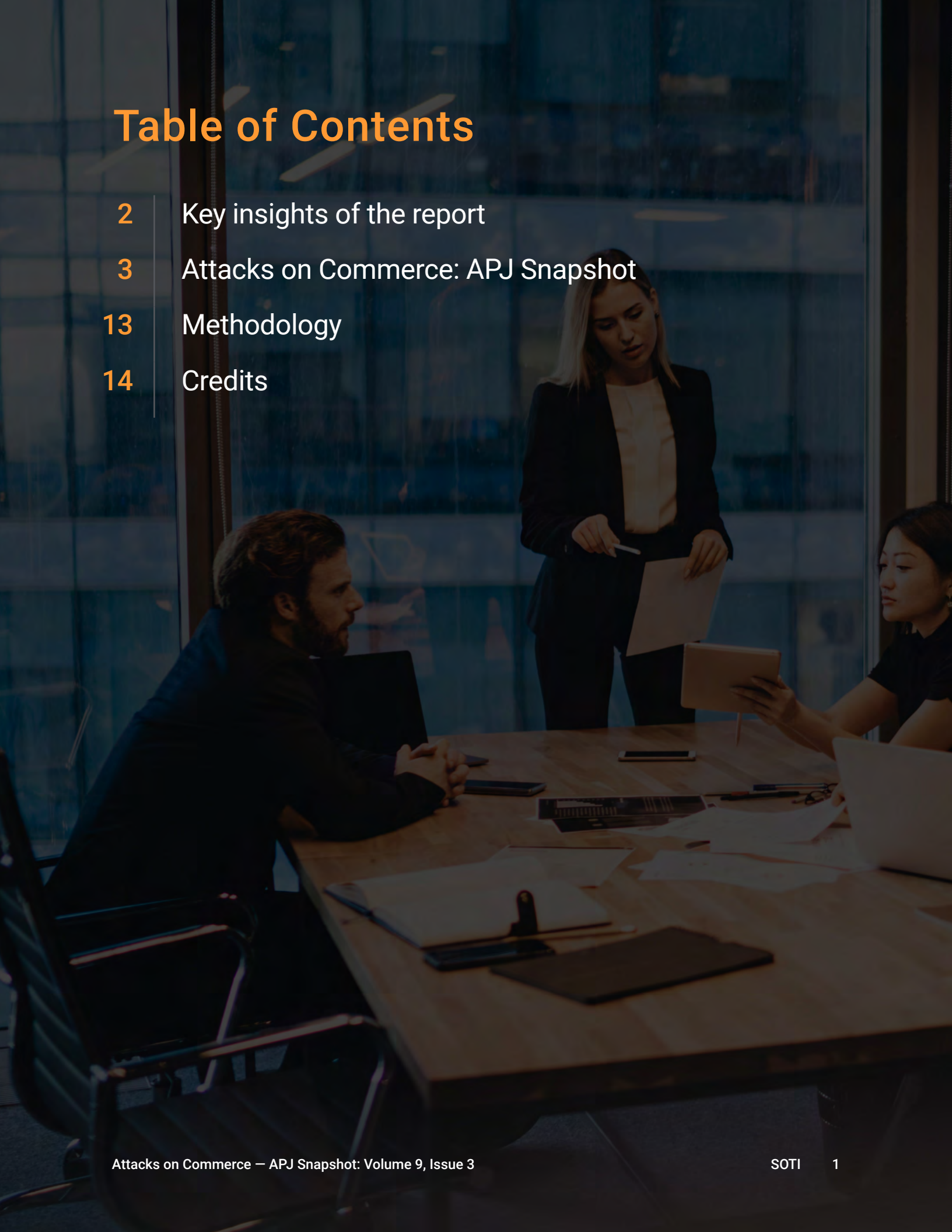
Attacks on Commerce:

APJ Snapshot

Akamai

Table of Contents



Key insights of the report

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, as well as recommendations and best practices to safeguard your organization against application and API risks.

Compared to other industries like financial services and healthcare, commerce is less heavily regulated but needs the same security maturity level, as it remains one of the most attacked industry verticals. In APJ, commerce is the second-most frequently targeted vertical for web application and API attacks. This is consistent with previous Akamai research, 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. 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.

In this APJ Snapshot, we'll delve into the attack trends in commerce and what they mean for you, including:

- During the period of January 2022 through March 2023, web attacks on the retail sub-vertical accounted for 57% of commerce attacks in APJ, and hotel and travel accounted for 39%. As a region, APJ is second to North America in web attacks on hotel and travel, driven by Australia in combination with India.
- Consistent with findings in the global report, Local File Inclusion (LFI) is the most popular attack vector, and can lead to remote code execution and allow for broad network access and breaches such as ransomware attacks.
- The use of third-party scripts used by commerce organizations is higher (57%) than for other verticals (48%) and contributes to a growing attack surface.
- During 2022, bot usage was on the rise by commerce organizations to drive sales, but also by nefarious actors for purposes like price scraping. However, in Q1 2023, malicious bot activity dropped significantly and returned to Q1 2022 levels.

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.

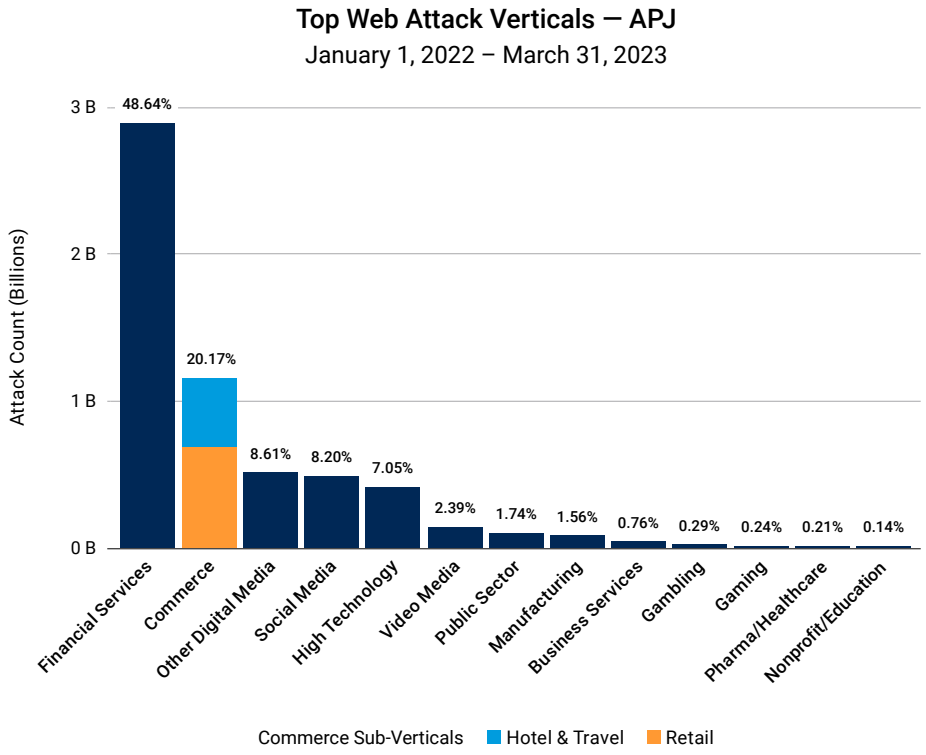


Fig. 1: Commerce (shown as hotel and travel in blue and retail in orange) is the second-most frequently attacked vertical in APJ

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).

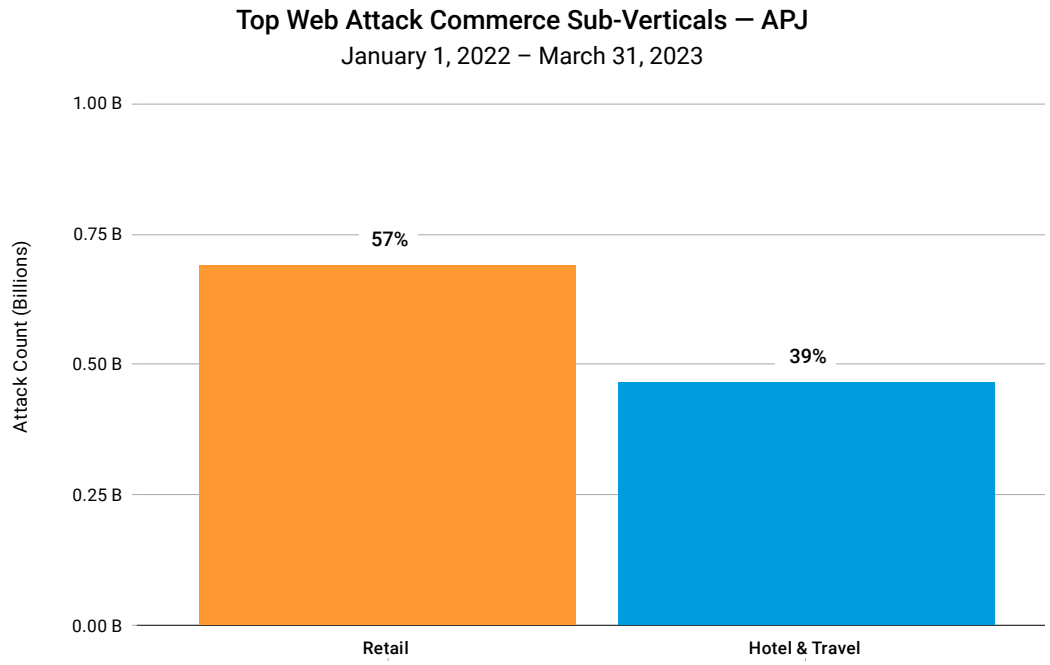


Fig. 2: Attacks on retail versus hotel and travel sub-verticals in APJ

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).

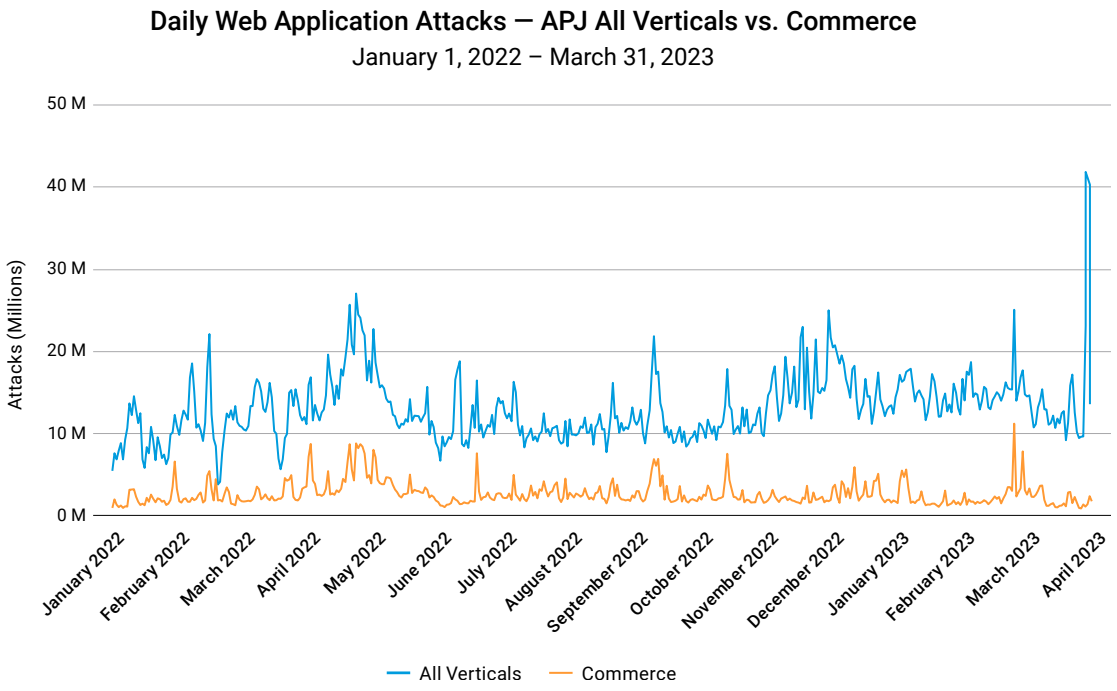


Fig. 6: Daily web application attacks on commerce vs. all verticals

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.

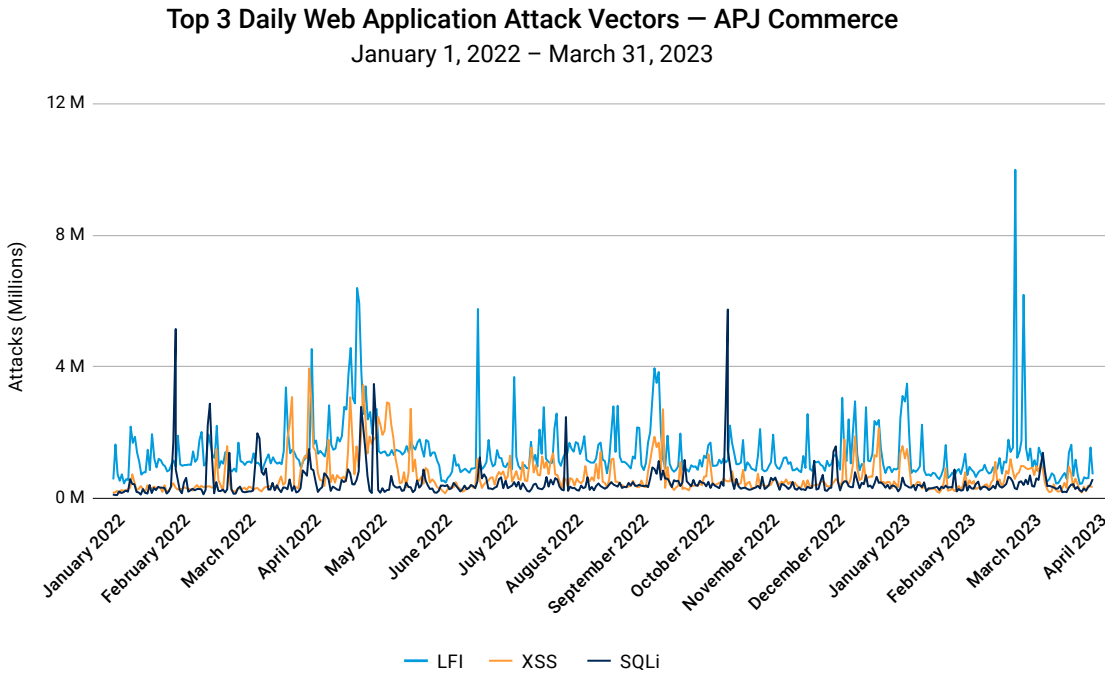


Fig. 7: Daily web application attack vectors for APJ commerce

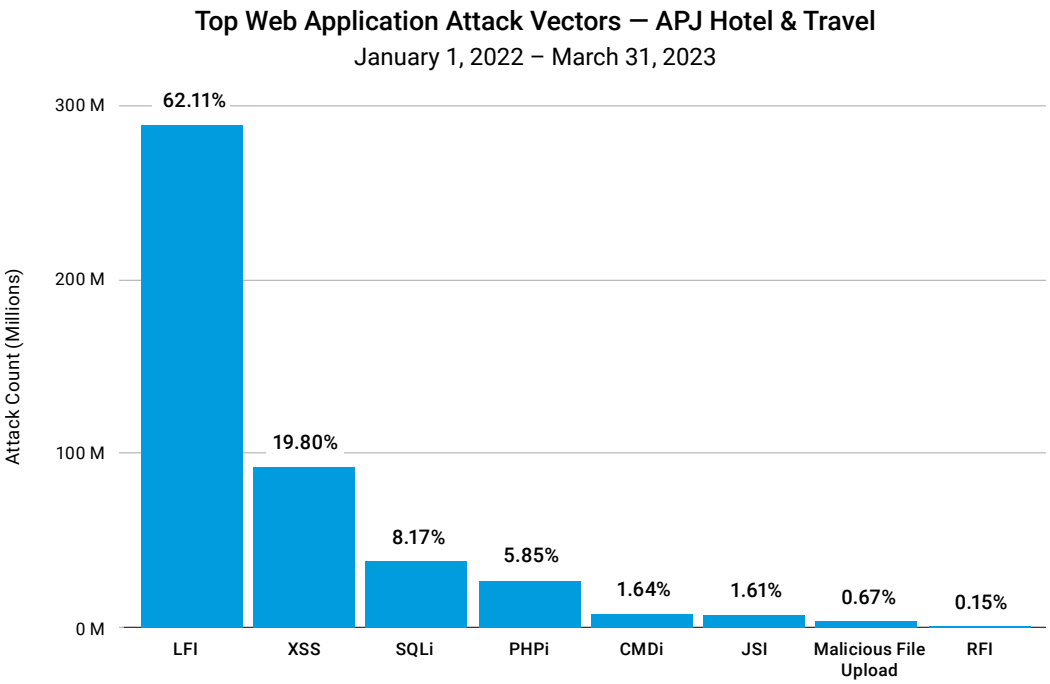


Fig. 8: LFI usage is 3 times higher than the next closest attack vector within APJ hotel and travel

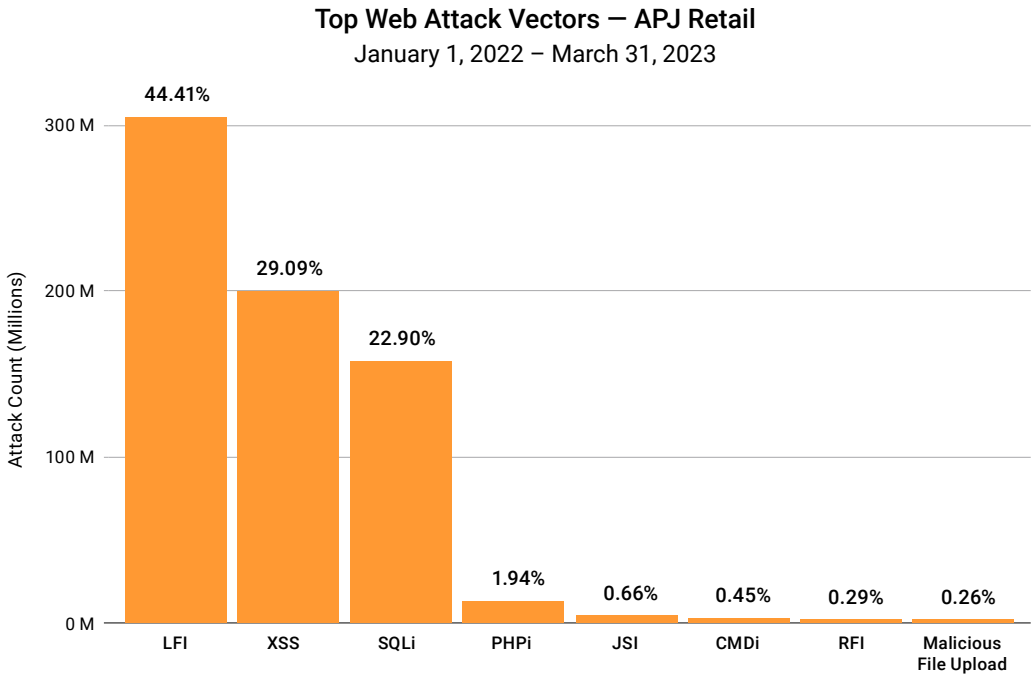


Fig. 9: Top web attack vectors in APJ retail

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).

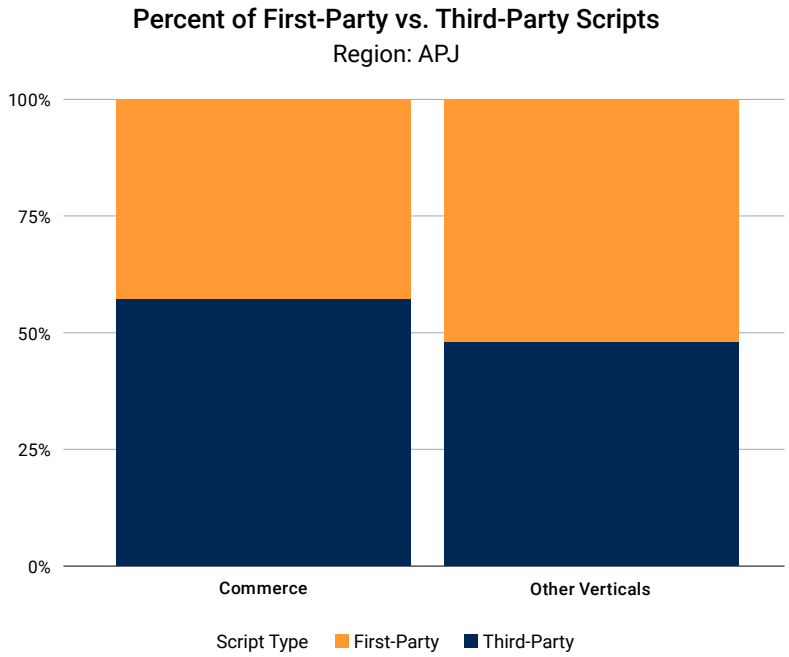


Fig. 10: Commerce organizations use more third-party scripts (57%) than other verticals (48%), which makes them more prone to security risks associated with using scripts from third-party vendors

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).

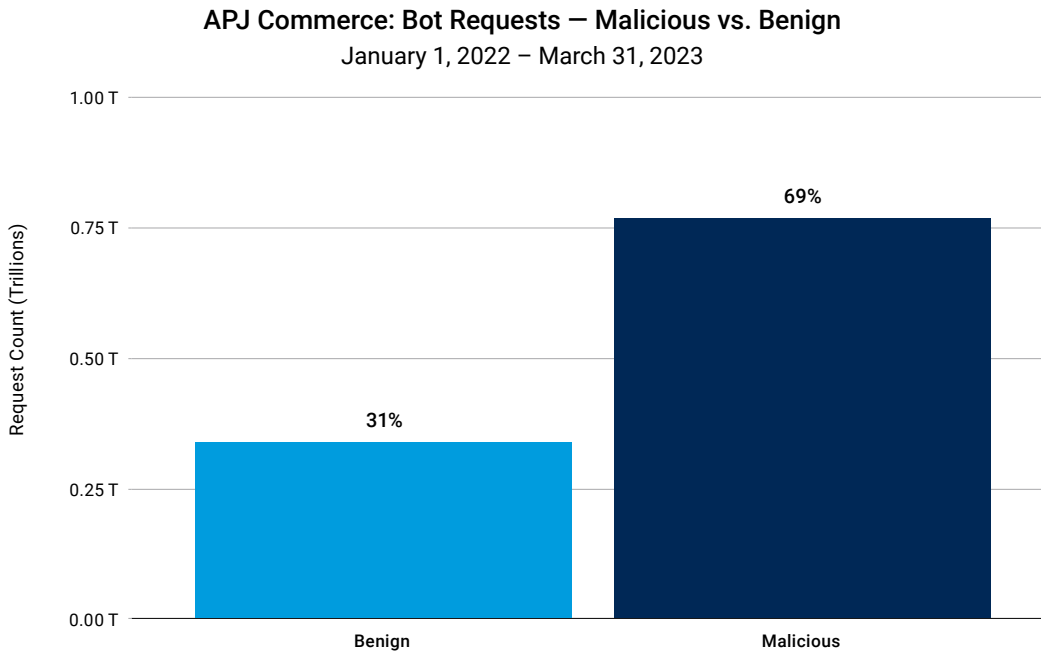


Fig. 11: The number of malicious bot requests exceeded 765 billion between January 2022 and March 2023

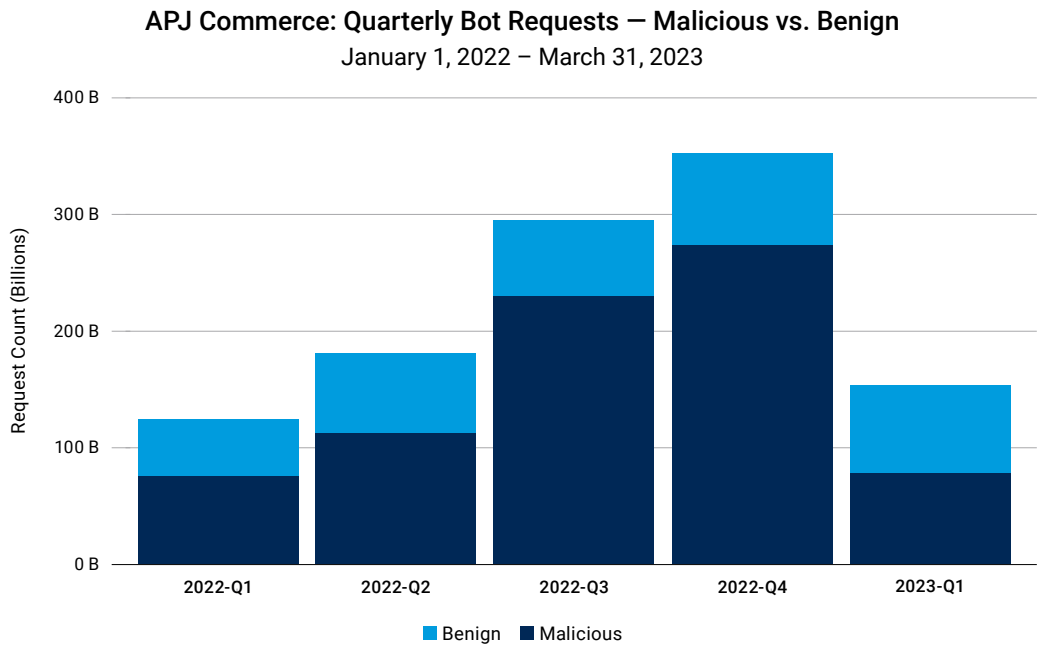


Fig. 12: After quarter-on-quarter growth, malicious bot activity dropped significantly in Q1 2023

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 (in English only).

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 Lvovksy
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 8/23.