SOTI

V10 ISSUE 04

10 YEARS
OF SECURITY INSIGHT

Threats to Modern Application Architectures

EMEA Snapshot

Akamai

State of the Internet/Security

Table of Contents

Key insights of the report

The EMEA 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 EMEA 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.

The number of Layers 3 and 4 DDoS attacks grew steadily in the Europe, Middle East, and Africa (EMEA) region, surpassing the number of attacks in North America for five of the past seven months. The financial services sector bore the brunt of these attacks.

Monthly web application and API attack activity in EMEA trended upward during this period, growing 21% from Q1 2023 to Q1 2024, with attacks that targeted APIs averaging 40% of monthly web attacks.

Commerce was the most impacted industry for web attacks in EMEA driven by a high percentage of API attacks, and was also the most impacted industry for Layer 7 DDoS attacks.

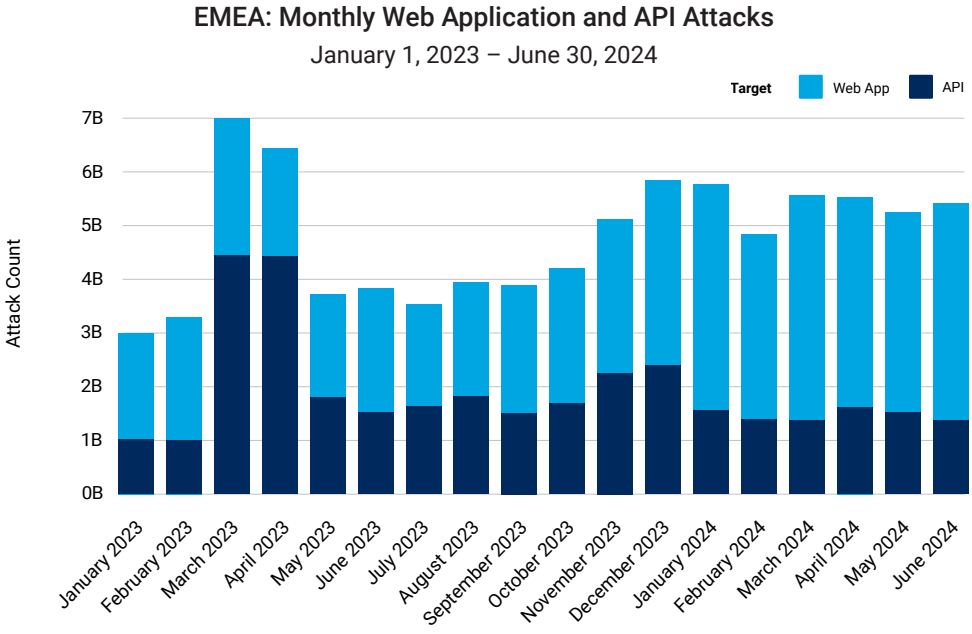
Ransomware and other attacks on applications and the internal workloads between them is a growing concern. Organizations are turning to software-based microsegmentation for the visibility and granular controls required to protect this expanding attack surface.

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 the vulnerabilities in this 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 attack activity in EMEA grew 21% from Q1 2023 to Q1 2024 and remained elevated through Q2 2024. Attacks against APIs contributed to that sustained level of activity, averaging 40% of monthly web attacks during the period (EMEA Figure 1).



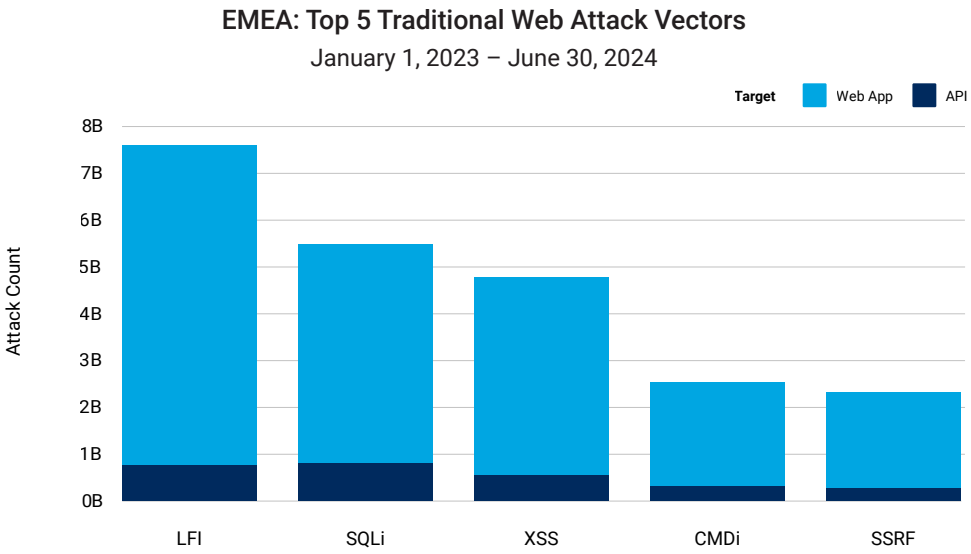
EMEA Fig. 1: Monthly web application and API attacks remain elevated in 2024

(NOTE: The spike in API attacks is related to the commerce sector in Spain, a country with an already huge API attack concentration.)

Within EMEA, the United Kingdom (20.5 billion), the Netherlands (15.6 billion), and Spain (12.7 billion) experienced the most web application and API attacks. Germany (8.7 billion), Austria (7.4 billion), France (4.8 billion), Israel (3.0 billion), Italy (2.7 billion), Switzerland (2.5 billion), and Belgium (2.3 billion) rounded out the top 10.

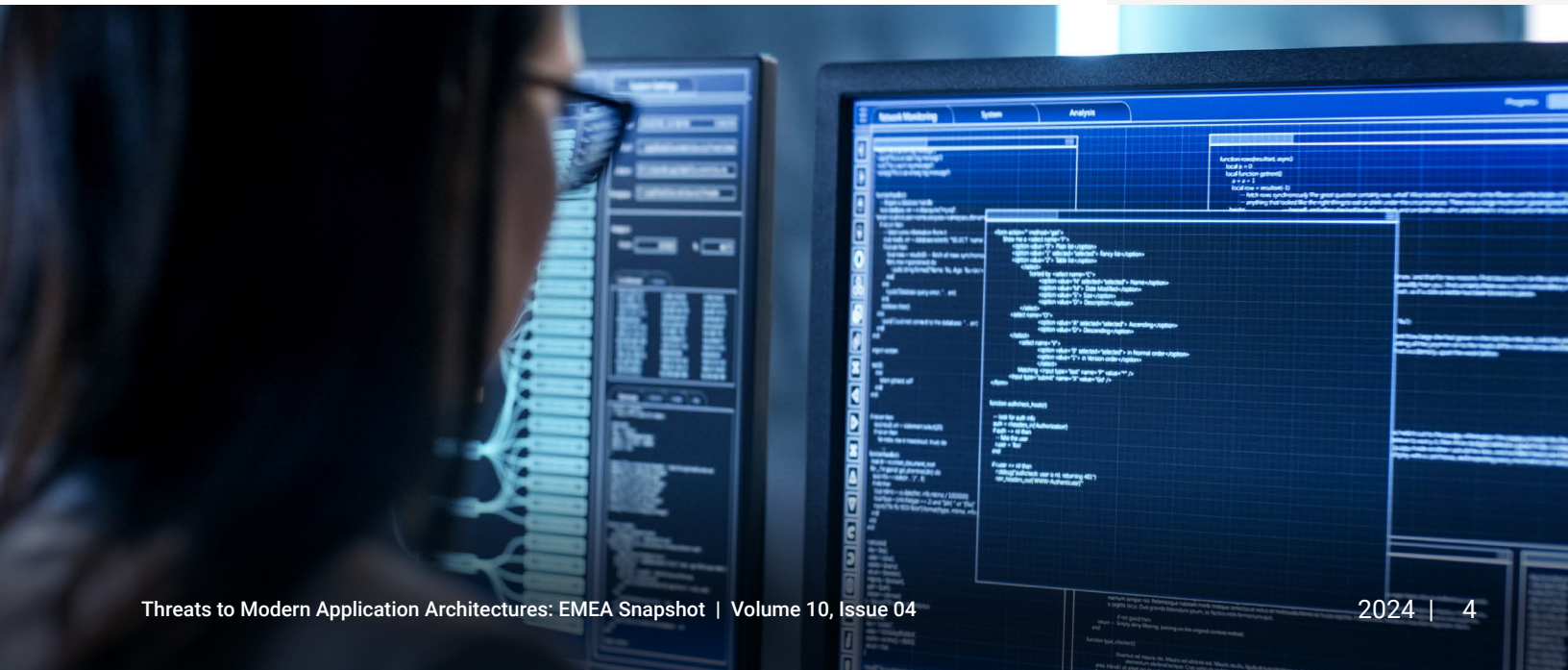
Akamai also tracks several web attack vectors. In this report we're focusing on the top five traditional vector-based attack methods.

Consistent with previous reports, local file inclusion (LFI) remained a preferred attack vector, but other vectors, like structured query language injection (SQLi) and cross-site scripting (XSS), are also areas of concern (EMEA Figure 2).

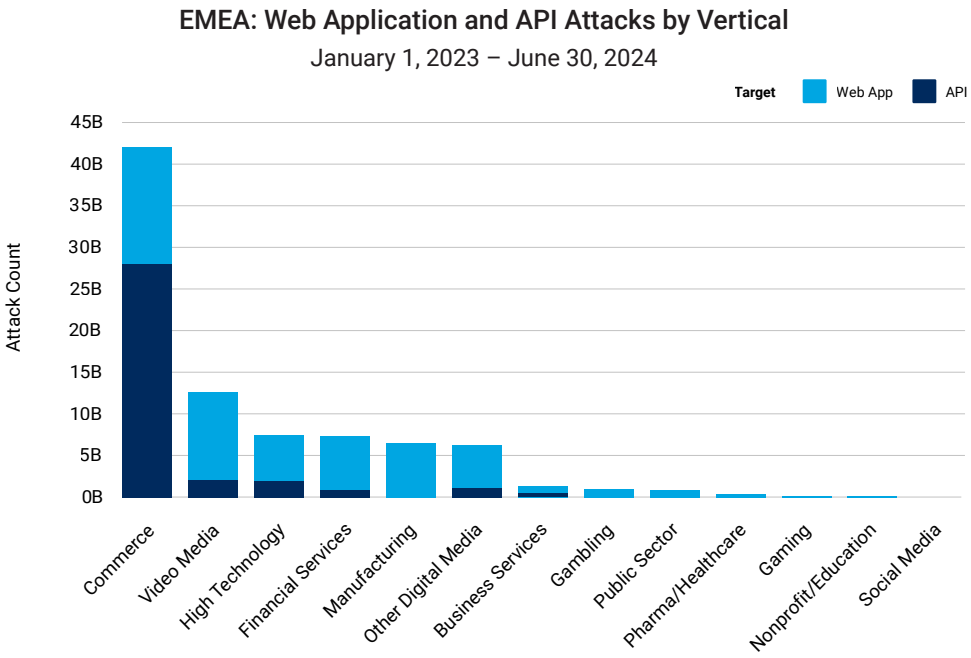


EMEA Fig. 2: LFI, SQLi, and XSS are driving growth in web application and API attacks

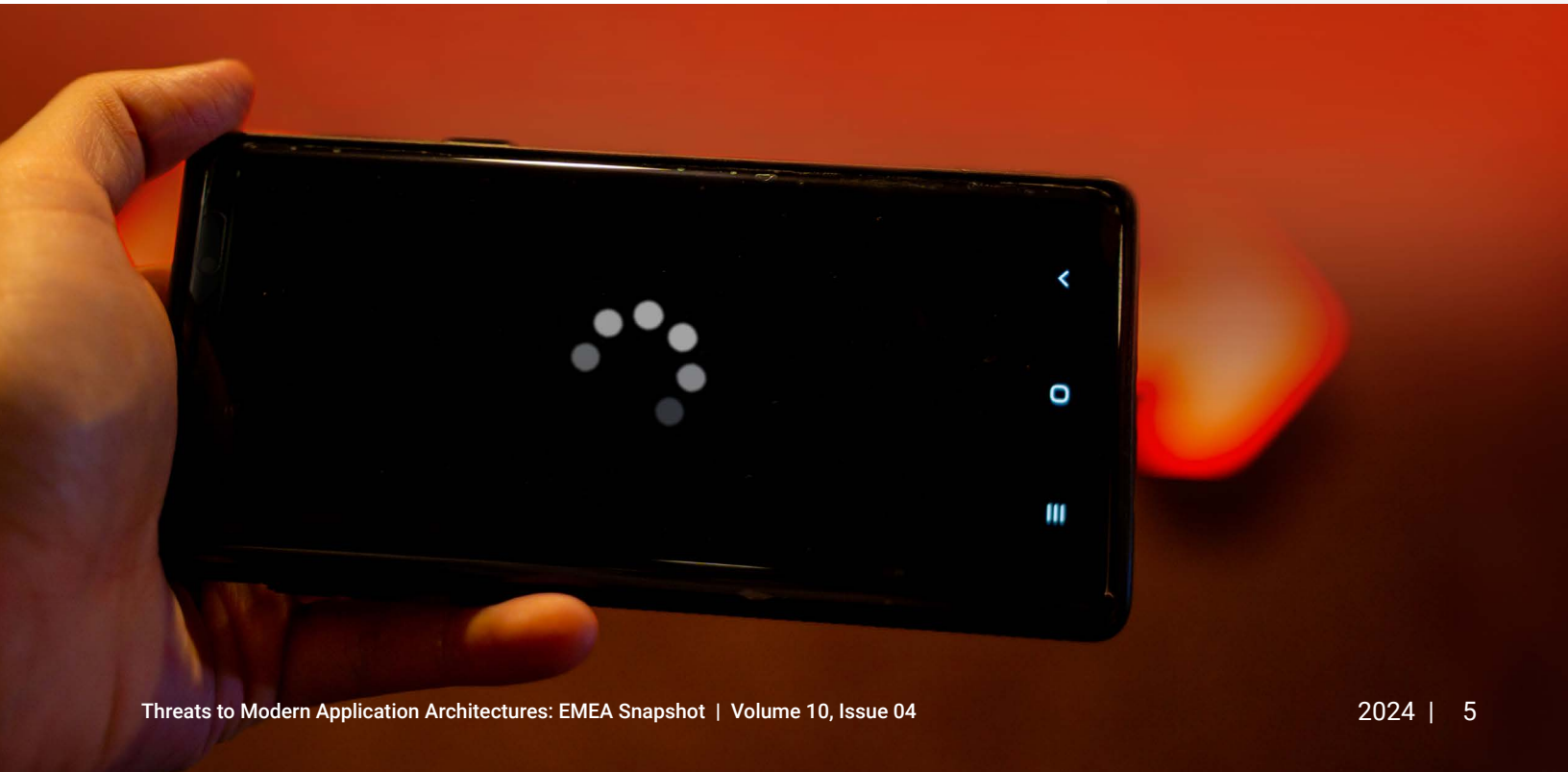
It is not uncommon for attackers to use traditional tactics like LFI and SQLi in order to access their intended targets' data. Additionally, LFI enables attackers to gain a foothold in their intended targets and perform remote code execution, thus compromising their security.



Continuing the trend observed in previous reports, commerce and video media were the top industries impacted by web application and API attacks in EMEA. Additionally, as we reported in our API security SOTI, commerce continued to experience the highest percentage of API attacks compared with other sectors in the region (EMEA Figure 3).



EMEA Fig. 3: Because of a huge percentage of API attacks, commerce was the sector most impacted by web attacks, followed by video media, high technology, and financial services



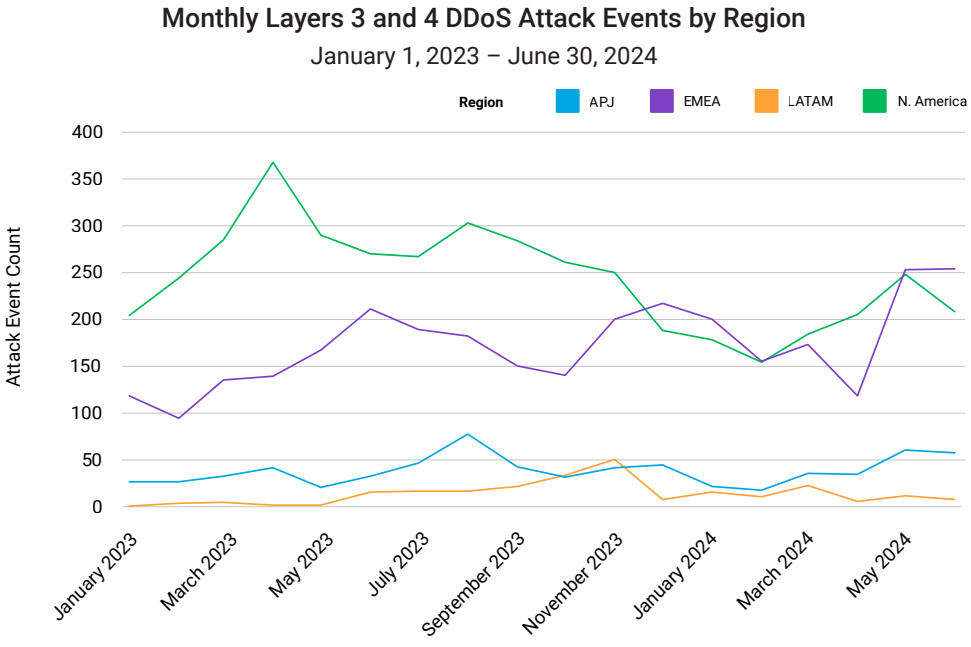
DDoS attacks threaten application uptime

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 infrastructure (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.

The gamut of DDoS attack types and trends in the region was explored in depth in our recent EMEA 2024 SOTI. Here, we include some updated data that demonstrates the continued rise of Layers 3 and 4 and Layer 7 DDoS threats 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 the number of Layers 3 and 4 DDoS attack events grew steadily in EMEA, surpassing the number of monthly DDoS attack events in North America for five of the past seven months (EMEA Figure 4).



EMEA Fig. 4: Monthly Layers 3 and 4 DDoS attack event numbers in EMEA surpassed those for North America for five of the past seven months

Within EMEA, the top countries impacted by DDoS Layers 3 and 4 attack events were Saudi Arabia (957) and the United Kingdom (576), followed by Switzerland (240), Turkey (205), Italy (203), Germany (189), and Poland (115).

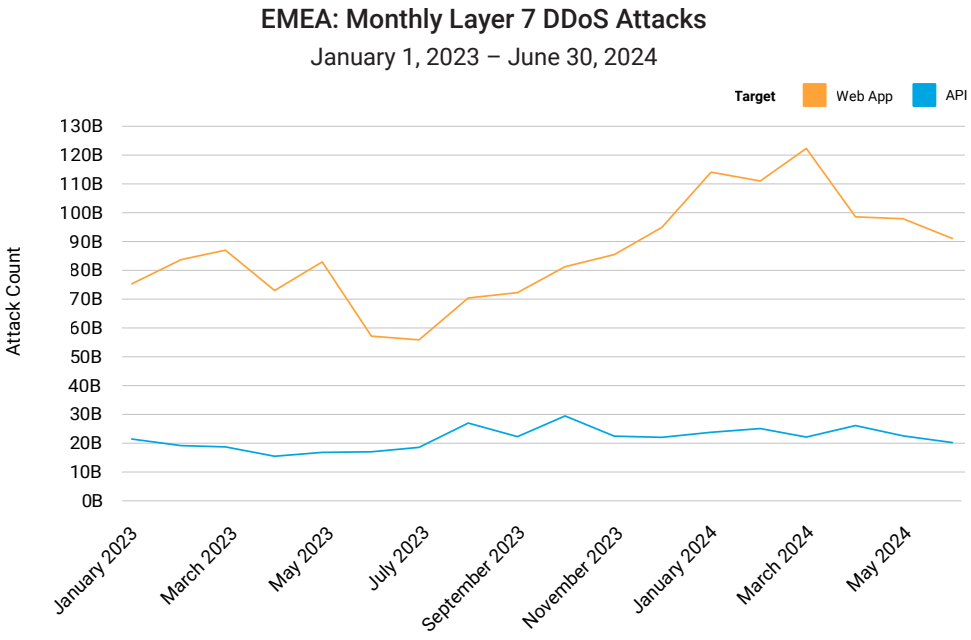
As discussed in our EMEA SOTI, DDoS is a popular tool for politically motivated hacktivists and nation-state–sponsored attackers, and the Russia-Ukraine and Israel-Hamas wars have led to increased attacks.

From an industry perspective, the financial services (1,523) and manufacturing (890) industries experienced the highest number of DDoS Layers 3 and 4 attack events, followed by gaming (189), commerce (151), gambling (105), and high technology (95).

Application-layer DDoS attacks

In addition to Layers 3 and 4 DDoS attacks, the region was also impacted by application-layer (Layer 7) DDoS attacks. During the 18-month reporting period from January 2023 through June 2024, our researchers found that EMEA was the third most impacted region by Layer 7 DDoS attacks, experiencing 1.9 trillion versus 8.7 trillion in North America and 5.1 trillion in APJ.

Although they are lower than in other regions, it is important to note that EMEA's Layer 7 DDoS attack numbers are on the rise. Following a dip in May 2023 to 74 billion, monthly Layer 7 DDoS attacks trended upward significantly, nearly doubling by March 2024 before ending Q2 2024 with a monthly average of 119 billion attacks targeting web applications and APIs (EMEA Figure 5).

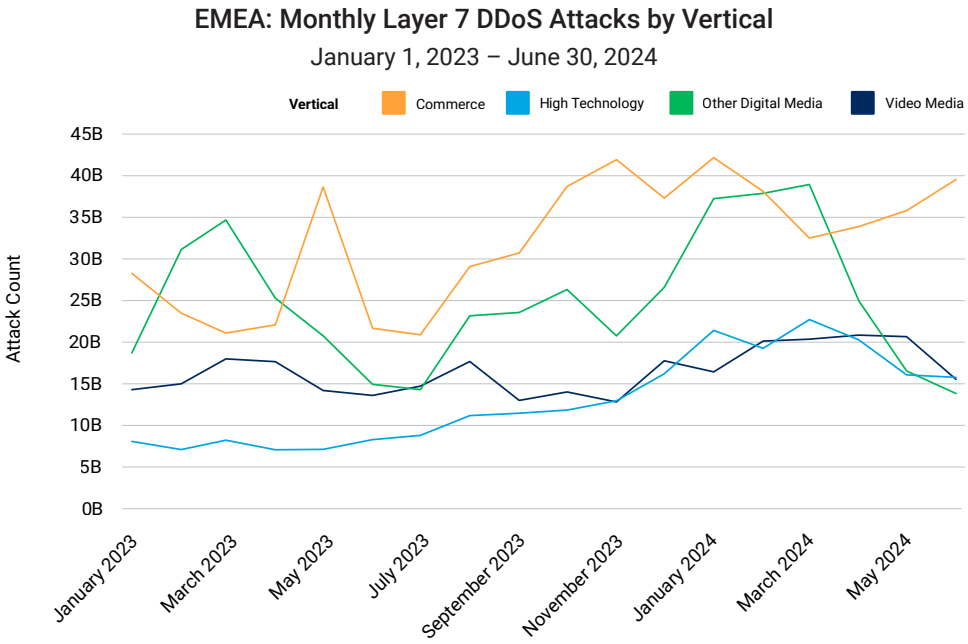


EMEA Fig. 5: Layer 7 DDoS attacks increased significantly since June 2023, ending Q2 2024 at a monthly average of 119 billion attacks

Throughout this period, DDoS attacks on APIs remained fairly steady and accounted for 25% of those attacks. So, in addition to defending against the attack vectors discussed earlier with respect to web application and API attacks (see EMEA Figure 2), defending APIs from DDoS attacks is a clear imperative, particularly as directives and regulations continue to drive the use of APIs.

Within EMEA, the areas with the highest number of Layer 7 DDoS attacks were Germany (461 billion) and the United Kingdom (366 billion), followed by Sweden (167 billion), Israel (151 billion), Italy (125 billion), Malta (113 billion), Switzerland (112 billion), France (90 billion), the Netherlands (79 billion), and Spain (77 billion).

Looking at sectors reveals that commerce started and ended the period as the industry most impacted by Layer 7 DDoS attacks, followed by other digital media, video media, and high technology (EMEA Figure 6).



EMEA Fig. 6: The commerce industry was the most impacted by Layer 7 DDoS attacks

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 applications 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, which can protect 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. It allows for thorough network visualization and extremely granular governance controls. 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 EMEA region that exemplify how enterprises are securing critical workloads and advancing Zero Trust.

EMEA case study #1: To protect critical systems and sensitive data that relate to trading and payments, the chief information security officer (CISO) at a leading investment bank regularly reviews the security of its technology infrastructure to strengthen the security posture of all its domains. Stopping ransomware attacks is a big focus, as are scalability and coverage of different operating systems and cloud environments. Additionally, the CISO wanted a way to reduce the attack surface without incurring the costs and delays associated with upgrading legacy firewalls. Application workloads were ringfenced from one another by the implementation of a software-based microsegmentation approach that creates secure zones across data center environments. If a workload is attacked, it can be isolated, preventing malicious software from spreading through the network.

EMEA case study #2: A media and software vendor needed an easier way to advance its Zero Trust framework to better protect critical workloads and customer data. To realize this improvement, segregating high-value components like identity management and enterprise resource planning systems from one another with precise segmentation policies was imperative. The goal was to minimize incoming and outgoing traffic and tighten access policies on hundreds of enterprise servers. At the same time, the company wanted to avoid making major ecosystem changes that might cause disruptions and increase security risk. A software-based microsegmentation approach with granular visibility into interaction patterns, as well as alerts, empowered the team with capabilities to prevent malicious lateral movement within the entire network.

Conclusion

In this EMEA 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, current and upcoming legislation also make it imperative to secure applications.

Within EMEA, in the European Union, key legislation in this regard includes the updated Network and Information Systems (NIS2) Directive, the Digital Operational Resilience Act, the Cyber Resilience Act, the European Programme for Critical Infrastructure Protection, the new Payment Card Industry Data Security Standard v4.0, and the upcoming revised EU Payment Services Directive (PSD3).

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**.

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn.
Published 08/24.