IDC
Analyze the Future

IDC ANALYST CONNECTION

John Grady
Research Manager, Security Products and Services

DDoS Prevention: Time for "Defense in Depth"

April 2014

In 2013, IDC saw a sharp increase in distributed denial-of-service (DDoS) attacks in terms of frequency, bandwidth volume, and application orientation. With attacks on the rise, organizations need to be aware of, and protect their infrastructure from, the advanced methods used by today's DDoS attackers. According to IDC, the worldwide market for DDoS prevention solutions will grow by a compound annual growth rate (CAGR) of 18.2% from 2012 through 2017 and reach $870 million. Based on findings from a recent end-user survey, IDC expects that demand for fully managed DDoS solutions will increase roughly 24% in 2014.

The following questions were posed by Fortinet to John Grady, research manager with IDC's Security Products and Services group, on behalf of Fortinet's customers.

Q. What are the most prevalent trends in DDoS attacks today, and what should datacenter managers be on the lookout for in the years ahead?

A. DDoS attacks have been around for over a decade, though the motivations and methods have changed. Typically, the goal of a DDoS attack is to starve network or application resources, thus impacting business processes or Web site availability. 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 a DDoS attack, hackers may be working to gain access to customer financial data, passwords, or intellectual property. DDoS attacks can last days, weeks, and even months, causing lost revenue, exorbitant expense, and diminished customer trust.

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. Recently, attacks leveraging holes in DNS security have been able to create massive amounts of traffic. In the future, we expect a continued increase in attacks focusing on the application layer as well as a rise in attacks targeting SSL — both targeting the protocol itself as a tactic to starve resources and using encrypted traffic to bypass defenses.

Q. Who are the primary attack targets in the latest threats, and what additional risks are there for these organizations?

A. Originally, many targets were online gaming and gambling organizations, with attackers holding sites ransom until a specified sum was paid. With the rise of Anonymous in 2010, "hacktivism" became the prevalent motivation — that is, more ideologically oriented. Recently, however, state-sponsored attacks aimed at financial institutions, as well as a return to DDoS under the threat of extortion, have become common.

Basically, attacks are now 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.

DDoS attacks are in the news so often because they are comparatively "loud" and very impactful to customers. Targeted stealth attacks are where hackers try to gain a foothold in an organization and exfiltrate data without being detected — oftentimes compromising an organization's security for months or years without anyone knowing. But with DDoS attacks, the results are known and felt immediately. Customers are unable to access an organization's Web site or applications and are impacted along with the organization. Ultimately, organizations risk lost revenue, lost customers, and lost brand equity as a result of DDoS attacks.

Q. What recommendations would you make to a datacenter manager to protect against DDoS attacks today and in the future?

A. Dedicated, on-premise solutions are a key component of DDoS defense. This type of defense provides dedicated resources aimed at protecting other components of the infrastructure (e.g., routers, firewalls, IPS) from becoming overwhelmed by malicious traffic. Further, dedicated DDoS solutions are able to dig deeper into traffic dynamics to detect machine-generated requests and correlate source requests with resource responses to detect and mitigate Layer 7 attacks while limiting false positives.

Layers 3 and 4 remain the most common attack targets today, but 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 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.

Q. Based on your experience with DDoS attack mitigation platforms, what are the pros and cons of signature-based and behavior-based methods of attack detection?

A. Signature-based defenses are strong at detecting known attack methods quickly and efficiently. They are able to run inline and immediately detect and drop or clean malicious traffic when an attack starts. However, when a new attack method arises, or an attack uses legitimate traffic for malicious purposes, signature-based defenses may not detect the attack. Behavior-based solutions solve this problem by digging deeper into the types of traffic and how resources react to requests and correlating with threat intelligence feeds and other sources to determine if traffic is malicious or not, regardless of whether it appears legitimate or is the result of a zero-day exploit.

Historically, the downside of solutions using these methods is that they often had to be deployed out of band to reduce latency issues. Additionally, false positives were a potential issue. However, advances in hardware technology have addressed the latency issue, and the impact of big data analytics on threat intelligence feeds has helped reduce the issues around false positives, making behavior-based solutions more viable and, in many cases, a more desirable option.

Q. How concerned should a datacenter manager be about the risk of false-positive attack detections, and what can be done to minimize the impacts they cause to legitimate users?

A. In general, false positives are a key concern for IT administrators. Historically, Web application firewalls have been used only in detection mode because the risk of false positives was deemed too high by datacenter managers. The problem DDoS attacks present is an interruption in service to customers — both internal and external. If a DDoS prevention solution regularly alerts to false positives or, worse, blocks legitimate users from accessing the resource they're attempting to reach, the result for those users is the same as if the organization were under a DDoS attack. All the perception, brand equity, and lost revenue issues detailed previously arise, albeit on a smaller basis.

As mentioned previously, a strong intelligence feed is one way to reduce false positives. Solutions that continually monitor for known bad IP addresses allow more resources to be deployed to analyze questionable IPs and to dig deeper before actually blocking the traffic. Further, solutions that leverage bidirectional data feeds to continually improve their intelligence in real time through a closed-loop feedback model have a significant advantage in ensuring that only malicious traffic is blocked.

ABOUT THIS ANALYST

John Grady is a research manager with IDC's Security Products and Services group. In this role, Mr. Grady conducts primary research on the network security market 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.