

March 13, 2015

The Expanding Role of Service Providers in DDoS Mitigation

Stratecast Analysis by
Chris Rodriguez



**Stratecast Perspectives and Insight
for Executives (SPIE)**

Volume 15, Number 10

The Expanding Role of Service Providers in DDoS Mitigation

Introduction¹

Cyber security awareness is at all-time highs in the wake of record-breaking data breaches, cyber espionage, cyber warfare, and sophisticated threats. While threats to data confidentiality and network integrity remain a top-of-mind concern, businesses are reminded daily of the importance of protecting availability as well.

Distributed denial-of-service (DDoS) is a type of attack that leverages the massive stolen computing power provided by infected endpoints to flood targets with traffic. The goal of a DDoS attack is to disrupt the online operations of a target organization by consuming available network bandwidth or server resources. Attack success is determined by the lack of available computing resources for legitimate end users.

Businesses that rely heavily on an Internet presence, such as e-commerce, online gaming, and financial services, are the most common targets. The attacker profile is expanding rapidly as nation-states, criminal organizations, and hacker activist groups are utilizing or commissioning others to launch DDoS attacks against selected targets. Cyber criminals develop, maintain, and rent out a botnet (the network of infected computers controlled remotely by hackers) to mount DDoS attacks against selected targets, for as little as \$10 an hour, according to Verizon's 2014 Data Breach Investigations Report.²

In 2014, DDoS attacks reached record levels both in terms of scale and frequency. The largest single reported DDoS attack targeted CloudFlare, and reached a peak of 400 Gbps. According to Arbor Networks research, the largest attacks (over 100 Gbps) were reported four times as often in 2014 as compared to 2013.³ Furthermore, Neustar found that "nearly twice as many companies (60%) reported being attacked in 2013."⁴

DDoS mitigation is a problem not only for enterprise networks but also for service providers that enable their Internet access. DDoS attacks can degrade or cause loss of service, and increase bandwidth consumption in the network. Service providers also play an important factor in the DDoS mitigation process. This SPIE examines the role, capabilities, and advantages of service providers in the DDoS mitigation process, as well as how this role might develop in the future.

¹ In preparing this report, Stratecast conducted interviews with representatives of the following companies:

- Allot Communications – Yaniv Sulkes, AVP of Product Marketing
- Arbor Networks – Rakesh Shah, Sr. Director of Product Marketing and Strategy
- Level 3 Communications – Chris Richter, SVP of Managed Security Services

Please note that the insights and opinions expressed in this assessment are those of Stratecast and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

² *Data Breach Investigations Report*, Verizon, 2014 <http://www.verizonenterprise.com/DBIR/>

³ *Worldwide Infrastructure Security Report (WISR)*, Arbor Networks, 2015, <http://www.arbornetworks.com/resources/infrastructure-security-report>

⁴ *Annual DDoS Attacks and Impact Report*, Neustar, 2014, <http://www.neustar.biz/resources/whitepapers/DDoS-protection/2014-annual-DDoS-attacks-and-impact-report.pdf>

The Need for Intelligent DDoS Mitigation Solutions in the Enterprise

Intelligent DDoS mitigation solutions are designed to protect against multiple types of DDoS attacks such as:

- **Volumetric attacks** – These attacks operate by sending more connection requests (such as transmission control protocol (TCP) synchronize or SYN messages) than can be processed by the target.
- **Application layer attacks** – A common type of application layer attack uses HTTP GET or HTTP POST requests to overwhelm a Web server. HTTP GET requests retrieve static content from Web servers, and so are easy to craft. HTTP POST requests retrieve more dynamic content, and can be used to tie up processing power or generate large responses.
- **Reflection and amplification attacks** – These attacks target and exploit network protocols such as domain name system (DNS), character generation (CHARGEN) and network time protocol (NTP). Amplification attacks generate large responses from small requests; and reflection attacks use spoofing to direct unwanted responses to a target IP address.
- **Stealthy attacks** such as Slowloris. Slowloris is designed to exhaust the resources of targeted Web servers by sending partial HTTP requests at regularly timed intervals to keep connections open as long as possible. Eventually, all connections are blocked for legitimate users. The result is a stealthy, low bandwidth attack that disables a specific Web server in a way that avoids triggering volumetric-based detection mechanisms. Slowloris is but one example of the sophisticated, precise, and stealthy DDoS attacks that challenge traditional means of DDoS mitigation.

As a result of the mix of attack types being used in DDoS attack “campaigns,” and the building preponderance of targeted stealthy attacks, traditional methods of DDoS detection and mitigation—such as over-provisioning and rate-limiting—are simply inadequate against the varied and dynamic methods of DDoS attacks now employed by hackers. For example, rate-limiting uses rules or algorithms to restrict the number of queries that can be made by a certain IP address (source or destination). Rate-limiting must be set in advance, limiting its effectiveness against persistent or sophisticated attackers.

Another option—over-provisioning—is the practice of deploying additional machines to support peak demands. This strategy solves immediate availability problems, but will fail against future, larger attacks. By deploying additional servers to support attack traffic, companies are simply treating a symptom rather than the disease—working harder rather than smarter. Additional servers and resources require unnecessary investments in hardware, power consumption, cooling costs, management costs, and other operational costs. Considering these extra costs, over-provisioning solely for the purpose of reducing the effect of DDoS attack is tantamount to success for attackers because they have succeeded in their effort to inflict harm on the target (in this case, financially).

Intelligent DDoS mitigation solutions are available for, and often necessary in, enterprise networks. Enterprise DDoS mitigation solutions leverage the vendor’s insight into global network traffic. Arbor Networks, for example, monitors up to 120 Tbps of global Internet traffic. DDoS mitigation solutions also utilize IP reputation to identify known bots, spam, scanners, and malware hosting sites, and then use blacklisting and geolocation-based policies to reduce the DDoS attack risk.

However, the ability for a massive volumetric attack to overwhelm the businesses’ network connections continues to present a challenge for customers.

Limitations of DDoS Mitigation Solutions in Enterprise Networks

Enterprise solutions are limited in their ability to mitigate large attacks. In particular, attacks that utilize reflection and amplification of vulnerable network protocols are able to achieve massive scale. For example, hackers can scan for and exploit publicly-accessible NTP servers to overwhelm a targeted server with traffic. This is considered an amplification attack because the query can generate a response that is up to 1,000 times in size. Attackers have already abused open NTP servers to generate high-bandwidth, high-volume DDoS attacks. Additionally, there are other ways to achieve large scale attacks. In the case of the multi-stage campaign of cyber attacks against large financial institutions in 2012 (named Operation Ababil), hackers utilized compromised servers with large connections and processing power to launch high bandwidth DDoS attacks. The drastic growth of DDoS attacks is illustrated in Exhibit 1.

Exhibit 1: The Changing Nature of DDoS Attacks, 2005 and 2014

	LARGEST ATTACK SIZE	MOST PROMINENT ATTACK TYPE	TOP CONCERNS
2005	8 Gbps	 90% of respondents cited volumetric flood attacks as the biggest threat	 DDoS Attacks + Worms
2014	400 Gbps	 65% of all attacks were volumetric flood attacks; increasingly driven by reflection/amplification	 DDoS Attacks Attacks targeting customers and service provider's own infrastructure

Source: Arbor Networks

High-end DDoS mitigation appliances can defend against attacks of up to 40 Gbps, but can be overwhelmed with larger attacks. A common practice is to daisy-chain additional DDoS mitigation appliances to achieve greater scalability. Yet, the largest DDoS attacks can completely overwhelm an organization’s network edge connections, and even cause saturation upstream in the provider network.

Businesses also have the option to subscribe to a dedicated DDoS mitigation service. These dedicated services feature high-capacity cloud scrubbing centers, or leverage the infrastructure of a content distribution network (CDN) to eliminate malicious traffic.

In practice, businesses often use a hybrid solution with an on-premises appliance for manageable network-based attacks and stealthy attacks that require application layer visibility. They then switch to a cloud-based service for large attacks that pass a preset threshold. A hybrid solution should perform this switch seamlessly, but this requires cloud signaling standards and integration between vendors.

Service Providers Require Intelligent DDoS Mitigation Solutions

With the growth in DDoS attacks, sales of intelligent and purpose-built DDoS mitigation solutions are on the rise. DDoS mitigation solutions are designed for use in service provider or enterprise networks, and are provided by companies such as Arbor Networks, Radware, and Allot Communications, among many others. The Arbor Networks Peakflow solution samples NetFlow and metadata from sensors deployed in customer networks, to identify anomalous patterns indicative of an attack. After detecting the anomalous attack traffic with the sensors, the solution will normally divert traffic, using Border Gateway Protocol (BGP), to centralized intelligent mitigation centers to block the attack traffic. From there, they re-inject the “good” traffic back into the provider network. Arbor Networks provides the vast majority of service provider DDoS mitigation equipment, including to nearly all Tier 1 service providers, powering more than 50 Internet service provider (ISP)-based, managed DDoS mitigation services.

Many communications service providers (CSP) use these commercial solutions to improve their DDoS mitigation capabilities. This methodology is an improvement over simple black hole routing and traditional clean pipes, which provide IP-based filtering of known “bad traffic.” But service providers should place a greater emphasis on DDoS mitigation because customers are increasingly expecting quality access rather than just access.

Evolving Customer Expectations Drive Interest in DDoS Mitigation Solutions

Businesses expect communication services to be high quality and reliable rather than simple connections. Clean pipes are comparable to public transportation. Access to an underground subway system is adequate but not very useful if unsafe. City managers may install surveillance systems or deploy security patrols to improve safety. These actions increase the value of the system to riders, not simply by moving them from point A to point B, but by doing so safely.

Businesses expect communication services to be high quality and reliable rather than simple connections.

Furthermore, businesses increasingly expect their service providers to offer “secure pipes” services that go beyond well-known “clean pipes” services that have been offered for some time. Clean pipes services filter traffic, identifying and purging known bad traffic from the traffic flow before it reaches the organization’s network. A secure pipes service builds on this by adding analytics to detect (expose and predict) and eliminate malicious traffic before it reaches the customer. Service providers that provide clean and secure pipes services reduce the need for customers to filter out known bad traffic in their own networks.

The secure pipes concept integrates network firewall and intrusion prevention system (IPS) capabilities, email and Web filtering, and advanced security analytics, in addition to DDoS mitigation. While Stratecast | Frost & Sullivan expects interest in “secure pipes” solutions to grow, customers that are focused on tactical solutions are likely to distinguish between defenses for malware and DDoS. Service providers that are not offering a secure pipes solution would still benefit by offering a DDoS mitigation service.

Service Provider Needs Will Only Increase in the Future

The need for service provider DDoS mitigation capabilities will only increase in the future. Service provider networks are going to continue to change in ways that expose them to availability concerns, such as the Internet-of-Things (IoT) and bandwidth-heavy applications. Mobile network operators

are already identifying the need to protect their networks due to growing adoption of LTE, increasing mobile malware levels, and the importance of data and the customer experience.

For example, researchers have identified the practice of hackers scanning mobile devices to identify open devices. Attackers can continually wake-up mobile devices in a type of DDoS attack that drains device batteries and limits radio spectrum availability for legitimate connections. Additionally, attackers can target the Gi/SGi interface to flood mobile networks and cause an effective DDoS attack that blocks network access for customers. In both cases, the customer experience is negatively impacted, and the service provider reputation is tarnished.

Service Providers Have Advantages in the DDoS Mitigation Process

Service providers have a global view of network traffic that provides tremendous insight into attack patterns, which can be used to improve attack detection. For example, Verizon manages 300,000 endpoints worldwide. DDoS detection is improved by identifying compromised hosts, and understanding the network activities preceding an attack. This can be useful in reducing the time between detection and response, and in improving detection accuracy.

Furthermore, filtering attack traffic closest to the attack origination is more effective than mitigating at the point of delivery. This effect is analogous to US highway and roadway systems. The limitations of a residential street would be unable to handle a rush of hundreds of cars, whereas this same traffic could easily navigate a highway. There are many reasons for this difference in road capacity, including the flow of traffic, road design, and road condition. There is a hierarchy to these road systems that enables the flow of traffic to be optimized: access road traffic defers to highways, main roads defer to access roads, and residential streets defer to main roads. Well designed roadways provide measurable benefits such as reducing congestion, reducing fuel consumption, decreasing pollution, and minimizing collisions.

Service providers offer similar high capacity and high performance “roadways,” which also benefit from optimizing traffic. To do so, a DDoS attack needs to be mitigated far from the customer networks, in the carrier’s network backbone and, if possible, at the network edge closest to the offending hosts. In the highway analogy, mitigating a DDoS attack can be compared to redirecting traffic several exits upstream from an accident, and even preventing new traffic from entering, rather than attempting to redirect traffic only 50 feet from an accident. For service providers, route optimization in the core network using real-time traffic analysis and routing algorithms will have quantifiable benefits in terms of reduced latency for legitimate traffic, minimal wasted bandwidth, and ensuring a satisfactory customer experience.

The Service Provider Role in DDoS Mitigation Today

Service providers use DDoS mitigation solutions to protect their own infrastructure, and therefore ensure availability of the services they offer to their customers. Many report growing customer demand for DDoS mitigation services, and have responded by developing commercial DDoS mitigation services.

For customers, DDoS mitigation from service providers and dedicated enterprise DDoS mitigation solutions are a necessary layered approach to security. However, most businesses lack the budget and expertise needed to deploy an enterprise DDoS mitigation solution. Instead, the growing sentiment is that service providers should mitigate these threats—or, at least, as many as possible.

But increasingly, customers should ask: do service providers offer new security value or is their value related to deployment and management of related services?

Service providers can use black-hole routing to dump all traffic to one customer during an attack, in the interest of protecting service for the rest of their customers. Many Tier 1 service providers go a step further and leverage purpose-built DDoS mitigation solutions for protecting their networks. Service providers provide this protection as a value-add, or offer a premium service that guarantees a level of uptime. But increasingly, customers should ask: do service providers offer new security value or is their value related to deployment and management of related services?

DDoS Mitigation as an Essential Differentiator

DDoS mitigation is becoming a key differentiator for service providers. Many promote their level of visibility into global Internet traffic through their network footprint (for accurate and advanced detection), and the size of their network backbone (for mitigation of detected attacks). Tier 1 service providers are wealthy in this “raw material” category of data, but are challenged to make this intelligence actionable. For example, AT&T has dedicated a significant amount of resources to work on DDoS defense, as evidenced by its Security Operations Center (SOC) with over 1,500 security experts. Other considerations are customer service, support, and monitoring.

Verizon, AT&T, and Level 3 Communications are examples of large service providers with varying levels of DDoS mitigation capabilities. However, overall, service providers vary in terms of DDoS mitigation capabilities and support. Some service providers go beyond basic DDoS mitigation and clean pipes, typically through a partnership with a DDoS mitigation specialist. For example, AT&T offers a DDoS Mitigation service with Akamai’s KONA Site Defender for protection of CDN resources.

Companies Providing Successful DDoS Mitigation Services

CDN providers also have an important role in the DDoS mitigation process, and have taken the most significant steps to incorporate DDoS mitigation as a core service offering. This step is a natural evolution for CDN providers, and a logical value-add for customers that are already considering subscribing to these services. CDNs are judged on availability and speed, so DDoS mitigation services are a logical value-add. CDN providers such as CloudFlare and Akamai use advanced analytics to detect and block DDoS traffic in their networks.

Level 3 is an example of a service provider that has developed strong DDoS mitigation capabilities. Level 3 claims to have visibility into as much as 70 percent of Internet traffic, and is able to monitor and study attack traffic. Level 3 uses this intelligence to build and maintain a global IP reputation database of botnets and their command and communications (C&C) systems. It can then block IP addresses that are known to be malicious using access control lists (ACLs) and rate-limits. Level 3 is working to bring these capabilities to market as a full service offering. The company offers formal DDoS mitigation services based on cloud scrubbing centers, and has plans to support on-premises solutions as managed security services by Q4 2015. In both cases, Level 3 will use best-of-breed solutions from DDoS mitigation specialists, supported by its own research intelligence.

Restraints for Service Provider Participation in DDoS Mitigation

However, there are barriers that prevent service providers from developing best-of-breed DDoS mitigation capabilities. Security experts are in high demand, and a SOC can be costly to build. These

costs may be difficult to justify for service providers that have otherwise considered this a third-party responsibility.

Another major challenge is lack of customer awareness of the benefits of integrated network services and security. The traditional mindset of separating networking, IT operations, and information security is problematic with regards to DDoS attacks. DDoS attacks affect business operations, tarnish the customer experience, and increase risk of a data breach. It is not always clear which IT organizations should be responsible for DDoS protection, response, planning, and budgeting. Ultimately, an effective DDoS response strategy will involve multiple decision makers and business units. Yet, service providers remain divided on the best approach for this; with some, such as AT&T, claiming that DDoS mitigation should happen entirely in the cloud; and others, such as Verizon and Level 3 Communications, pursuing a hybrid solution with managed security services for the on-premises DDoS mitigation component.

The Effect of Service Provider Participation on the DDoS Mitigation Market

DDoS mitigation focuses primarily on stopping known attacks using signatures, and stopping unknown attacks using behavior anomaly detection and behavioral analysis. A service provider has far more network visibility and data to collect and analyze for threats compared to even a large enterprise network. This visibility gives service providers a great advantage in the effort to identify attacks. Next, service providers can block threats upstream at the network edge closest to the malicious hosts. By combining these two advantages, service providers may be able to block attacks by identifying the activities that precede a DDoS attack, such as pings and scans.

Combined, advanced detection and mitigation of DDoS attacks by service providers can enable the most effective predictive DDoS mitigation possible. This may change the economics of DDoS mitigation, and the very nature of how to deal with these attacks—possibly eliminating the need for “bolt-on” security DDoS mitigation solutions.

The advancement of service provider DDoS mitigation services wouldn't necessarily compete with enterprise DDoS mitigation solutions, as many organizations will continue to require an on-site solution that can complete their DDoS protection strategies. However, hybrid and cloud models are currently the most effective mitigation strategies for defending against the largest DDoS attacks. Greater DDoS mitigation capabilities by service providers could cause a shift in how customers approach a hybrid DDoS mitigation solution.

Stratecast The Last Word

DDoS mitigation has been the goal for service providers and enterprise businesses for years. DDoS mitigation requires visibility, analytics, and security expertise. Service providers have tremendous insight into network activities, and so should not simply manage purpose-built DDoS mitigation solutions, but should leverage their insight to better identify attacks.

The participation of service providers in the identification of DDoS attacks can help to mitigate threats at (or very near) their point of origin. Collaboration between service providers and DDoS mitigation providers can help identify the signs of a pending DDoS attack, bringing customers closer to the ever-elusive “predictive” protections that are important for defense against future DDoS techniques. As a result, service providers may play an important role in advancing the industry from mitigation of DDoS attacks to elimination of DDoS attacks.

In the meantime, every organization is different in terms of network needs, disposition to risk, and technological sophistication and security expertise. The most effective DDoS mitigation strategy is one that leverages multiple layers of detection and mitigation, including any and all protections offered by service providers.

Chris Rodriguez

Senior Industry Analyst – Information & Network Security

Frost & Sullivan

Chris.Rodriguez@frost.com

About Stratecast

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit <http://www.frost.com>.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.