The Cybersecurity Chef:

Crafting the ultimate cookbook for Layer 7 DDoS resilience

Table of Contents

Introduction

Concocting the right defense against today's distributed denial-of-service (DDoS) attacks can be a challenge for even the most accomplished of security professionals. This is particularly true for Layer 7 DDoS attacks, which carry additional complications. One thing that can come in handy is a step-by-step set of instructions with different approaches to the different threats, or in other words, a Layer 7 DDoS cookbook.

Different adversaries will prepare DDoS attacks differently. Attacks at Layers 3 and 4 are more a function of strength. Who has better network capacity, the attacker or the defense? Layer 7 attacks, on the other hand, target the application layer of the Open Systems Interconnection (OSI) model, which is responsible for interacting directly with software applications. They aim to overwhelm a web server, database, or application by exploiting capacity, memory allocations, or weaknesses in the way these systems handle requests.

Layer 7 DDoS attacks therefore have specific challenges when it comes to mitigation, since such requests often appear as legitimate traffic, making it difficult to filter out malicious requests without impacting legitimate users. What's more, the availability of automation and cloud resources has made it easier than ever for attackers to launch these attacks quickly and at scale.

In this paper, we address the challenges of mitigating Layer 7 DDoS attacks with detailed recipes that include the tools and techniques that attackers use, detection and mitigation tactics to counter them, and post-event analysis and recovery suggestions.

Thanks to Akamai's history in content delivery, cybersecurity, and a distributed cloud platform with more than 4,200 points of presence around the globe, we have a unique perspective on today's DDoS attacks. As application-layer DDoS attacks continue to become more complex and multifaceted, it's important to have that perspective and a thorough strategy toward defense. We bring that here.

Whether you're a frontline security professional looking for help with a specific threat or vulnerability, or a CISO seeking to improve your security posture, this cookbook provides the recipe for success.

Common targets and examples of Layer 7 DDoS attacks

Layer 7 DDoS attacks target the top layer of the OSI model, the application layer. These attacks aim to overwhelm a target’s resources by exploiting the way web applications process requests. Common targets of Layer 7 DDoS attacks include:

Web servers: Attackers target web servers to disrupt the delivery of content to legitimate users. This can cause websites to load slowly or become completely inaccessible.

Web applications: Applications that rely on databases or back-end services are vulnerable to Layer 7 DDoS attacks, as the assault can exploit weaknesses in how applications parse queries, process requests, or manage sessions.

Application programming interfaces (APIs): APIs are a critical component of modern web services and mobile applications. Attackers target APIs to disrupt the interaction between different software services, affecting the functionality of applications that rely on those APIs.

DNS services: Although DNS attacks can also occur at other layers, Layer 7 attacks can involve bombarding the DNS service with malicious requests to disrupt the resolution of domain names, leading to widespread accessibility issues. Increasing adoption of DNS over HTTP/TLS could result in an increase in such attacks.

Email servers: Targeting email servers can disrupt communications, affecting both inbound and outbound emails.

Payment gateways and financial services: These are lucrative targets for attackers looking to disrupt transactions and sow chaos in financial operations.

Akamai’s State of the Internet (SOTI) reports and security insights routinely examine the evolving landscape of Layer 7 DDoS attacks, highlighting the diversity of attack vectors and the industries most at risk.

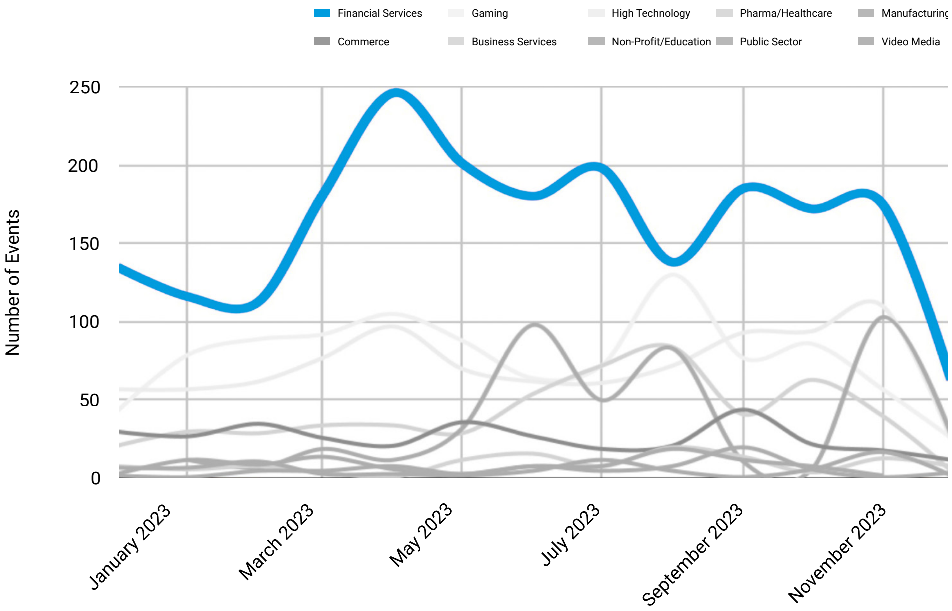
Attack vectors

- Web application and API attacks: Adversaries usually target website entry points, including API endpoints that usually aren't cached due to their content or configuration. Some of the commonly seen targeted paths include "/", "/home", "/en-us", "/pricing/", etc.
- It's common to see attack vectors such as:
  • HTTP GET / POST flood on home pages
  • HTTPS GET flood on a randomized paths and query strings
  • Slow read attacks
  • Large file upload floods

Additionally, the number of companies that face a DDoS attack has historically increased year over year, but now the "how" is different. First, the type and volume of properties being attacked has changed. For example, instead of 10 attacks against the same or similar endpoints, 100 attacks might take aim at different IPs in the network space. Those attacks do not just target Layer 3, but also Layer 7 at the same time.

Industries targeted

The number of distributed denial-of-service (DDoS) attack events against the financial services, gambling, and manufacturing sectors saw an uptick in 2023, particularly in EMEA, where these exceeded the numbers in all other regions combined.

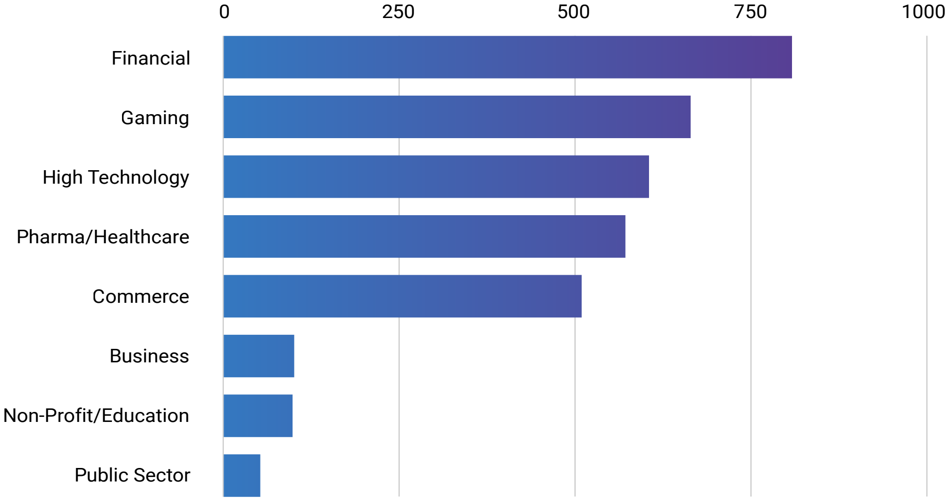


DDoS: Here to Stay, March 2024

Financial services in particular have become a growing target for Layer 7 DDoS attacks. Since 2021, Akamai has seen a distinct and noticeable surge in the number of DDoS attacks against financial services firms. Over a third (35%) of the attacks on all industries were on financial services institutions in 2023, making the sector a more enticing target than gaming. Akamai's analysis shows that banking was the target of 63% of DDoS attacks globally. Almost three-quarters (72%) of attacks in EMEA and 91% in APAC were focused on banking. In the Americas, however, DDoS attacks were spread more evenly across banking, insurance, and other financial services institutions.

Americas: Financial services represents 28% of DDoS attacks

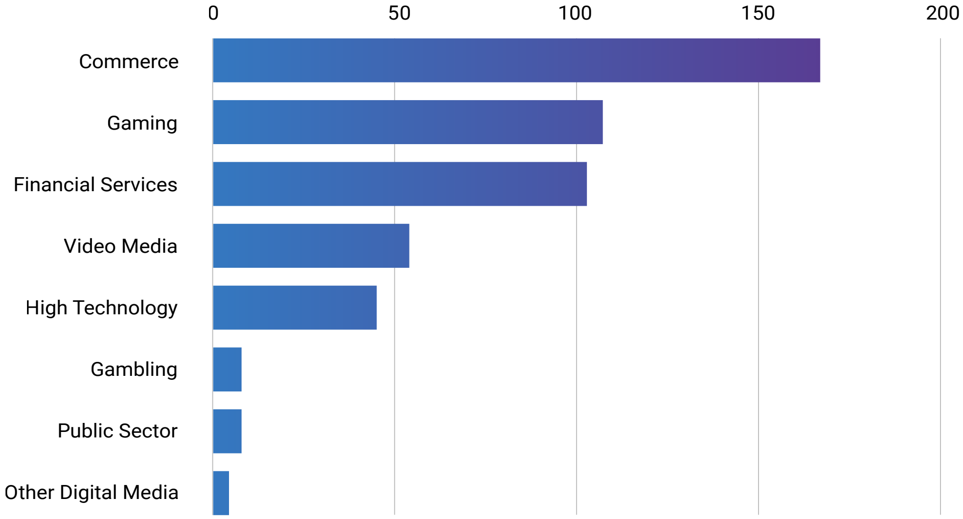
June 2023 – December 2023



DDoS: Here to Stay, March 2024

APAC: Financial services represents 11% of DDoS attacks

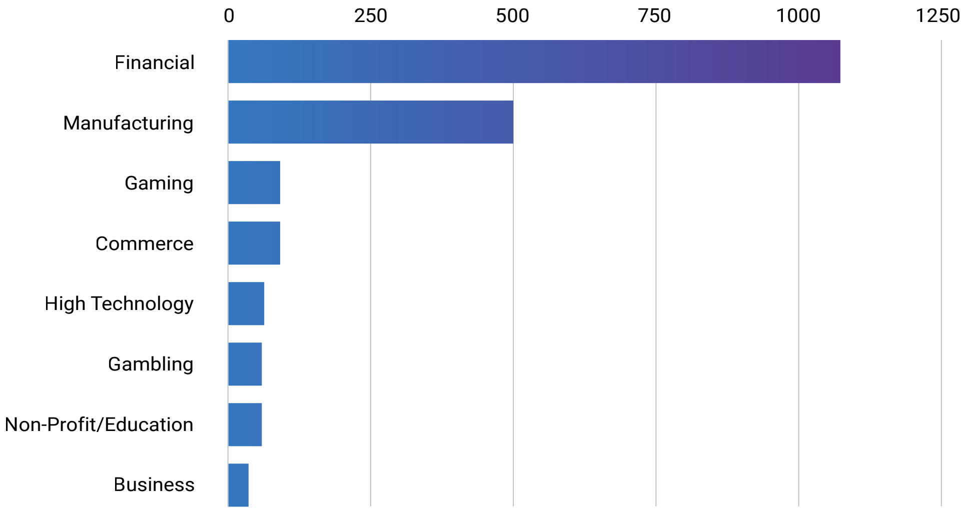
June 2023 – December 2023



DDoS: Here to Stay, March 2024

EMEA: Financial services represents 66% of DDoS attacks

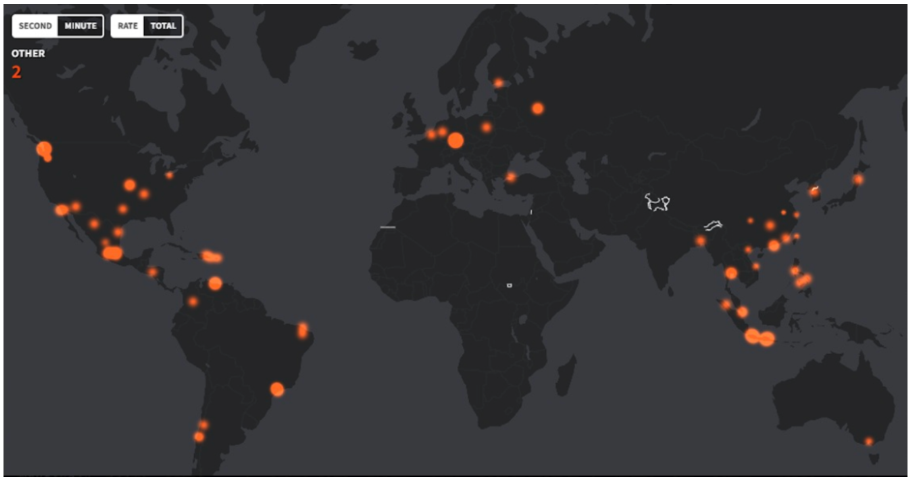
June 2023 – December 2023



DDoS: Here to Stay, March 2024

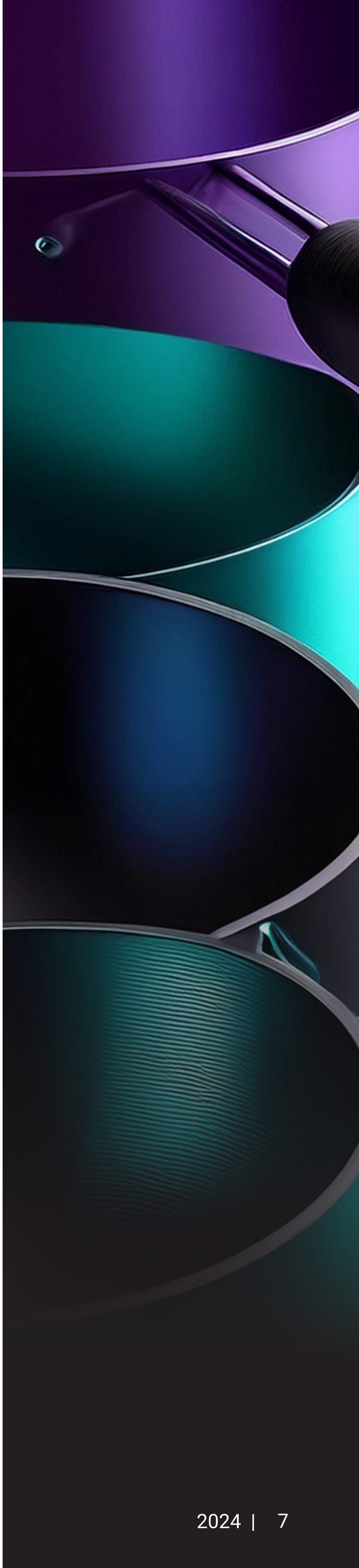
In one such recent example of a sophisticated Layer 7 DDoS attack targeting one of Akamai's financial services customers, cyber adversaries utilized automation and created a highly distributed attack. This attack used HTTP GET flood targeting mostly non-cacheable URLs (like home page and login endpoints). Utilizing various proactive controls, this attack was successfully mitigated without any impact to the customer origin. This attack source heat map underscores the growing use of cloud service providers, Tor exit nodes, and anonymous or open proxy nodes:

DDoS attacks by autonomous system



Visualization of an application-layer attack on a financial institution that took place in Q1 2024 across more than 100 countries, which Akamai helped to mitigate

DDoS attackers have the ability to construct and coordinate a broadly dispersed attack infrastructure, leveraging dynamic IP addresses throughout extensive networks, spanning numerous countries and regions worldwide.



Tools and techniques used by attackers

Unfortunately, DDoS attackers and their methods do not remain stagnant. As attackers continue to find ways to monetize their acts, they adapt their techniques, take advantage of new tools, and find new methods. There are a number of factors that demonstrate this evolution.

Automation: Attackers are using automated scripts and bots to mimic legitimate user behavior, making detection significantly more challenging. Additionally, attackers are now turning to machine learning algorithms that adapt and evade traditional detection.

Multi-vector attacks: Adversaries are increasingly employing multi-vector strategies, combining different attack types (such as GET and POST flood) and DNS targets (such as amplification and fragment attacks) with other combinations to overwhelm both network and application resources.

API targeting: As businesses increasingly rely on APIs to power their applications, attackers are finding new opportunities by exploiting API vulnerabilities in their DDoS attacks. These attacks aim to exhaust server resources by requesting thousands of connections simultaneously, or to exploit logic flaws, causing disruptions in service.

IoT device exploitation: The proliferation of poorly secured IoT devices provides a vast army for botnets. These devices are often hijacked and used to launch massive DDoS attacks, exploiting their network connectivity and computational power.

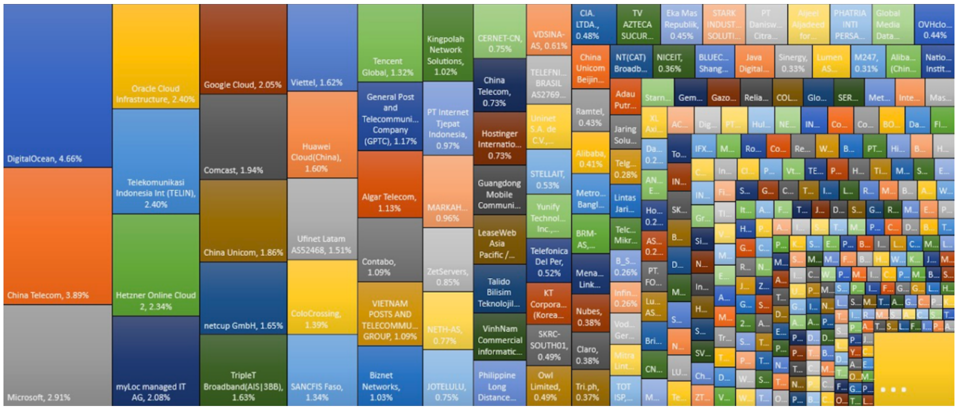
Rise in sophistication

With these new tools and techniques, there's been a corresponding rise in the complexity and frequency of DDoS attacks, with attackers using sophisticated methods to bypass traditional defenses. Some of the noticeable trends include:

Encryption: A notable shift toward HTTPS-based DDoS attacks has made mitigation more challenging. These attacks, which are encrypted, masquerade as legitimate traffic, making them harder to detect and filter out, as traditional DDoS protection measures have limitations in decrypting application-layer SSL/TLS traffic.

Botnets and proxies: Given the significant growth of DDoS botnets and the prevalence of anonymous proxies by attackers, requests are now being sent from a multitude of IP addresses (typically more than 10,000 IPs per attack). Attackers use this strategy to bypass mitigation measures that count requests from a single IP. The prevalence of cloud hosting platforms and the adoption of cloud-based services is only making it easier to craft these high-intensity and highly distributed attacks.

DDoS Attacks by Autonomous System



Visualization of a recent application-layer DDoS attack — 650,000 transactions per second (TPS), 20 Gbps, 9 billion+ total requests — against an Akamai financial customer

DDoS attackers are able to create and coordinate extremely distributed attack infrastructure, mostly from cloud providers.

One evolving approach defenders are employing is tracking requests per TLS fingerprint, which is composed of multiple TLS layer signals, like cipher types and their order. While this approach is susceptible to false positives, if used correctly it can provide more effective mitigation when an attacker is operating from various machines and IPs because the same software is installed on the compromised devices. These devices exhibit similar environmental characteristics, one of which is the shared TLS library.

Ingredient sourcing

While the available tools on the market change frequently, the evolution of attack techniques suggests a move toward more sophisticated and less detectable methods. These include:

- **Compromised IoT devices:** Attackers continue to use compromised IoT devices in botnets as a method for launching large-scale DDoS attacks, highlighting the continued vulnerability of these devices.
- **DDoS-for-hire services:** The availability of DDoS-for-hire services has lowered the entry barrier for launching attacks, enabling individuals without extensive technical knowledge to conduct attacks at significant scale.

- **Evasion techniques:** Advanced evasion techniques, such as randomized header parameters and dynamic request arguments, have become more common. These techniques challenge traditional detection and mitigation approaches by making the malicious traffic harder to distinguish from legitimate requests.

Vulnerabilities typically exploited in such attacks

The vulnerabilities that attackers exploit in Layer 7 DDoS attacks are often related to the ways that web applications process user inputs and manage data. To mitigate these vulnerabilities, it's crucial to employ a combination of security measures.

In recent years, one of the most significant vulnerabilities attackers exploited when carrying out application-layer DDoS attacks was the HTTP/2 Rapid Reset flaw, which was widely published during late 2023. Such attacks exploited a flaw in the HTTP/2 protocol, which is fundamental to the operation of the internet and all websites. The exploitation of this vulnerability led to a 65% overall increase in HTTP DDoS attack traffic in one quarter compared to the previous one, highlighting the severity and impact of the attacks utilizing this vulnerability.

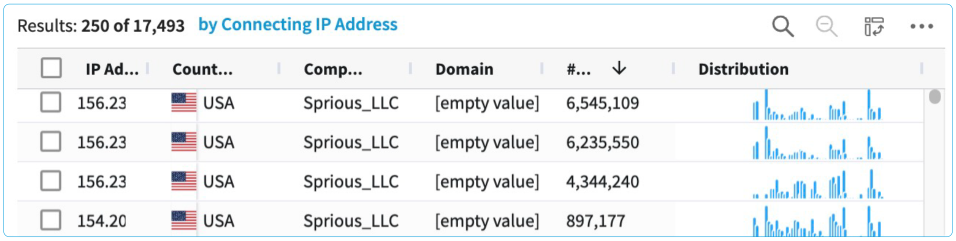
This particular vulnerability allowed attackers to generate a higher impact by leveraging cloud computing platforms and exploiting HTTP/2, enabling hyper-volumetric DDoS attacks with relatively small botnets. The industries most targeted by these attacks included gaming, IT, cryptocurrency, computer software, and telecom, with the U.S., China, Brazil, Germany, and Indonesia being the largest sources of these attacks.

In response, an industry-wide coordinated effort disclosed the HTTP/2 Rapid Reset vulnerability (CVE-2023-44487) to shed light on DDoS attacks using this flaw. It targeted various providers, including leading cloud and CDN services providers, among others.

Real-life examples: Using automation in a DDoS attack

Attackers often use multiple DDoS tools for carrying out the same DDoS attacks, with each leveraging several techniques in combination with one another to bypass security products or at least make them less efficient. One such example of an attack is outlined below using Akamai Web Security Analytics.

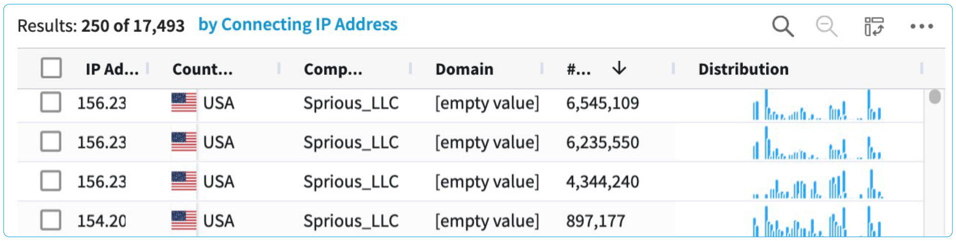
- Attack seen from more than 17,000 IP addresses



Results: **250 of 17,493** by Connecting IP Address

☐	IP Ad...	Count...	Comp...	Domain	#... ↓	Distribution
☐	156.23	USA	Sprious_LLC	[empty value]	6,545,109	
☐	156.23	USA	Sprious_LLC	[empty value]	6,235,550	
☐	156.23	USA	Sprious_LLC	[empty value]	4,344,240	
☐	154.20	USA	Sprious_LLC	[empty value]	897,177	

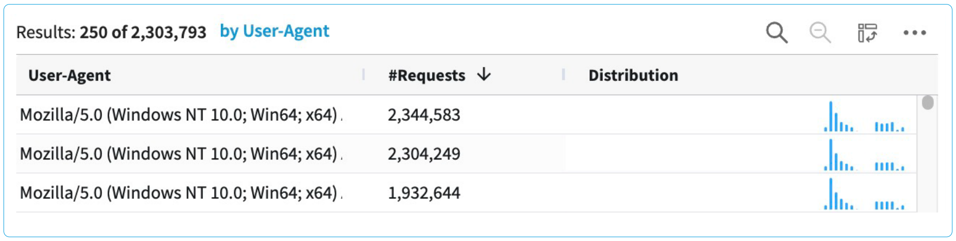
- Attack sources from more than 400 networks



Results: **250 of 17,493** by Connecting IP Address

☐	IP Ad...	Count...	Comp...	Domain	#... ↓	Distribution
☐	156.23	USA	Sprious_LLC	[empty value]	6,545,109	
☐	156.23	USA	Sprious_LLC	[empty value]	6,235,550	
☐	156.23	USA	Sprious_LLC	[empty value]	4,344,240	
☐	154.20	USA	Sprious_LLC	[empty value]	897,177	

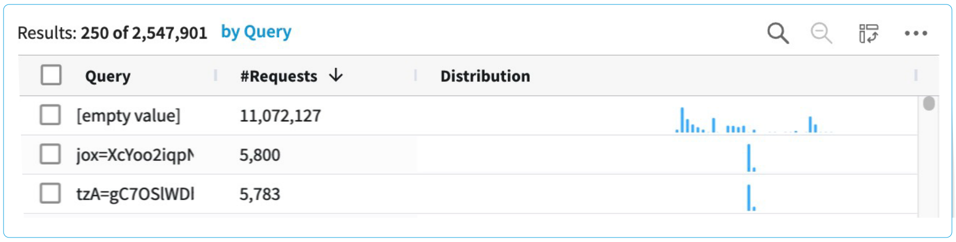
- 2,303,793 unique user agents



Results: **250 of 2,303,793** by User-Agent

User-Agent	#Requests ↓	Distribution
Mozilla/5.0 (Windows NT 10.0; Win64; x64) .	2,344,583	
Mozilla/5.0 (Windows NT 10.0; Win64; x64) .	2,304,249	
Mozilla/5.0 (Windows NT 10.0; Win64; x64) .	1,932,644	

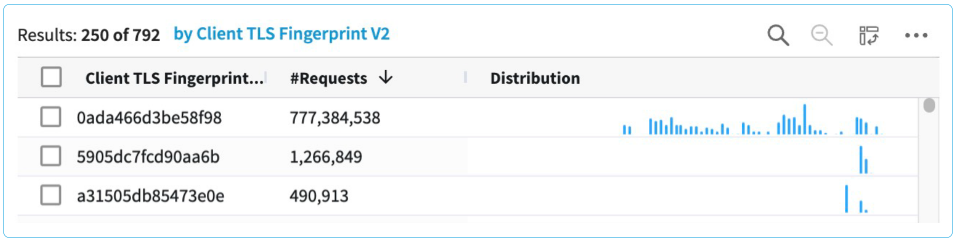
- 2,547,901 unique and random query strings



Results: **250 of 2,547,901** by Query

☐	Query	#Requests ↓	Distribution
☐	[empty value]	11,072,127	
☐	jox=XcYoo2iqpN	5,800	
☐	tzA=gC7OSlWDI	5,783	

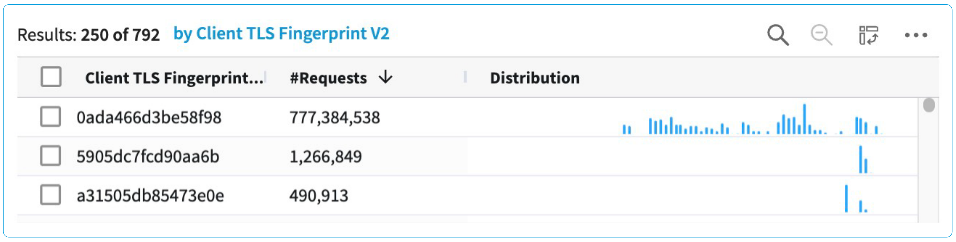
- HTTP header rotation (e.g., Accept-Language, Referer)



Results: 250 of 792 by Client TLS Fingerprint V2

□	Client TLS Fingerprint...	#Requests ↓	Distribution
□	0ada466d3be58f98	777,384,538	
□	5905dc7fcd90aa6b	1,266,849	
□	a31505db85473e0e	490,913	

- TLS setting rotation



Results: 250 of 792 by Client TLS Fingerprint V2

□	Client TLS Fingerprint...	#Requests ↓	Distribution
□	0ada466d3be58f98	777,384,538	
□	5905dc7fcd90aa6b	1,266,849	
□	a31505db85473e0e	490,913	

Mitigating such sophisticated attacks requires a layered protection strategy. Using both proactive and reactive controls, such as an advanced combination of request matches and source traffic characteristics in rate limiting, or source reputation controls, can be helpful.

Adversaries level up: TLS signal impersonation

Recent observations have shown malicious actors more frequently using TLS signals in their DDoS tools to evade detections by making such connections look like they are coming from legitimate Chrome browsers. Instead of using a resource-intensive headless version of Chrome, which might slow down the attack, the attackers might have employed a modified version of the TLS library, allowing them to set and impersonate the TLS signals of any genuine browser. While there are tools designed to replicate TLS fingerprinting, they are not commonly found in DDoS attack tools. The use of this type of attack suggests growth in the attackers' technical prowess and a deep knowledge of the defenses — that's why Layer 7 DDoS attack defense strategies must include regular research into the latest attack trends. This also seems to suggest that the DDoS tools that include TLS spoofing are becoming more common.

Look around: Assessing risk and identifying vulnerabilities

You can significantly enhance your Layer 7 DDoS mitigation strategy by identifying your critical assets and determining where they might be vulnerable to a DDoS attack. This risk assessment helps prioritize which resources to protect based on their importance and vulnerability. By understanding potential attack vectors and their impact, organizations can implement specific countermeasures, such as rate limiting, web application firewalls, and behavior analysis, to efficiently mitigate risks. Additionally, a continuous risk assessment enables a defense strategy that evolves in response to new threats and changing business requirements.

Different industries and businesses may take a different approach to application-layer DDoS risk assessments. For example:

> **Ecommerce:** Ahead of a major sale event, a risk assessment might identify the checkout process as a critical vulnerability. Mitigation measures might include implementing a web application firewall (WAF) and rate limiting to protect the service.
>
> **Financial services:** For a banking application, risk assessment may determine the login page is a prime target for DDoS attacks. The bank could then employ a combination of endpoint-tailored rate limiting and behavioral detection to distinguish between legitimate users and attack traffic.

Understanding specific vulnerabilities enables targeted defenses and augments critical services during an attack.

Avoiding too many cooks: Roles and responsibilities

Establishing clear roles and responsibilities are crucial steps for an effective Layer 7 DDoS strategy because it maximizes the opportunity for a coordinated and efficient response in the event of an attack. Without clear roles, response efforts can become chaotic, with overlapping duties and gaps in defense. Defined responsibilities assist with identifying each team member’s specific tasks, from monitoring traffic and identifying anomalies to implementing mitigation strategies and communicating with stakeholders. This coordination helps to minimize the impact of attacks, maintain service availability, and protect critical assets.

Indeed, having too many decision-makers without clear roles can lead to delayed responses during a DDoS attack. For instance, if both the network operations and cybersecurity teams independently decide on different mitigation approaches without coordination, they might inadvertently neutralize each other's efforts or overlook critical vulnerabilities. The right strategy involves predefined roles, such as a designated incident response leader, communication coordinator, and technical response team, ensuring swift, unified actions against attacks, minimizing downtime and streamlining post-incident analysis.

Choosing the right tools for your kitchen

Detecting and mitigating an application-layer attack can be challenging, because it is so difficult to distinguish between legitimate and malicious traffic. In response to these evolving threats, we recommend a multifaceted approach to defense:

- **Focus on always-on vs. on-demand:** Make sure DDoS security controls are always active and update incident response plans to swiftly address emerging threats.
- **Establish a resilient and reliable architecture:** Anticipate a single point of failure, as attackers will likely target multiple services — including DNS, web applications, APIs, and data center and network infrastructure. Using the right architecture will be crucial in protecting against Layer 7 DDoS attacks. These architecture considerations may include choosing edge or CDN-based DDoS protection, which is always on. Don't overestimate your reliability. The scale of today's DDoS attacks can easily overwhelm most infrastructure.
- **Assess your provider's SLAs** and align them with your strategy.
- **Review your provider's readiness:** Choose a provider that regularly demonstrates a review of its critical network components and evaluates different DDoS protection mechanisms to gain insight into their effectiveness against current attack methods.
- **Review your DDoS attack response playbook:** Pull together your IT, operations, security, and customer communication staff to enhance your preparedness in the event of an attack.
- **Emergency DDoS protection:** Have a plan ready to onboard a DDoS mitigation solution provider in case of a crisis. If you have a vendor partner in DDoS protection, call their DDoS support hotline.

Recipes for detection and mitigation

Effective DDoS protection at Layer 7 requires multiple detection and mitigation strategies. There are several methodologies to apply, each of which have their strengths and key considerations.

Behavioral and anomaly-based detection

Strengths: This approach relies on using machine learning and statistical analysis to understand your normal traffic patterns and then identify deviations that might indicate a DDoS attack. It is highly effective against complex, previously unseen attacks.

Considerations: Effective detection requires a learning period that may take up to several weeks to establish a baseline of “normal” traffic, during which detection may not be as effective. The model may return false positives if it isn’t accurately trained.

Rate- and throughput-based detection

Strengths: Simple to implement, this method monitors the rate and volume of requests, triggering alerts or mitigation processes when traffic exceeds predefined thresholds. It’s effective for quickly identifying large-scale volumetric attacks.

Considerations: Legitimate traffic spikes, such as those during promotional events, can be mistaken for DDoS attacks. It may not detect low-volume, slow-rate attacks that stay under the radar.

Signature-based detection

Strengths: By comparing traffic against a database of known attack patterns, this method can quickly identify and block recognized threats. It’s highly effective against common and previously identified attack vectors.

Considerations: It cannot detect new or modified attacks that do not match existing signatures. Regular updates are necessary to maintain effectiveness.

Challenge-response tests

Strengths: This approach issues challenges to incoming traffic if it is generated by humans or bots. CAPTCHA or JavaScript computations can effectively mitigate bots and automated attack tools.

Considerations: The challenges may disrupt the user experience if they're implemented aggressively. More sophisticated bots may be able to pass some challenge-response tests, requiring regular updates to your challenge mechanisms.

Hybrid approaches

Combining multiple detection and mitigation strategies can offer more comprehensive protection. For instance, using anomaly-based detection to flag potential attacks, supplemented by rate-based and signature-based methods for broader coverage, allows for more robust defense mechanisms. Challenge-response tests can further filter out sophisticated bots from legitimate users.

Conventional methods

IP and geographic filtering: Blocking or limiting traffic from certain IP/CIDR ranges and geographic regions not relevant to your business can reduce your exposure to attacks originating from those areas. While this method can be useful where the origin of business users is known and limited, it can often pose challenges in ongoing maintenance and updating the list of accepted sources. Also, experienced hackers can make use of proxies to bypass geoblocking. Nevertheless, this still remains a popular choice and initial defense strategy against Layer 7 DDoS attacks.

Application layer protocol analysis: This method can mitigate Layer 7 DDoS attacks by scrutinizing the data within application-layer protocols to detect anomalies or malicious patterns, enabling proactive defense mechanisms. This method can prevent sophisticated DDoS attacks that bypass conventional security measures but can adversely have high resource consumption for deep packet inspection and higher chances of false positives, which could inadvertently block legitimate traffic.

Finding the right and balanced recipe for a multilayered DDoS defense strategy

Crafting a multilayered DDoS defense strategy involves a nuanced approach, tailored to an organization's specific risk profile and the evolving landscape of cyberthreats. At its core, this strategy requires an initial assessment to identify critical assets and likely attack vectors, followed by the implementation of baseline protections such as rate limiting and firewalls. Advanced steps require a mix of anomaly-based detection for new threats, signature-based detection for known attacks, and challenge-response mechanisms to filter bots.

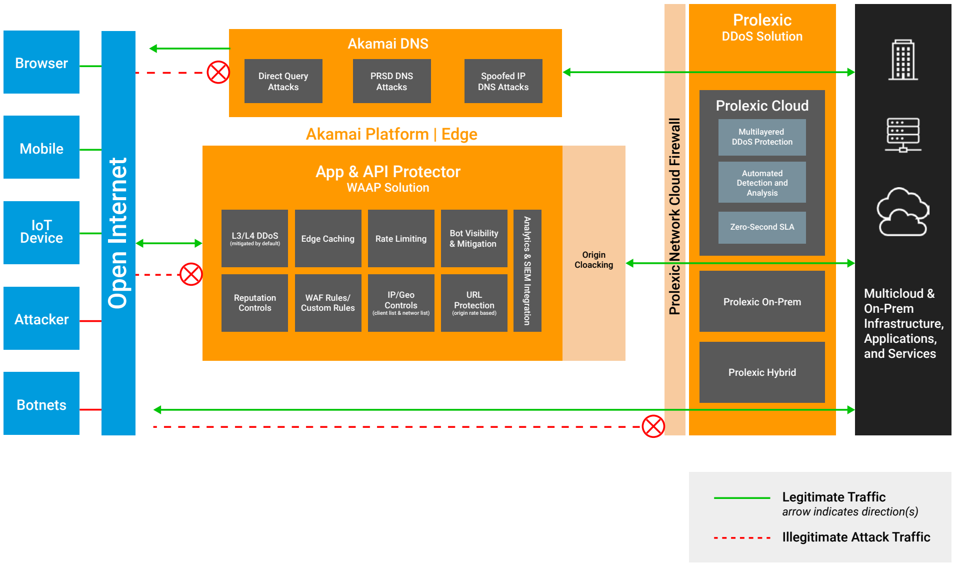
Incorporating adaptive threat intelligence such as algorithms that determine TLS fingerprint patterns of known and emerging DDoS attack sources, the security system can automatically adapt its mitigation to block or challenge traffic exhibiting that fingerprint, effectively mitigating the attack. A comprehensive incident response and recovery plan is crucial for minimizing damage and maintaining trust during and after an attack. Continuous learning and adjustments based on past attacks and emerging trends keep the defense strategy effective and resilient.

A financial institution facing sophisticated, multi-vector DDoS attacks offers a clear example of the importance of having a balanced, multilayered defense strategy. The impact that downtime can have on their operations and customer trust make these institutions prime targets.

By integrating a combination of detection and mitigation methods such as traffic anomaly detection, using conventional methods such as rate limiting, IP/geo filtering, IP reputation, and real-time threat intelligence, along with a robust incident response plan, they can protect their critical assets against disruptions while ensuring the continuity of service to their customers. This comprehensive approach exemplifies how organizations can defend against the multifaceted nature of DDoS attacks in today’s digital landscape.

Prepare: Defense-in-depth strategy with Akamai edge architecture

Akamai's approach to application-layer DDoS protection is multilayered, comprehensive, and adaptive — designed to safeguard websites, applications, and APIs against the most sophisticated attacks. Our App & API Protector leverages several key capabilities that provide comprehensive protection, combining a web application firewall, bot visibility and mitigation, API security, and Layer 7 DDoS protections into a single product to offer broad protection.


Browser
Mobile
IoT Device
Attacker
Botnets
Open Internet
Akamai DNS
Direct Query Attacks
PRSD DNS Attacks
Spoofed IP DNS Attacks
Akamai Platform | Edge
App & API Protector
WAAP Solution
L3/L4 DDoS (mitigated by default)
Edge Caching
Rate Limiting
Bot Visibility & Mitigation
Reputation Controls
WAF Rules/ Custom Rules
IP/Geo Controls (client list & networ list)
URL Protection (origin rate based)
Analytics & SIEM Integration
Origin Cloacking
Prolexic Network Cloud Firewall
Prolexic
DDoS Solution
Prolexic Cloud
Multilayered DDoS Protection
Automated Detection and Analysis
Zero-Second SLA
Prolexic On-Prem
Prolexic Hybrid
Multicloud & On-Prem Infrastructure, Applications, and Services
Legitimate Traffic
arrow indicates direction(s)
Illegitimate Attack Traffic

Reference architecture for holistic DDoS protection using Edge DNS, App & API Protector, and Prolexic solutions

Akamai's DDoS protection strategy is built on an edge defense architecture routing traffic through Akamai's massively distributed platform, where every request is inspected in real time. This setup defends against DDoS, web app and API attacks, and malicious bots right at the edge, preventing them from reaching the applications or infrastructure. This enhances business continuity by maintaining a fast, highly secure, and always-available architecture that scales with attacks.

Akamai's robust suite of tools and ingredients provide both proactive and reactive controls, each serving a distinct purpose in the overall defense strategy.

Proactive controls

Proactive controls help to prevent attacks before they happen, focusing on strengthening the security posture to minimize vulnerabilities. They include:

- **IP controls (block IP, CIDR ranges, and ASNs):** A fundamental layer of defense, these controls block known malicious IP addresses or ranges identified through threat intelligence.
- **Geo controls (block certain geographies):** By allowing or limiting traffic from specific regions, organizations can preemptively limit exposure to attacks originating from high-risk areas.
- **Web application firewall (WAF) rules:** Implementing rules against known vulnerabilities and attack vectors, such as DDoS tools like FiberFox, offers a strong first line of defense.
- **IP reputation controls:** Using intelligence through heuristics of known malicious resources of DDoS, web scraping, and other malicious activity allows preemptive blocking or scrutiny of suspect traffic.
- **Platform DDoS intelligence:** DDoS attack insights from the globally distributed Akamai edge platform can help to create a proactive mitigation strategy in fighting application-layer DDoS attacks.
- **Caching:** Optimizing content caching can significantly reduce the load on origin servers, indirectly mitigating DDoS impact by serving requests from the edge cache.
- **Site Shield:** Origin cloaking by only allowing requests to origin(s) via Akamai edge network can further reduce server loads.

Reactive controls

Reactive controls are responses to a detected attack, aiming to mitigate its impact and maintain service availability.

- **Rate limiting (rate policies):** These are crucial for mitigating sudden traffic spikes that can indicate a DDoS attack. Configuration can be set up and tailored for customer-specific traffic profiles. Rate limiting often helps as the first line of defense in protecting the customer origin from volumetric and distributed DDoS attacks.
- **Slow POST protection:** Specifically targeting slow HTTP POST attacks, this control reacts to abnormal traffic patterns that aim to exhaust server resources.

- **Custom rules in the WAF:** You should be able to tailor rules quickly in response to emerging threats, offering flexible and dynamic defense mechanisms.
- **Bot visibility and mitigation:** With machine learning to detect browser impersonation, you can identify and block sophisticated DDoS attacks that are sourced through automation.
- **URL protection with intelligent load shedding:** Controls that limit excessive requests to the origin and prioritize legitimate users over malicious traffic can help you maintain service uptime during a DDoS attack.
- **Platform DDoS intelligence:** Load shedding is a category in URL protection that uses DDoS attack insights from the globally distributed Akamai platform and enables our customers to create a proactive mitigation strategy to fight application-layer DDoS attacks.

Mixing ingredients, achieving the balance with your recipe

- **Example:** A large financial services organization assembles an in-depth defense strategy with the Akamai WAAP solution

Some organizations may find themselves a more frequent target of DDoS attacks. For example, according to Akamai research, over a third of DDoS attacks in 2023 targeted financial services institutions. One large financial services organization, an Akamai customer, found itself confronting a targeted attack on its login page. It was able to follow a proven recipe for defense. You can do the same.

Attacker Profile: Hacktivist

Target: Login endpoint

Method: HTTP POST flood

Attack sources: ~66,000 IP addresses and ~140 countries

Recipe

Mitigating an HTTP POST flood attack

Ingredients:

Proactive controls:

- **IP controls**: Use threat intelligence to block IP addresses or CIDR ranges associated with known malicious entities.
- **Geo controls**: Blocklist traffic from geographies known for harboring hacktivist groups, such as regions associated with “Anonymous Sudan.”
- **Web application firewall (WAF) rules**: Implement rules specifically designed to counteract known DDoS tools and tactics, including patterns typical of HTTP GET floods.
- **IP reputation controls**: Carefully monitor or actively block (in real time) traffic from sources with poor reputation scores.
- **Platform DDoS intelligence**: Apply insights from Akamai’s global DDoS attack data to anticipate and counteract emerging threat vectors.
- **Site Shield**: Enable firewall access control lists (ACLs) to only allow traffic from the Akamai edge network and block the rest.

Reactive controls:

- **Rate limiting**: Establish rate policies to mitigate sudden spikes in traffic, setting appropriate thresholds for requests per second to the home page. Optimize your rate limiting by (1) lowering time windows to measure request velocity to one request per second, and (2) applying rate limiting based on the geography and reputation score of connecting IP sources while allowlisting sources, such as the financial institution’s corporate IP addresses and partners.
- **Custom rules in WAF**: Create tailored rules in response to the specific characteristics of the attack once it’s detected. Using traffic sampling controls in your custom rules will help in traffic analysis, to more efficiently look at top attack sources, whereas use of IP/geo controls in custom rules can help in quick mitigation.
- **Bot visibility and mitigation**: Use browser impersonation detection to identify and block requests that mimic legitimate user behavior but are part of the flood.
- **URL protection**: Enforce controls to limit request rates specifically to the login URL, preserving bandwidth for legitimate users. Setting up intelligent load shedding with categories such as proxies, Tor exit nodes, basic bots, low-reputation IPs, etc., will help prioritize real user traffic over these likely malicious sources.

Method of preparation:

Review phase:

- **Review the configuration**: Conduct a thorough review of your current security posture. Configure your proactive controls based on what you find, ensuring all relevant geo and IP controls are appropriately managed.
- **Configuration optimization**: Tune the configuration to recognize and mitigate unusual traffic patterns, including those characteristic of HTTP POST flood attacks.

Detection and mitigation phase:

- **Monitoring and alerting**: Akamai's edge defense architecture can monitor incoming traffic for patterns that might indicate a DDoS attack. You can set up alerts for abnormal traffic spikes or patterns that match the known DDoS methods such as HTTP POST flood.
- **Detection and mitigation**: Various proactive controls such as IP reputation, caching, and IP/geo controls automatically provide detection and mitigation capabilities if set up correctly.

  Once an attack is detected, controls such as rate limiting, URL protection, and browser impersonator detection kick in automatically without any user intervention.
- **Analysis and adaptation**: Continuously analyze attack patterns and adapt your defensive measures in real time to counteract evolving tactics. For example, create tailored custom rules or rate limiting policies based on recent attack traffic analysis.

Recovery and post-attack analysis:

- **Log analysis**: Post-attack, conduct a detailed traffic log analysis to identify the attack vectors and effectiveness of the controls deployed.
- **Adjustments**: Make necessary adjustments to the proactive and reactive controls based on the insights gained from the attack analysis.

Serving suggestions:

- Regularly review and update your defense strategy to adapt to evolving DDoS tactics. Such reviews can significantly vary across different organizations, influenced by their specific needs, threat exposure, and industry best practices. A financial services organization may need such reviews every quarter, whereas an ecommerce platform could target semiannual reviews to prepare for seasonal shopping peaks.
- Engage in continuous training for the security team to recognize and respond to new DDoS attack vectors.
- Conduct simulated attacks to test the effectiveness of the deployed measures and establish the team's preparedness for real-world incidents.

Akamai

Recovery and post-attack analysis

In defending against application-layer (Layer 7) DDoS attacks, the post-attack phase is crucial for strengthening future defenses and understanding your adversary. This involves two critical steps: analyzing the attack pattern and enhancing your defenses based on your analysis. These steps are pivotal in crafting a resilient defense strategy and ensuring the continuity and integrity of online services.

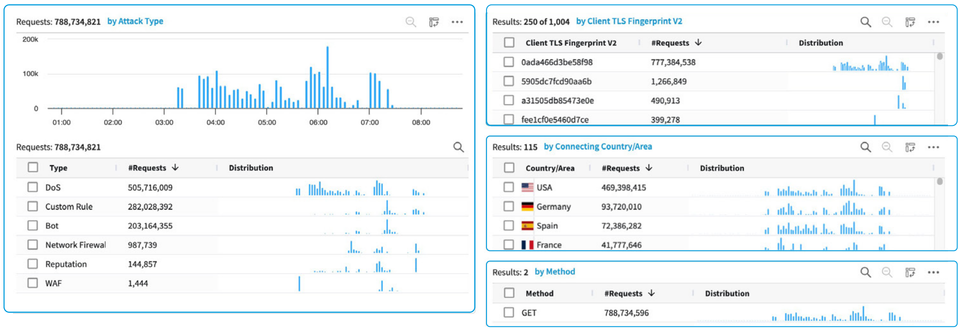
Analyzing the traffic and attack pattern

The next step after you handle an attack is to analyze the incident to understand which strategy worked and which did not work as anticipated. This assessment encompasses longer-term factors such as the impact on customer trust, data integrity, and potential financial losses. Comprehensive security analytics systems such as Akamai Web Security Analytics are indispensable tools in this phase, enabling organizations to understand the attack traffic and its impact.

This analysis involves dissecting the tactics, techniques, and procedures (TTPs) used by the attackers. Key questions to address include:

- What was the nature of the traffic spike?
- Were specific application functionalities targeted?
- Did the attack exploit any known vulnerabilities?

Akamai Web Security Analytics can identify anomalies in traffic patterns, pinpoint the geographic origin of the attack, and classify the attack type based on observed behaviors. The following example shows some of the traffic characteristics or dimensions that can be applied to investigate a DDoS attack.



Requests: 788,734,821 by Attack Type

Requests: 788,734,821

□	Type	#Requests ↓	Distribution
□	DoS	505,716,009	
□	Custom Rule	282,028,392	
□	Bot	203,164,355	
□	Network Firewal	987,739	
□	Reputation	144,857	
□	WAF	1,444	

Results: 250 of 1,004 by Client TLS Fingerprint V2

□	Client TLS Fingerprint V2	#Requests ↓	Distribution
□	0ada466d3be58f98	777,384,538	
□	5905dc7fcd90aa6b	1,266,849	
□	a31505db85473e0e	490,913	
□	fee1cf0e5460d7ce	399,278	

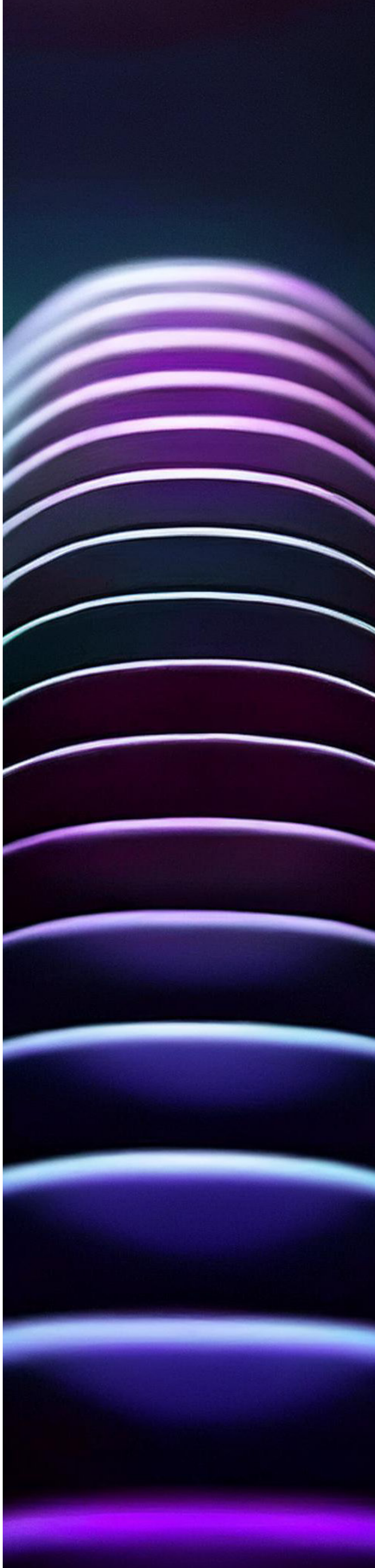
Results: 115 by Connecting Country/Area

□	Country/Area	#Requests ↓	Distribution
□	USA	469,398,415	
□	Germany	93,720,010	
□	Spain	72,386,282	
□	France	41,777,646	

Results: 2 by Method

□	Method	#Requests ↓	Distribution
□	GET	788,734,596	

Images shown are from Web Security Analytics, which provides unprecedented visibility and proactive analysis of security events



Review and update defense strategies based on your attack analysis

Reviewing and updating defense strategies based on attack analysis is a critical component of strengthening an organization's cybersecurity posture. By examining the specifics of a past attack, organizations can identify vulnerabilities in their current defenses and make informed adjustments. Here are some examples of how this process can be applied using Akamai Web Security Analytics.

Example 1: Updating WAF rules based on attack patterns

Scenario: An organization faces a Layer 7 DDoS attack targeting its web application with a barrage of malicious requests toward the application home page.

Review: The attack analysis reveals that the existing web application firewall (WAF) rules adequately detected and blocked more than 90% of the attack traffic, but the remaining nearly 10% leaked through because there was an explicit geo allowlist allowing attack sources from that geo to overwhelm the application.

Update: Based on this analysis, the organization updated its WAF configurations to use a custom WAF rule matching on specific characteristics of the attack traffic from that particular geo. Overrides can keep allowing the geo but block the specific attributes of the attack traffic. Additionally, the rate limiting settings for that particular geo were made more strict.

Example 2: Enhancing origin protection

Scenario: The login process of a retail website is hit by a highly distributed and sophisticated Layer 7 DDoS attack leveraging automated bots.

Review: Post-attack analysis indicates that the attack traffic was highly distributed coming from more than 150 countries and hundreds of TLS fingerprints that look like legit browsers. A good chunk of the traffic originated from cloud providers, some of which were allowlisted as trusted partner sources. While the attack was effectively mitigated, analysis revealed the need for additional defense measures.

Update: To protect high-compute URLs like a checkout process, this organization implemented URL protection, a feature that is specifically designed to protect compute-heavy URLs and API endpoints from highly distributed application-layer DDoS attacks. A security architect also enabled intelligent load shedding for bots, proxies, IP reputation, etc. This sub-feature of URL protection helps prioritize real user traffic by denying requests from likely malicious sources first.

The organization also decided to enable inbuilt bot protection functionality in WAF that was previously not given proper consideration by the business due to the presence of an on-premises bot solution that couldn't scale during this high-velocity attack.

Example 3: Implementing rate limiting for API endpoints

Scenario: An API endpoint of a financial services application is overwhelmed by a flood of fraudulent transaction requests, indicating a Layer 7 DDoS attack aimed at exhausting server resources.

Review: The attack pattern analysis shows that the attackers specifically targeted less-protected API endpoints incapable of processing a high volume of requests.

Update: In response, the organization implemented strict rate limiting on all API endpoints, especially those identified as vulnerable. It also adopted a dedicated API security add-on that provides advanced layers for API security, including API logic abuse, threat of shadow APIs, and API vulnerability monitoring.

Strategic takeaways

- **Continuous monitoring and logging:** Establish robust monitoring and logging systems to promptly detect anomalies and accurately assess damage both during and after an attack.
- **Vulnerability management:** Regularly update and patch systems to mitigate known vulnerabilities, reducing the risk of exploitation.
- **Attack pattern analysis:** Use appropriate visibility tools for deep analysis of attack patterns to understand attackers' methodologies and intent.

Post-attack analysis

Assessing the damage and analyzing the attack pattern are critical components of a robust Layer 7 DDoS defense strategy. These steps not only aid in understanding and mitigating the immediate impacts of an attack but also inform the continuous improvement of defense mechanisms, ensuring better preparedness for future threats.

Maintaining and updating your recipes

Maintaining a strong Layer 7 DDoS defense demands constant monitoring of the latest trends and techniques.

Attackers consistently blend attack patterns, leveraging new tools and vulnerabilities. To proactively counter these threats, organizations must invest time and effort in researching, monitoring, assessing defenses, automating protections, and collaborating with the threat intelligence community.

Monitoring the leading cybersecurity forums is only a good starting point. We suggest a more prescriptive approach:

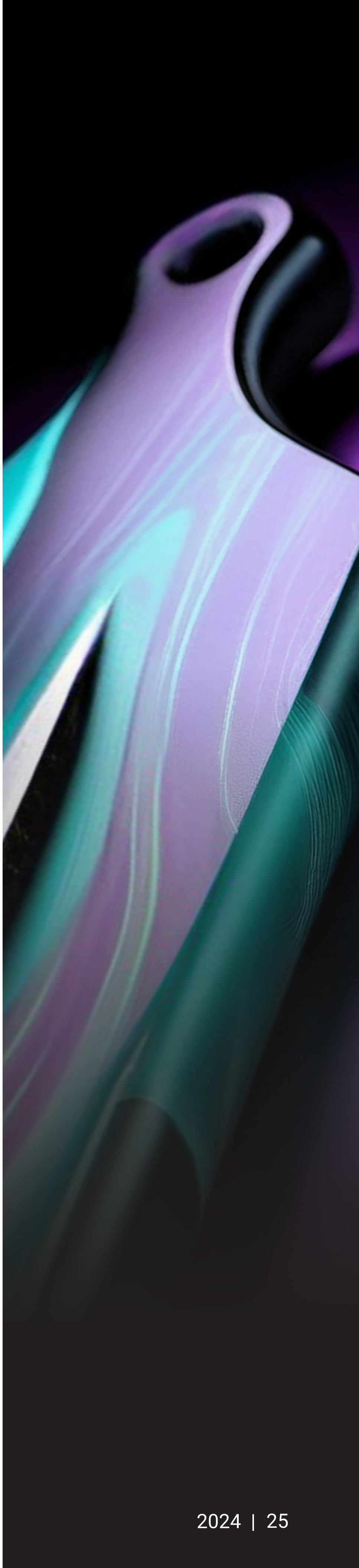
Monitor and assess continuously — Regularly monitor your network and application performance to detect new patterns or anomalies that indicate emerging threats. Use this data to assess the effectiveness of your existing defense mechanisms, identifying areas for improvement or adjustment.

Form an anti-DDoS team — Establish your go-to person or a team within the organization that will research and monitor the DDoS attack landscape and report back to the wider organization at least quarterly with any key findings and recommendations.

Engage with the threat intelligence community — Attackers are communicating amongst themselves about the latest, most effective methods. There's no reason you shouldn't be communicating with colleagues in other companies and industries about the best defenses. Stay informed with the latest threat intelligence. Subscribe to security feeds, participate in cybersecurity forums, and collaborate with peers in your industry. This information will help you anticipate new attack vectors and adjust your defenses accordingly.

Lean on your cybersecurity vendor — Technology vendors often have dedicated threat research groups, and those with a content delivery network can provide insights that are unavailable elsewhere. Take advantage of these learning opportunities whenever and wherever you can. It also makes sense to bring in security consulting experts periodically.

Test your own defenses — Those who fail to prepare are preparing to fail, practice makes perfect … whatever your cliché, the message is the same: Conducting regular testing and drills pays off.



Conduct periodic reviews and simulated attack scenarios (red-team exercises) to test the resilience of your defense strategies. These exercises can reveal weaknesses in your current setup and provide insights into how attackers might exploit your system.

Conduct a test of your network at least once a year. Recent attack profiles can also be good reference for a test case, particularly one that's happened to a company in your industry.

Share your learnings with the community — It's worth reiterating: Just as attackers share their tools and tactics, organizations should also engage in knowledge-sharing about successful defense strategies.

By documenting both successes and failures, cybersecurity professionals can provide real-world insights that enrich the collective knowledge base. Engaging in industry forums, offering mentorship to those newer to the field, and participating in collaborative projects are critical for fostering a robust defense ecosystem. Such efforts not only contribute to the development of more effective strategies and tools but also allow for a diverse pool of experiences and insights that can adapt to the changing tactics of threat actors. This collaborative spirit is essential for staying ahead in the cybersecurity landscape, making each contribution valuable in building a stronger, more resilient digital world.

Key takeaway

The landscape of DDoS threats is dynamic, with attackers constantly seeking new ways to bypass defenses. Maintaining and updating your Layer 7 DDoS protection strategies is a continuous process that requires vigilance, adaptability, and a proactive approach. By staying informed, engaging in regular testing and reviews, and fostering a culture of continuous improvement, you can maintain a robust defense against present and future threats.

Conclusion

It's clear that Layer 7 DDoS attacks have not only become more sophisticated, but easier to launch thanks to advances in automation and coordination among attackers. Meanwhile, organizations must defend a larger, more complex landscape even as the costs of failure rise.

Indeed, concocting a defense recipe is no easy task. No single method offers a panacea for Layer 7 DDoS attacks. As we've demonstrated, a multipronged approach, combining several detection and mitigation strategies, provides the most robust defense.

Additionally, the choice of methods should be guided by the specific needs, traffic patterns, and risk profile of the application or service being protected. You cannot build a defense without an understanding of your business, your traffic, and your vulnerabilities. Regular updates and adjustments to these strategies are essential to adapt to the evolving landscape of DDoS threats.

Finally, it's also become clear that your work is not over once an attack is over. Post-attack analysis and adjustments are critical to ongoing success and can help play a large part in knowledge sharing and career development while you're at it.

Fortunately, Akamai is well positioned to provide assistance every step of the way. From app and API protection, to unmatched insights into global traffic, to expert post-attack analysis, many companies are taking advantage of the opportunity to source all the Layer 7 DDoS protections they need from a single provider.

See Akamai's Layer 7 DDoS protections at work.
Start a free trial of App & API Protector.

Credits

Editorial and writing

Aseem Ahmed
Barney Beal

Review and subject matter contribution

Abdeslam Bella
Sean Flynn
Alex Marks-Bluth
Nitesh Shrivastava
Prathmesh Verma
Dennis Birchard
Ryan Gao
Pawan Sajnani
Patrick Sullivan
Danielle Walter

Marketing and publishing

Georgina Morales Hampe
Shivangi Sahu

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. 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 10/24.