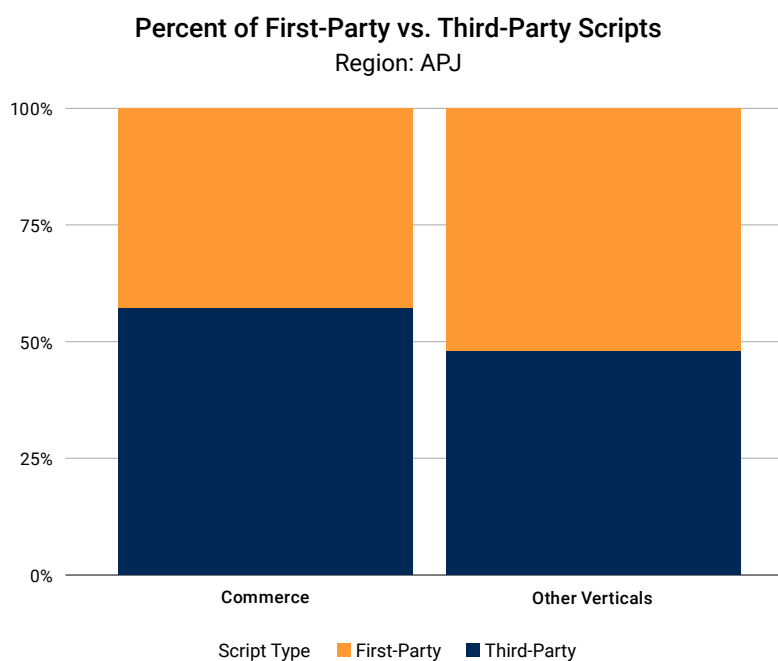


Fig. 10: Commerce organizations use more third-party scripts (57%) than other verticals (48%), which makes them more prone to security risks associated with using scripts from third-party vendors

Although using third-party scripts does not necessarily mean that they are less trusted or malicious in nature, any flaws that exist put consumers at risk of fraud or stolen payment details. It also means increased challenges with meeting the requirements around PCI DSS 4.0 regarding script management.

The hotel and travel sub-vertical is a particularly attractive target since the bulk of all transactions are conducted online. As noted earlier, in APJ the online travel market is projected to grow faster than in any other region, which elevates the risk. All commerce organizations should seize the opportunity to get ahead of these threats before they ramp up further by deploying tools and best practices to mitigate the risk of attacks that take advantage of third-party scripts.

Bot traffic — consumers and retailers under attack

Malicious bots are being utilized by attackers as vehicles to commit fraud or other malicious attack attempts. Even benign bots can damage the customer experience by slowing down website performance or luring customers away to a competing site by conducting price scraping that feeds into audience hijacking tactics.

Between January 2022 and March 2023, the number of malicious bots targeting the APJ commerce vertical exceeded 765 billion (Figure 11). The number and frequency of holiday shopping events throughout APJ and the growth in online travel booking contribute to this level of bot traffic. That said, after quarter-on-quarter growth throughout 2022, malicious bot activity decreased substantially in Q1 2023 (Figure 12).

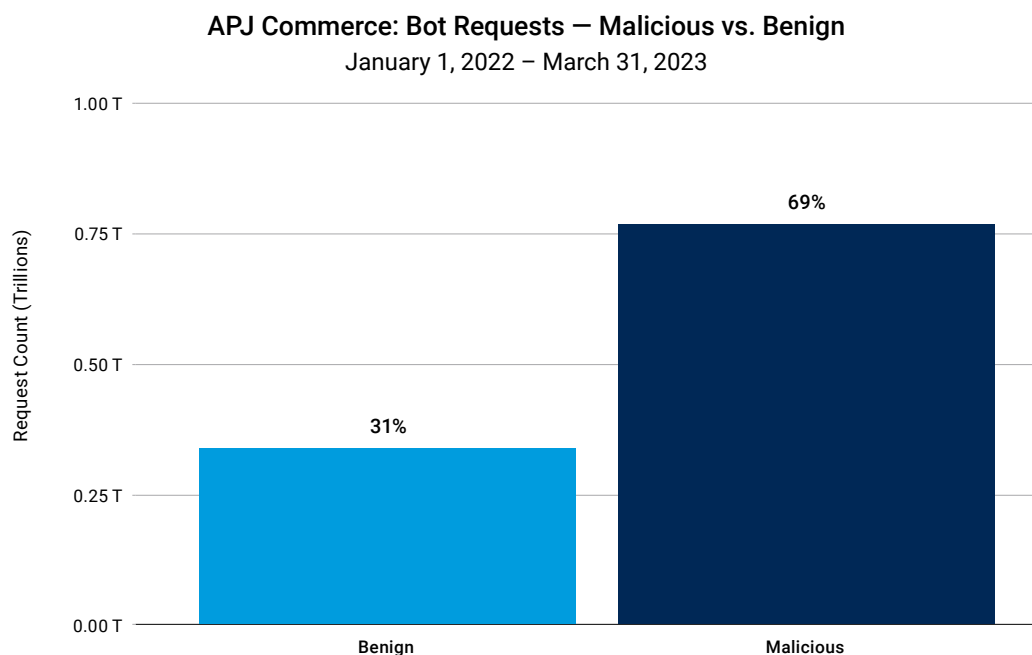


Fig. 11: The number of malicious bot requests exceeded 765 billion between January 2022 and March 2023

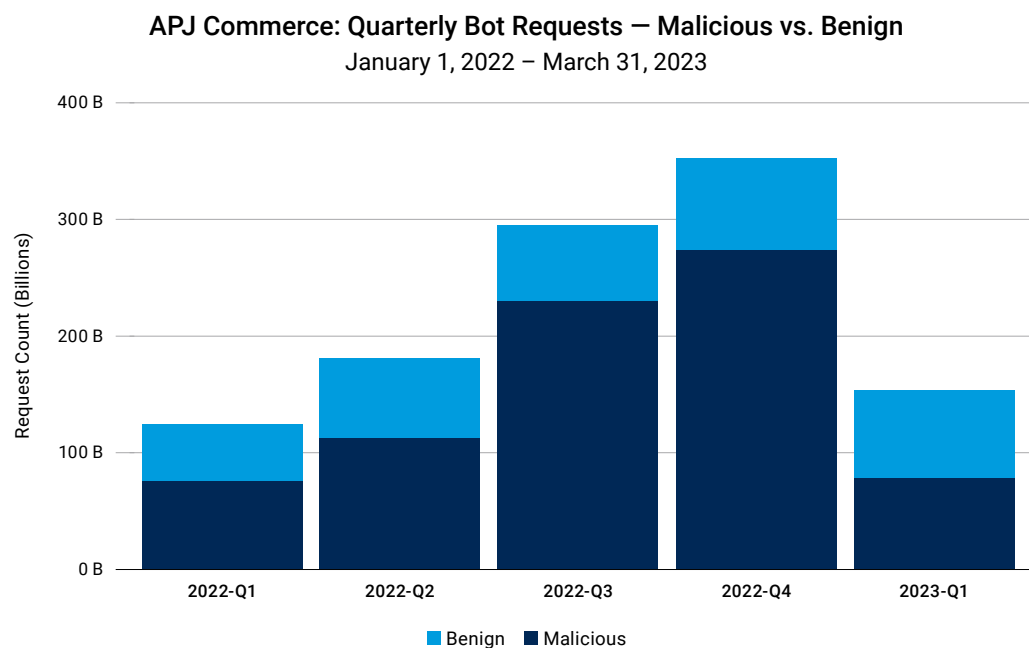


Fig. 12: After quarter-on-quarter growth, malicious bot activity dropped significantly in Q1 2023

There are many use cases where bots figure prominently in the proliferation of credential stuffing, leading to account takeover for the retrieval of personal information and passwords, which can be used to conduct fraudulent activities or sold in the underground markets or on the dark web. Attackers also use them to grab and resell limited-edition items, or scout for bargains they can resell for a profit.

For detailed insights into how these attacks unfold and how bots could impact your customers, refer to our global commerce SOTI report, *Entering Through the Gift Shop: Attacks on Commerce*.

Attacks on Commerce:

EMEA Snapshot

The EMEA Snapshot is a companion piece to our larger commerce SOTI report, *Entering Through the Gift Shop: Attacks on Commerce*. Please refer to that report for detailed descriptions of how adversaries leverage the attack vectors we described below, recommendations and best practices to safeguard your organization against application and API risks, and our research [methodologies](#).

Web application and API attacks

Consistent with the trend in our recently released [app and API SOTI report](#), web application and API attacks on the commerce vertical in EMEA are the most prevalent, making it by far the top web attack vertical at 51%, with video media a distant second at 13% (Figure 1).

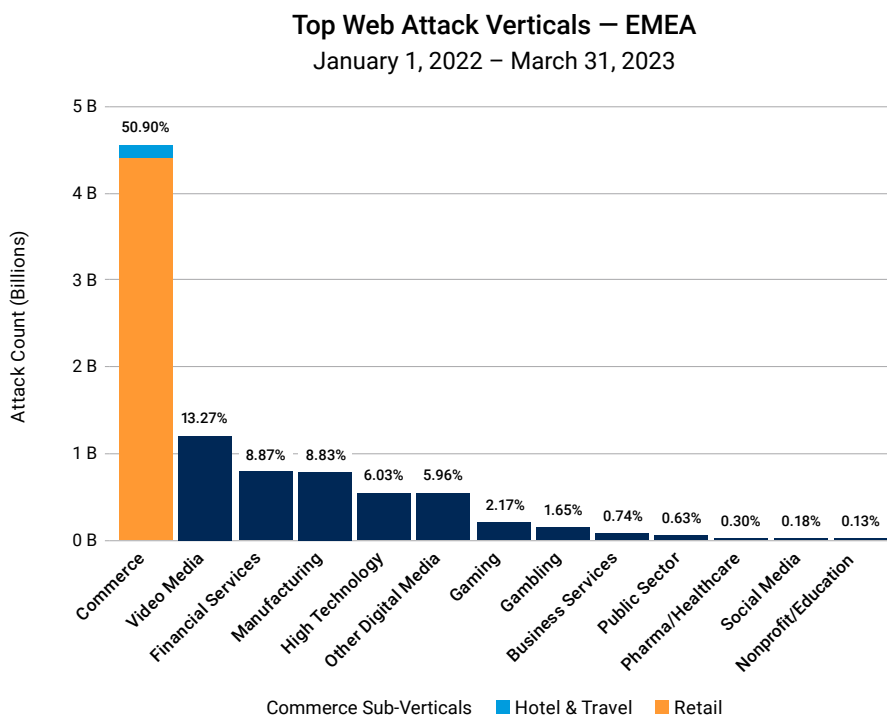


Fig. 1: Commerce (shown as hotel and travel in blue and retail in orange) is the most frequently attacked vertical in EMEA

Several factors can be attributed to the proliferation of web application and API attacks in the commerce vertical, including an expanding attack surface, as more organizations have been releasing vulnerable applications into production in a pandemic-induced rush to deploy apps to enhance customer experience and drive business. Adversaries know this and are taking advantage of poor coding, design flaws, or security gaps, as observed by their attempts to abuse web-facing servers and applications. However, as discussed later, [attacks](#) due to the Russian invasion of Ukraine and the geopolitical environment are additional factors that could have put the region at heightened risk.

In EMEA, attacks on commerce between January 2022 and March 2023 are heavily skewed toward the retail sub-vertical, which accounts for 96% of attacks, vs. 3% for hotel and travel (Figure 2).

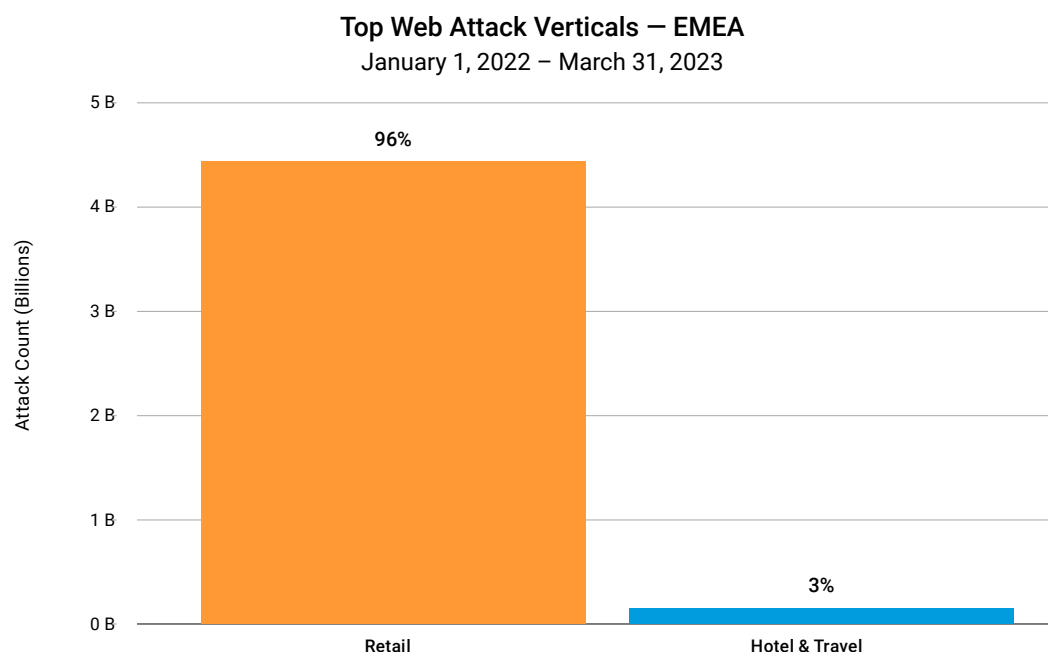


Fig. 2: Attacks on retail dominate in EMEA

A closer look at sub-verticals

Attacks on retail are so prevalent that EMEA is now the overall top attack region for commerce retail at 49%, surpassing North America at 41% (Figure 3).

Top Web Attack Regions – Retail

January 1, 2022 – March 31, 2023

Region	Attack Count	Percentage
EMEA	4,415,642,861	48.66%
N. America	3,767,783,115	41.52%
APJ	687,033,016	7.57%
LATAM	204,679,686	2.26%

Fig. 3: EMEA tops the list of web attack regions for retail

Although the top area for web attacks on retail is the U.S. at 37%, Germany is a close second at 34%, and the U.K. comes in third at 4% (Figure 4). So Germany is driving EMEA's overall top retail attack ranking, with attacks in the U.K. being a key contributing factor.

Top 5 Web Attack Target Areas – Retail

January 1, 2022 – March 31, 2023

Target Area	Attack Count	Percentage
United States	3,386,219,965	37.31%
Germany	3,129,721,504	34.49%
United Kingdom	396,817,996	4.37%
Canada	381,563,150	4.20%
India	274,691,549	3.03%

Fig. 4: Top web attack target areas for retail

Articles and [reports](#), as well as [statements by government agencies](#), point to several factors that may have put Germany in the bull's-eye. However, Akamai researchers believe the situation observed within the commerce industry in Germany could be viewed as an indication of things to come – the potential for a perfect storm of factors to drive such spikes in attacks could happen to any country. With Germany, there were several key factors that likely contributed to this level of attack traffic: the publicized support of Ukraine, the continued rise of LFI attacks (discussed later and in [previous reports](#)) that can lead to remote code execution (RCE) and allow for broad network access and breaches such as ransomware attacks, and the impact of negative social media campaigns.

Across the region, Sweden, Switzerland, and the Netherlands round out the top five web attack target areas in retail (Figure 5).

Top 5 Web Attack Target Areas – EMEA Retail

January 1, 2022 – March 31, 2023

Target Area	Attack Count	Percentage
Germany	3,129,721,504	70.88%
United Kingdom	396,817,996	8.99%
Sweden	174,397,404	3.95%
Switzerland	159,276,524	3.61%
Netherlands	138,574,309	3.14%

Fig. 5: Top web attack target areas for EMEA retail

Daily web application attacks against retail trend upward during the period, while attack activity in hotel and travel remains comparatively consistently low (Figure 6).

Daily Web Application Attacks – EMEA Retail vs. Hotel & Travel

January 1, 2022 – March 31, 2023

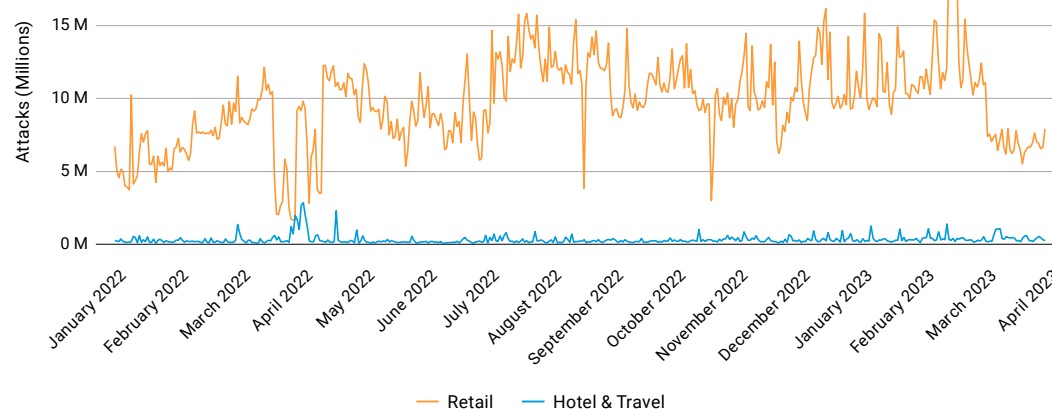


Fig. 6: Daily web application attacks in EMEA retail trend upward

Top injection vectors

EMEA commerce and the sub-vertical retail follow the same global commerce trend in terms of attack vectors, with Local File Inclusion (LFI) being the most popular, followed by Cross-Site Scripting (XSS) and SQL injection (SQLi) (Figure 7).

LFI has risen in popularity over other attack vectors, as attackers have found the exploitation of LFI vulnerabilities to be more helpful in scanning networks for targets and exposing information, leading to directory traversal attacks and deeper breaches. These exploited LFIs may often lead to RCE via attack chaining.

Given the prevalence of attacks on retail and the use of LFI in that sub-vertical (Figure 8) as well as in hotel and travel, all commerce companies should focus on uncovering LFI vulnerabilities while using tools and best practices to protect against LFI-based attacks.

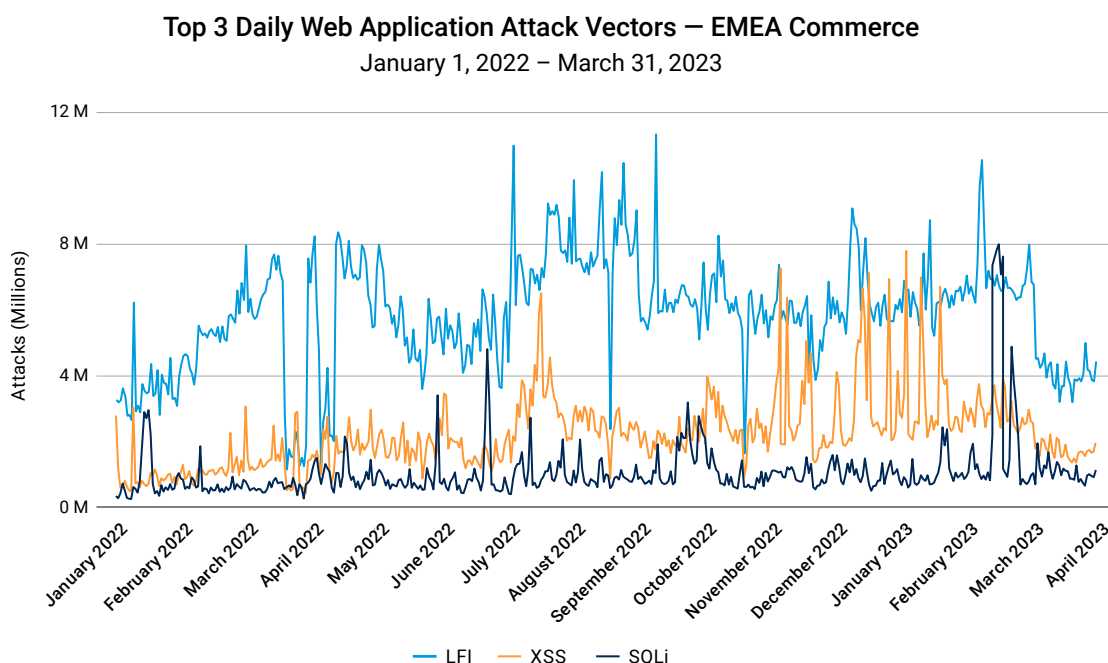


Fig. 7: Daily web application attack vectors for EMEA commerce

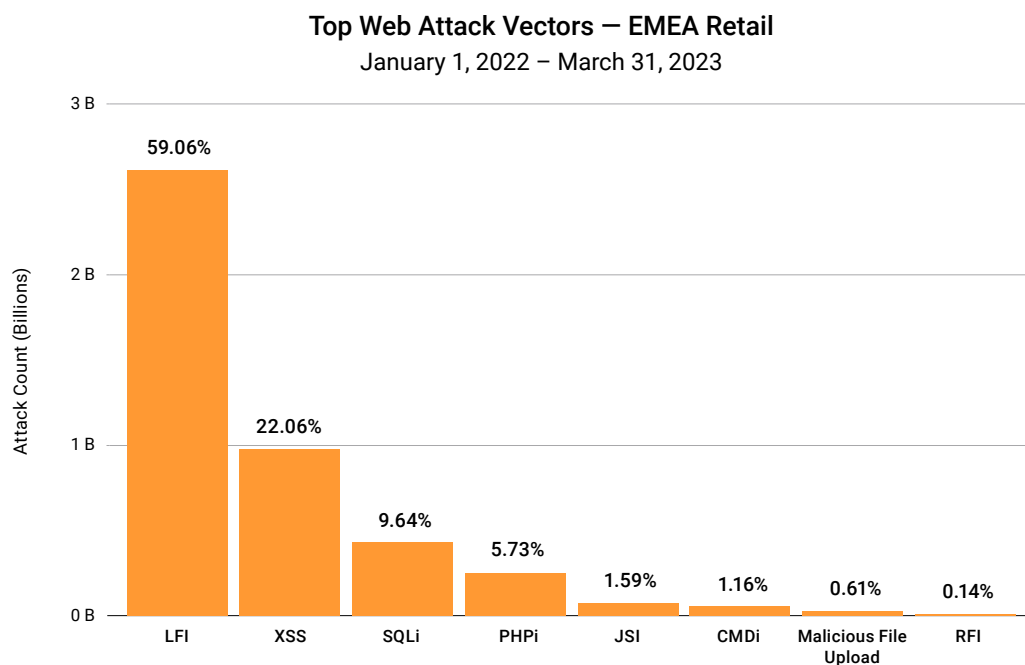


Fig. 8: LFI usage is more than 2x higher than the next-closest attack vector within EMEA retail

Looking at the hotel and travel sub-vertical, usage of these vectors is more in parity, with SQLi and XSS reversing positions (Figure 9). This is likely due to a spike in the use of SQLi-based attacks in February 2023.

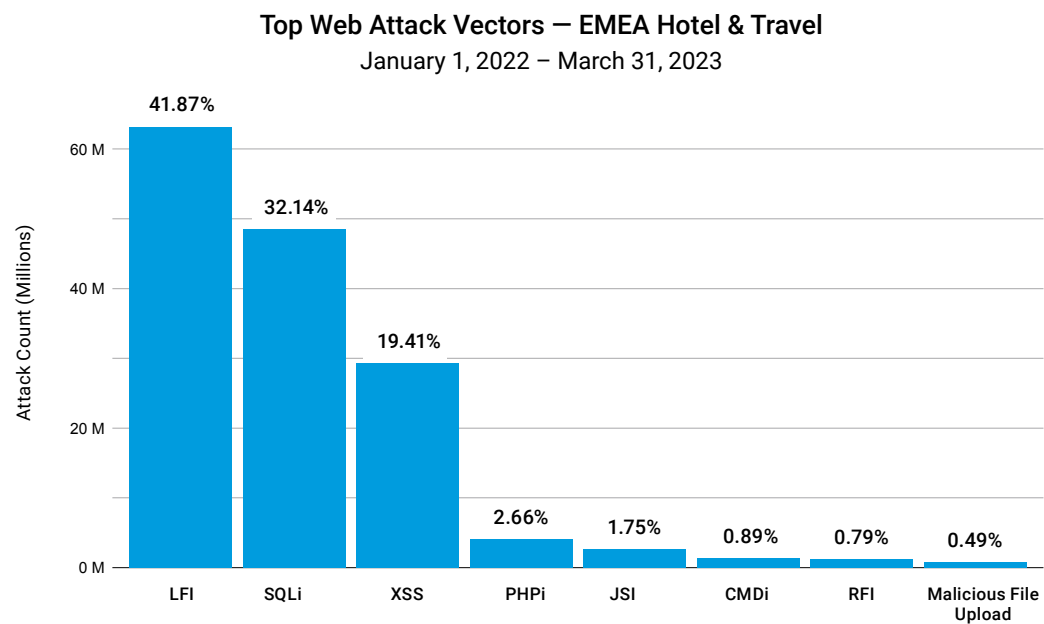


Fig. 9: Top web attack vectors in EMEA hotel and travel

Third-party scripts: A growing attack surface

Commerce organizations use third-party scripts to quickly add functionality like payment processing, chatbots, and metrics tracking, and to enhance the overall user experience. But because these scripts are out of their control, they have little visibility into the development and testing of the code and potential vulnerabilities. Additionally, third-party scripts may use code from other third parties, which creates more blind spots and pathways for attacks.

Our data shows that 51% of the scripts used by commerce organizations in EMEA come from third parties, substantially higher than the amount of third-party scripts used by other verticals (31%) (Figure 10).

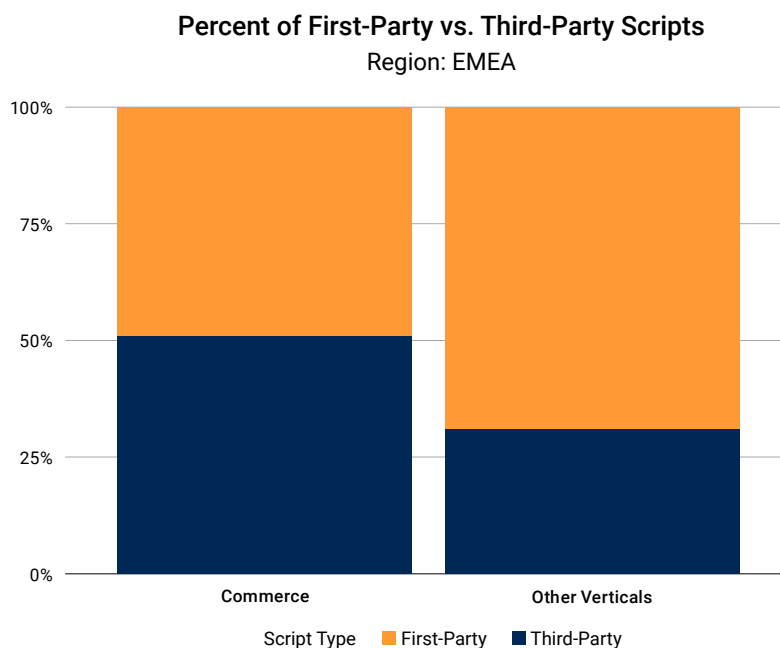


Fig. 10: Commerce organizations use more third-party scripts (51%) than other verticals (31%), which makes them more prone to security risks associated with using scripts from third-party vendors

Although using third-party scripts does not necessarily mean that they are less trusted or malicious in nature, any flaws that exist put consumers at risk of fraud or stolen payment details. It also means increased challenges with meeting the requirements around PCI DSS 4.0 regarding script management.

Bot traffic — consumers and retailers under attack

Malicious bots are being utilized by attackers as vehicles to commit fraud or other malicious attack attempts. Even benign bots can damage the customer experience by slowing down website performance or luring customers away to a competing site by conducting price scraping that feeds into audience hijacking tactics.

Between January 2022 and March 2023, the number of malicious bots targeting the EMEA commerce vertical reached nearly 835 billion (Figure 11), peaking in Q1 2023 (Figure 12). That said, the ratio of malicious bots versus benign bots decreased substantially when comparing Q1 2022 and Q1 2023.

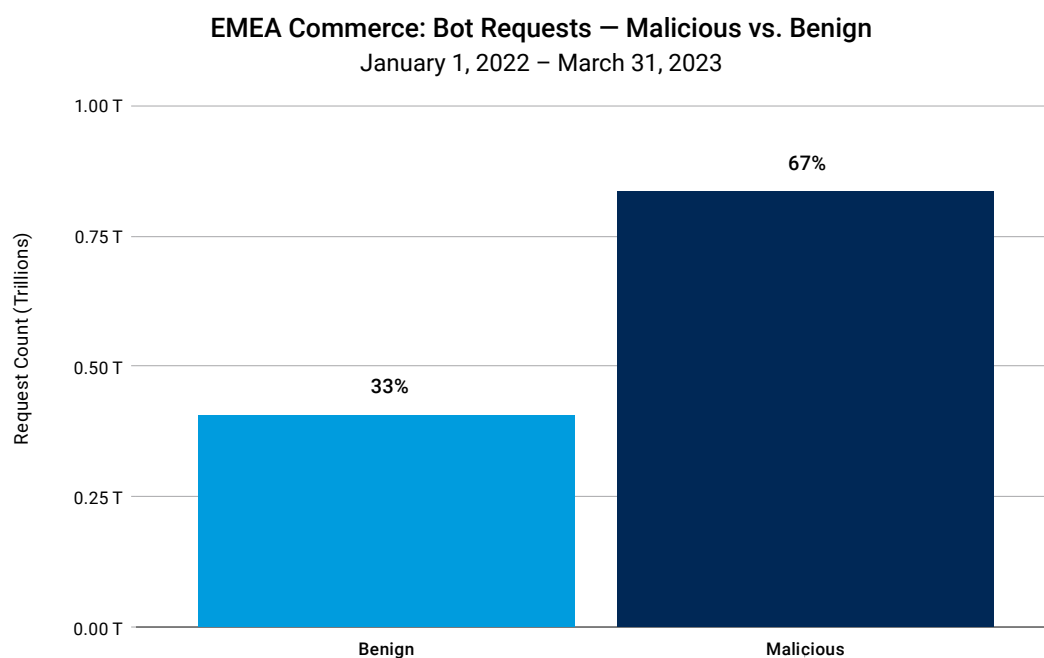


Fig. 11: The number of malicious bot requests exceeded 835 billion between January 2022 and March 2023

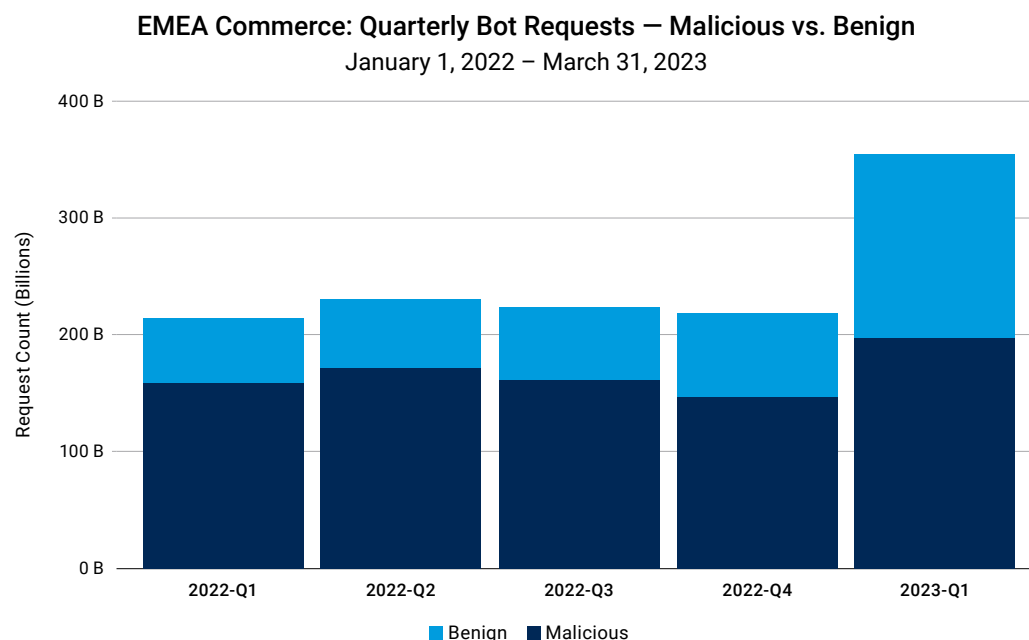


Fig. 12: Benign bot requests increased in Q1 2023, leading to a decrease in the ratio of malicious bots vs. benign bots during that period

Some of this malicious bot activity could be attributed to the current geopolitical climate, where bots have been used by threat actor groups to take over web pages to cause disruption or simply showcase their capabilities. However, there are many use cases where bots figure prominently in the proliferation of credential stuffing, leading to account takeover for the retrieval of personal information, which can be used to conduct fraudulent activities or sold on the dark web. Attackers also use them to grab and resell limited-edition items, or scout for bargains they can resell for a profit.

As for the increase in bots in Q1 2023, the rise in volume could be driven by economic and geopolitical uncertainty among consumers that is driving [increased price sensitivity](#). Consumers across the region are looking for ways to save money, be it through promotions or downtrading, including shifting to private labels or discounters. Retailers use [good bots](#) such as coupon-searching bots and comparison-searching bots to drive sales. However, nefarious actors may also be driving a surge in bot traffic for purposes like price scraping, which can be used to capitalize on consumer preferences.

For detailed insights into how these attacks unfold and how bots could impact your customers, refer to our global commerce SOTI report, [Entering Through the Gift Shop: Attacks on Commerce](#).

Conclusion: Combating attacks against commerce

Commerce has always been a target for criminals — and as more of the business moves online, the criminals have increased the attacks. Based on threat trends we are seeing across all the different industries across the globe on our security platform, we have covered shifts in malware, methodologies, and the regulatory landscape.

First was the continued focus on the edge, where we see transformation efforts being the focus of apps and API attacks, with a shift to LFI being the dominant attack technique. This was followed by some emerging remote code execution methods, especially Server-Side Request Forgery, Server-Side Template Injection, and Server-Side Code Injection. You can examine your logs to see if you are experiencing the same trends in techniques. Additionally, you can have your pen test and red teams validate that your detection and mitigation controls are effective.

Next, we covered how bots continued to be a growing problem, with scalpers and scrapers using them to beat out established loyal customers. This requires both visibility and playbooks that can adjust your security controls to protect your customers. Finally, we covered that Magecart and web skimming attacks are still operational threats and have driven new requirements in the latest version of PCI DSS (4.0). Any organization processing payment cards online must now have security controls in place to monitor, inventory, and alert on changes to scripts observed on payment pages.

Organizations continue to prioritize integration of security controls, the need for automation and machine learning to match the speed of attackers, the importance of visibility on both trends and specific investigations, and the ability to leverage expertise. We hope the data from this report provides insights to help you update your program and develop best practices.

Stay plugged into our latest research by checking out our [Security Research Hub](#).

Methodology

Web application and bot attacks

This data describes application-layer alerts on traffic seen through our web application firewall (WAF) and bot manager tool. The web app attack alerts are triggered when we detect a malicious payload within a request to a protected website or application. The bot alerts are triggered when we detect a bot payload within a request to a protected website or application. These bot alerts can be triggered by both malicious and benign bots. The alerts do not indicate the successfulness of an attack. Although these products allow a high level of customization, we collected the data presented here in a manner that does not consider custom configurations of the protected properties. The data was drawn from an internal tool for analysis of security events detected on Akamai Connected Cloud, a network of approximately 340,000 servers in 4,000 locations on 1,300 networks in 130+ countries. Our security teams use this data, measured in petabytes per month, to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

One significant attack in May 2022 was cut from some web app attack visualizations because of its tremendous volume. It remained in the dataset for all analytic purposes.

Page Integrity Manager data

This data describes scripts observed and analyzed within our Page Integrity Manager tool. Page Integrity Manager runs within the browser, and observes any scripts executed within the browser across protected web pages. The tool observes over 18 billion scripts on a daily basis, protecting nearly 10 billion web pages on a daily basis. Our security team uses this data to research script vulnerabilities, detect malicious behavior, and feed intelligence gathered into other Akamai security solutions.

The Page Integrity Manager data we analyzed for this report was a sample of data analyzed during Q1 2023.

Credits

Editorial and writing

Eliad Kimhy	Charlotte Pelliccia
Lance Rhodes	David Senecal
Badette Tribbey	Steve Winterfeld

Review and subject matter contribution

Tom Emmons	Or Katz
Reuben Koh	Roman Lvovsky
Emily Lyons	Bar Menachem
Susan McReynolds	Richard Meeus
Gal Meiri	

Data analysis

Robert Lester	Chelsea Tuttle
---------------	----------------

Marketing and publishing

Kimberly Gomez	Georgina Morales Hampe
Shivangi Sahu	

More State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports. akamai.com/soti

More Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/security-research

Access data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata

More on Akamai solutions

To learn more about Akamai solutions for threats targeting commerce, visit our [Ecommerce page](#).



Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on [Twitter](#) and [LinkedIn](#). Published 6/23.