IDC
Analyze the Future

I D C A N A L Y S T C O N N E C T I O N

John Grady
Program Manager, Security Products and Services

A Defense-in-Depth Approach to DDoS Prevention

May 2014

In recent years, high-profile attacks on the world's leading financial firms thrust denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks back into the headlines. According to research from IDC, the worldwide market for DDoS prevention solutions will grow by a compound annual growth rate (CAGR) of 18.2% and is forecast to reach $870 million by 2017. Volumetric attacks will continue to be the predominant attack type for the foreseeable future because of the relative ease with which botnets can send a bandwidth or packet flood in excess of what most enterprise infrastructures can handle. In addition, IDC expects to see an increase in the more advanced hybrid attacks that include application layer and encrypted traffic. As a result, DDoS attacks are now a mainstream security problem, and organizations must have a proven mitigation plan in place and a service provider they trust when an attack occurs.

The following questions were posed by Neustar to John Grady, program manager of IDC's Security Products and Services practice, on behalf of Neustar's customers.

Q. What should we know about DDoS attacks?

A. DDoS attacks are on the rise and confound traditional security. Attacks are occurring across all industries, although the most common targets remain financial services, ecommerce, online gaming, and cloud services. Additionally, energy, higher education, and media-focused organizations have all been victimized by DDoS attacks over the past 18 months. Typically, the goal of a DDoS attack is to starve network or application resources, thus impacting business processes or Web site availability. DDoS attacks can last from days to weeks and even months, leading to lost revenues, exorbitant expense, and diminished customer trust. Alternatively, DDoS attacks can be used as a diversionary tactic to draw attention away from an ulterior motive. For example, while IT and security staffs are busy trying to deflect DDoS attacks, hackers may be working to gain access to customer financial data, passwords, or intellectual property. One notable example of this strategy was a Christmas Eve DDoS attack against California's Bank of the West. Simultaneously, $900,000 was removed from the account of Ascent Builders.

Q. What is the difference between a volumetric attack and an application attack?

A. DDoS attacks are not new, but they have evolved over the years. Originally, attacks focused on Layers 3 and 4 via UDP floods, ping floods, or some other method that causes the network connection of the target to become saturated. Layers 3 and 4 remain the most common attack target today. That being said, attacks targeting Layer 7 Web applications (through HTTP Get or Post requests, for example) are on the rise. These application-focused

attacks are often harder to detect; resources may remain available, but they run incredibly slow. Similarly, attacks leveraging encrypted SSL connections can be difficult to detect without dedicated solutions designed to decrypt and analyze SSL traffic. Compared with volumetric and application-based attacks, SSL-oriented threats remain relatively low, but they are increasing. Most DDoS attacks use at least two of the three methods described previously, changing vectors repeatedly over the course of an attack. In part because of this, IDC suggests a hybrid approach that leverages both cloud and on-premise mitigation solutions to protect against all threat vectors.

Q. What exactly is a hybrid solution?

A. Hybrid solutions are the combination of on-premise mitigation and cloud-based scrubbing. Volumetric, high packet-per-second attacks can quickly overwhelm on-premise devices, and when the bandwidth of the Internet connection becomes the bottleneck, these devices are unreachable and thus useless. For these massive attacks, traffic needs to be diverted to the cloud for scrubbing before it ever enters the network, with only clean traffic being relayed back to the targeted organization. In the hybrid scenario, application layer attacks, and small volumetric attacks that do not saturate the Internet connection, are mitigated on-premise, where more granular visibility is possible. In true hybrid solutions, there is deep integration between on-premise equipment and the cloud, allowing attack details to be passed back and forth to aid in remediation.

Q. What are some key things to look for in a DDoS provider?

A. To begin with, the ability to both detect and mitigate is an important component of a DDoS solution. A number of products and services still focus on one or the other, but providers that have the capability to do both are generally better to consider. Another key component to consider when comparing DDoS providers is flexibility. Attacks have become larger and more dynamic, leveraging a number of methods to starve target resources. Providers of the hybrid solutions described previously can offer customers more targeted and in-depth protection compared with single solution providers, in whatever deployment works best for the customer.

When thinking about cloud providers specifically, customers should look for a company that has traffic scrubbing centers around the globe with significant mitigation capacity to reduce latency issues when diverting traffic. Publicly available statistics cite peak attack rates that are quite large. The ability to block attack volumes of a large size is critical to ensuring Web site availability. Outside of scale, buyers will benefit from a DDoS provider that has experience and skill in mitigating complex application layer attacks, including encrypted attacks. Another important consideration is support, relative to not only attack mitigation but also onboarding and testing. Ensuring that BGP redirection announcements are properly configured and false positives are nullified before an attack will help ensure a smoother mitigation process once an attack is actually under way. Finally, it is important to look at the pricing model of prospective providers. Many providers offer tiered plans, so understanding your organization's attack history can help in selecting the best fit and ensuring that overage charges (if any) are kept to a minimum.

ABOUT THIS ANALYST

John Grady is a program manager for IDC's Security Products and Services research practice. In this role, Mr. Grady conducts primary research on the network security market in order to develop accurate forecasts and insightful analysis for clients. His main areas of focus include firewall, VPN, intrusion detection and prevention, and unified threat management technologies. Additionally, Mr. Grady is responsible for the accurate and timely delivery of IDC's Worldwide Quarterly Security Appliance Tracker, which provides clients with valuable geographic, product line, and vendor market share data across the hardware segments of the network, Web, and messaging security markets.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com