WHITE PAPER

How to Avoid Party Chaos

with the Right Application-Layer DDoS Platform

What application-layer DDoS means for us today

As security experts around the world are painfully aware, DDoS, or distributed denial of service, is a cyberattack that tries to make a website or network resource unavailable by flooding it with malicious traffic so that it is unable to operate. DDoS attacks are still the most popular attack technique used by threat actors and have been on the rise in the last five years. For instance, one of the most recent large attacks (in terms of packets per second [PPS]) peaked at 809 MPPS in about two minutes.

A trend we've seen in this rise of attacks is more instances of application-layer DDoS attacks. Also known as Layer 7 DDoS, these attacks target and disrupt specific web applications (not entire networks). So while difficult for defenders to prevent and mitigate, high adoption of technology like automation and cloud services has given attackers easy access to the tools required to launch these attacks, making it easier than ever to compromise the application-layer.

The reality is, the requests used in this type of attack look like normal end-user requests, so there's no easy way to gauge the sophistication of an attack. The efficiency of affecting both the targeted server and the network means an attack creates more damage with less total bandwidth. In summary, application-layer attacks are easy to implement, hard to slow down or stop, and specific to a target.

In order to understand how application-layer DDoS attacks are uniquely affecting our organizations, we need to know how DDoS attacks affect us across all categories. Consider the categories of DDoS attacks like the pitfalls of a party. For example, you might open your home to a few guests to celebrate a special occasion or have fun on the weekend. However, a few scenarios can occur:

DDoS attack types

Scenario 1
Volumetric attack

Your guests are excited about your party and share too much information (perhaps on social media). Word gets out that your party is the event no one wants to miss, and on the day of your party, countless strangers arrive. This represents a volumetric DDoS attack, because all your resources are being consumed by people you didn't invite.

Scenario 2
Protocol attack

A guest you thought you trusted has been compromised! People who want to be invited to your party (and did not get an invite) overwhelm one of your guests with demands to know details of the event. The guest gives in, and a bunch of uninvited people have access to your party. This represents a protocol DDoS attack because someone who was supposed to keep your party confidential did not.

Scenario 3
Application attack

A malicious person hears about your party, and decides to enter your home disguised as a party guest to plan a theft and commit robbery in your home. This represents an application DDoS attack, because the person is mimicking an authenticated guest.

In all these scenarios, there is a common vulnerability — you have opened your home for an event. This is the unavoidable vulnerability that application-layer DDoS attacks take advantage of because it is the layer in which your organization interacts with the user. Additionally, because this is a layer you have less control over as it serves users directly, it can be harder to mitigate application-layer DDoS attacks.

Plus, if any of these problems occur, it's going to cost you extra. Whether it's dealing with the expense of more food and drink being consumed, strangers finding out personal information about you, or the fallout of an attack on your home, a party gone wrong is expensive.

Many security solutions increasingly promise to protect your systems, resources, and sensitive information from application-layer DDoS attacks, which are now more common and one of the most difficult to defend against. You've given them trust to protect what you have to offer. So in the end, your DDoS protections are only as good as the platform you lend your protections to. Let's look at the latest changes and trends to be aware of as you search for your application-layer DDoS protection platform of choice.

What is trending and changing

As always, when we craft solutions for a specific attack, hackers will adapt their strategies to counteract them. We've monitored that competition, and here are the four trends and changes we're seeing now:

1. Shifting to repeated, short-lived attacks

DDoS attacks are becoming less about prolonged attacks and more about attack size and frequency. Akamai has seen complex attacks with more than nine different attack vectors combining ARMs, SYN flood, UDP reflection (DNS, WS-Discovery, etc.), HTTP flood, and more.

2. Using multi-vector attacks more frequently

More than 20% of attackers are using multi-vector DDoS attacks, combining different DDoS attack methods into one short attack, and then repeating again soon after. According to Link11, the highest number of concurrent vectors observed was 18 – a 50% increase from 2021.

3. Increasing ability to avoid detection and subsequent mitigation

Distinguishing between attack traffic and normal traffic is difficult, especially in the case of an application-layer. For example, a botnet performs an HTTP flood attack against a victim's server. Because each bot in a botnet makes seemingly legitimate network requests, the traffic is not spoofed and may appear "normal" in origin.

4. Automating first, then tailoring tactics

With the prevalence of cloud platforms and IaaS/PaaS, attackers have easy access to automation and computing power, and it's easy to automate attacks and launch an assault quickly and at scale. So these attacks are not just volumetric, but more distributed, random, and cleverly crafted (randomizing parameters in requests, etc.).

As noted in the party scenario, your house could be compromised in three ways: by the consumption of resources, a vulnerable guest, or a disguised threat actor. With the trends and changes in application-layer attacks, your house could be experiencing chaos designed to pass under your radar. Instead, everything is orchestrated across those three categories to develop stealth, like checking out your house beforehand to see how many entrances there are to your home; finding out the party dress code in advance; or creating fake social media profiles to learn more about you to trick all the guests at your party into thinking the threat actors are close friends of yours.

Because of the increase in complexity with application-layer DDoS attacks, it’s helpful to have a more holistic strategy for protection than you might have had in the past. It used to be that any web application and API protection (WAAP) could cover your needs, even WAAPs that were built in-house. Now, your WAAP has to exceed the complexity of application-layer attacks happening today.

A holistic approach to application-layer DDoS protection

What makes application-layer DDoS attacks difficult to detect is that even when multi-vector attacks contain obvious patterns, a motivated attacker will monitor the attack response and modify it to dodge a determined defender. To address this challenge more consistently and accurately, you need to improve your WAAP capabilities across detection, mitigation, and self-service features.

Ultimately, you don't want your WAAP guarding only the front door of your house. You want it to be able to defend every entry point, to understand how to identify threat actors disguised as guests, and to be scalable if you're being faced with multiple attacks at once. The good news is: It's possible to adopt the right platform to mitigate the chaos of application-layer DDoS and continue business as usual. Your DDoS alleviation strategy must become more holistic and focus on the following:

The scalability of your platform

No matter how well your WAAP works day-to-day, if it cannot scale in order to absorb a volumetric attack, it will fail quickly. That's why the platform underneath the WAAP is just as important as the WAAP itself. You also want to know where the platform runs. For instance, Akamai has edge locations globally, often in the regions where attacks originate. It's much easier to stop a DDoS attack if the attack can be mitigated right where it began. Plus, scalability will make table stakes operations, like rate limiting and custom rules, much easier.

The data resources and output that inform your protections

While any WAAP can monitor the traffic and report data that you generate, consider a solution that is able to aggregate data from a global perspective. When your solution provider has visibility into the traffic across thousands of enterprises, the data you generate can be contextualized among organizations facing the same threats and can better inform the machine learning systems in place in your solution. Then, your own internal teams can source this data and use it to iterate and customize your solution.

Your solution's visibility and accuracy

Some detection methods should come by default, including behavioral/anomaly-based detections, which focus beyond incoming client traffic to origin connection rate and server performance parameters. However, when you have a scalable solution informed by a robust data set, your WAAP will be much more targeted and accurate. Plus, you'll get a more detailed understanding of what is happening on your traffic because the solution is adaptive and able to understand if an attack is hiding (like attacks that hide behind an open proxy on the internet). All of this will help make sure the right people get notified while drastically reducing false positives.

So, to bring all this together, if you were to plan a party that wasn't at risk of being overwhelmed, you'd want your house to be big enough (scalable) to hold extra guests that might not have been invited. You'd want to talk to other folks who have had bad party experiences (data resources) so that you know in advance the protections you should put in place. And you'll want to share the guest list in advance and greet all guests before they enter your house (visibility and accuracy) to make sure everyone is safe.

And if you don't want to do all of this work yourself, you can hire trusted reinforcements to do the job for you. Managed services can monitor for all the signals you have to be highly attentive to in order to distinguish a regular guest from a malicious one. Plus, you remove the stress of having to devote your staff's time and expertise to preventing attacks around the clock for this increasingly common and difficult-to-detect type of attack.

The conversation about application-layer DDoS is one filled with the variables and vulnerabilities that come naturally as a part of the application-layer. And it's a critical conversation because application-layer DDoS attacks can be the most damaging to your organization. However, defense against this type of attack does not have to be complicated or chaotic. All you need is a strategic, scalable, data-driven solution — and then you can party.

Learn more about how Akamai can support you with Layer 7 DDoS protections.