DDoS IS THE NEW SPAM

3 STRATEGIES TO TURN CATASTROPHE INTO ANNOYANCE
INTRODUCTION

As DDoS attacks grow larger, more complex, and more pervasive, it can feel like we face a future of inevitable service outages and anxiety.

However, we still don’t have a real handle on the DDoS problem. If we receive a preposterous-sounding email threatening a DDoS attack from someone who could be the very same Nigerian prince, we can’t just laugh it off or ignore it—we still have to take it seriously. This year, attackers have targeted a variety of organizations, across all sectors, with the aim of influencing political events, disrupting both Bitcoin and traditional financial trading, and leveraging ransom to squeeze profit from those businesses not equipped to mitigate the massive volumetric attacks that have become part of everyday operations online.

It’s clear that DDoS isn’t going away anytime soon, and as attacks and motivations evolve, so must we if we are to maintain service availability—and business continuity.

DDoS IS THE NEW SPAM: 3 STRATEGIES TO TURN CATASTROPHE INTO ANNOYANCE

WE’VE TAMED SPAM, BUT WHY IS DDoS STILL A THING?

The short answer is that dealing with DDoS is challenging because it can be difficult to predict, as well as to distinguish legitimate requests from malicious traffic. Any given network will have multiple chokepoints and areas of vulnerability, and today’s multi-vector attacks are increasingly sophisticated, employing a variety of tactics.

VOLUMETRIC ATTACKS

These are the ones we continually read about—they flood our networks with the aim of overpowering your upstream links to the Internet, making services unavailable for their intended user base.

LOW-AND-SLOW ATTACKS

Our adversaries are increasingly using low-and-slow attacks on application-layer resources, exploiting weaknesses such as resource-intensive database queries, to render the services unusable. Such attacks can be challenging to detect and defeat using traditional mitigation methods.

RESOURCE BOTTLENECK ATTACKS

With more than 50 percent of Internet traffic encrypted using SSL/TLS, demands placed on cryptography infrastructure such as TLS ASICs have skyrocketed.³ Attackers can overwhelm your network's decryption capabilities, causing your services to become unavailable over the necessary secure channels.

COMBINATION ATTACKS

Many attacks blend different attack vectors that run simultaneously, designed to find the weakest link in your infrastructure and then exploit it.

BUSINESS LOGIC ATTACKS

Not all attacks target vulnerabilities in your network or applications. Some attackers use bots to commit fraud on ecommerce sites, denying service to legitimate customers and driving up costs.

DDoS attacks are instigated based on a variety of motivations, ranging from political activism to petty revenge. DDoS is also increasingly used as a diversion to facilitate other attacks, a tactic commonly referred to as “smokescreening.” While you’re battling the flood of traffic to keep services online, the attacker slips past your defenses and steals corporate data, credentials, or other high-value assets. DDoS attacks can also be used to overwhelm existing security controls, such as an IDS and logging services that would otherwise be used to spot such activity, which leaves other parts of your network vulnerable.

To make matters worse, it’s incredibly cheap and easy to initiate a DDoS attack. For about $100, anyone can launch a six-minute, 125 Gbps attack, which is large enough to overwhelm most organizations’ upstream capacity. At such a minimal cost, DDoS attacks are available to anyone with a motive or even just a personal grudge—which means that everyone is theoretically at risk.

DDoS attacks can be used to overwhelm existing security controls, leaving other parts of your network vulnerable.

Don’t “DoS” Yourself

When people talk about distributed denial of service (DDoS), they’re often referring to those huge, botnet-driven volumetric attacks. However, remember that an attacker doesn’t have to completely overwhelm your systems to render them unsatisfactory to your customers. Just causing outages or poor service levels can be enough to cause your customers to abandon transactions, or drive them to a competing site. With that in mind, it’s important to carefully balance your security controls so as not to exceed customer tolerance and deter continued use of your services. Otherwise, you can actually “DoS” yourself.

It’s important to carefully balance your security controls so as not to exceed customer tolerance.

For about $100, anyone can launch a 6-minute, 125 Gbps attack.

7 https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/
3 STRATEGIES TO
UP YOUR DDoS GAME

These ever-evolving DDoS attacks are difficult to defend against. How do you balance costs and also scale up to serve spikes in demand and traffic, while continuing to deliver satisfactory service levels to your customers? Alternatively, how can you scale down flexibly to minimize costs? These considerations will come up for every organization at some point. Some forward-thinking enterprises have been testing the resilience of their infrastructure with simulated, and internally initiated, attacks occurring frequently and at random times.⁸ Necessity is the mother of invention—and so maybe the upside of the difficulty in dealing with DDoS attacks is that the effort will force everyone to up their DDoS game, driving more resilient network and application architectures.

⁸ https://medium.com/netflix-techblog/tagged/simian-army
Wouldn’t it be great if our systems could train themselves to analyze traffic behavior, recognize DDoS attacks, and stop them automatically? Good news: Smart solutions are doing just that. By continuously monitoring service health and ongoing traffic patterns, advanced defensive technology can leverage behavioral analytics and machine learning to understand the context and baseline of normal traffic using numerous data points. It is increasingly feasible to identify anomalous transactions or workflows, take action to reduce the impact of suspicious clients, and refine the data to improve the process over time. One caveat: While behavioral analytics works well to stop layer 7 DDoS attacks, it’s not really useful for defending against large-scale volumetric floods; the unwanted traffic will simply drown out any legitimate requests.

Having a high degree of network and attack visibility will be invaluable when it becomes necessary to fine-tune your controls to better manage an attack. For example, if you know that 90 percent of your customer base is located in the United States, and you identify lots of attack traffic originating from non-U.S. IP addresses, it may be necessary to block all the non-U.S. traffic for the duration of the attack in order to preserve service availability for the broadest swath of your customer base. After the flood subsides, you can pare down such controls and restore global availability.

Alternatively, if you see repeated application layer requests from particular IP addresses or strains of malware, you may simply want to block traffic from those clients at the network layer and not process it at all. You can also implement quality of service (QoS) policies for them to reduce the impact of their requests.

Smart solutions will allow you to establish traffic baselines, set parameters to manage that traffic, and automatically ratchet up controls based on predefined conditions. Behavioral analytics and fingerprinting can offer a more nuanced view into the intentions of any given remote endpoint—whether human or bot, benign or malicious—which can help you assign it an appropriate traffic classification.

---

CLOUD SCRUBBING KEEPS YOUR BUSINESS ONLINE DURING AN ATTACK

While partial-saturation, authentication-based, and application-level attacks can generally be addressed with an always-on cloud or on-premises solution, those huge volumetric attacks will easily overwhelm all but the most robust defenses. You will need a plan to leverage more capacity than your adversaries can bring to bear, which is where cloud scrubbing comes in.

Any organization that delivers content or applications over the Internet can use a cloud-based scrubbing service to keep their business online during an attack with minimal impact to users. Scrubbing is the process of inspecting and analyzing traffic, requests, input data, and more, both for utility and validity. As traffic traverses the offsite scrubbing center, it’s continuously analyzed to ensure that the malicious requests are being filtered. At the end of the process, all the “clean” traffic is shipped back to you, so that you can service legitimate requests and continue operating normally.

Cloud scrubbing services generally operate in one of two modes: on-demand and always-on. The on-demand model involves routing traffic through the scrubbing center only when you’re getting more traffic than you can handle—be it sheer volume or taxing, resource-intensive requests. Alternatively, an always-on cloud scrubbing service handles this for you at all times, and can reduce or eliminate your time to remediation. It may also act as a deterrent to potential attackers when they’re looking for victims—much as a having a dog in your yard can dissuade thieves from targeting your home.

CLOUD SCRUBBING

When organizations that deliver apps or content over the Internet need more capacity, they use cloud-based scrubbing services to inspect and analyze their traffic.
As long as DDoS remains effective and profitable, attack vectors and tactics will continue to evolve. A robust solution should encompass mitigation capabilities for all kinds of attacks, from the low and slow to the volumetric flood. But how can you optimize your systems so they work efficiently and keep you online during an attack?

“Signaling” integrates on-premises equipment with cloud-scrubbing services, allowing them to communicate with each other in the event of an attack. This technology enables the fast activation of on-demand cloud-based scrubbing, seamlessly re-directing attack traffic through the scrubbing service, which can prevent even the largest volumetric attacks from saturating your upstream connections. The Internet Engineering Task Force (IETF) has a working group developing a standards-based approach for real-time signaling between on-premises solutions, scrubbing services, and other network elements and services.¹⁰ As the technology matures, signaling will become even more effective—and it just might be your best line of defense in a comprehensive DDoS protection strategy.

Depending on the solutions you currently employ, you may be able to use signaling to protect your network and your apps. You can trigger a switch to your cloud scrubbing service, or set your system to do it automatically via policies and thresholding. While the automatic method requires preparation and testing (especially for layer 7 mitigations requiring SSL offload), it can save you a lot of time and effort when you become an active target.

The lesson, as is true for all DDoS protection strategies, is to plan and prepare before the worst happens. You will need to spend a little time working with your scrubbing provider to determine the best way to seamlessly transition the traffic to and from the scrubbing service, but setting it up now will serve you well when you need it most.

¹⁰ https://datatracker.ietf.org/wg/dots/about/
As signaling and scrubbing technology evolve (and as your solutions become more and more adaptable), DDoS attacks will become less effective and less attractive to would-be adversaries. The time will soon come when a 1 Tb attack from an IoT botnet will seem like a mere annoyance, rather than a catastrophic event—if you even notice it at all.

So how do you get there faster? Plan ahead by designing a defense-in-depth DDoS strategy and partner with a trusted security provider to handle the large attacks. Upfront preparation will pay off when the threat of DDoS attacks no longer keeps you up at night.

For more information on the threats that affect your organization, and what you can do to defend against them, visit f5.com/security.
Always-on, always-connected apps can help power and transform your business—but they can also act as gateways to data beyond the protections of your firewalls. With most attacks happening at the app level, protecting the capabilities that drive your business means protecting the apps that make them happen.