SOTI

V10 ISSUE 04

10 YEARS
OF SECURITY INSIGHT

Digital Fortresses Under Siege

Threats to Modern Application Architectures

Akamai

State of the Internet/Security

Table of Contents

Introduction

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

Fueled by the adoption of microservices, cloud computing, the need for integration across systems and services, and, most recently, the rapid adoption of artificial intelligence (AI) features, application and API security is now central to any strategic defense.

Meeting that strategic imperative, however, can be complex.

Applications run nearly every aspect of business, making trillions of connections easier — but also more vulnerable to attack. Protecting those trillions of connections requires attention to who is verified to access which parts of your network and business, and how workflows are accessed and verified from server to server. Priority must also be given to fighting bots and botnets that dominate internet traffic, since so many of them are being used for potentially unsafe purposes.

That's why we've devoted this State of the Internet (SOTI) threat intelligence report to web application strategy. Our data analysis aims to help serve as a valuable compass for your organization's application security strategy. Regardless of your current approach, we believe the insights we provide can help you strategically prioritize and implement future security controls.

This guidance is designed to enhance protection without impeding the crucial process of digital innovation. By striking this balance, you can fortify your applications while maintaining the agility necessary to stay competitive in today's rapidly evolving digital landscape.

Key insights of the report

Web attacks against applications and APIs surged by 49% between Q1 2023 and Q1 2024. The exponential growth in demand for applications and APIs has transformed them into lucrative targets for threats actors who are seeking to exploit security gaps to gain unauthorized access to their intended target's valuable data.

108 billion API attacks were recorded from January 2023 through June 2024. The relentless assaults against this critical digital interface, which serves as an invisible gateway to organizations, can potentially lead to data theft, damages to brand reputation, and regulatory fines, amounting to significant financial losses.

API abuse is a growing concern for businesses that rely on APIs to provide access to their data and services, and it can occur in various forms, including data breaches, unauthorized access, and distributed denial-of-service (DDoS) attacks.

The commerce vertical was victim to the most web application and API attacks, experiencing more than double the amount of attacks than any other industry.

DDoS attacks challenge traffic over all ports and protocols on Layers 3 and 4 and Layer 7. This also includes the Domain Name System (DNS) protocol, which Akamai researchers observed to be a component of 60% of the Layers 3 and 4 DDoS attack events identified in the past 18 months.

Akamai researchers observed high technology, commerce, and social media to be the top three industries in application-layer DDoS attacks, experiencing more than 11 trillion attacks (75% of the attacks) in just 18 months.

Akamai

Web of vulnerabilities: A deep dive into application and API security risks

APIs and web applications were the targets of multiple web attacks in 2023 as cybercriminals exploited the swiftly growing API economy for new avenues of attack. In one breach, a United States telecommunication company fell victim to attackers who exploited an authorization vulnerability in their API, exposing 37 million customer records. Ransomware groups like CL0P — that are relentlessly swift to adopt new attack methodologies — also used web application vulnerabilities to strike organizations.

During the reporting period of January 2023 through June 2024, Akamai research saw the frequency of web attacks that targeted web applications and APIs grow significantly. At the start of 2023, we monitored nearly 14 billion attacks per month, which increased to more than 26 billion monthly attacks in June 2024 (Figure 1). This represents a 49% growth in web attacks from Q1 2023 to Q1 2024.

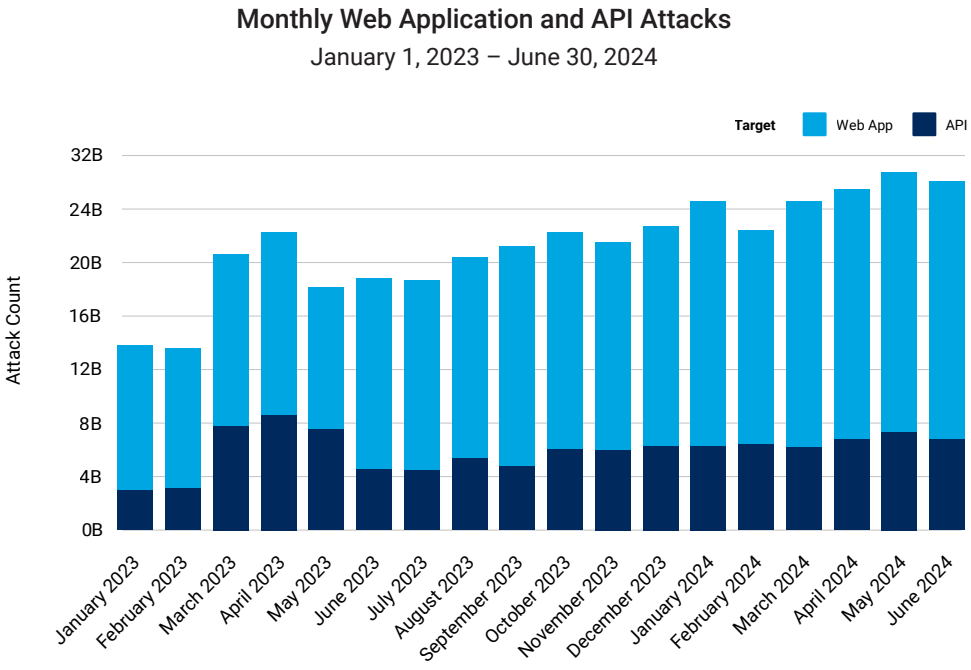
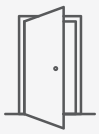


Fig. 1: Attackers are increasing their use of traditional web attacks to target web applications and APIs as exemplified by the 49% year-over-year growth

Although zero-day exploits continue to garner media attention, they are not the only means through which attackers infiltrate networks. Unpatched vulnerabilities — some of which are several years old — continue to provide entry points for adversaries. In June 2024, Akamai researchers discovered a campaign targeting ThinkPHP applications that are vulnerable to CVE-2018-20062 and CVE-2019-9082. The vulnerabilities have been in the wild since at least 2018, but because they remain unpatched in some organizations, attack activity continues today.

Several high-profile data breaches in recent months have been linked to API abuse or exploitation of API vulnerabilities, indicating that attackers are increasingly targeting this crucial digital interface.

Prioritizing patch management is mainstay counsel from cybersecurity organizations, yet many companies still struggle to implement successful patch management protocols. Using application and API protection solutions and microsegmentation can significantly mitigate exploitation attempts and their potential impact on organizations until patching can be completed. Such solutions provide a critical layer of defense, even when immediate patching is not possible, by protecting and ringfencing vulnerable systems from malicious traffic.



Unpatched vulnerabilities — some of which are several years old — continue to provide entry points for adversaries.

LFI, XSS: Attackers' favored tactics

Our data shows that local file inclusion (LFI), cross-site scripting (XSS), SQL injection (SQLi), command injection (CMDi), and server-side request forgery (SSRF) attacks remain prevalent vectors that target business applications and APIs. These attack methods persist due to their effectiveness in exploiting common vulnerabilities in web applications and APIs, which often stem from inadequate input validation and improper security configurations. LFI, for instance, increased by 120% from Q1 2023 to Q1 2024 (Figure 2). Similarly, SQLi and CMDi attacks saw a significant uptick, with attacks rising by 25%. However, it is important to point out that although these are prevalent attack vectors, Akamai also continuously evolves threat detection capabilities to address the dynamic nature of cyber adversaries' techniques.

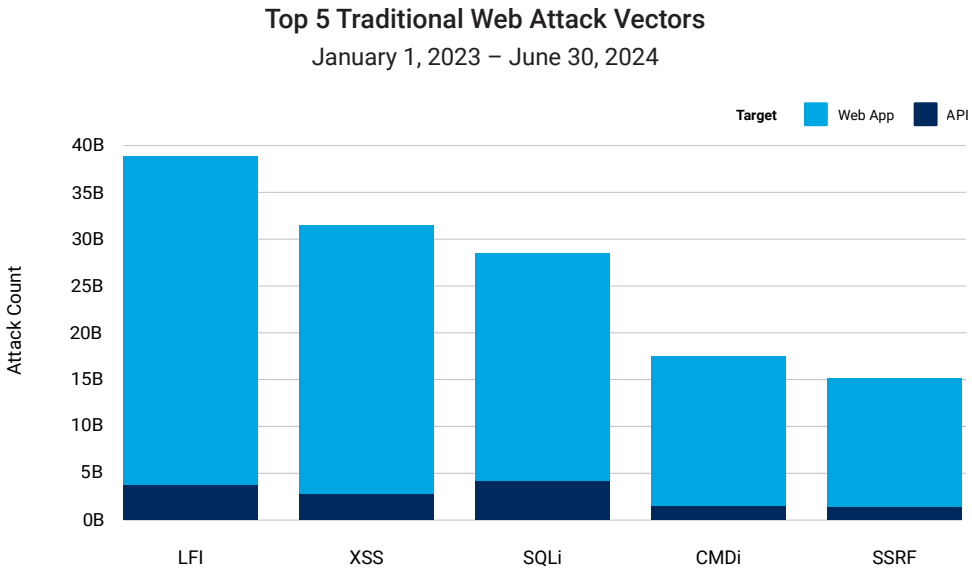


Fig. 2: LFI, XSS, and SQLi vectors are driving the growth in traditional web attacks

LFI, XSS, and SQLi attacks have been successful for many years because they exploit fundamental weaknesses in web application design and development practices. Despite increased awareness, these vulnerabilities continue to appear in new applications due to factors such as rapid development cycles, legacy code maintenance, and insufficient security testing.

Additionally, the growing complexity of modern web applications and the widespread use of APIs have expanded the attack surface, providing more opportunities for attackers to leverage these well-established techniques.

In February 2024, an attack group dubbed ResumeLooters exploited SQLi and XSS vulnerabilities to target numerous retail and job listing websites, which primarily impacted users in the Asia-Pacific region. The campaign reportedly resulted in the theft of more than 2 million unique email addresses and more than 2.1 million user data records. Additionally, the attackers attempted to peddle stolen information via Telegram channels.

Emerging attack vectors like SSRF have gained prominence as organizations increasingly rely on cloud services and microservices architectures. These attacks exploit the trust relationships among internal systems and can bypass traditional security controls, making them particularly dangerous in modern, distributed environments.

The growing complexity of modern web applications and the widespread use of APIs have expanded the attack surface, providing more opportunities for attackers to leverage these well-established techniques.

Industry trends: The steady increase of web attacks in commerce

Consistent with a 2023 SOTI report, Slipping Through the Security Gaps: The Rise of Application and API Attacks, organizations in the commerce industry experienced the highest volume of web attacks (164 billion), with more than double the number of attacks seen in the high technology sector (59 billion), from January 2023 through June 2024 (Figure 3).

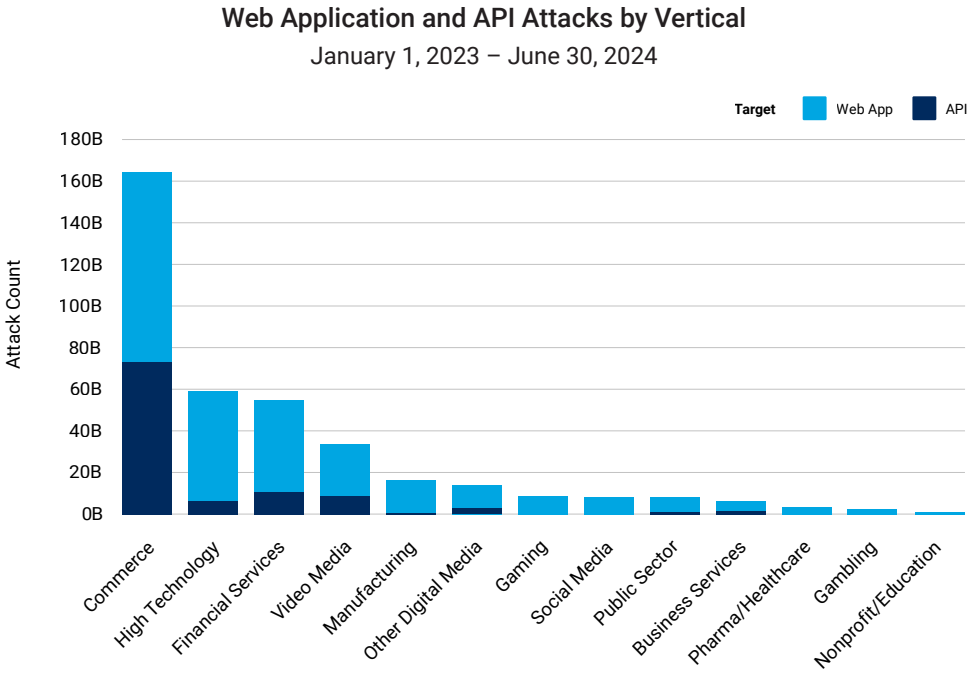


Fig. 3: The top verticals impacted by web application and API attacks are commerce, high technology, and financial services

The commerce vertical likely remains in the top position because of two factors: First, organizations in this vertical heavily rely on web applications and APIs. Second, speed-to-market pressures may cause some commerce organizations to provide inadequate protection solutions as new web apps are deployed. The combination of these two factors makes the commerce industry a continuously reliable and lucrative target for cybercriminals.

In third place was financial services with 55 billion recorded web attacks during the reporting period. Attacks in this vertical are often particularly problematic for organizations and customers alike, since they can potentially lead to compromised user account information. This opens up opportunities for credential stuffing and other forms of abuse across an entire organization's application landscape.

The manufacturing vertical also fell victim to web application and API attacks, coming in fifth this year. Unlike their commerce counterparts, manufacturing organizations are not often customer-facing, but an uptick in Internet of Things (IoT) use and data sharing make them prime targets for these attacks.

Attack trends in APIs

In March 2024, Akamai researchers released a report that analyzed the different attack types adversaries use to target APIs. That report identified runtime and posture challenges, and indicated the areas of API security that organizations should focus on to remain safer.

Our examination of the data revealed a concerning trend: APIs are increasingly targeted, as demonstrated by a consistently increasing number of attacks (Figure 4). In the first half of 2024 alone we observed 40 billion API attacks (compared with 35 billion in the same period last year). When compromised, APIs can provide unauthorized access to sensitive information, potentially leading to a slew of repercussions; chief among those repercussions is data theft and fraud. However, the ramifications of successful API attacks extend beyond data loss to the erosion of customer trust, damage to brand and reputation, and potential compliance issues.

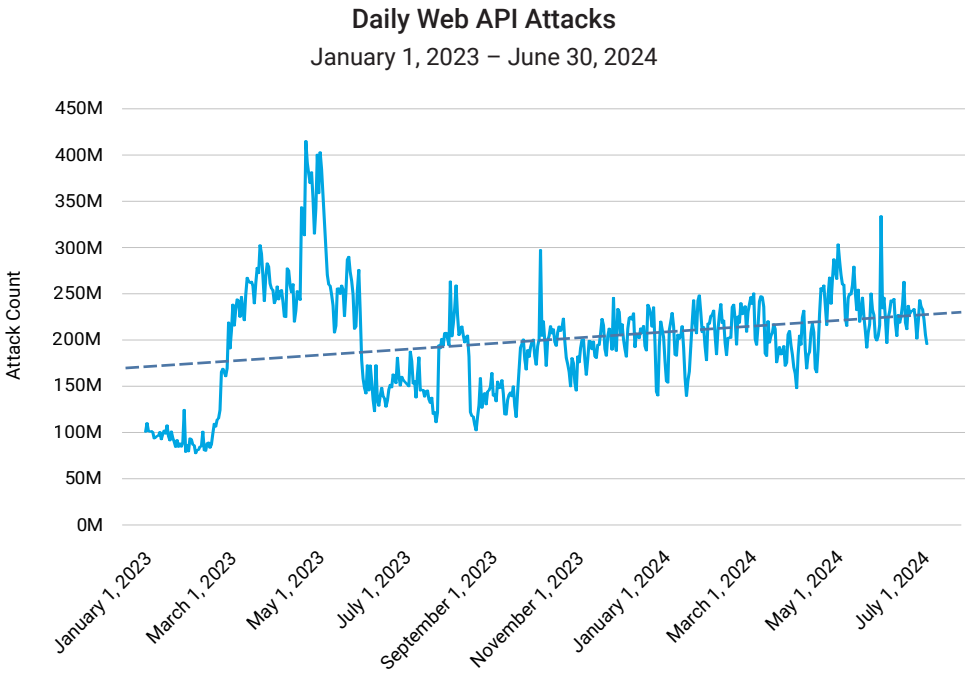


Fig. 4: API attacks steadily increased over the past 12 months with a few significant spikes throughout the reporting period

When compromised, APIs can provide unauthorized access to sensitive information, potentially leading to a slew of repercussions; chief among those repercussions is data theft and fraud.

Two factors may explain why it is challenging to defend against API attacks.

1. Time-to-market pressures strain both development and security resources, often leading to overlooked security processes, process protocols, and solutions needed to help protect apps once they're deployed. Applications that lack a proper security posture could be more exposed to attackers who have a keen eye for weaknesses and are quick to abuse them. Additionally, unsecure coding can result in vulnerabilities — another prime hunting ground for cybercriminals.

2. Security teams face unique challenges given the volume, speed, and complexity of the API environment in many organizations. Many companies lack cross-team visibility into their API footprint, which leads to an incomplete picture of the overall security landscape. Knowing both the full inventory of an attack surface and having security controls in place to protect that surface is crucial to keeping intruders out of a network. Special consideration should be given to understanding undocumented or shadow APIs, and identifying and prioritizing apps that expose sensitive data.

Combatting business logic abuse

Securing APIs requires a holistic approach and is not limited to fixing design flaws — it also covers both internal and external systems, including web application. Business logic abuse is particularly challenging to detect and prevent as attacks of this type often abuse legitimate access to breach APIs. It is important to note that API abuse can happen in various shapes and forms as it comes from users or activities that leverage approved connections or credentials.

To combat abuse of logic, organizations need to continuously monitor APIs and continuously learn and adapt to evolving API behaviors. Once that is happening, implementation of a comprehensive security strategy should follow, and it should include:

- Understanding the business logic and application workflows thoroughly
- Conducting thorough threat modeling to identify potential misuse cases
- Implementing robust API security measures and maintaining visibility of all APIs, including shadow APIs
- Employing advanced security solutions that can detect and prevent business logic abuse using behavioral analytics and AI

Ensuring a robust comprehensive API security posture

To ensure robust API security, a multifaceted approach is essential. First, it is imperative to implement comprehensive inventory management and detection mechanisms to minimize the prevalence of rogue or shadow APIs. Subsequently, the establishment and enforcement of stringent coding standards are crucial to mitigate risks associated with the Open Web Application Security Project (OWASP) Top 10 API Security risks.

Validation of these security measures should be conducted through the use of vulnerability assessment and security posture testing tools. For operational systems, it is advisable to dedicate a team to focus on the detection and response to potential threats. This team should be equipped to address both traditional attack vectors, such as LFI and SQLi, as well as API-specific vulnerabilities, including Broken Authentication and Unrestricted Access to Sensitive Business Flows.

Furthermore, the implementation of user activity monitoring is paramount in identifying potential API abuse. All these security measures should be complemented by rapid mitigation strategies and efficient reporting mechanisms in the event of security incidents. Finally, it is crucial to adopt a proactive approach to minimizing the attack surface across all environments, thereby reducing the overall risk exposure of the API infrastructure.

Security spotlight:
Read mobile app fine print carefully, not “approxi”mately

Mobile app user agreements are often accepted by users without reading the details. In some apps, the fine print may include the acknowledgment that users agree that their device can be included as part of a mobile proxy network, in exchange for the services provided by the app. Mobile proxies are portable devices, such as smartphones or tablets, that use mobile data to connect to the internet through proxy servers.

The installation of proxy services can be voluntary, and some mobile app users can enroll their devices in these networks and exchange their bandwidth for financial compensation.

However, some apps have also converted mobile devices and other residential IoT devices into proxy network nodes automatically, without the awareness of users. This may occur either by app developers including it as part of the original functionality of the application, or by a threat actor who maliciously installs malware. In the case of malicious conversion, threat actors may then proceed to steal bandwidth and sensitive information from the user.

There are also data extraction companies that are motivating game developers with incentives to include their mobile software development kit (SDK) in their gaming applications. An SDK is a collection of tools that assist developers with building and updating mobile apps. This allows the game studio to offer the user an ad-free or premium experience in exchange for including their device in a proxy network when the app is running. After the user agrees to allow their device to be part of the collection of web data, the device may still be active as a proxy even if the SDK is running in the background of the app.

It is crucial for mobile app users to research apps and understand the agreements associated with them. The good news is that most legitimate apps don’t use a device as a proxy without user knowledge or consent, and there are ways to uncover which apps are safe and which may not be. These include:

- **Checking the app’s privacy labels:** Apple and Google Play require developers to disclose their data collection practices. Although this doesn’t specifically mention proxy use, it can give you an idea of how the app handles network connections.
- **Reading the app description:** Some apps, especially those designed for network testing or VPN services, may mention proxy-related features in their descriptions.
- **Reviewing user feedback:** Check the ratings and reviews section for any mentions of unexpected network behavior or proxy use.
- **Looking for security features:** Apps that implement certificate pinning or other security measures may be less likely to allow proxy connections, as these features can detect and prevent machine-in-the-middle attacks.

In all cases, it is wise to thoroughly read an app’s user agreement before accepting it.

Defending applications and the infrastructure that powers them

When it comes to defending application infrastructure, security teams need to think about firewalls, patch management, access control policies, network segmentation, and more.

DDoS is one of the favored attack types of cybercriminals. DDoS attacks can target firewalls, networks, and servers and exploit vulnerabilities within infrastructure and applications themselves. These attacks challenge traffic over all ports and protocols on Layers 3, 4, and 7, including DNS, so proper protection of these layers is essential.

DDoS attacks that affect applications can be categorized into two main groups: infrastructure and application.

1. Infrastructure DDoS attacks have been around the longest and focus on the protocols in the networking (Layer 3) and transport (Layer 4) layers of the Open Systems Interconnection (OSI) model, which include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) traffic. Layers 3 and 4 attacks are often volumetric DDoS attacks, including SYN flood, Smurf DDoS, DNS amplification or reflection, UDP flood, and ICMP flood, among others. Attackers are increasingly employing multiple attack types and vectors to create complex, multidestination, sophisticated DDoS attacks. These require a robust and comprehensive DDoS protection platform that uses automation and machine intelligence to prevent damages.

2. Application layer (HTTP layer/web traffic layer) DDoS attacks are also on the rise and are becoming a more popular avenue for threat actors. Some exploit the logic of protocols used in Layer 7. The HTTP/2 logic vulnerability discovered in 2023 is an example of how attackers exploited a seemingly benign logic to bundle multiple requests into a stream and create the largest recorded Layer 7 DDoS attack. Part of what makes the application layer more attractive to DDoS threat actors is that attacks do not require much bandwidth, many packets, or numerous devices and are lower in magnitude (often less than 1 Gbps). These kinds of attacks are generally also more stealthy and severe — often the requests sent by attackers to crash an app appear legitimate. These attacks also focus on the more costly parts of the application, disabling access for users.

DDoS attacks on the DNS have also become increasingly common. If an organization's DNS goes down, their online presence disappears, making DNS a high-impact and highly lucrative target for cybercriminals. Depending on the type of the DNS DDoS attack, it could impact Layer 7 as well as Layers 3 and 4 of a network. In the past 18 months, 60% of the Layers 3 and 4 DDoS attack events identified by Akamai internal data had a DNS component. And within this category, DNS resource exhaustion attacks, otherwise also known as NXDOMAIN attacks, pseudo-random subdomain attacks, or DNS water torture attacks, make up more than 50% of the DNS DDoS attacks in Layers 3 and 4. In today's digital-first world, DNS DDoS attacks are also opportunistically used by cybercriminals to degrade the online performance of high-touch organizations, such as sports-betting companies or online-commerce companies during a major shopping season.

It is important to note that while DDoS attacks are sometimes segmented as Layers 3, 4, or 7 or as DNS attacks for easier understanding, attackers often employ vectors that target multiple layers and protocols to overwhelm a victim's applications and the underlying infrastructure. A robust and effective DDoS defense-in-depth strategy must include a comprehensive platform of solutions that can protect all layers, ports, protocols, and components from malicious actors.

The top 3 most targeted industries for Layer 7 DDoS: High technology, commerce, and social media

Globally, we've observed Layer 7 DDoS attacks to be most prevalent in the industries of high technology, commerce, and social media.

High technology

High technology has a significant lead among all industries, with an attack count of more than 5 trillion from Q1 2023 through June 2024 (Figure 5).

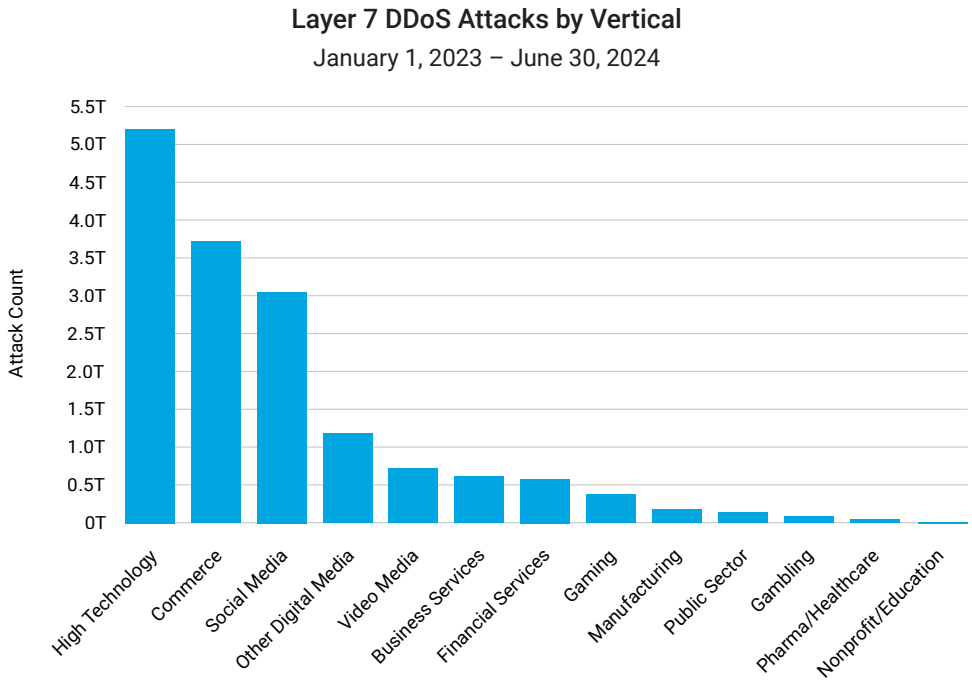
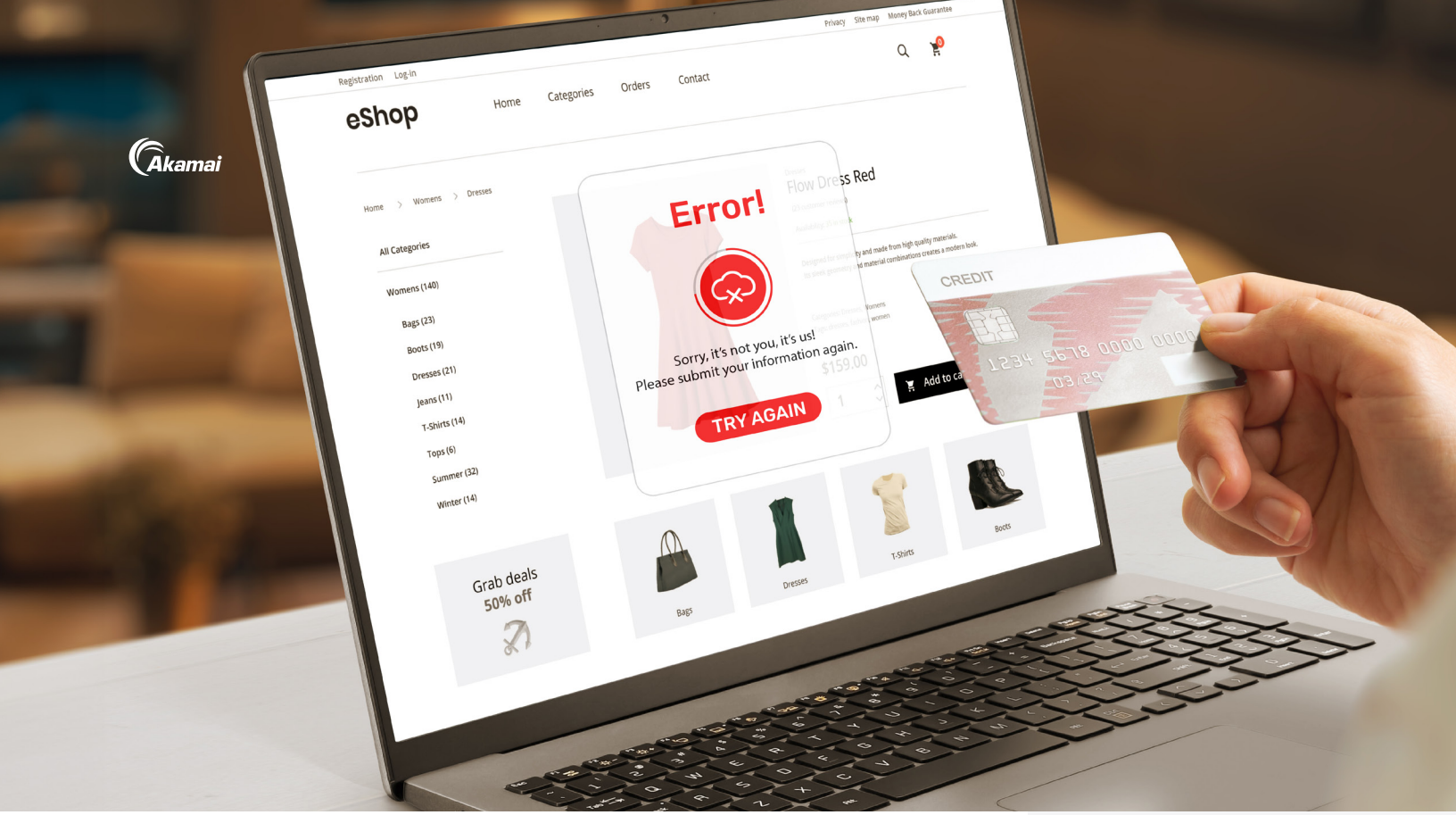


Fig. 5: High technology, commerce, and social media each have more than double the number of application-layer DDoS attacks than any other vertical

High technology consists of companies that rely on online services. The DDoS attack traffic we see may include cloud services and blockchain technology, which have both been strongly affected by Layer 7 DDoS attacks.

Cloud computing is no stranger to DDoS attacks. Cloud computing has become both the fuel and the target for such attacks, as security practitioners have seen attacks on businesses connected to the cloud as well as threat actors' use of the cloud itself as an easier way to launch DDoS attacks. Organizations with web applications supported by the cloud are not exempt from vulnerability to Layer 7 DDoS whether they are in commerce, finance, healthcare, or some other industry. Moreover, these application-layer DDoS attacks are even trickier to identify in the cloud environment because of the numerous options of attack paths.



There has been a noteworthy recent increase in the number of DDoS attacks in blockchain networks. Even though blockchain is decentralized by design, attackers have resorted to other DDoS methods outside of the traditional network flooding. We have observed cybercriminals using spam transactions to flood the blockchain, which causes a slow down in the completion of legitimate transactions. Additionally, we've seen HTTP flood attacks in blockchain DDoS attacks, and the smart contract network within blockchain has also been susceptible to DDoS. Protocols within the transport layer are mainly where compromise occurs in blockchain networks in these kinds of attacks.

Commerce

As we know from our recent EMEA SOTI report, the commerce vertical had the most Layer 7 DDoS attacks in that region, but globally it was second. We posit the commerce vertical ranked so high in Layer 7 DDoS attacks because of the significant revenue disruption opportunities these attacks offer threat actors. These types of attacks are especially crippling for commerce organizations because they can make an online store inaccessible or a reservation system unavailable, leading to a significant revenue loss for the victim company. At the same time, they may be deployed as a distraction tactic that consumes incident response resources, while attackers steal lucrative customer data (such as payment card information) from other areas in the victim's network.

Commerce was the most targeted vertical for Layer 7 DDoS attacks in the EMEA region, and globally it ranks second.

Social media

Layer 7 DDoS attacks rose globally in 2023, experiencing a spike in June (Figure 6). It's interesting to note that although social media has not been immune from this overall increase, that vertical saw a sharp rise of Layer 7 DDoS attacks for a 10-month period starting in April of 2023, a full two months earlier than the global spike (Figure 7).

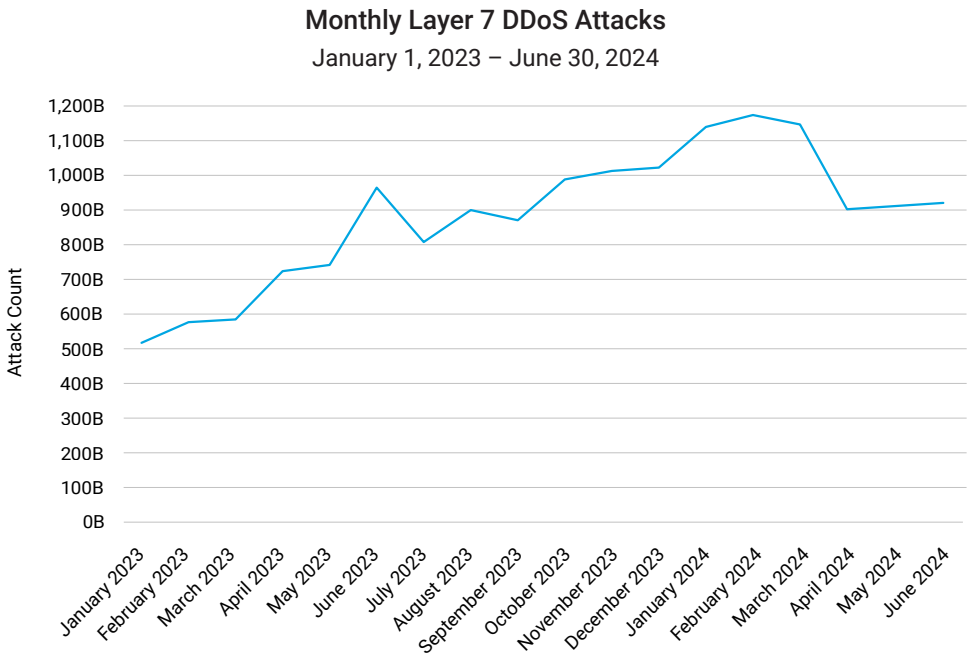
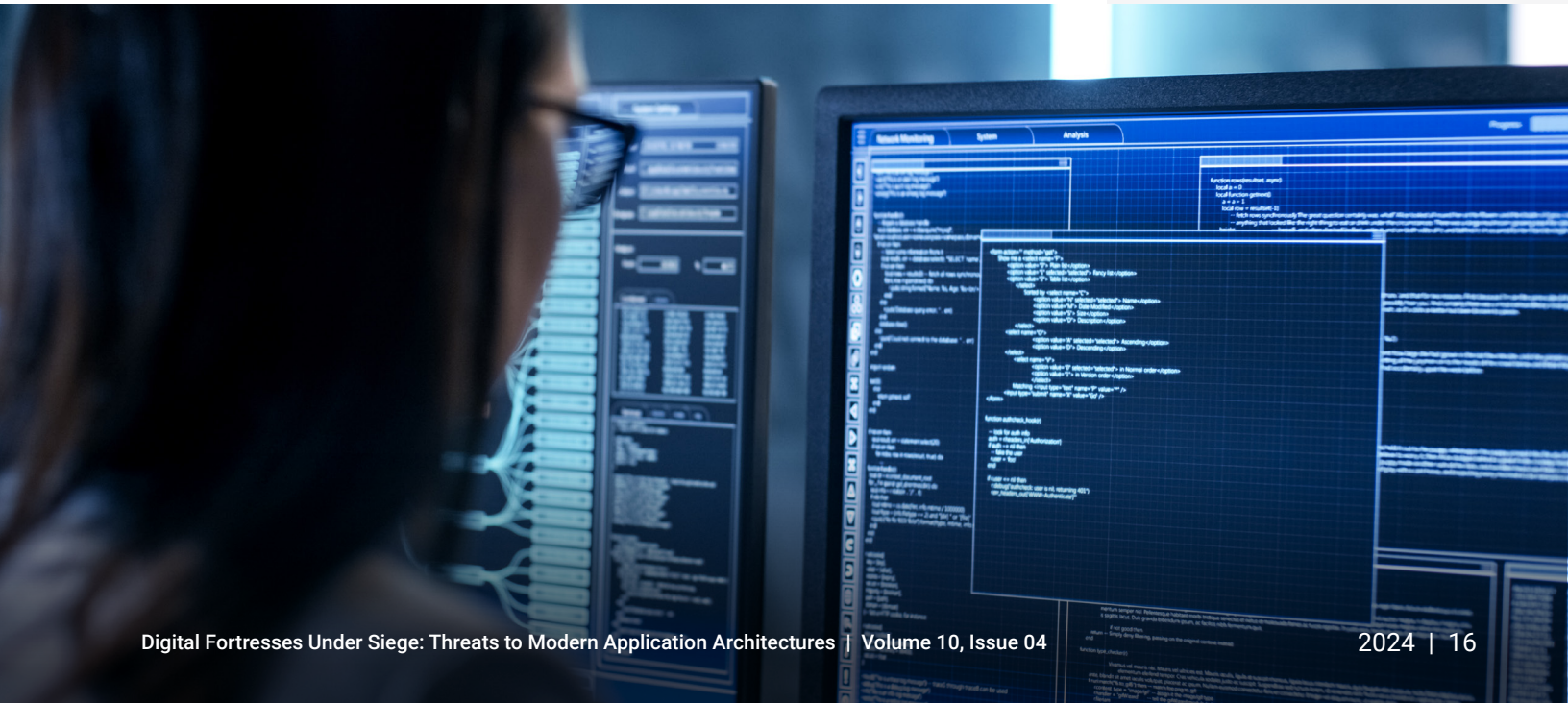


Fig. 6: A general rise of global Layer 7 DDoS attacks can be observed throughout the period with a sharp increase in June 2023



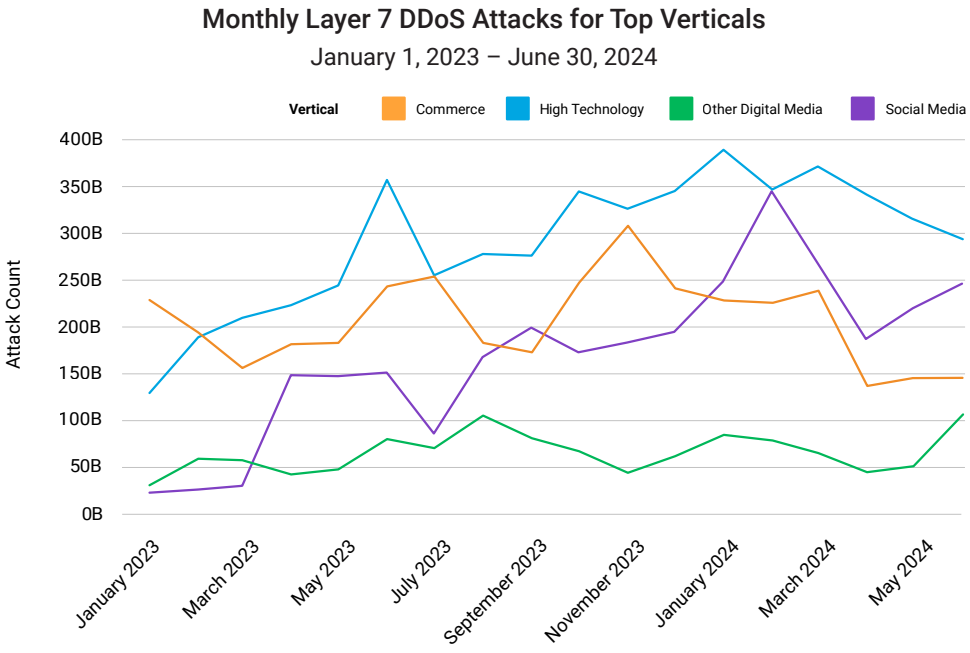


Fig. 7: The social media vertical has incurred a significant amount of impact from Layer 7 DDoS attacks

These Layer 7 DDoS attacks in the social media industry correlate with ongoing geopolitical events and pressures.

First, in 2024, multiple media outlets began to report on a surge of fraudulent pro-Russia social media accounts and spoofed news sites designed to amplify divisive political topics. These Russian influence operations target a wide range of global audiences and topics, but they consistently aim to erode support for Ukraine, discredit democratic institutions and leaders, and exploit existing political divisions.

Second, large-scale and highly mediated electoral events and country leadership questions often lead to politically motivated cyberattacks in various regions, including DDoS attacks, as actors seek to exploit the heightened political atmosphere for their agendas.

Third, hacktivism related to the ongoing Russia-Ukraine and Israel-Hamas wars has risen, and may have contributed to the increase in attacks as well.

Threat actors will likely continue to leverage social media platforms to spread misinformation and disinformation rapidly and widely. The proliferation of AI tools has made it easier to create and disseminate convincing false content — and made it more difficult to combat. As 2024 is an election year in Asia-Pacific and Japan (APJ) and in the United States, there are growing concerns about the potential impact of political AI-generated disinformation.

Social media companies have implemented various policies to combat misinformation, but their effectiveness remains unclear. The evolving nature of disinformation tactics and the rapid advancement of AI technologies continue to pose significant challenges for combating the spread of false information on social media platforms as we move further into 2024.

Web application Layer 7 DDoS attacks are more common than API attacks – but API attacks see a holiday bump

Web application firewalls and other security solutions, like smart DNS resolution services and healthy security architecture with CDNs, often help protect web applications and their infrastructure from DDoS attacks. Yet, both web applications and APIs are still widely targeted; in fact, both have their own lists of OWASP security risks. When it comes to the threat landscape, North America leads the way regionally for both web application and API Layer 7 DDoS attacks (Figure 8). Following North America is APJ for web applications and Europe, the Middle East, and Asia (EMEA) for APIs.

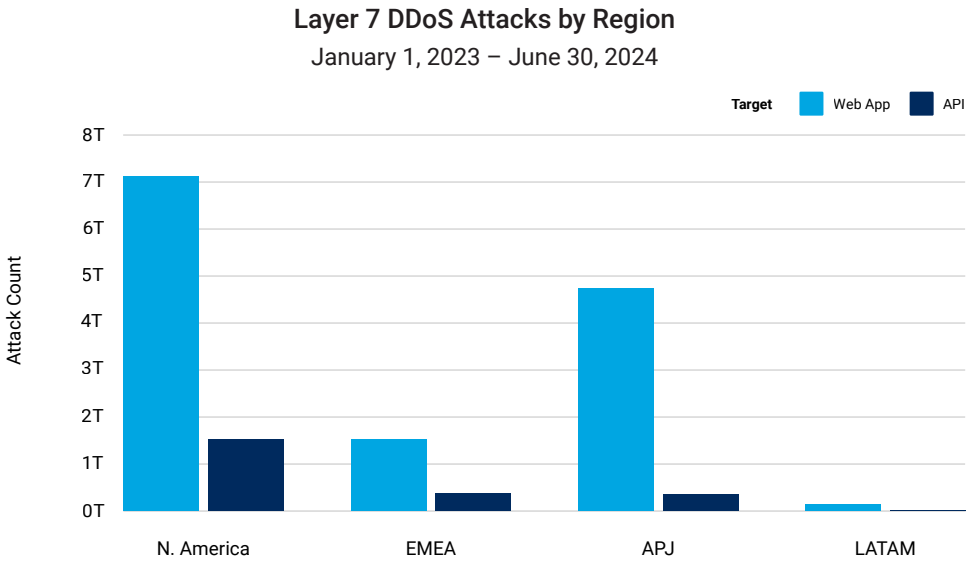


Fig. 8: Globally, we have observed Layer 7 DDoS attacks target more web applications than APIs; regionally, North America is the most targeted region for both web applications and APIs

An overload of requests, as in a DDoS attack, can cause APIs to crash (just like applications). Akamai lists DDoS attacks in the top 5 highest security risks for APIs that businesses and organizations should protect against. It is interesting to note a rise in Layer 7 DDoS attacks on APIs going into and through Q4 2023 (Figure 9).

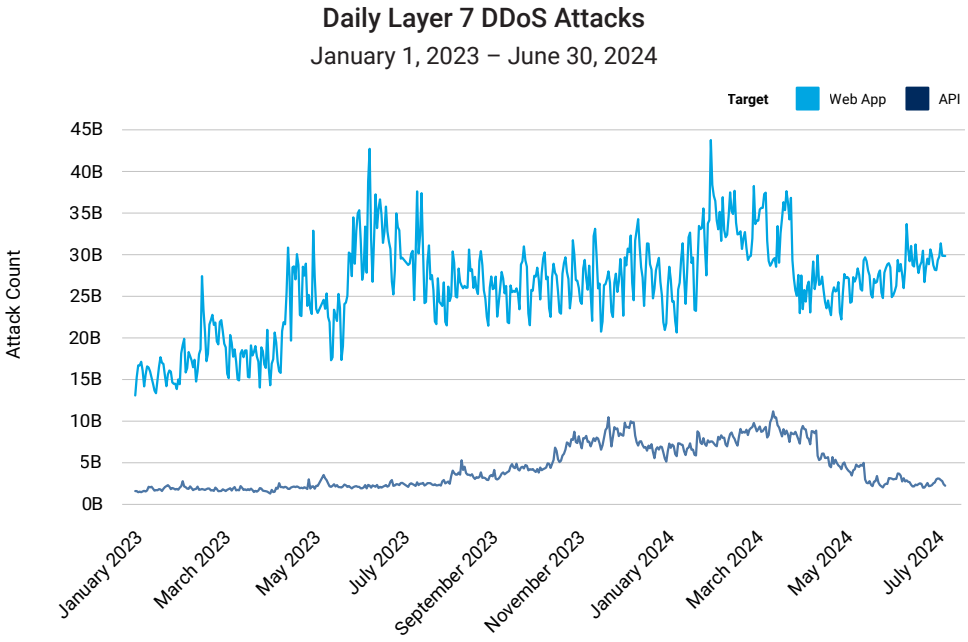


Fig. 9: Layer 7 DDoS attacks on APIs increased significantly during Q4 of 2023 and persisted through Q1 of 2024

The timing of the holidays and the opportunity for attackers to have a higher negative impact on a company's revenue typically increases attacks toward the end of the year. And our research shows a direct correlation between the winter holiday season and a rise in the number of cyberattacks. Specifically, the commerce vertical experiences a significant number of these attacks during this time when fewer security personnel and incident response resources are available to assist with a threat.

Ransomware Layer 7 DDoS groups

Unfortunately, the threat landscape has widened as attacks have become more complex, and ransomware groups play a large part in the ongoing advancement of attack tactics, techniques, and procedures (TTPs). One such example of an advanced TTP is triple extortion attacks, also known as ransom DDoS (RDDoS). With RDDoS, DDoS is added to an attack to hinder a victim's business while also encrypting a victim's data, stealing it, and threatening to publish the data unless a ransom is paid for it. Some popular ransomware groups that use RDDoS include Killnet, DarkSide, and Lazarus.

The Lazarus ransomware group commonly sends Layer 7 HTTP and HTTPS request floods to web properties of targets, and the observed attack volumes throughout this attack campaign have ranged from 50 Gbps to 300 Gbps and 150 Kpps to 150 Mpps. Lazarus has claimed to have as much as 2 Tbps of DDoS attack capacity. Thankfully, no attacks approaching this magnitude have occurred — yet. The Killnet ransomware group also uses DDoS attacks on Layer 7 (high-volume POST/GET requests) to cause resource exhaustion and system failure. These are just a couple of examples of the many threat actors focused on damaging organizations through Layer 7 DDoS attacks.

Layers 3 and 4 DDoS attack traffic

In addition to the application layer, DDoS attack events have had a significant impact on the infrastructure. We continue to observe Layers 3 and 4 DDoS attacks to go in waves, with attack activity rising and falling depending on the nature of co-occurring events (Figure 10). Over the past 6 months, EMEA and North America have been alternating as the most-targeted region. The EMEA region experienced more Layers 3 and 4 DDoS attack events than North America in five of the past seven months. The financial services industry still has the most Layers 3 and 4 DDoS attack events globally, and we can assume it will likely continue to be on top for a while given the consistent lead it has had for some time.

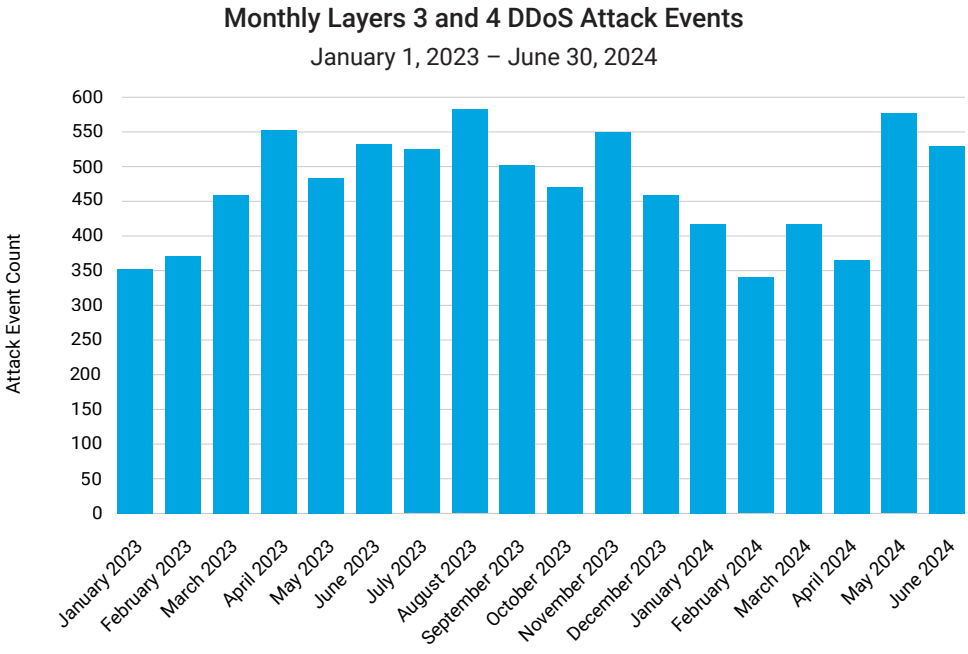


Fig. 10: DDoS levels in Layers 3 and 4 continuously rise and fall and can be observed varying by more than 200 attack events throughout the past 18 months

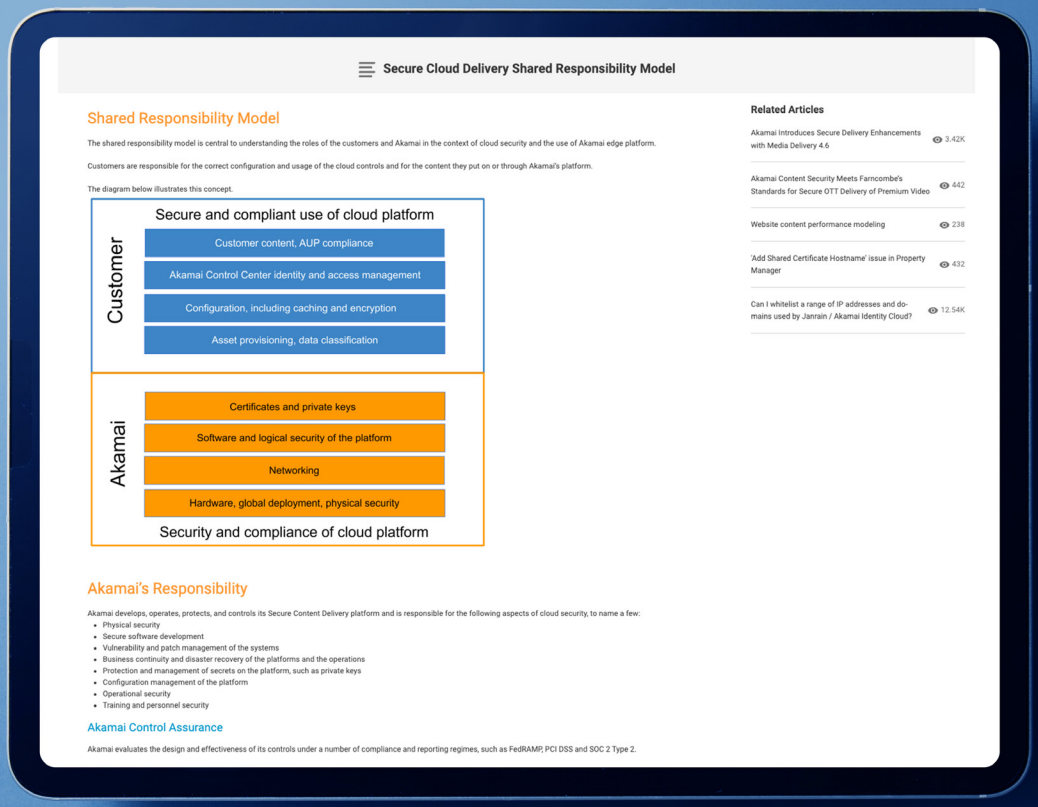


Image: Akama/Secure Cloud Delivery Shared Responsibility Model

Attackers zero in on application workloads

Zero Trust strategies are often thought of in terms of how they relate to network security. Web applications are sometimes overlooked when an organization implements a Zero Trust philosophy, but including them is a critical step to maximizing overall posture: The attack surface may be different on Layer 7, but it is not immune to the threats that affect Levels 3 and 4. In fact, unsecured web applications can increase entry points into your network that can lead to lateral movement or privilege escalation.

When overlooked, web applications can be exposed externally, as can the internal workloads between applications. This extended attack surface that results from web application deployment further complicates the already difficult job of security teams. For applications to function — whether in the cloud, on-prem, or hybrid — every individual workload must operate seamlessly. Workloads traverse multiple security jurisdictions as they move through the network, and each new jurisdiction adds a potential entry point for an intruder. Although Zero Trust is often thought of as a technology philosophy, human trust also needs to be a staple of application security since multiple vendors must share responsibility for securing workload pathways.

Implementing a proper Zero Trust framework is often a heavy lift for organizations. If it is done from hardware (traditional segmentation), it has to be architected with that specific goal in mind. For security practitioners that often means a "rip and replace" exercise that is resource intensive on all fronts. Application segmentation is similar, but typically a bit easier to implement, though it still relies on Layer 4 for controls. It is not, however, the optimal safeguard against intruders.

Software-based segmentation makes application security a considerably lighter lift since it can be deployed in minutes, which also allows it to double as a viable incident response measure. This approach is much more aligned to cover the deft developer's plight — making it an effective introduction of DevSecOps into an organization.

True Zero Trust implementation minimally requires microsegmentation, which can protect against ransomware or attacks on the workloads themselves. Microsegmentation allows for thorough network visualization and extremely granular governance controls, which are required to detect and mitigate a jeopardized workload or container. Sanctioned activity can then be governed with highly specific policies that are not affected by IP address spoofing or attempts to execute attacks over allowed ports.

Without this kind of robust posture, threat actors can gain a foothold and deploy ransomware and block workloads from completing wherever the application lives, effectively rendering an application useless until a ransom is paid.

Microsegmentation allows for thorough network visualization and extremely granular governance controls, which are required to detect and mitigate a jeopardized workload or container.

Real-world application of Zero Trust

Trust is required for effective communication, including the communication between the machine and the executable. While trust may be desirable in an interpersonal relationship, when it comes to access, Zero Trust is something organizations should make every effort to attain. Inside a network, lateral movement is required for ransomware or other threats to move through the system — and it's significantly more difficult to get through six different doors than one single door.

In this section, we present two case studies from the field that exemplify how Zero Trust aids enterprises by closing gaps in, and enhancing, their overall security posture.

Use case #1: Breaking the ransomware killchain

A communications infrastructure provider in the United States could have suffered from US$1 million in losses due to a ransomware attack if not for the Zero Trust framework that they'd recently deployed to their environment. Since this solution allows organizations to see events at a granular level, the security teams were alerted to the brute-force attacks and numerous failed log-in attempts to their Remote Desktop Protocol (RDP). After further investigation, the provider concluded that they were being targeted by a major ransomware group. The attack attempt was successfully thwarted by implementing a new policy that disabled RDP before any real damage to their systems and data occurred.

Use case #2: Insider threats

Insider threats pose critical dangers to organizations since sensitive information can be pilfered and used for fraudulent purposes. Regardless of industry type, insider threats are a risk for every organization, which makes it imperative to use solutions to identify malicious east-west traffic and to block unauthorized lateral movement.

The need for visibility into any internal communication among applications and systems prompted an educational institution in the United States to ringfence critical assets like Active Directory and SQL Server. With segmentation, this organization gains visibility of their data flows among applications, and can monitor unwanted traffic and block it if deemed malicious. Additionally, the organization can block RDP access to its web servers from third-party vendors.

Inside a network, lateral movement is required for ransomware or other threats to move through the system — and it's significantly more difficult to get through six different doors than one single door.

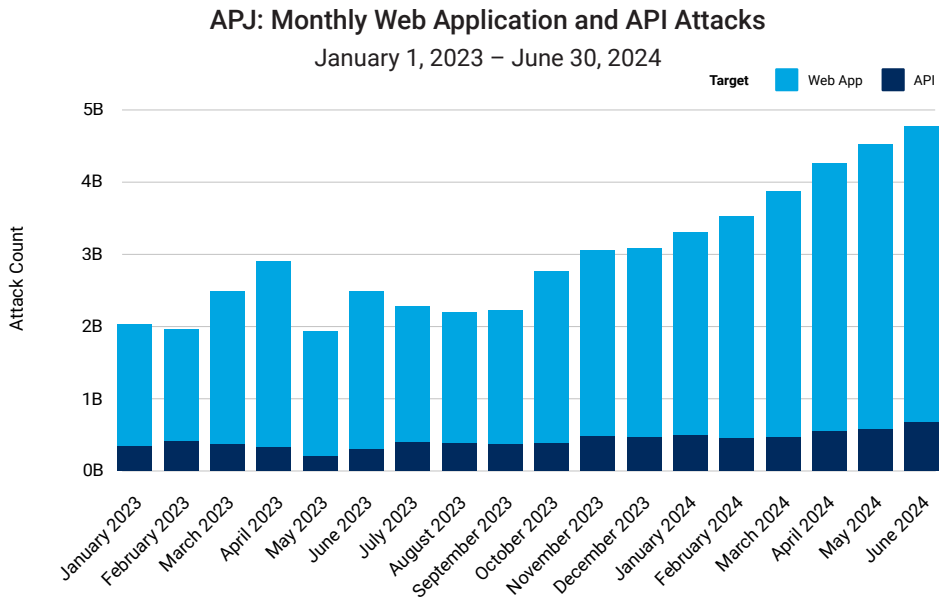
The APJ Snapshot is a companion piece to our larger secure apps SOTI report, Digital Fortresses Under Siege: Threats to Modern Application Architectures (available in English only). Please refer to that report for detailed descriptions of how adversaries exploit the expanding attack surface, recommendations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

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).



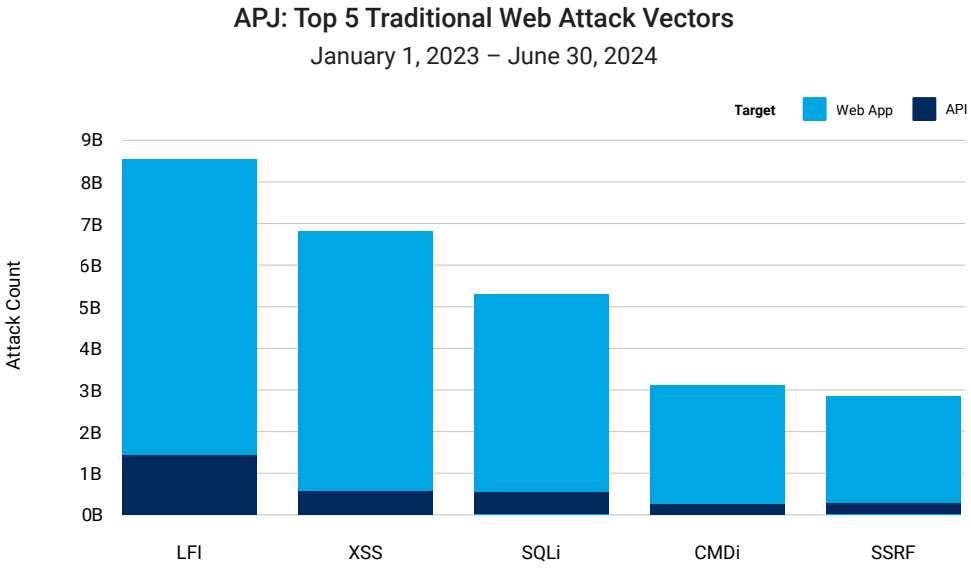
APJ Fig. 1: Web application and API attacks climbed 65% year over year

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.

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.

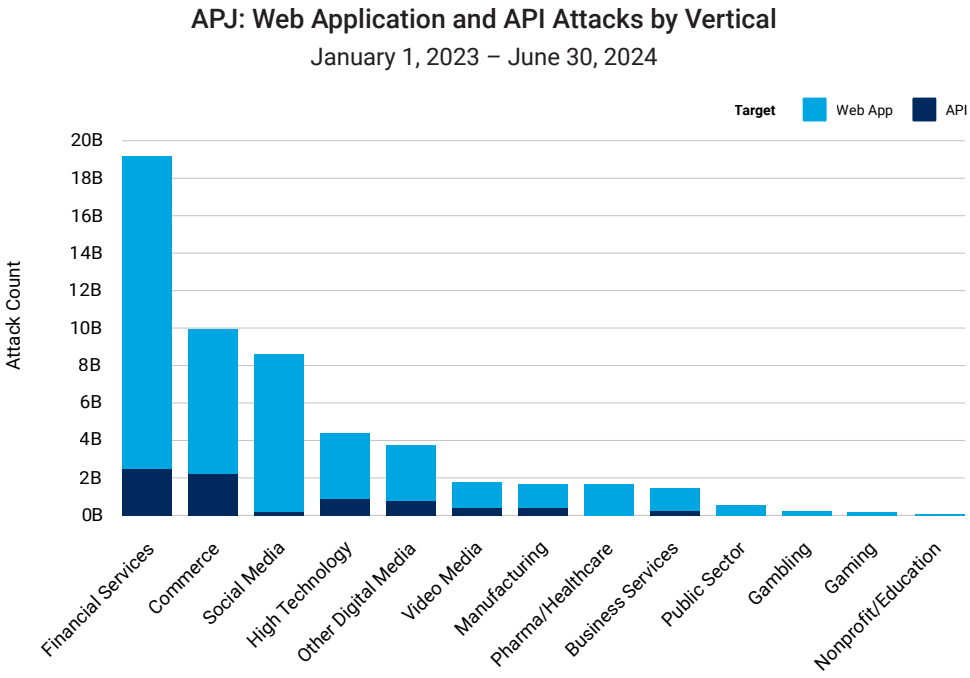
Consistent with previous reports, local file inclusion (LFI) remained a preferred attack vector, but other vectors, like cross-site scripting (XSS) and structured query language injection (SQLi), continued to pose risks (APJ Figure 2).



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 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

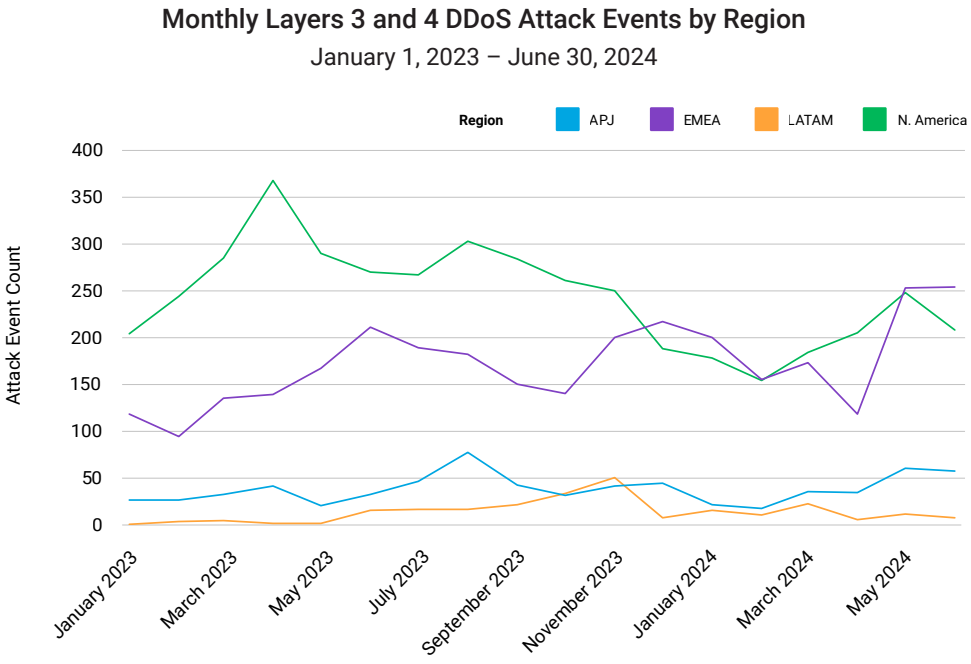
DDoS attacks threaten application uptime

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.

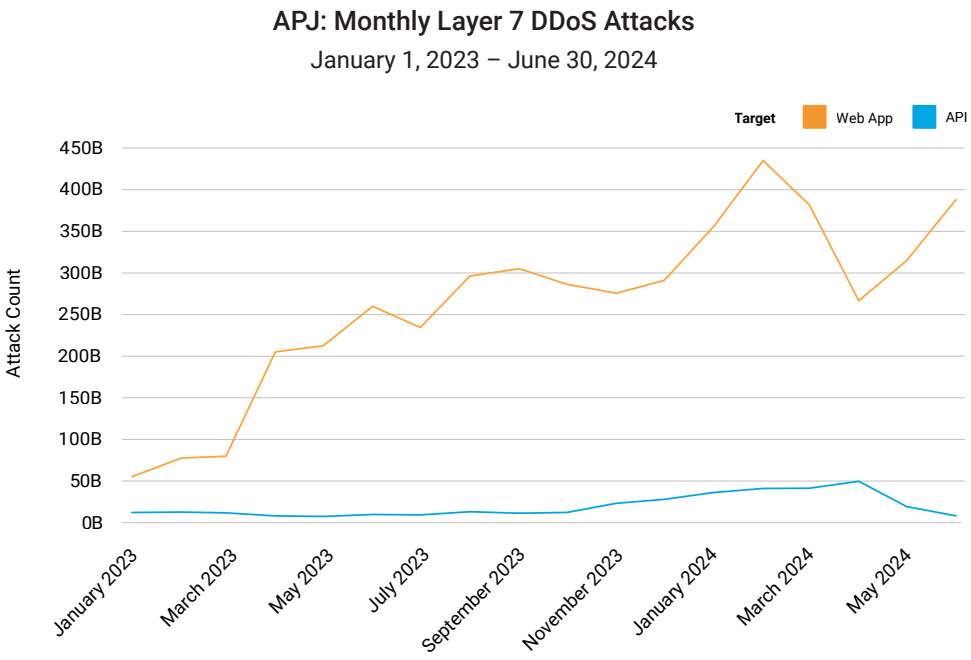
From an industry perspective, the commerce (207) and gaming (158) industries experienced the highest number of DDoS Layers 3 and 4 attack events, followed by financial services (120), video media (91), and high technology (63).

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.

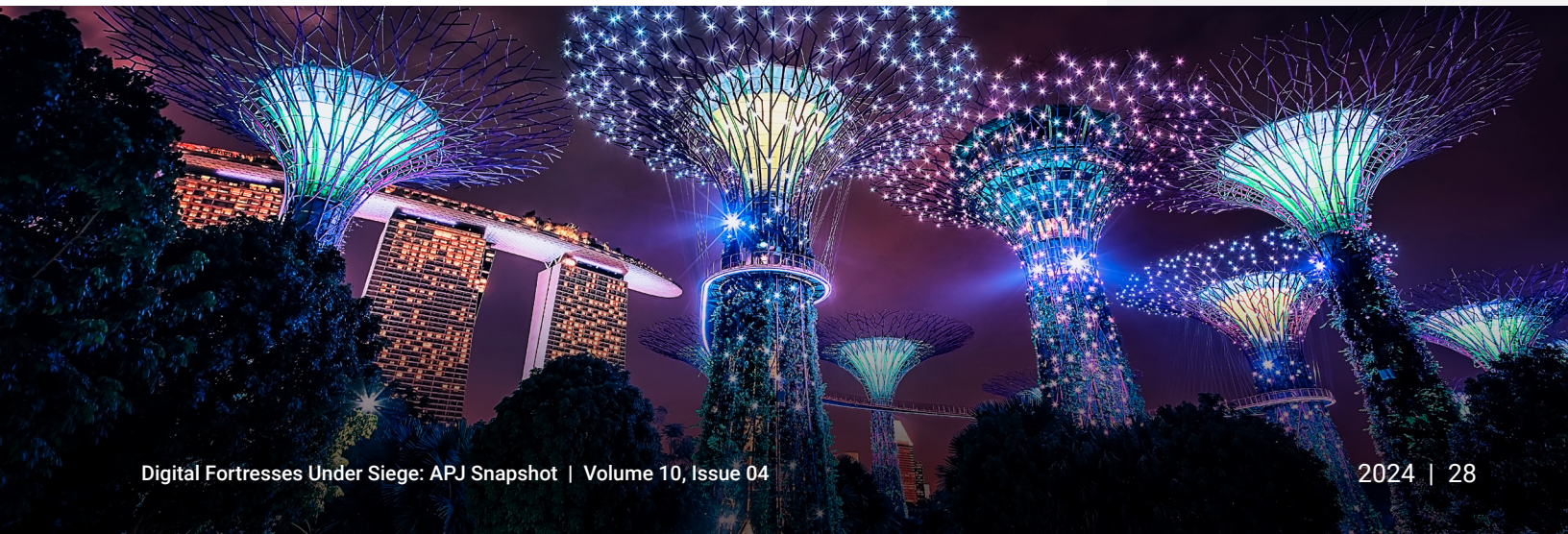
During the 18-month reporting period from January 2023 through June 2024, Akamai researchers found that APJ was second in the number of Layer 7 DDoS attacks, experiencing 5.1 trillion attacks versus 8.7 trillion in North America.

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.

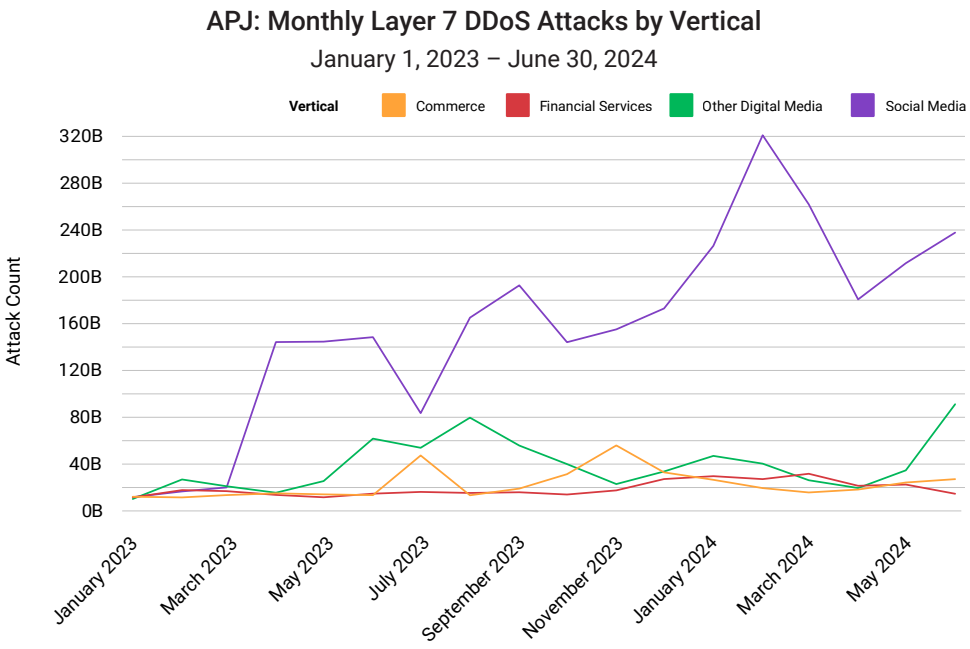


APJ Fig. 5: Layer 7 DDoS attacks grew fivefold from January 2023 through June 2024

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.

Akamai

EMEA Snapshot

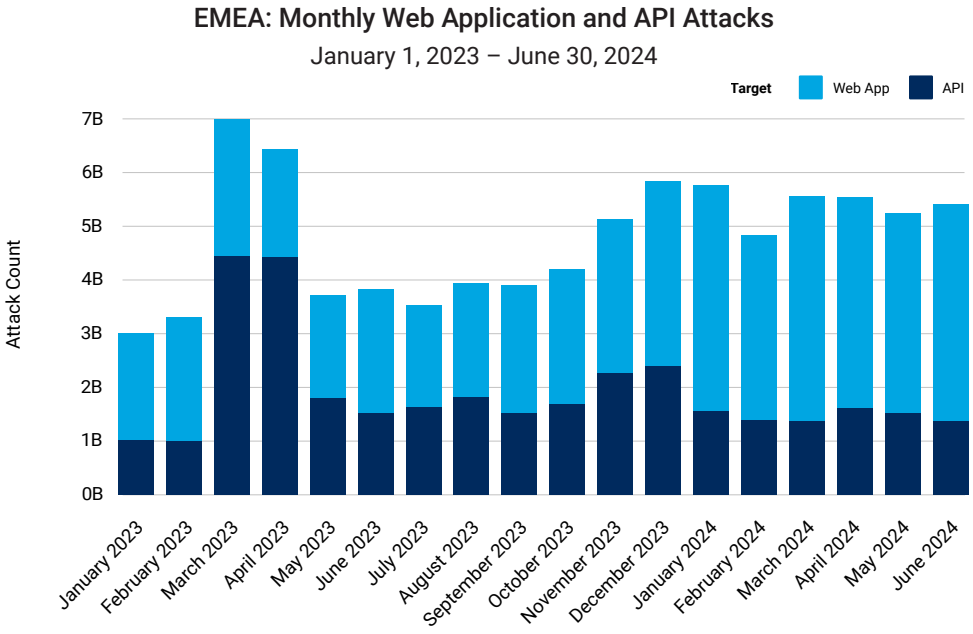
The EMEA Snapshot is a companion piece to our larger secure apps SOTI report, Digital Fortresses Under Siege: Threats to Modern Application Architectures (available in English only). Please refer to that report for detailed descriptions of how adversaries exploit the expanding attack surface, recommendations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

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).

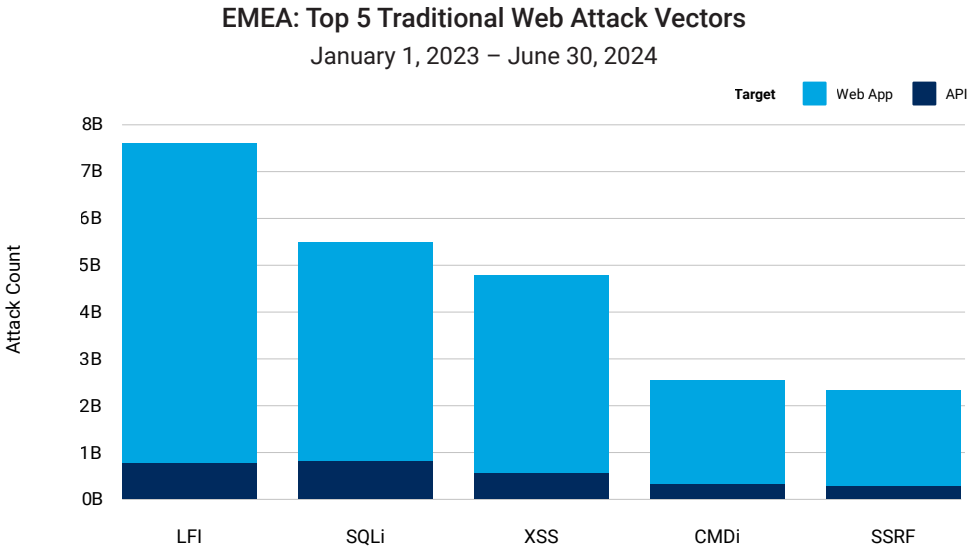


EMEA Fig. 1: Monthly web application and API attacks remain elevated in 2024 (NOTE: The spike in API attacks is related to the commerce sector in Spain, a country with an already huge API attack concentration.)

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.

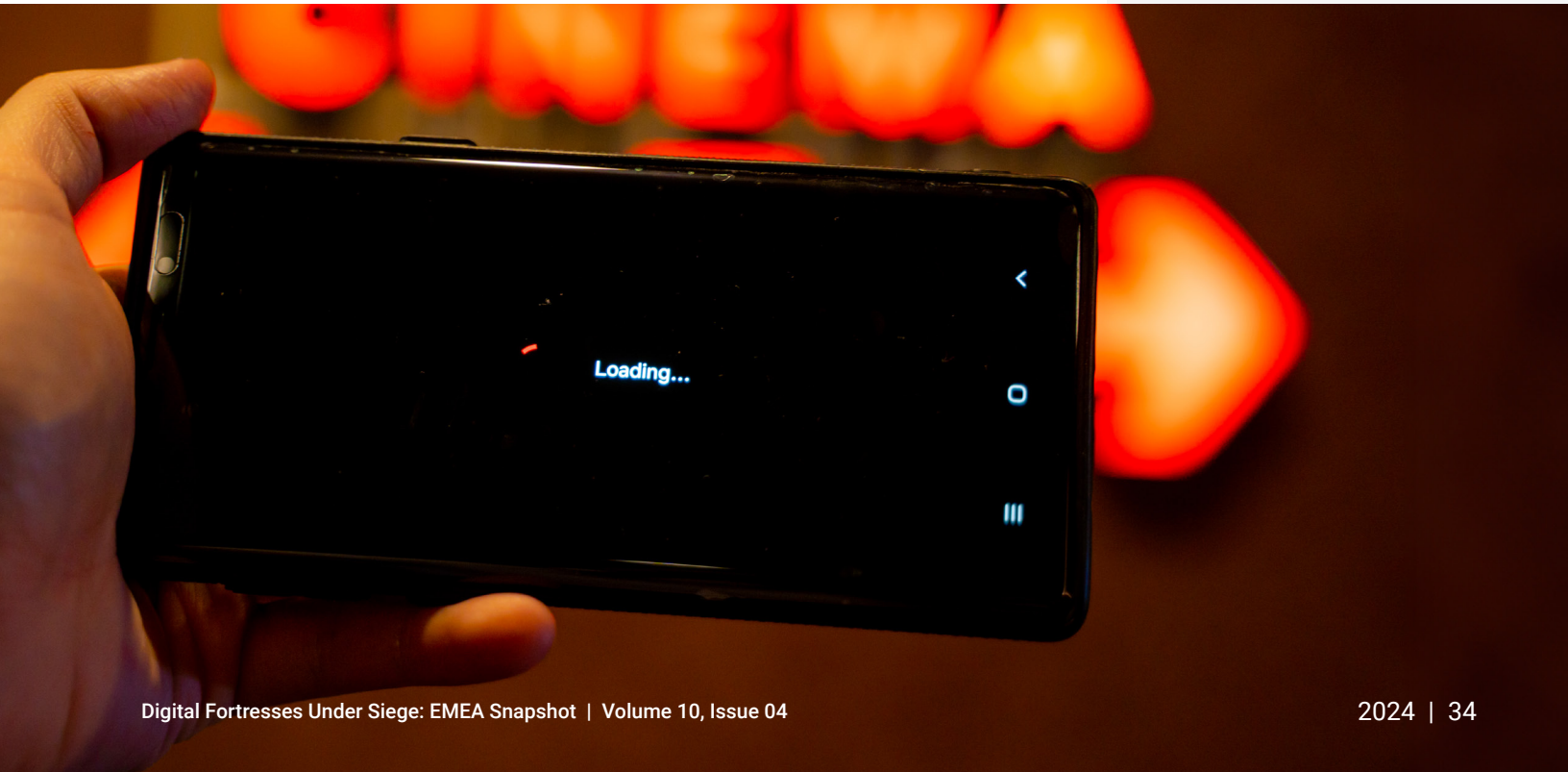
Akamai also tracks several web attack vectors. In this report we're focusing on the top five traditional vector-based attack methods.

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).

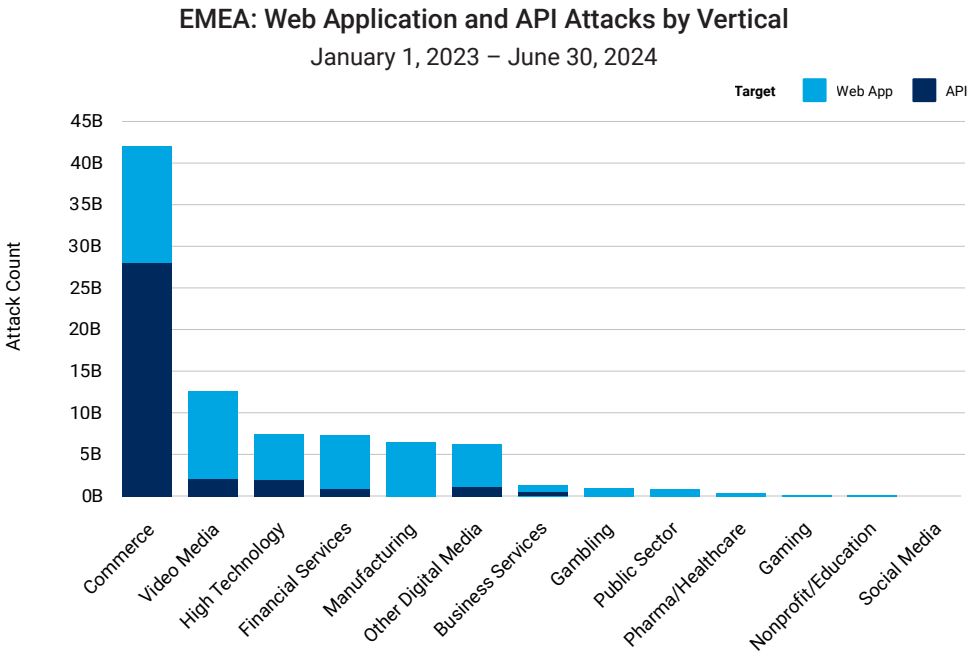


EMEA Fig. 2: LFI, SQLi, and XSS are driving growth in web application and API attacks

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

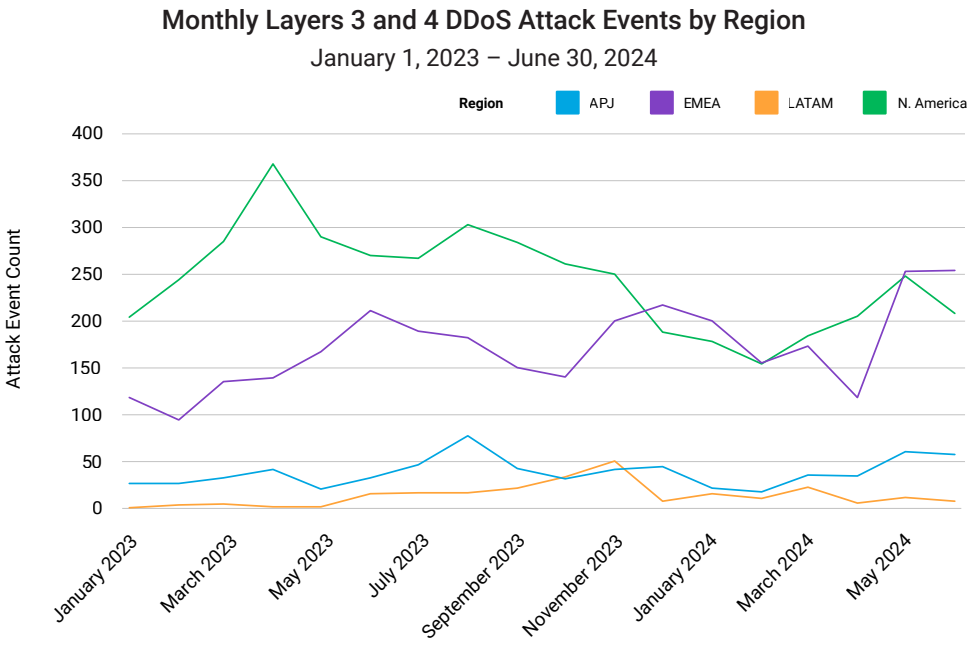
DDoS attacks threaten application uptime

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).

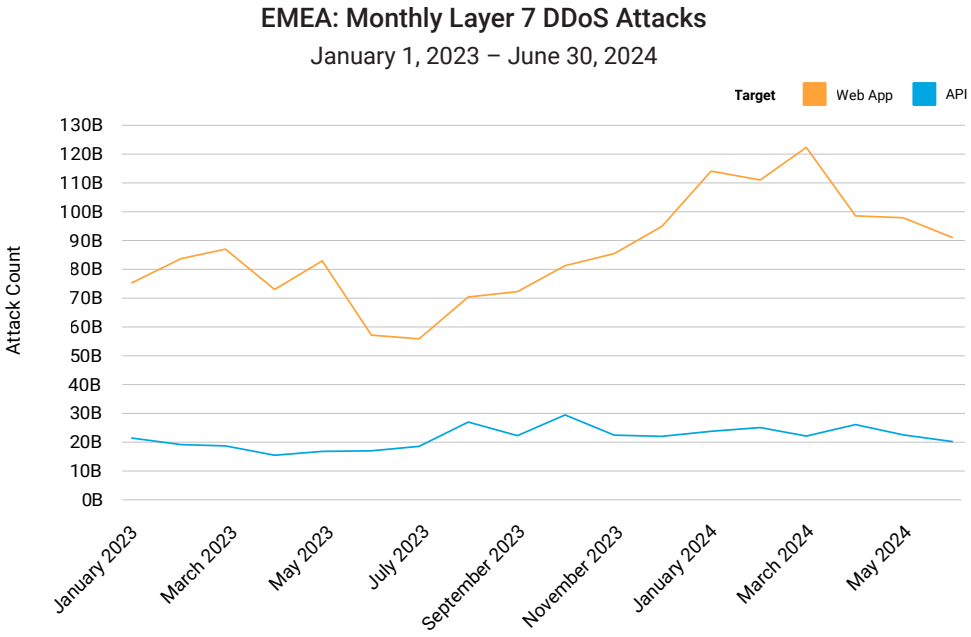
As discussed in our EMEA SOTI, DDoS is a popular tool for politically motivated hacktivists and nation-state–sponsored attackers, and the Russia-Ukraine and Israel-Hamas wars have led to increased attacks.

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).

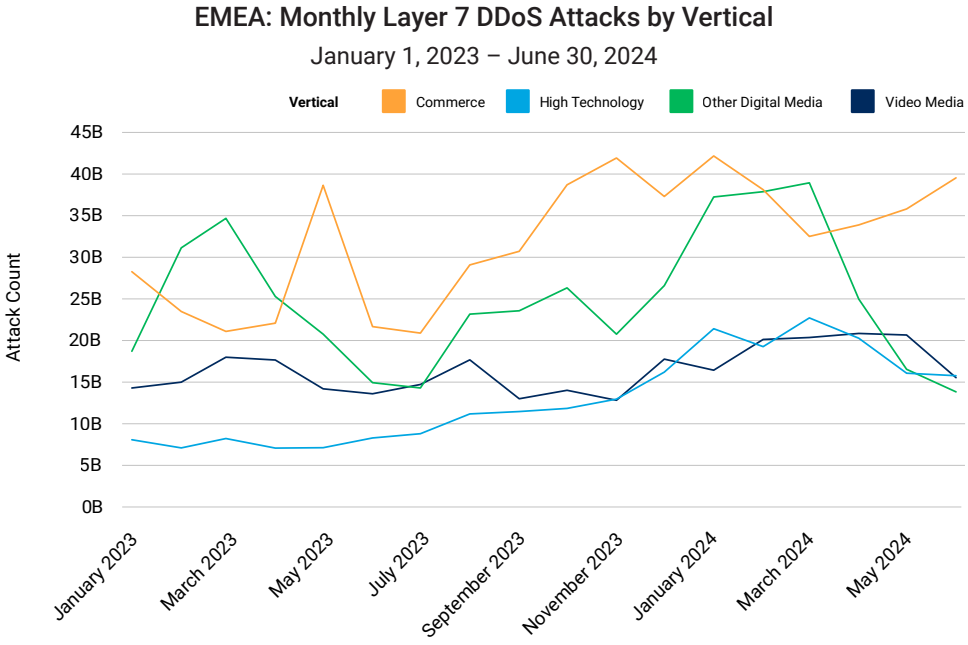


EMEA Fig. 5: Layer 7 DDoS attacks increased significantly since June 2023, ending Q2 2024 at a monthly average of 119 billion attacks

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.

Mitigation: Defending your applications and APIs against attacks

Protecting your application and APIs may seem like a herculean task, with the gargantuan demand for them in most companies, and the many ways applications can be targeted. The crux of the matter is that every web application and API is a potential attack surface or doorway to your organization and your confidential information.

A holistic approach in securing application and APIs is imperative, beginning at the design/build stage and continuing until after production. Vulnerabilities and security gaps stemming from poor coding issues in your applications make them ripe for exploitation. The OWASP has a checklist for implementing good coding practices that developers can reference. Once these applications and APIs are in the wild, protecting your team becomes the responsibility of your security team, and not having an accurate accounting of APIs can leave your team with blind spots. Shadow APIs can lurk in your environment without your knowledge and can be subject to abuse. The scale and magnitude of API use can also impact timely testing for vulnerabilities, but solutions that have API testing capabilities can minimize their risk exposure against potential exploitation.

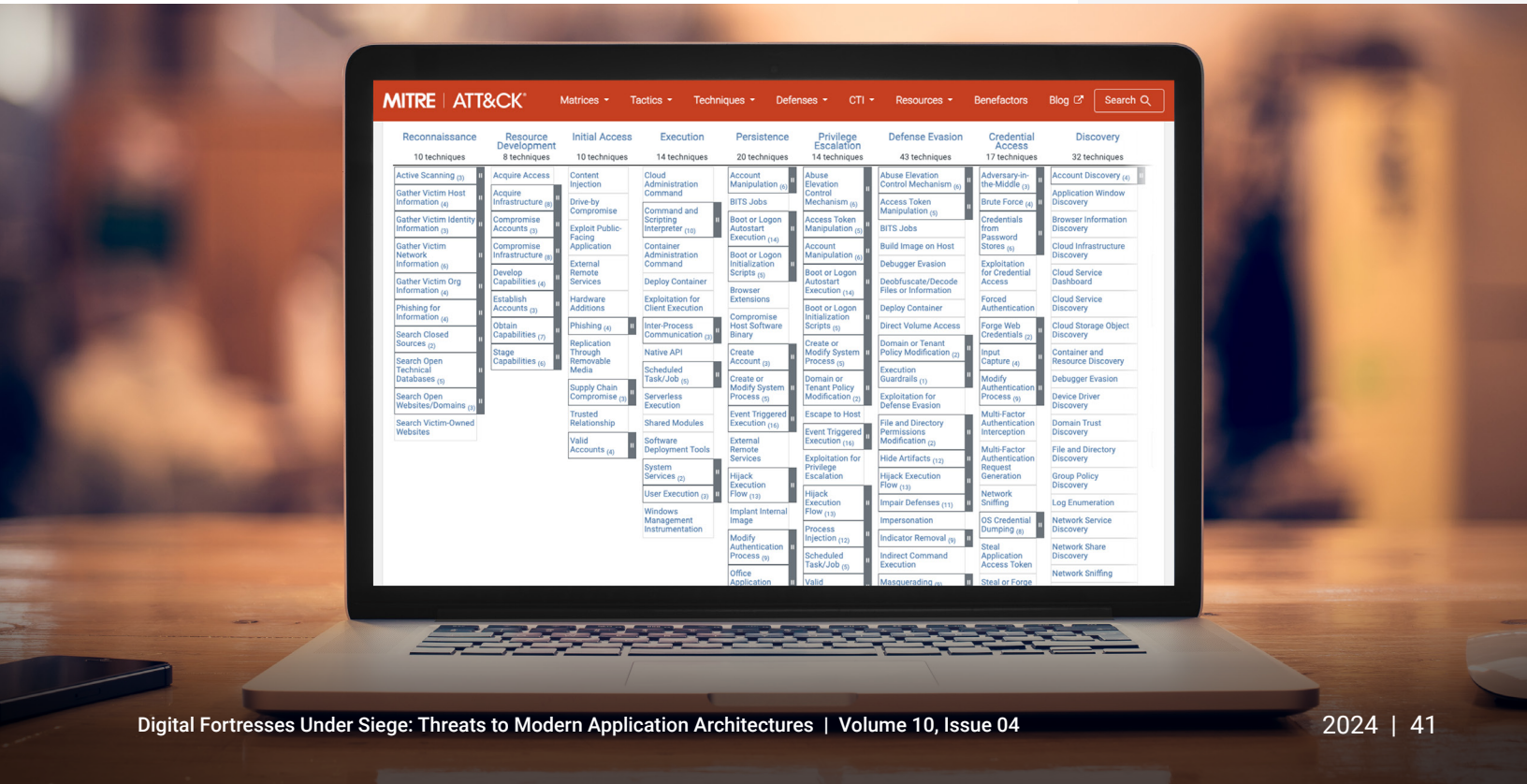
Akamai recently announced our acquisition of Noname Security and, with this addition, we can help you with API visibility and discovery (of legacy and zombie APIs, etc.), including an accurate inventory of the API estate, to give you a better understanding of your attack surface. The truth is: You can't protect what you don't know.

One of the key findings in this report is that attackers continue to be interested in exploiting older CVEs to breach their targets. And while it's a race against time to update vulnerable systems or servers, timely patching may not be readily feasible for some organizations. However, with solutions that include Adaptive Security Engine, exploitation attempts against companies — and their potential impacts — can be minimized by denying malicious traffic.

Additionally, the assaults against the application layer by way of DDoS are growing significantly — we're halfway through 2024 but we've already seen a staggering 5 trillion+ Layer 7 DDoS attacks for the top three targeted industries. The best defense of your digital assets, applications, and infrastructure from DDoS includes a combination of awareness and continuous mitigation. This means staying up-to-date with safeguarding measures, such as patch management, incident response plans, mitigation controls (for DDoS-exposed IP addresses and critical subnets), access control policies, network segmentation, firewalls, and more. There are also other proactive solutions that may be taken, such as configuring rate limiting, caching content on a CDN, and using products specific for DDoS detection, mitigation, and protection. To protect your DNS infrastructure, it's also beneficial to continuously monitor and analyze inbound DNS traffic and use a hybrid platform instead of a traditional DNS firewall.

When it comes to ransomware attacks and other risks to your workloads, implementing a Zero Trust solution can prevent these damaging threats from moving to the deeper parts of your networks by blocking both east-west and north-south traffic. Microsegmentation also aids in safeguarding critical applications as this offers granular visibility on the data flows among your applications, and you can assess whether to trust or allow any access request. Finally, your security team can use the MITRE ATT&CK framework to gain insights to the prevalent tactics and techniques used by attackers, and update their playbooks accordingly.

Image: MITRE ATT&CK®/ ATT&CK Matrix for Enterprise



Conclusion: Putting the puzzle together

In this report, we attempted to provide a 10,000-foot view of the different ways threat actors can target your applications and APIs. Unfortunately, as the astronomical demand for applications and APIs grows, so does the number of your entry points. As more businesses run on applications, safeguarding them from all fronts is more important than ever. This report offered an overview of the critical security considerations for safe digital transformation, while underscoring essential protective measures across three key areas:

1. **Applications and APIs**
2. **Application workloads**
3. **Infrastructure behind apps and APIs**

Successful attacks against your applications and APIs can impact your revenue and reputation, and you can end up facing hefty fines due to compliance or regulatory issues. In the first section of this report, we discussed attacks that affect your customers (or the home users) — they can become victims of fraud when their credentials and other personal information get stolen via web attacks and API abuse. Then, we examined the dangers of DDoS attacks when it comes to business continuity. Finally, we noted that attacks on application workload focus more on how adversaries are targeting your employees (via phishing and ransomware) to gain a foothold to your network.

We hope that this report provided valuable insights and strategies to protect, secure, and defend your application and API universe.

Stay updated on the latest threats by checking out our security research hub.

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.

Akamai

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**.