WHITEPAPER

A Smarter Approach For Combating Distributed Denial-of-Service Attacks

As DDoS attacks become more prevalent, focused and severe, organizations need to consider new options to protect their infrastructure, applications and data.

Distributed denial-of-service (DDoS) is hardly a new threat to IT and security executives, but the expanding footprint, complexity and impact of those attacks is ratcheting up the stakes for organizations. Even though DDoS is not necessarily considered a breach or an intrusion, it typically results in similar levels of damage as other threat vectors. DDoS often is a catalyst for financial losses, productivity snags and damage to organizations' brand reputations and customer loyalty.

Failure to address this growing problem carries severe financial, operational, regulatory, legal and customer confidence implications.

Did you know:

DDoS attacks accounted for 22% of unplanned outages in 2016, up from a mere 3% in 2010.[1]

The average cost of those outages has spiked to an all-time high of more than $740,000.[1]

1 "2016 cost of data center outages," Ponemon Institute, January 2016

TechTarget | Custom Media

WINDSTREAM ENTERPRISE

Clearly, legacy approaches to spotting the sources of a DDoS attack and mitigating its impact are insufficient. Instead, DDoS defenses now require a modernized, refined approach—in large part because the threats are becoming increasingly sophisticated and multi-faceted. In fact, nearly three quarters of DDoS attacks tracked in the second quarter of 2017 employed multiple attack types, and 25% of the attacks peaked at greater than 5 gigabytes per second.[2]

There's another problem with traditional DDoS mitigation solutions: They are typically expensive to purchase, time consuming to deploy and resource intensive to manage and to monitor DDoS threats. And many legacy DDoS systems fail to fully account for important potential vulnerabilities such as mobile endpoints and Internet of Things-based systems. This means updating and upgrading existing DDoS mitigation solutions can be a budget-buster for even the largest enterprises, and is often far beyond the financial means of mid-sized organizations—ones that often are directly in the crosshairs of DDoS attacks.

Of course, there still remain some skeptics who believe their DDoS defenses are sufficient to meet the onslaught of new threats. For many organizations, it's akin to over-buying insurance for catastrophic events with a low likelihood of occurring. "Odds are that we just won't need it," they may tell themselves. Well, be aware of this reality: Even if your organization hasn't been hit yet with a more powerful and complex DDoS attack, don't let your guard down. Your organization is likely to be victimized soon.

Examples of DDoS attacks and impacts in key vertical industries

DDoS attacks can—and often do—victimize organizations of all sizes and geographies. And while no industry or vertical market is immune to DDoS attacks, certain industries have the potential for significant vulnerabilities and negative impact. These include:

Financial Services. Global financial operations—retail banking, credit unions, insurance, ATM machines and many other forms of financial activities—require around-the-clock availability. Every minute systems are unavailable due to a DDoS attack costs financial institutions untold economic losses. Additionally, consumer confidence for financial markets hinges heavily on having the utmost trust in the security, safety and availability of electronic systems. Research has consistently pointed to financial services as the industry most often hit by DDoS attacks, such as the 2016 episode experienced by financial services giant HSBC. The bank said that while it was able to fight off the attack sufficiently to avoid disrupting most customer transactions, its services were unavailable to many customers on the day of the attack.[3] This undoubtedly cost the bank in both potential revenue and in the invaluable customer experience.

Healthcare. With hospitals now connecting so many of their clinical, research, operational and financial systems over common network infrastructure, DDoS attacks have great potential to paralyze healthcare providers. And, as healthcare organizations increasingly adopt the Internet of Things in such methods as smart medical instruments and sensor-based clinical equipment, DDoS attacks can significantly disrupt the delivery of quality healthcare to patients. And keep in mind that healthcare records are considered the most valuable and most-sought-after data on the black market, making DDoS attacks a source of potentially huge financial, legal and regulatory problems. Research indicates that DDoS attacks in healthcare rose 13% from 2016 to 2017.[4] For example, when Boston Children's Hospital was hit with a DDoS attack, it prompted them to step up their efforts to identify, block and remediate DDoS attacks with a more strategic, comprehensive approach.[5]

Education. More and more education processes are driven, enabled, facilitated and supported by technology, making networks at colleges, public schools and vocational education institutions highly vulnerable to DDoS. Not surprisingly, security vulnerabilities in the education market prompt significant concerns over privacy and identity theft, and colleges—many of which also run prestigious, money-producing research labs—are

especially prime targets. In 2015, the Minnesota Department of Education twice had to suspend its state testing after students experienced problems logging into an online assessment system after a DDoS attack.[6]

Retail. Whether you're talking about traditional brick-and-mortar storefronts or, especially, online stores, retailing has a high risk profile when it comes to DDoS. In fact, retail may be the industry most susceptible to economic problems due to the loss of consumer confidence in the event of system availability problems. The economic impact of systems not being able to conduct transactions is enormous—especially at peak timeframes such as year-end holidays and back-to-school season. The loss of brand reputation can be nearly incalculable, and hacked retailers can suffer potentially catastrophic impact on their competitive positions. Leading online retailer Amazon is the most prominent victim of a DDoS attack in recent years, but it is by no means the only one.

2 "Verisign distributed denial of service trends report," Verisign, Q2 2017Advantage: SD-WAN
3 "DDoS is most common cyber attack on financial institutions," ComputerWeekly, February 2016
4 "Denial-of-service attacks on healthcare poised to explode," Healthcare IT News, May 2017
5 "Healthcare DDoS Attack: Mitigation Lessons," Careers InfoSecurity, September 2014
6 "Protecting education networks from DDoS attacks," AT&T Business

What a modernized DDoS mitigation solution can and should deliver

These and many other organizations that have been victimized by DDoS attacks have realized that they need upgraded, modernized and more efficient solutions. Specifically, IT and security decision makers looking for optimized, cost-efficient DDoS mitigation solutions should insist on:

Ability to get up and running ASAP after an attack, in order to mitigate the impact of lost business and application availability interruptions.

Service-level agreements (SLAs) that actually go a step further by ensuring "service-level objectives" with even faster response and mitigation windows.

Automated steps for monitoring, identifying or verifying attack, notification and mitigation.

Integrated monitoring and mitigation.

Cost-effective pricing and low total cost of ownership (TCO) that balances low pricing with improved staff productivity and business continuity.

Access to a graphics-based portal for real-time metrics and reports.

Critical asset monitoring.

Windstream Enterprise's DDoS Mitigation Service

As organizations grow increasingly reliant on reliable, compliant and highly available Internet access, many also have felt the brunt of DDoS attacks. But in the face of high purchase prices, deployment complexity and ongoing management challenges, IT and security decision makers have been seeking new classes of solutions.

Windstream Enterprise's Distributed Denial of Service Mitigation solution is optimized for customers looking to ensure secure, available Internet access in the face of mounting DDoS attacks. It delivers proactive monitoring and customer notification in the event of a DDoS attack, with a 15-minute service-level agreement for both alerts and mitigation.

The service mitigates layers 3, 4 and 7 DDoS attacks, and provides access to a DDoS portal for real-time metrics and reports. Additionally, the service provides an auto-mitigation feature for rapid mitigation against a subset of attacks.

Optional features are also available, including emergency mitigation that provides 24-hour protection for Windstream Enterprise Internet customers under attack. Critical asset monitoring functionality also is available for additional instances of monitoring against subnetworks.

Windstream Enterprise's DDoS Mitigation ensures Internet circuits and web-facing applications remain up and available when confronted with DDoS attacks. Mitigation functionality is integrated into the backbone network and offers seamless integration without customer manual intervention.

Windstream Enterprise's pricing for the service is based on the return rate of clean traffic, with service tiers reflecting bandwidth ranging from 50 Mbps to 10 Gbps. This approach results in a lower subscription price than those offered by competitive offerings, and it ensures low TCO by freeing up IT and security staff from manual monitoring and mitigation and rapid return to operations, if an attack does hit.

Windstream Enterprise's DDoS Mitigation is part of an extensive portfolio of products and services that ensures business customers of all sizes and across all industries can utilize web services for their most essential day-to-day activities with high confidence in system and network resource availability and performance.

Conclusion

DDoS attacks are accelerating in frequency and becoming more difficult to mitigate. At the same time, their impact on organizations is expanding, often causing great financial, regulatory, legal and brand damage. Because so many legacy DDoS solutions are expensive to procure, time consuming to deploy and resource-intensive to manage, security and IT professionals need new solutions.

Specifically, they need a DDoS safeguard that is cost effective, reliable and adaptable to ever-changing DDoS attacks. And they need a solution that is available from a proven single source, rather than having to purchase multiple DDoS solutions from different providers and try to duct-tape them into a comprehensive, enterprisewide defense.

More and more organizations are turning to Windstream Enterprise's DDoS Mitigation Service to address their needs, while also putting in place an adaptable, flexible DDoS mitigation framework for the future. When attacks inevitably occur, IT and business leaders will have the confidence in knowing that they have an emergency service reliably available when they are under attack.

About Windstream Enterprise

Windstream Enterprise collaborates with businesses across the U.S. to drive digital transformation by delivering solutions that solve today's most complex networking and communication challenges.

To learn more about DDoS Mitigation Services, visit windstreamenterprise.com

WINDSTREAM ENTERPRISE

CONNECT. TRANSFORM. ELEVATE.