DDoS IMPACT AND OPPORTUNITY IN THE SERVICE PROVIDER ENVIRONMENT

corero
FIRST LINE OF DEFENSE

A Distributed Denial of Service (DDoS) attack is an organized attempt to take your business's online service offline by overwhelming it with traffic from multiple sources. Malicious users generate floods of traffic through botnets and other means to blast a given target. In a typical scenario, a botnet might flood your server with more connection requests than it can handle, or send the target huge amounts of random data to devour your bandwidth. Another malicious variation is the difficult-to-detect application-layer (Layer 7) Low and Slow DDoS attack, which avoids detection by sending seemingly legitimate packets at a low rate or a slow speed—and eventually exhausting your resources or rendering your services unavailable.

DDoS attacks can zero in on all kinds of important resources (e.g., your website, your email, your network, your security perimeter). These attacks pose major challenges to businesses of all types—but particularly to Internet and hosting providers, which can suffer blows to bandwidth, reputation, and bottom line.

DDoS ATTACKS POSE MAJOR CHALLENGES TO BUSINESSES OF ALL TYPES—BUT PARTICULARLY TO INTERNET AND HOSTING PROVIDERS, WHICH CAN SUFFER BLOWS TO BANDWIDTH, REPUTATION, AND BOTTOM LINE.

Unfortunately, DDoS attacks are becoming more common and more intelligent, and as such, they are one of the top security and availability threats you will face. Service providers facilitate a larger attack surface, and it's only a matter of time before your company's online presence becomes a DDoS victim. A DDoS mitigation and defense plan is clearly key to your successful security strategy. The question you need to ask yourself is whether you want to be in a position where you're responding to attacks that have already happened—or are prepared for the inevitable future attack.

Corero conducted a survey of Internet service providers, hosting providers, telecommunications companies, and cable operators to understand their needs and begin formulating a value proposition for how those providers might not only derive a security benefit from deploying DDoS protection in their environment but also use that protection as a revenue stream for selling to its customers. Corero sees a great opportunity in providing a sophisticated threat response to users as part of an enterprise-grade solution that will open up important new revenue streams while maintaining customer loyalty.

This survey had involvement from providers serving other service providers (68 percent), enterprises (60 percent) and public-sector organizations (47 percent), in the data center and online services realm (30 percent), as well as cloud providers (15 percent). Respondent service providers offer such services as Voice over IP (VoIP) and Unified Communications (UC), transit, hosting services, public and private cloud services, and E-Line and E-LAN functionality.

INCREASING BANDWIDTH AND LINK SIZES

One of the primary ways a DDoS attack can compromise your infrastructure is by flooding your bandwidth, essentially jamming your organization's Internet connections and forcing legitimate users out. Bandwidth attacks can be devastating, and as a company's bandwidth increases, so does the size of the attack surface. The more bandwidth you have as a service provider, the more bandwidth is available for funneling attacks into the network and toward customers. Similarly, as providers expand, add, or increase the size of their links, the DDoS threat expands.

Asked about what total connected Internet bandwidth they anticipated in their environment, a majority of survey respondents pointed to increasing levels. A third of survey respondents expected that they would need more than 40–100Gbps of bandwidth, and 20 percent expected that they would require more than 100Gbps. That's a full 54 percent of respondents who anticipate more than 40Gbps total connected Internet bandwidth—some of them, much more. In addition, most of the

surveyed companies (63 percent) expected to increase the size of their links in the next 6 to 12 months.

THE IMPORTANCE OF DDoS PROTECTION

Corero recently conducted a **survey** at the U.S. RSA Conference 2016 in which it asked enterprise respondents whether DDoS attacks were having a direct impact on their bottom line. At the time, 35 percent of respondents indicated that DDoS attacks had led to lost revenues, and 45 percent indicated that loss of customer confidence was the most damaging effect to their business, as a result of DDoS. When enterprise respondents were asked if they agree that upstream Internet service providers should offer additional security services to their subscribers, the overwhelming answer was yes—at close to 90 percent.

On the flip side, in this particular survey—aimed at Internet service providers, carriers, and the like—Corero asked respondents to rate the importance of DDoS defenses in relation to other types of security for their customers, and an overwhelming number (83 percent) said DDoS protection was equally important or more important. More than half of respondents (51 percent) said it was more important.

Clearly, enterprises are demanding more protection, and Internet service provider are motivated to deliver DDoS protection, but are they getting the most out of their current methodologies?

CURRENT METHODS

There are many options available for mitigating DDoS attacks—from simple in-house server configurations to advanced data center–based hardware solutions. Most service providers use one (or a combination) of several common approaches:

- ***BLACKHOLE ROUTING.*** Blackhole routing involves creating an IP traffic route that goes nowhere. Also known as null routing, blackhole routing focuses on DDoS attacks that attempt to exhaust the target's Internet uplink capacity. In this scenario, the uplink operator discards all traffic to the victim's IP address, thus freeing the uplink channel. Blackhole routing is available on most commercially available routers.
- ***SCRUBBING CENTER.*** A scrubbing center is a service that processes incoming traffic, identifies threats based on a traffic characteristics and attack styles, and then removes the threat. Clean ("scrubbed") traffic returns to the network without any impact to your business.
- ***IN-HOUSE SECURITY/SUPPORT.*** Some in-house security departments have the foresight and intelligence to keep on top of the security community—and even work closely with the botnet hunter community—to control their environments. This team might even have special equipment to stop or lessen the impact of an attack.

Nearly half of our survey respondents use the blackhole routing method (49 percent), 46 percent direct traffic through a scrubbing center (46 percent), and 37 percent call on security/support staff to handle the events.

The survey concluded that most companies surveyed are using a variety of solutions to handle the DDoS threat—possibly solutions from multiple vendors, with varying degrees of efficacy. Many of these companies would do well to avoid the hassles of a pieced-together, reactive approach and investigate the potential of an inline, automatic mitigation solution.

IDEAL FEATURES

We asked respondents about the features they deem essential in a DDoS mitigation solution. The common features we asked about included the following:

- Ability to maintain bandwidth/throughput
- Ability to handle high-volume, indiscriminate attacks
- Ability to handle attacks aimed at disrupting specific applications
- Ability to handle other non-DDoS network attacks
- Ability to provide reporting and visibility into attack types and mitigation that was utilized
- Low false positive blocking rate
- Little to no human intervention required

In a surprising development, all features ranked somewhat evenly, suggesting that—given varying

needs and environmental idiosyncrasies—most of these features are important. The ability to maintain bandwidth/throughput barely received the most "must-have" votes, followed by the ability to handle high-volume, indiscriminate attacks and the ability to handle attacks aimed at disrupting specific applications. The next tier of important features included the ability to handle other non-DDoS traffic, the ability to provide reporting and visibility into attack types and mitigation that was utilized, a low false positive blocking rate, and an ability to handle encrypted attacks.

FOR PROVIDERS, THERE IS A GREAT OPPORTUNITY IN PROVIDING A SOPHISTICATED DDoS THREAT RESPONSE TO USERS AS PART OF A SOLUTION THAT WILL OPEN UP IMPORTANT REVENUE STREAMS WHILE MAINTAINING CUSTOMER LOYALTY.

Clearly, service providers' DDoS needs cover a wide variety of concerns. Unfortunately, traditional tools in this market address only a handful of these needs—certainly not all of them. They might tackle a specific feature very well but leave out important ancillary functionality. Rarely are customers going to find a single security solution that addresses all the aforementioned "must-have" features.

BARRIERS AND OPPORTUNITIES

Some providers have been reluctant to begin offering DDoS protection services (for a fee) for their customers. In our survey, the most common "top reason" for not providing this protection (at 27 percent) is the belief that customers simply expect DDoS protection to be part of their overall investment and would balk at paying a fee. That point of view is understandable, but it's important to consider the level of protection those customers are receiving with their current solution. It is probably not a comprehensive, automatic, inline solution, and those customers are probably experiencing a certain amount of downtime or latency before their provider can actually fix the problem.

A smaller segment of respondents suggested that they aren't concerned with the impact of DDoS attacks. And yet according to the results of **a Kaspersky Lab and B2B International study in 2014**, "DDoS attacks cost small-to-medium-sized businesses (SMBs) an average of $52,000 per incident; for larger enterprises, the cost of a DDoS attack is even more significant, resulting in an average of $444,000 in lost business and IT spending." For many organizations, such expenses can have a devastating financial impact and do great harm to reputation.

Considering the increasing alarm with which the industry acknowledges the impact of DDoS attacks, more and more providers are sure to become concerned soon.

As a provider, your ability to maintain service availability during and after a DDoS attack is extremely important to maintaining your reputation as a business, as well as keeping (and gaining) customers. When a customer struggles with latency issues that harm the user experience or is blocked from accessing your applications because your network is overwhelmed, you are experiencing a blatant impact to your bottom line.

Considering these realities, we asked respondents to rate the business opportunity behind offering DDoS protection services to customers, and more than 80 percent saw either a modest or significant opportunity.

CONCLUSION

Service providers identified a number of factors preventing them from investing in an automatic, inline mitigation solution. Foremost was cost (62 percent), followed by lack of experience with such solutions

(57 percent), a preference for human intervention (42 percent), and vendor lock-in with an existing solution (39 percent). Considering the very real (and very high) price of not investing in a comprehensive solution to mitigate devastating DDoS attacks, these factors become small.

As a service provider, you need your services to be available to consumers at all times. You don't have time to be reactive to the latest security threats—particularly DDoS attacks. Effective DDoS mitigation can not only eliminate or minimize downtime from a DDoS attack, it can keep you prepared. A proactive stance against these kinds of security threats could save you lost revenue and help protect your business's reputation. By providing DDoS protection as an essential part of your services, you also enhance your revenue potential to security-minded customers.

Service providers and end users alike can benefit from the clear advantages of a comprehensive, real-time, automatic DDoS protection service. Considering the results of the survey—which highlighted the significance of providing strong DDoS protection and gave equal weight to many "must-have" features in such a solution—the time is right for the type of appliance-based DDoS mitigation that the Corero SmartWall Threat Defense System provides. This complete solution provides all the aforementioned "must-have" features from a single interface.

ENTERPRISES ARE DEMANDING MORE PROTECTION, AND INTERNET SERVICE PROVIDERS ARE MOTIVATED TO DELIVER DDoS PROTECTION, BUT ARE THEY GETTING THE MOST OUT OF THEIR CURRENT METHODOLOGIES?

Corero SmartWall protects Internet and hosting providers from DDoS attacks in the cybersecurity space. The appliance sits at the network edge in your environment, monitoring and mitigating DDoS attack traffic in real time. The solution does not pull attack traffic deeper into the network to a scrubbing center environment, does not rely on human intervention, and does not rely on legacy tools or techniques that some network and security departments use to eliminate DDoS attacks. Rather, it prevents a wide range of DDoS attacks while maintaining full connectivity and avoiding the disruption of legitimate traffic.