SOTI

V10 ISSUE 04

10 YEARS
OF SECURITY INSIGHT

Threats to Modern Application Architectures

APJ Snapshot

Akamai

State of the Internet/Security

Table of Contents

Key insights of the report

The APJ Snapshot is a companion piece to our larger secure apps SOTI report, Digital Fortresses Under Siege: Threats to Modern Application Architectures (available in English only). Please refer to that report for detailed descriptions of how adversaries exploit the expanding attack surface, recommendations to safeguard your organization, and an explanation of our research methodologies.

Overview

Over the past two decades, web applications have grown exponentially in both number and capabilities, streamlining business operations, enhancing the customer experience, and driving growth through features like real-time communication, data analytics, and process automation. APIs — the bedrock of communication among applications — have also proliferated and are now poised for their own exponential leap.

Applications run nearly every aspect of business, making trillions of connections easier but also more vulnerable to attack. In this APJ Snapshot, which spans January 2023 through June 2024, we take a holistic view of the threats that impact applications — including web attacks, distributed denial-of-service (DDoS) attacks, and threats to critical workloads — with a focus on what they mean for you.

Web attacks against applications and APIs grew 65% from Q1 2023 to Q1 2024 in the Asia-Pacific and Japan (APJ) region and continued to rise, peaking at 4.8 billion in June 2024. Consistent with prior reporting, the financial services and commerce sectors experienced the most web attacks in the region.

The APJ region experienced a five-fold growth in Layer 7 DDoS attacks, for a total of 5.1 trillion attacks during the period, and was second to North America. Social media was the most impacted industry with hacktivism and nation-state–aligned actors contributing to the rise in Layer 7 DDoS attacks against the sector in response to geopolitical events and tension.

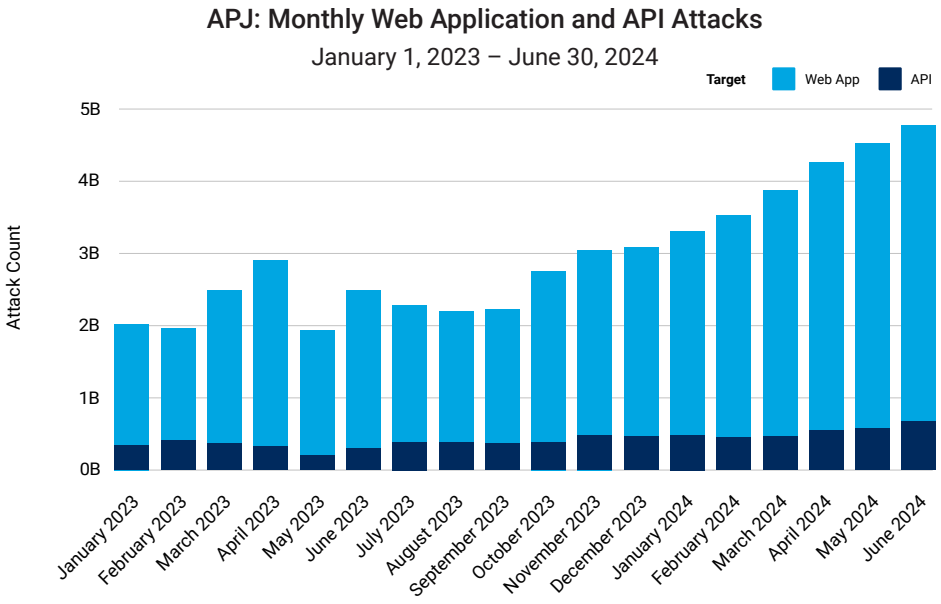
Ransomware and other attacks on applications and the internal workloads between them is a growing concern. Organizations are turning to software-based microsegmentation for the visibility and granular controls required to protect this expanding attack surface.

Web applications and APIs: Rich sources for security risks

Web application and API attacks proliferate as organizations rush to deploy apps to enhance customer experience and drive business. Threat actors are taking advantage of this expanding attack surface (e.g., web applications with poor coding and design flaws and several years' old vulnerabilities). Additionally, the rapid expansion of the API economy has presented cybercriminals with further opportunities for vulnerability exploitation and business logic abuse.

Attack trends by the numbers

In our first SOTI report of 2024, we examined API attack trends in 2023 within the context of overall web application attacks. By looking back at the past 18 months, from January 2023 through June 2024, Akamai researchers found that monthly web application and API attacks in APJ reached an 18-month high, peaking at 4.8 billion in June 2024. This represents a 65% growth in web attacks from Q1 2023 to Q1 2024 with growth continuing through the subsequent quarter. Attacks against APIs climbed slightly, reaching 670 million by the end of the period (APJ Figure 1).



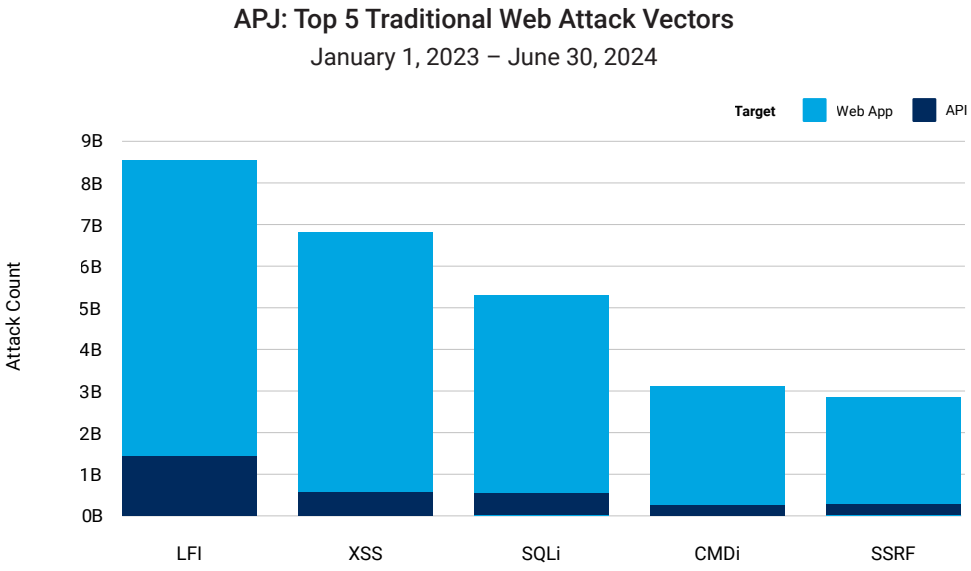
APJ Fig. 1: Web application and API attacks climbed 65% year over year

Within APJ, Australia (14.6 billion), India (12.0 billion), and Singapore (10.7 billion) bore the brunt of web application and API attacks during that period, followed by China (4.3 billion), Japan (4.0 billion), New Zealand (2.1 billion), South Korea (1.6 billion), and Hong Kong SAR (1.5 billion).

Akamai also tracks several web attack vectors. In this report we're focusing on the top five traditional vector-based attack methods.

Akamai researchers found that monthly web application and API attacks in APJ reached an 18-month high, peaking at 4.8 billion in June 2024.

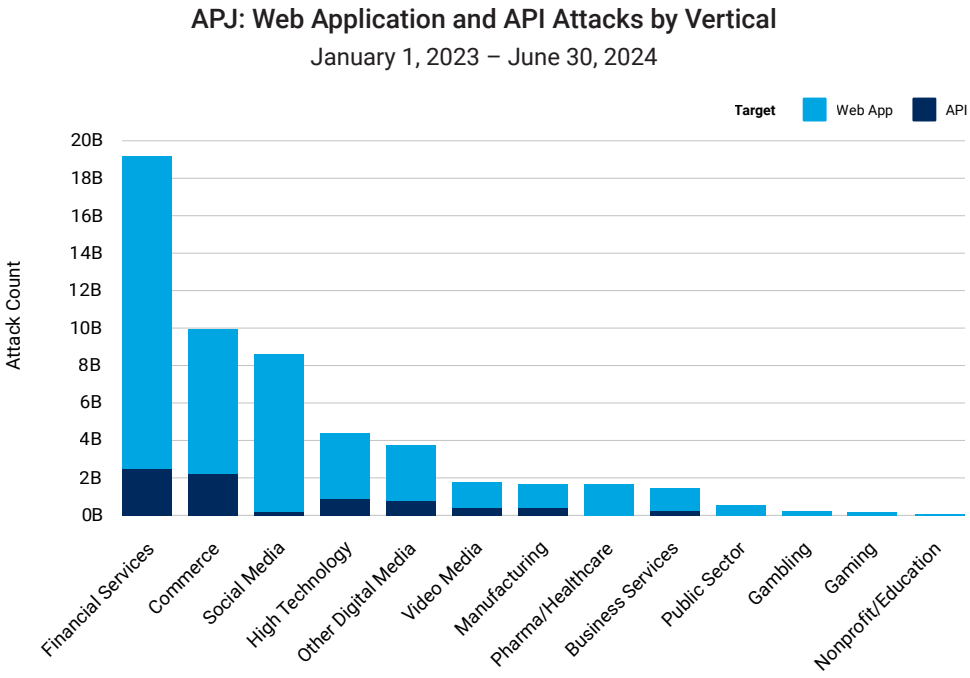
Consistent with previous reports, local file inclusion (LFI) remained a preferred attack vector, but other vectors, like cross-site scripting (XSS) and structured query language injection (SQLi), continued to pose risks (APJ Figure 2).



APJ Fig. 2: LFI, XSS, and SQLi are driving growth in web application and API attacks

It is not uncommon for attackers to use traditional tactics like LFI and XSS to access their intended targets' data. Additionally, LFI enables attackers to gain a foothold in their intended targets and perform remote code execution, thus compromising security.

From an industry perspective, the top five industries impacted by web application and API attacks are also consistent with a previous report, with financial services and commerce in the lead. When looking at API attacks specifically, we see a shift from our API security SOTI report, as the number of attacks on the gaming sector has dropped significantly (APJ Figure 3). This shift does not imply that attackers are not focused on gaming as a target. As we'll see later in this report, gaming was among the most targeted industries for Layers 3 and 4 DDoS attacks.



APJ Fig. 3: Cybercriminals continue to set their sites squarely on financial services

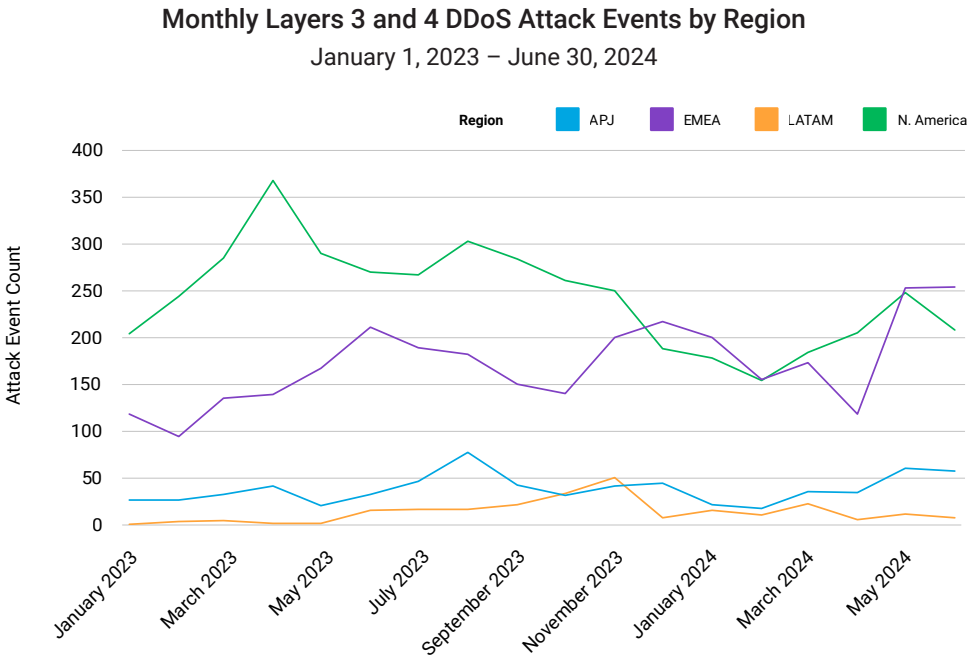
DDoS attacks threaten application uptime

As the attack surface continues to expand, so do the DDoS attack types that affect applications. As discussed in greater detail in the global SOTI report, traditional Layer 3 and Layer 4 DDoS attacks have been around the longest and aim to overwhelm the network or application server capacity. Application-layer (Layer 7) DDoS attacks exploit vulnerabilities and exploit loopholes and/or flaws of the business logic in the application layer. They are capable of causing significant damage with even a relatively small amount of malicious traffic. Regardless of the attack vector, the impact of a successful DDoS attack is application downtime.

Our latest research shows an ongoing threat of Layers 3 and 4 and Layer 7 DDoS attacks to the infrastructure that powers applications, as well as to the applications themselves.

Infrastructure DDoS attacks

During the 18-month reporting period from January 2023 through June 2024, Akamai researchers found that APJ experienced lower levels of Layers 3 and 4 DDoS attack events than other regions. However, we can see an uptick in attack events since February 2024 (APJ Figure 4).



APJ Fig. 4: APJ's Layers 3 and 4 DDoS attack event numbers were lower than in other regions, but are trending up in 2024

The most impacted area was Taiwan (409), followed by Australia (105), Pakistan (51), Hong Kong SAR (49), Japan (38), and Singapore (29). As we see here and in the next section on application-layer attacks, DDoS attacks are becoming the cyber weapon of choice in APJ, largely driven by geopolitical unrest and tensions where both nation-state–aligned actors and hacktivists are getting more involved.

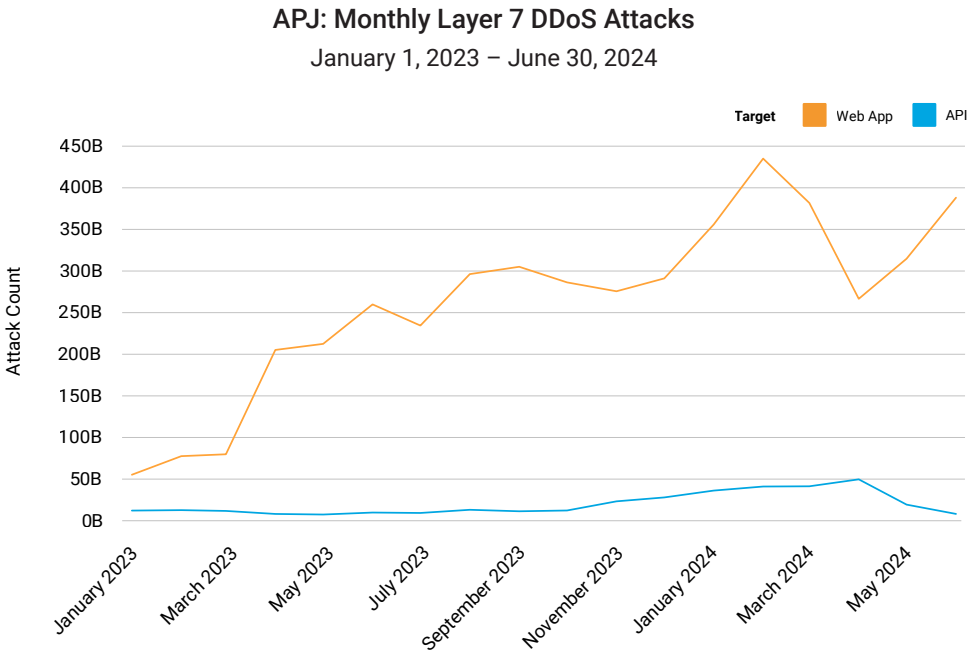
From an industry perspective, the commerce (207) and gaming (158) industries experienced the highest number of DDoS Layers 3 and 4 attack events, followed by financial services (120), video media (91), and high technology (63).

Application-layer DDoS attacks

In addition to Layers 3 and 4 DDoS attacks, the region was also subjected to targeted application-layer (Layer 7) DDoS attacks. During the 18-month reporting period from January 2023 through June 2024, Akamai researchers found that APJ was second in the number of Layer 7 DDoS attacks, experiencing 5.1 trillion attacks versus 8.7 trillion in North America.

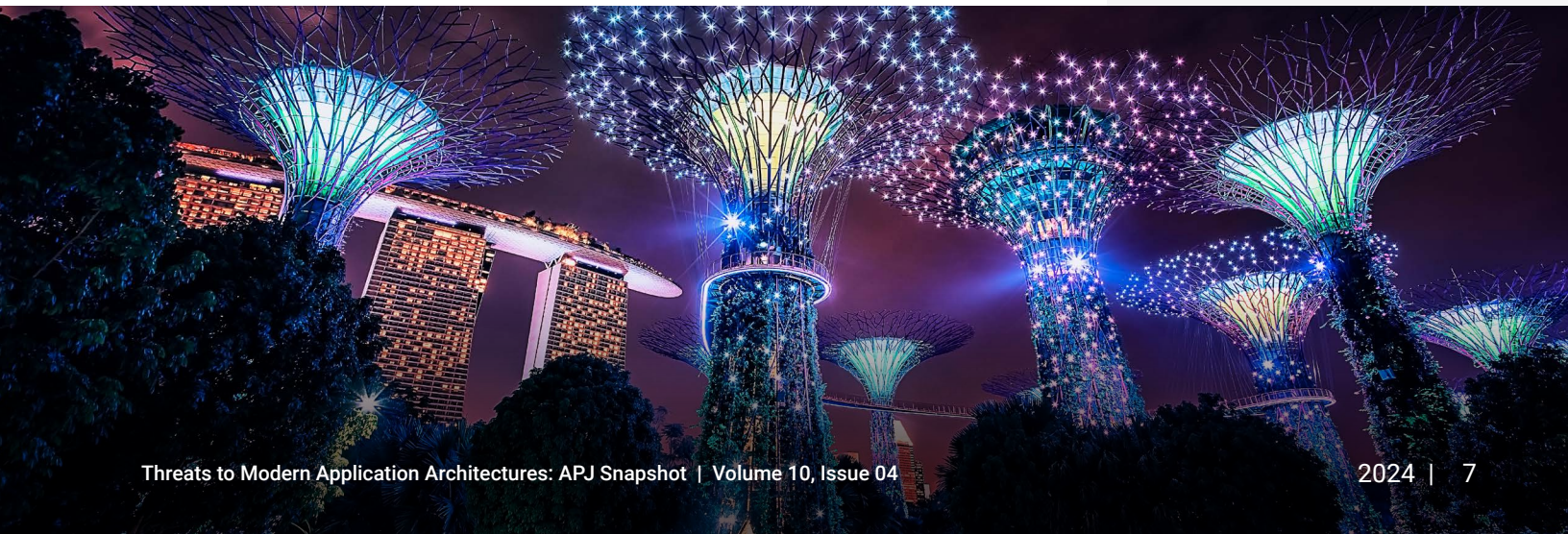
During the 18-month reporting period from January 2023 through June 2024, Akamai researchers found that APJ was second in the number of Layer 7 DDoS attacks, experiencing 5.1 trillion attacks versus 8.7 trillion in North America.

Digging deeper into the data, we see that the monthly volume of Layer 7 DDoS attacks rose significantly during the reporting period, starting at 70 billion attacks in January 2023 and experiencing a more than fivefold growth to end at 399 billion in June 2024. Additionally, although less than 10% of Layer 7 DDoS attacks in APJ targeted APIs (APJ Figure 5), the risk was trending upward. It's an ever-changing landscape, and as API adoption in the region continues to rise, so too will exposure to risk.

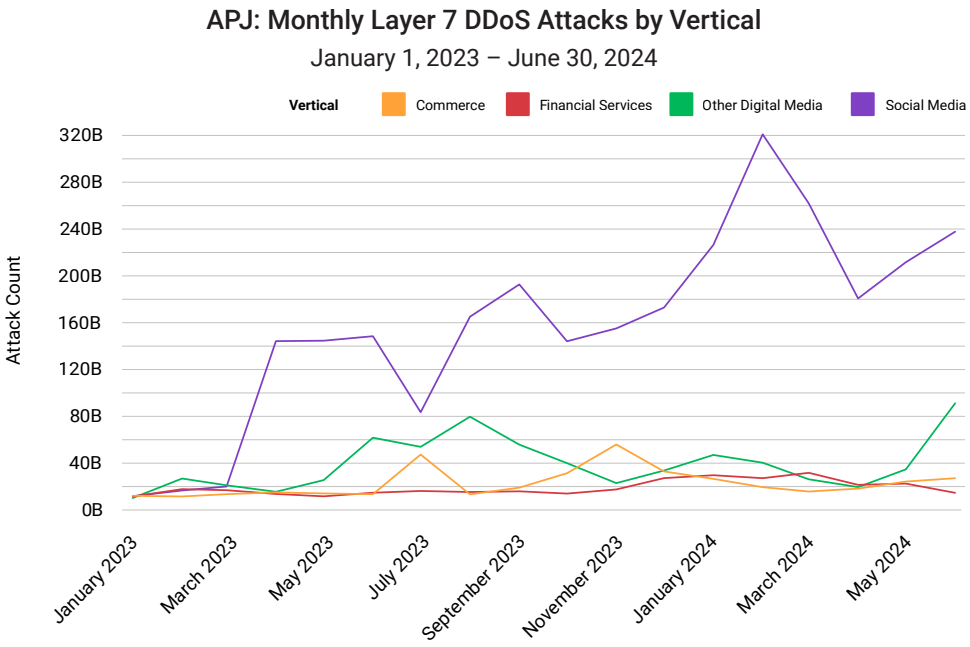


APJ Fig. 5: Layer 7 DDoS attacks grew fivefold from January 2023 through June 2024

Of those attacks, Singapore experienced the highest concentration of attacks at 2.9 trillion, followed by India (959 billion), South Korea (544 billion), Indonesia (260 billion), China (188 billion), Japan (83 billion), Australia (74 billion), and Taiwan (50 billion).



Looking at trends by vertical reveals that the increase in Layer 7 DDoS attack activity can be largely attributed to attack attempts against the social media sector (APJ Figure 6).



APJ Fig. 6: The rise in social media attacks aligns with a larger global trend and correlates with broader military conflicts and highly mediated electoral events worldwide

Social media platforms are known to receive a lot of attack traffic in response to geopolitical upheaval, and APJ was not immune to this uptick. As discussed in more detail in the global SOTI, this activity included a surge of fraudulent pro-Russia social media accounts and spoofed news sites designed to amplify divisive political topics. These attacks also correlate with ongoing geopolitical upheaval across the globe. Large-scale and highly mediated electoral events and presidential/country leadership matters often lead to politically motivated cyberattacks, including DDoS attacks, in various regions as actors seek to exploit the heightened political atmosphere for their agendas. Hacktivism related to the ongoing Russia-Ukraine and Israel-Hamas wars may have contributed to the rise in attacks as well.

The rise in artificial intelligence (AI) tools makes it easier to spread convincing false content — and social media platforms are a huge communication channel for content of all kinds. Combined with the fact that 2024 is an election year in APJ and in the United States, it is likely we'll continue to see threat actors target social media platforms in all regions.

The attack trend data in this report reminds us that attackers are relentless in their pursuit for disruption and financial gain, and they can quickly switch their focus among industries, geographies, and tactics. So, all organizations must remain vigilant and ensure proper defenses against all types of attacks to protect their applications from downtime.

Attackers zero in on application workloads

Zero Trust is typically discussed within the context of network security. However, web applications and the internal workloads between them can also be exposed to threats like ransomware that look for any entry point and pathway to reach their intended targets.

As discussed in detail in the global report, for an application to function — whether in the cloud, on-premises, or in a hybrid environment — every individual workload must operate seamlessly. Workloads traverse multiple security jurisdictions as they move through the network, and each new jurisdiction adds a potential point of entry for an intruder. Protecting this extended attack surface is critical to strengthening overall security posture, but further complicates the already difficult job for security teams.

Implementing a Zero Trust framework from a traditional hardware-based approach is a resource- and time-intensive effort that necessitates downtime. Additionally, a true Zero Trust implementation requires microsegmentation to secure against ransomware or attacks on the workloads themselves.

Software-based microsegmentation is quick and easy to implement and operate so it can even serve as a viable incident response measure, and as a control to isolate critical systems in support of regulatory compliance. Because of these advantages, organizations are increasingly turning to this approach to detect and mitigate a jeopardized workload or container across their dynamic data center, cloud, and hybrid cloud environments.

Real-world lessons in protecting application workloads

In this section, we present two case studies from the APJ region that exemplify how enterprises are securing critical workloads and advancing Zero Trust.

APJ case study #1: A social network with services, including messaging, games, and social media, as well as capabilities to buy financial services, needed a way to ensure customer communication was secure. Preventing hackers from gaining access to customer conversations and then moving laterally into other networks and databases is the chief information security officer's top priority. The multiple different operating systems and applications customers are using, makes it impossible to know which device is vulnerable. Isolating devices and networks with granular segmentation policies is a fundamental way the company maintains the trust required for communication.

APJ case study #2: A leading IT distributor with a global footprint serves a significant number of customers in the financial services sector. Protecting payment servers that are critical to banks' business operations is of paramount importance. Deep expertise in microsegmentation — deploying and enabling network visualization and extremely granular governance controls at scale and across some of the most complex environments — has enabled the company to accelerate growth based on a foundation of customer trust and the strength of Zero Trust capabilities.

Workloads traverse multiple security jurisdictions as they move through the network, and each new jurisdiction adds a potential point of entry for an intruder.

Conclusion

In this APJ Snapshot, we've attempted to provide a holistic view of the different ways threat actors can target your applications and APIs. From a security and risk management perspective, it's imperative that organizations understand and defend against threats to applications and APIs, infrastructure, and critical workloads. In addition, existing laws and emerging reforms also make it imperative to secure applications.

The changing landscape in APJ includes Singapore's recent amendments to its cybersecurity bill, Japan's updates to the National Center of Incident Readiness and Strategy for Cybersecurity laws, and the Payment Card Industry Data Security Standard v4.0, among other new legislative measures (e.g., an overhaul of India's IT Act, starting with the passing of the Digital Personal Data Protection Bill and the 2023–2030 Australian Cyber Security Strategy, etc.). Additionally, the region has an opportunity to get ahead of the open banking directive that is driving the use of APIs in Europe, the Middle East, and Africa and is likely to spread to other regions.

Applications are more important than ever to business, but also more vulnerable to attack. With capabilities and best practices to address the challenges of an ever-expanding attack surface, organizations can protect the applications they build everywhere, every time, without compromising performance or customer experience.

For more information, please refer to the global secure apps SOTI report, "Digital Fortresses Under Siege: Threats to Modern Application Architectures."

Methodology

Web application and Layer 7 DDoS attacks

This data describes application-layer alerts on traffic seen through our web application firewall (WAF). The web application attack alerts are triggered when we detect a malicious payload within a request to a protected website, application, or API. The Layer 7 DDoS alerts are triggered when we detect volumetric anomalies in the number of requests to a protected website, application, or API. These alerts can be triggered by both malicious and benign requests. Typically, the requests themselves are benign, but the high volume of requests indicates malicious intent. 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 more than 4,000 locations on nearly 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.

This data covered the 18-month period from January 1, 2023, through June 30, 2024.

2024 data update

We are happy to announce some updates to our datasets for our 10th anniversary! Our web application attack dataset has received a few updates. The collection method has been transformed, streamlined, and optimized. The range and depth of our insights has been broadened. Classifications for additional attack vectors, such as SSRF, have been added. Identification of attacks targeting API endpoints have also been added to the dataset. We enjoyed highlighting some of these new improvements in this report, and we are looking forward to continuing to share these updates throughout the year and beyond as we celebrate this SOTI/Security milestone with our readers.

DDoS (Layers 3 and 4)

Akamai Prolexic Routed defends organizations against DDoS attacks by stopping the attacks and other unwanted or malicious traffic before they reach applications, data centers, and cloud and hybrid internet-facing infrastructure (public or private), including all ports and protocols. Experts in the Akamai Security Operations Command Center (SOCC) tailor proactive mitigation controls to detect and stop attacks instantly, and conduct live analysis of the remaining traffic to determine further mitigation as needed. These mitigated attacks are organized and grouped into attack events, and all the associated data is recorded by the SOCC to be analyzed.

This data covered the 18-month period from January 1, 2023, through June 30, 2024.

Credits

Research director

Mitch Mayne

Editorial and writing

Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Review and subject matter contribution

Sven Dummer
Reuben Koh
Tony Lauro
Richard Meeus
Menacham Perlman
Sandeep Rath
Steve Winterfeld

Data analysis

Chelsea Tuttle

Promotional materials

Barney Beal

Marketing and publishing

Georgina Morales
Emily Spinks

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 that Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata

More on Akamai solutions

To learn more information on Akamai solutions for application and API attacks, visit our Application and API Security page.