Byline – Submitted to Cloud Computing Journal

May 23, 2019

DDoS Managed Security Services Create Benefits and New Revenue Opportunities for Hosting Providers

By Dave Larson, COO, Corero Network Security

Hosting providers are often judged by their ability to ensure network availability/uptime. Unfortunately, distributed denial of service (DDoS) easily impact service availability and, in some instances, completely take down a hosting platform. As DDoS attacks continue to increase in size and frequency, hosting providers have more difficulty ensuring uptime.

Hosting providers are favored targets because the number of customers they service and the aggregate Internet peering bandwidth they utilize greatly increases their attack surface. Unfortunately, a DDoS attack on a single customer—such as a high-traffic gaming service—can create major collateral damage to other hosted customers. These innocent bystanders are placed in the unfortunate situation of suffering from second-hand damage because they are hosted on the same shared facilities as the intended victim. Unplanned server outages are often devastating, for both the hosting provider and their customers.

Hosting providers are under intense pressure to prevent DDoS attacks from infiltrating their networks for several reasons:

1. Network downtime equates to unhappy customers who may cancel their subscription, and/or loss of reputation in the marketplace, both of which lead to lost revenue;
2. Their customers expect them to provide "clean pipe." Hosting providers are the conduit of Internet connectivity for many businesses, therefore many customers believe that providers have an obligation to adequately protect them from DDoS attacks;
3. It costs money and personnel time to monitor a network and recover from the damage of attacks.

Past Solutions

In the past hosting providers had two choices in handling a DDoS attack: either "black hole" the bad traffic or swing it out to a scrubbing center for cleaning. Neither is ideal. Black holing involves having a carrier black-hole the IP address of the DDoS victim, so that all traffic destined for that IP address is discarded by upstream peers. This protects everyone else on the carrier infrastructure, but it shuts down the customer entirely. In effect, this represents a perfect denial of service, so it's not at all a true mitigation solution. Intentionally taking companies' services offline is a poor way to treat customers, and it damages a hosting provider's reputation of providing good service.

The alternative, a DDoS scrubbing center, involves "swinging out" infected (bad) traffic out to a DDoS scrubbing center, for cleaning and rerouting. This approach tends to be much too expensive for the majority of hosting providers.

Even if a hosting provider can afford a scrubbing center, it's not 100% effective. Low-threshold, shorter-duration, multi-vector, highly effective, quick DDoS strikes are on the rise, and it is these types of attacks

that often go un-noticed by IT security staff. According to our research, the vast majority of DDoS attacks experienced by Corero customers are less than 1Gbps in size. More than 95 percent of these attacks lasted 30 minutes or less. As attackers look for new ways to leverage DDoS attacks, they have realized that short duration sub-saturating attacks are more difficult to defeat because they evade traditional cloud-based scrubbing centers. By the time on-demand scrubbing defenses are engaged, the damage has been done: security has been compromised, and/or the network performance has degraded.

New Solutions, New Revenues

Emerging DDoS mitigation techniques have evolved to provide automated threat detection and mitigation, distributed across the network and capable of identifying and managing potential attacks *before* they cause disruption. Providers can now deploy their DDoS mitigation operations at peering or transit points, using technology that is scalable and responsive. These systems are automated, always on, and capable of responding to attacks in real time – eliminating DDoS headaches for hosting providers and their customers.

This new technology not only optimizes network performance and availability; it also presents a potential new revenue stream for hosting providers. It's possible to design policies uniquely for customers and ensure that they get only good traffic flowing through their pipes. Several Corero hosting provider customers incorporate DDoS mitigation into their service offerings to their customer base. They usually label their anti-DDoS service as a premium service, recouping their investments within a couple of months.

Hosting subscribers are demanding more—and are willing to pay for it. In Corero's 2016 survey of network and IT professionals in enterprise organizations, a majority (74%) clearly indicated that they would like to have extra protection and services dedicated to keeping their pipes clean and defended against DDoS attacks. Fifty-two percent indicated that they would even pay for a premium service that eliminates the DDoS challenge to their environment.

Proactive hosting providers have an opportunity to leverage this sentiment and incorporate premium DDoS managed security services into their customer contracts. By doing so, they differentiate themselves from their competition, generate new revenue streams, and improve customer experience and customer loyalty. With these benefits, hosting providers quickly realize a return on their investment in DDoS protection technology.

Bio for Dave Larson, Chief Operating Officer, Corero

Dave Larson, Chief Operating Officer is responsible for directing the Corero technology strategy as the company continues to invest in its next phase of growth; providing next generation DDoS attack and cyber threat defense solutions for the Service Provider and Hosting Provider segments. Larson brings over 20 years of experience in the network security, data communication, and data center infrastructure industries. Most recently, Larson served as Chief Technology Officer for HP Networking and Vice President of the HP Networking Advanced Technology Group. In this role he was responsible for creating the long-term technology vision and strategy for HP Networking across a variety of product divisions and geographies.

Larson was instrumental in establishing HP's leadership in SDN including driving the creation of the OpenDaylight open-source SDN controller initiative as one of the founding executive sponsors of

that consortium, along with technology leaders that included Cisco, IBM, NEC, Citrix and the Linux Foundation. Under Larson's leadership, HP created the category for SDN security applications for enterprises as evidenced by the HP Network Protector SDN Application, which combines IP-reputation DNS security with HP's Virtual Application Networks SDN Controller to deliver botnet command-and-control and malware mitigation at the first touch point in the Ethernet access layer. Prior to that, he served as Chief Technologist for security and routing, and was a senior member of the Advanced Technology Group within HP Networking.

Prior to HP, Larson was Vice-President of Integrated Product Strategy for TippingPoint, where he was instrumental in transitioning the business to develop a line of Next-Generation Firewalls and vice-president of Security Product Line Management for 3Com Corporation where he defined global security products strategy across R&D development facilities in the U.S., U.K., and China.

Larson has also held senior marketing and product roles with Tizor Systems, Sandburst Corporation and Xedia Corporation. He has a Bachelor of Science degree in Physics from Gordon College in Wenham, Mass.