IDC VENDOR SPOTLIGHT

DDoS Attacks: The Need for Mitigation Services

March 2014

Adapted from *Worldwide DDoS Prevention Products and Services 2013–2017 Forecast* by John Grady, Christian A. Christiansen, Curtis Price, and Christina Richmond, IDC #239954

Sponsored by Neustar

While much of the focus in the security market centers on newer threats from emerging technologies such as cloud, mobility, and targeted malware, a decade-old issue is seeing renewed attention in recent months. 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 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 the next year.

This Technology Spotlight explores the trends affecting DDoS security and discusses the role that Neustar plays in the increasingly important market for DDoS solutions.

Introduction

The methods and motivations behind denial-of-service (DoS) and DDoS attacks have evolved noticeably over the course of the past decade. Originally, DDoS attacks centered more on brute force tactics, with little focus on stealth or circumventing defenses. An attacker would gain control of a system with an abundance of bandwidth and use it to quickly starve the target of network resources through ping floods, fragmented ICMP packets, or other methods. As attack exploits evolved and resources became more distributed, motivations changed as well. The threat of extortion became more prevalent, especially toward gaming, gambling, or other targets with less reputable business models.

DDoS attacks were thrust back into the mainstream consciousness in recent years by high-profile attacks on the world's leading financial firms. These attacks reinforced the fact that any business is vulnerable to a DoS attack, with potential impact on both revenue and brand equity. Further, these recent instances highlighted the newest type of attack in which DDoS is used as a diversionary tactic while advanced malware and vulnerability exploitation simultaneously target sites for financial information and intellectual property. Among the trends that IDC has identified are the following:

- Volumetric attacks will continue as the dominant type of DDoS attacks because botnets can easily send a bandwidth flood in excess of what most enterprise infrastructures can handle.
- Despite the popularity of volumetric-based attacks, growth in more advanced hybrid attacks, including application layer and encrypted traffic in addition to volumetric methods, will help drive growth in the on-premise equipment market.

- Hybrid defense scenarios (on-premise equipment married with cloud services) will become more prevalent as organizations seek to defend against all vectors of DDoS attacks and solution providers and product vendors work more closely to deliver joint solutions.

The capabilities inherent in firewalls, intrusion prevention system (IPS) appliances, and other devices may be helpful for very basic attacks or additional intelligence. In reality, however, these security devices can become targets themselves because they are unable to recognize seemingly legitimate traffic that is actually part of a flood attack.

Benefits of Mitigation

Three mitigation solutions are available today to help organizations defend against DDoS attacks:

- **On-premise.** Technically, many on-premise devices offer DoS protection, including routers and switches, intrusion prevention systems, and firewalls. These products typically lose the ability to adequately mitigate a DoS attack when it is over 1Gbps or occurs at the application layer. Some organizations still rely heavily on these built-in defenses. In addition, purpose-built, standalone solutions are sold directly to enterprises, governments, and telecommunication (telco) and service providers to protect their own infrastructures from attack.
- **Cloud.** Equipment is sold to telcos and cloud providers that in turn build a mitigation services offering that can be sold to enterprises and governments. These cloud-based services provide monitoring and mitigation via the providers' security operations center (SOC) and scrubbing centers. Another branch of cloud DDoS service is one in which the solution is part of another offering, such as content delivery; this solution is always on and inline, automatically diverting tainted traffic — once detected — away from the end customer's network.
- **Hybrid.** A number of end-user organizations are now considering a combination of on-premise and cloud defenses. In this option, the service provider manages the client's on-premise equipment while incorporating additional management and mitigation from its SOC and scrubbing centers.

"Defense in Depth" Protection

A true hybrid solution combines an on-premise appliance, which provides protection against smaller volumetric attacks and application layer attacks, with cloud defenses. The level of visibility and quick response offered by being on-premise is arguably much higher, especially in relation to the application layer traffic. That said, large-scale volumetric attacks can quickly overwhelm an enterprise network, and it is costly and unreasonable for an organization to consider perpetually increasing its bandwidth. In the event of such large-scale attacks, the cloud solution is able to divert the traffic into a scrubbing center before rerouting back to the customer network. The on-premise solution provides valuable information about the attack dynamics that the cloud provider can then use to more efficiently clean the traffic.

True joint solutions have historically not been common, but with the increased diversity of attacks, IDC sees this situation starting to change. Managed services provide additional resources and intelligence during an attack, and mitigation is increasingly moving to on-premise and/or in the cloud.

Both cloud and hybrid solutions must always be inline and on and able to automatically divert attack traffic (as in the case of a content delivery network provider) or able to provide both BGP and DNS routing.

Key Considerations

Dedicated solutions that can correlate traffic across sessions and can detect and mitigate application layer attacks are necessary to adequately prevent DDoS attacks. Any organization with a sizable online presence should consider adding dedicated DDoS protection if it has not already done so, especially if it has customer data, intellectual property, or financial assets to protect. All of these are key targets.

When determining whether to add DDoS protection capabilities, organizations need to consider not only the actual revenue impact that a loss of service would entail but also the impact on customers and on the brand itself. Studies by DDoS mitigation experts place the cost of a DDoS attack somewhere between $10,000 and $50,000 an hour. This can add up quickly to over $1 million a day in some cases. Both large and small companies are equally at risk.

It is worth noting that the company immediately under attack may not be the target; rather, it may be the conduit to the ultimate target. For example, a year and a half ago, a heist targeted a small construction company to steal money from a regional bank. Although the construction company was not the target of theft, it still was negatively affected — damage to brand reputation is the hardest to quantify, and the impact may not be immediately felt.

Organizations that decide to prioritize DDoS defense would be well served to make it an itemized part of the security budget rather than draw from another area (such as IPS). The decision on how to implement a prevention solution should be guided by the business impact determination along with resources and budget. Administrative requirements are also a factor. These requirements differ among on-premise solutions, content, and cloud solutions. For organizations that cannot commit the additional staffing resources, many providers offer additional managed services to help configure defenses and mitigate attacks in real time.

The best solution, when resources permit, is often a combination of on-premise appliance and cloud service. With a combination approach, on-premise appliances offer the ability to detect and mitigate smaller application layer attacks, while cloud-based mitigation can take over for larger more sophisticated attacks if the on-premise solution is overrun or the customer bandwidth is overwhelmed. For example, even if the on-premise solution provides 10Gbps of scrubbing capability, the customer bandwidth may not be able to keep up, in which case diverting to a cloud scrubbing center would be critical.

Considering Neustar

Neustar SiteProtect is available both as a standalone DDoS mitigation solution and as a managed service. It provides carrier-grade cloud-based and premise-based DDoS mitigation that utilizes a blend of partner mitigation technologies alongside Neustar's 24 x 7 Security Operations Center team. In addition, Neustar has scrubbing centers in globally distributed locations. SiteProtect allows customers to maintain control with on-demand DNS or BGP deployments or as a hybrid solution (on-premise mitigation equipment + cloud DDoS capability) that is fully or partially managed depending on customer choice. SiteProtect is designed to stop numerous types of attacks, including those involving Layer 3 (network), Layer 4 (transport), Layer 7 (application), IPv6, and encrypted traffic. In addition, the company offers DNS protection, which it sees as invaluable in tandem with DDoS mitigation. SiteProtect is always on and always inline.

Challenges

Given the dynamic nature and increasing sophistication of DDoS attacks, providers of anti-DDoS products and services should continue to expand partnering relationships to address the evolving nature of attacks. At the very least, the coordination and communication between on-premise devices

and cloud services should continue to improve, even if the hybrid solution scenario is not formalized. Neustar offers an advanced hybrid solution and is one of only a few DDoS mitigation experts that offer it as a fully managed hybrid solution. The company can expect that DDoS attacks will evolve and that mitigation service providers will continue to enhance their offerings in the managed hybrid DDoS arena.

Conclusion

IDC expects the market for DDoS mitigation solutions to continue to see robust growth. With businesses becoming only more dependent on hosted services and online transactions, protecting infrastructure (whether onsite or offsite) from DoS attacks will remain a high priority for organizations. If Neustar can continue to address the challenges highlighted in this paper, IDC believes the company has a significant opportunity to succeed in the important market for DDoS mitigation products and services.
