IDC TECHNOLOGY SPOTLIGHT

Sponsored by: A10 Networks

Debilitating distributed denial-of-service (DDoS) attacks are more difficult to detect and mitigate than ever. Artificial intelligence and machine learning (AI/ML) as well as automation are the keys to mounting a rapid-response DDoS defense.

DDoS Defenses Enter the AI Era: Automation Drives Business Resilience and Growth

June 2021

Written by: Christopher Rodriguez, Research Manager, Cybersecurity Products

Introduction

Distributed denial-of-service (DDoS) risk took a giant leap forward in 2020. Security researchers reported a spike in DDoS activity over the course of last summer that coincided with a general increase in cybercrime. In what proved to be another year of record-breaking attacks, cloud service providers fended off a DDoS campaign spanning a three-day period that peaked at 2.3Tbps of attack traffic. A 2.5Tbps attack that involved another major provider was reported shortly afterward. These assaults, and many others, obliterated the previous high-water mark of DDoS scale.

While massive-scale attacks continue to capture headlines each year, attackers are adapting their tactics to harass online organizations on a daily basis. An example of this trend is the use of quick-hitting "bursty" DDoS attacks. As a result, the DDoS threat is more sophisticated and sustained than ever. DDoS risk is an ongoing pain point as businesses grapple with how to operationalize DDoS mitigation for maximal value. Clearly, defenses must become smarter and more efficient to keep pace.

AT A GLANCE

KEY STATS

» Multiple record-breaking attacks topped 2.3Tbps and 2.5Tbps in 2020.

According to IDC surveys:

» 15% of enterprises faced over 100 attacks in a year.

» 30% of organizations experienced attacks lasting under four hours.

» 69% of enterprises reported DDoS attacks that were under 10Gbps.

KEY TAKEAWAYS

DDoS attacks are more frequent and destructive than ever. AI/ML and automation are the keys to a rapid-response DDoS defense that drives business resilience and customer retention.

Benefits

DDoS mitigation is a foundational requirement for all service providers and service provider-like organizations. This group includes large enterprises with their own datacenters as well as universities, gaming companies, and other internet-dependent organizations. Successful DDoS defenses enable service providers and enterprises alike to ensure business resilience and avoid costly disruptions. Intelligent and fast DDoS mitigation allows service providers to reduce costs, including the wasted costs of transporting attack traffic across the network backbone and peering points. DDoS mitigation also helps enterprise IT organizations avoid the expense of overprovisioning network resources in anticipation of attack traffic.

For service providers, the ability to deliver performant, reliable connectivity is tantamount to success. Service providers furnish foundational connectivity for fickle consumers and demanding enterprises. Degraded or disrupted performance directly translates to lost sales and workforce productivity, which is especially true for remote or traveling workers.

Furthermore, expectations are constantly changing. Communications service providers are being asked to support increasing amounts of traffic, with growth rising sharply due to digital transformation trends such as the Internet of Things (IoT), digital media consumption, and cloud-centric business models. IDC expects service providers to redouble their efforts in service expansions, with a particular focus on new areas of growth like edge and 5G, in order to handle the increase in traffic.

Similarly, enterprises rely on cloud service providers for many and varied lines of business, with workloads spread across hybrid cloud environments, on-premises datacenters, private cloud environments, and public infrastructure-as-a-service (IaaS) environments. These companies also have extensive reliance on productivity applications such as software as a service (SaaS) (e.g., collaboration tools, email, customer relationship management [CRM], and productivity suites). Cloud service providers also have steep customer expectations to meet in terms of speed and constant uptime.

Not all DDoS defenses are the same. Modern DDoS defenses offer numerous advantages over legacy approaches, including:

- **Leveraging artificial intelligence (AI) and machine learning (ML) for automated detection and mitigation of attacks.** Legacy approaches rely on identification of attack patterns, heuristics or signatures, malicious IPs, and other techniques to identify and block known threats. By comparison, ML trains algorithms to recognize zero-day, never-before-seen attacks that might otherwise require lengthy investigations, costly work stoppages, and end-user complaints.
- **Reducing the need for manual intervention, investigation, and response.** Modern DDoS defenses mean that security operations center (SOC) analysts, already stretched thin, are able to do more with less time. The reduction of manual, human-driven investigations and response shifts the economic advantage to defenders. Attackers must work harder to generate disruptions, resulting in less motivation and fewer attacks.
- **Aligning with business outcomes.** Service providers are updating DDoS defenses to improve service-level agreements (SLAs) and customer experience. For enterprises, modern DDoS mitigation solutions provide greater deployment flexibility and more business-friendly licensing models.

Trends

In 2020, large cloud service providers reported the biggest DDoS attacks since the 2018 Memcached assaults. The AWS attack exploited vulnerable CLDAP servers, with a 70x amplification factor, reaching a peak magnitude of 2.3Tbps over the course of three days. Shortly afterward, Google revealed a six-month attack that peaked at 2.5Tbps.

While DDoS attack scale is already in record-breaking territory, threat actors continue their arms race by focusing heavily on IoT device and bot recruitment. IDC forecasts the overall number of "connected" IoT devices will reach over 42 billion by 2025. A significant number of these devices represent potential resources for future attacks. IoT device manufacturers continue to focus on speed to market, shipping products with vulnerabilities such as simple default passwords that most users never change, leaving the organization open to simple brute-force attacks. As a consequence, the number of potential DDoS weapons is constantly increasing.

Digital transformation also offers fresh attack vectors for cybercriminals in the form of new technologies. For example, HTTP/3 leverages QUIC, a next-generation protocol for more efficient, lower-latency web communications. QUIC establishes multiplexed UDP-based connections for web applications in place of TCP. QUIC connections are encrypted, using TLS 1.3, by default, resulting in a potential new threat vector that legacy DDoS mitigation solutions may be unable to inspect. Overall, the DDoS threat vector is becoming more and more complex.

The expansion in resources and opportunities provides direct financial gain for cybercriminals in the form of illicit "DDoS for hire" service offerings or DDoS-based extortion schemes. To maximize financial gain, cybercriminals continue to find new and more efficient methods, such as reusing DDoS attack code and adapting it to various campaigns.

Besides record-breaking attacks, security researchers reported an increase in overall DDoS activity as cybercrime soared in 2020. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned of ongoing, targeted DDoS attacks against financial and business organizations worldwide in September 2020; it again warned of DDoS attacks by nation-state actors in December 2020. These same underlying factors persist today and point to a generally elevated risk of DDoS attacks in coming years.

Notably, attackers have demonstrated a preference for short, destructive "bursty" attacks. IDC research found that 15% of enterprises said their organization experienced over 100 DDoS attacks in a year, with 30% of attacks lasting under four hours. Ostensibly, an ongoing campaign of quick bursty DDoS attacks may feel more disruptive than the massive attacks that capture headlines. For example, 69% of enterprises experienced DDoS attacks under 10Gbps, which is unlikely to capture headlines but will cause headaches and challenge the best defenses. Record-breaking attacks tend to set off alarms in an organization, resulting in responses from SOC teams, the broader IT organization, partners, and service providers. With bursty DDoS attacks, the goal is attrition, as attackers launch sustained campaigns of smaller attacks that end before detection and response can occur.

DDoS threats and mitigation technologies have shifted in recent years, leading to a change in buyer type and requirements. While most organizations face similar DDoS threats, the nuances of how they are detected and mitigated require slightly different approaches.

For the typical enterprise, an on-premises approach makes the most sense if DDoS attacks are a regular occurrence. The sheer scale of the largest DDoS attacks today may require the organization to enlist the assistance of a communications service provider or a cloud provider. More sophisticated attacks may also require a managed security service arrangement. However, an on-premises DDoS mitigation solution may address most attacks without the need for expensive "emergency" services or the added latency of routing traffic to the cloud. Overall, the various options allow enterprises to select the DDoS mitigation approach that best suits their requirements for availability and performance, deployment flexibility, on-demand access, and business value.

For service providers and enterprises with an extensive online presence, large networks, and datacenters, the expectations for performance and availability rise dramatically. Global, digitally transformed enterprises require the same level of low-latency, rapid-response DDoS protection as service provider networks. For these organizations, such as gaming companies, universities, and large financial institutions, downtime is often measured by the millions of dollars per hour.

Overall, a misalignment remains between the rapid evolution of DDoS threat vectors, attacker resources, and motivation on the one end and the traditional approaches to DDoS mitigation on the other. Modern DDoS defenses require intelligent automation, scale for large attacks, and efficacy against emerging threats. Without these core capabilities, defenders will be unable to disrupt the economic advantage that cybercriminals currently enjoy.

Considering A10 Networks

A10 Networks offers a set of high-performance DDoS mitigation solutions called the Thunder Threat Protection System (TPS), available as a hardware appliance or a virtual appliance. The Thunder TPS product line sits alongside a robust portfolio of application delivery and security solutions such as Thunder Application Delivery Controller (ADC), Thunder Carrier Grade Networking (CGN), Thunder Convergent Firewall (CFW), Thunder SSL Insight (SSLi), and a Non-stop DNS service.

The Thunder TPS solution offers benefits in terms of advanced DDoS mitigation and business value:

- **Performance provides massive scale and reduces latency for business resilience.** A10 Networks offers its Thunder TPS as a lineup of seven appliances or as virtual appliances (three licenses available). Thunder TPS is designed to withstand large-scale attacks in terms of both bandwidth and packets per second. A10 Networks' largest model, the Thunder TPS 7765 offers 1.2Tbps of hardware-based threat blocking and 500 million packets per second of attack mitigation capacity in a two RU form factor, while the virtual appliances reach up to 100Gbps. The solutions can be clustered for additional scale.
- **AI/ML enables automated signature generation to block anomalies.** In 2019, the company introduced its Zero-day Automated Protection (ZAP) engine for rapid, automated detection of DDoS attacks including never-before-seen zero-day attacks. ZAP uses a two-pronged approach, with ML-based algorithms to recognize and generate signatures of attack patterns and a heuristics-based behavior analysis to identify and block anomalous behavior.
- **Response automation provides options for escalated/graduated policies.** A "five-level" adaptive policy mitigation engine, coupled with continuous baselining, enables automated escalation of responses. This adaptive approach lets organizations defend against attacks while minimizing false positives by applying more aggressive responses on each consecutive escalation level as needed. Additionally, policies and protections are provided "out of the box" for immediate protection, while customizable policies provide opportunities for highly tuned defenses in organizations facing sophisticated, dedicated threat actors.
- **Threat research and intelligence enable risk mitigation.** A10 Networks publishes a biannual DDoS Weapons Report to educate the market about emerging threat vectors. For example, researchers discovered a record 12.5 million potential DDoS weapons in 2020, including five protocols that are leveraged as DDoS weapons far more frequently than the CLDAP weapons used in the AWS attack. This intelligence helps security professionals identify and manage risk by understanding the threat landscape and adjusting policies and resources accordingly. This research is also made actionable as part of the included threat intelligence feeds consumed by the Thunder TPS solution. The feeds are augmented with data from multiple leading security organizations to give a high level of security efficacy.
- **Readiness to address service provider needs is baked in.** The Thunder product line is designed for large service provider needs, which is particularly suited for building out DDoS cloud scrubbing centers. For example, Thunder TPS includes multitenant operation, enabling different tiers of service with granular policy control for tens of thousands of business tenants while ensuring customer privacy. The solution offers a subscriber portal for centralized cloud management and includes APIs for portal customization. A Thunder TPS deployment helps service providers meet or exceed SLAs to enhance subscribers' business value at high scale levels.
- **Flexible deployment models and portable licensing are available.** Support for cloud and on-premises environments, combined with portable, flexible licensing and options for subscription billing, enhances business agility and value. Of note, the subscription model also covers hardware upgrades to meet increased security needs as attacks increase or the network grows.

Challenges

A10 Networks faces growing competition in the enterprise market from providers of cloud-based DDoS mitigation solutions that offer high scalability and turnkey deployments for enterprises and smaller organizations. However, solution providers such as A10 Networks continue to play a pivotal role in the DDoS mitigation ecosystem as suppliers to those cloud-based DDoS mitigation providers as well as to various service providers, cloud/SaaS providers, and other large datacenter-dependent organizations (e.g., large financial institutions, universities, and gaming companies).

Other challenges include:

- **Complacency.** Companies are gaining an understanding of the elevated risk levels but are content with their current approaches. In some cases, changes will occur slowly until external forces, such as DDoS attacks, stimulate a sudden sense of urgency.
- **Lack of awareness.** Some IT organizations are unaware of the extent or scale of DDoS activity in current network and traffic conditions. For example, just as failure to decrypt TLS/SSL traffic can hide threats, the load on infrastructure may include misdiagnosed, and undetected, DDoS traffic.

Conclusion

At its core, DDoS mitigation is about business resilience and value. Modern DDoS defenses leverage automation and AI/ML for fast, scalable, and accurate detection that enables business resilience. With this assurance of reliability and trustworthy performance in place, service providers can provide high-value service offerings to customers, and large enterprise organizations can continue to serve their customers well. While ongoing buyer education efforts are required, the march to adopt a modern DDoS mitigation solution is well underway. It is critical for organizations to modernize and automate their DDoS defenses to protect their customers against sophisticated modern DDoS attacks that only continue to increase in size and frequency.

The march to adopt a modern DDoS mitigation solution is well underway.

About the Analyst

Christopher Rodriguez, *Research Manager, Cybersecurity Products*

Chris Rodriguez is a Research Manager in IDC's Network Security Products and Strategies program covering technologies designed to secure today's complex enterprise networks. The Network Security Products and Strategies practice covers specific functions, including firewall/UTM, IDS/IPS, VPN, DDoS mitigation products, cloud security gateway, messaging security, web security, and web application firewall.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com