Analysis of the Global Distributed Denial of Service (DDoS) Mitigation Market – Abridged Version

Rise of the DDoS Attack Spurs Demand for Comprehensive Solutions
## Executive Summary—CEO’s Perspective

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>DDoS attacks are increasing in frequency and severity, and are gaining recognition as top threats to information security and business continuity.</td>
<td></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>As a result of intensifying online presence by commercial and public organizations, market demand for DDoS mitigation solutions is greater than ever.</td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Elevated customer interest in DDoS mitigation solutions has prompted many information security companies to develop and market solutions.</td>
<td></td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Though organizations of all sizes are interested in DDoS solutions, there are many DDoS mitigation options available contributing to fragmentation in the DDoS mitigation solutions market.</td>
<td></td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan
Market Overview

DDoS Attacks Disrupt IT and Business Operations

• DDoS attacks are denial-of-service attacks that leverage the massive, distributed, and stolen computing power from infected endpoints to flood target networks and Web applications 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.

• The success of a DDoS attack is determined by the lack of availability of computing resources to legitimate end users. Most DDoS attacks target Web applications and Web sites.

• Financial and government organizations are often targets of DDoS attacks, though these organizations are frequently targeted by online threat actors in general.

• Any organization that has a significant online presence, such as e-commerce organizations and online gaming, is a likely target and any organization with an online presence is a potential target.

• The actors behind DDoS attacks are skilled hackers and organized hacker groups.

• However, the attacker profile is expanding rapidly as nation-states, criminal organizations, and hacker activist groups (called hacktivists) are also utilizing DDoS attacks against selected targets or are commissioning hacker groups to perform DDoS attacks against specified targets.

Source: Frost & Sullivan
Market Overview (continued)

The Year of the DDoS Attack

• DDoS attacks have grown in prevalence and magnitude. In 2005, the largest observed DDoS attacks were 9 Gigabits per second (Gbps) and this number grew to 100 Gbps by 2010 according to the Arbor Networks *Worldwide Infrastructure Security Report*.

• In December 2013, attackers were utilizing Network Time Protocol (NTP) reflection to amplify their DDoS attacks up to 400 Gbps. Researchers have also identified an increase in the average attack size as well*.


DDoS Mitigation Market: Average Attack Size, Global, 2011-2013

*Source: Frost & Sullivan*
Drivers Explained

• **DDoS attacks are growing in frequency**
  
  o DDoS attacks are now common occurrences, with some research labs reporting thousands of attacks per day.

  o This increase in frequency is due to growing popularity of DDoS as an attack tool and many security research organizations posit that DDoS is becoming a preferred attack of choice for hackers.

  o Primarily, threat actors desire the ability to cripple and disrupt organizations of all sizes using DDoS attacks.

  o Furthermore, DDoS attacks require less effort by threat actors, compared to writing advanced malware and conducting long-term network penetration campaigns.

  o The growing frequency of attacks increases awareness of DDoS attacks as a threat. This effect is amplified when large organizations fall victim or when similar organizations are targeted.

Source: Frost & Sullivan
Drivers Explained (continued)

• DDoS attacks are increasing in magnitude
  o Historically, hackers grow the scale of DDoS attacks by infecting a greater number of computers with which to generate greater amounts of network layer traffic.
  o The number of potentially bot-infected devices on the Internet will only continue to rise, considering the explosive growth of smartphones and the “Internet-of-things” trend that will network everything from small appliances to automobiles.
  o However, threat actors have also developed new attacks methods that yielded sharp increases in DDoS attack size in late 2012 through early 2014.
  o First, hackers are targeting open or vulnerable Web sites and content management system (CMS) servers to host DDoS attack scripts such as the Brobot DDoS attack kit. Servers have more processing power than end-user devices and operate in hosted, cloud, and private cloud data centers with high bandwidth connections.
  o As a result, DDoS attacks that leverage compromised servers can achieve a significant increase in scale. DDoS attacks leveraging Brobot-infected servers reached over 100 Gbps in Operation Ababil in 2012.
  o In 2013, DDoS attacks reached a new high water mark in terms of scale by using amplification and reflection techniques.
Drivers Explained (continued)

- DDoS attacks are increasing in magnitude (continued)
  
  o Amplification attacks involve sending small requests to servers that return significantly larger responses. Reflections attacks allow attacks to spoof the identity of the request sender causing the unwanted response traffic to be directed to the victim’s IP address.

  o In March 2013, threat actors used a Domain Name System (DN) reflection attack to attack Spamhaus, generating a peak of 300 Gbps of attack traffic*.  

*Source: Arbor Networks.

Source: Frost & Sullivan
Drivers Explained (continued)

• **DDoS attacks are growing in sophistication**
  
  - Traditionally, threat actors have utilized Transmission Control Protocol (TCP) synchronize (SYN) or UDP floods to consume the available bandwidth of the target network with massive amounts of traffic. More recently, attackers have targeted application layer protocols and services with greater frequency and to great effect.
  
  - For example, Operation Ababil leveraged application-layer attacks by sending Hyper Text Transfer Protocol (HTTP) “GET” method requests for large Portable Document Format (PDF) files, thereby successfully exhausting server resources with few requests.
  
  - Hackers may also create significant latency by targeting “heavy URLs” that require complex database queries. These attacks are difficult to identify as they rely on logic to cause application latency per request rather than massive floods of requests.
  
  - Application-layer attacks (also called “low-and-slow” attacks) can quickly overwhelm a server with very little traffic and are therefore difficult to identify with traditional threshold-based DDoS mitigation practices. Additionally, application-layer traffic is often encrypted which complicates the inspection process.

Source: Frost & Sullivan
Drivers Explained (continued)

• DDoS attacks are growing in sophistication (continued)
  o Hackers increasingly blend both attack techniques, utilizing network-based attacks to generate large amounts of traffic that require significant bandwidth and application-layer attacks that are difficult to detect.
  o Essentially, blended attacks use massive volumetric attacks to fill the “pipes” of the victim organization and application-layer attacks to exhaust the server resources.
  o At minimum, the ability to mitigate blended threats requires a hybrid approach, using cloud-based scrubbing for volumetric attacks, and on-premises mitigation solutions to detect and block application layer attacks.
  o Consequently, businesses are more motivated to deploy both an on-premises DDOS mitigation products and subscribe to DDoS mitigation services for additional protection; a defense in depth strategy.

Source: Frost & Sullivan
Drivers Explained (continued)

- Internet access and Web services will increase in importance to businesses in every industry
  o The risk associated with a DDoS attack is related to the value of the Web services that are targeted. Currently, Web presence is very important in entertainment, financial, and e-commerce industries.
  o Businesses in these vertical markets have been early adopters of DDoS mitigation solutions because of the importance of their connection to the Web as an integral component of their business models.
  o In the future, a company’s Web presence, including Web sites, applications, and cloud services will only increase in strategic importance.
  o Moreover, businesses in every vertical and of every size will require a high level of public connectivity in order to ensure access for customers and partners.
  o As the value of Web and Internet connectivity increases to a greater number of organizations, the appeal of a DDoS mitigation solution will increase as well.

Source: Frost & Sullivan
Drivers Explained (continued)

- **DDoS mitigation offers a measurable return-on-investment (ROI)**
  - DDoS attacks disrupt operations and prevent users from accessing critical Web applications. This downtime is reflected by lost productivity, lost visitor traffic, lost e-commerce transactions, and other missed opportunities.
  - The value of these lost opportunities will vary across businesses and industries. However, businesses can and should measure the potential damages that a DDoS attack can cause in terms of dollars per hour.
  - For some financial and Web-based businesses, DDoS attacks can result in millions of dollars of damages per hour.
  - By measuring DDoS risk in numeric dollar terms, top decision makers will be better able to understand the risk and evaluate the available mitigation options under consideration.
  - By comparison, many security technologies provide value that is difficult to measure by protecting customer data and brand reputation—which are both valuable considerations but difficult to assign a dollar value.
  - This driver is tempered by the *high cost of DDoS mitigation solutions* that may outweigh the potential damages of a DDoS attack.

Source: Frost & Sullivan
Key takeaway: Changing technologies and customer requirements leave significant potential for advancement in the competitive landscape.

Competitive Landscape
Total DDoS Mitigation Market: Global, 2013

- Market Leader
- Market Challenger
- Market Contender
- Emerging Competitor

Source: Frost & Sullivan
Key takeaway: Arbor Networks is the top competitor in the DDoS mitigation product market.

Percent of Revenue
Product Segment: Global, 2013

- Arbor Networks: 60.4%
- Radware: 19.6%
- Juniper Networks: 4.1%
- Others*: 15.9%

n = 11

*A list of companies included in “Others” can be found in the appendix

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Product Segment—Competitive Landscape

Key takeaway: The market segment for DDoS mitigation products is becoming increasingly competitive.

Competitive Landscape
Product Segment: Global, 2013

Market Penetration

Meets Market Demands

Market Leader
Market Challenger
Market Contender
Emerging Competitor

Source: Frost & Sullivan
The Last Word—Customer Recommendations

1. A hybrid and layered approach to DDoS mitigation is strongly advised. Businesses should have multi-threaded DDoS mitigation strategies in place prior to an attack including “clean-pipes” services from ISPs and CSPs, on-premises DDoS mitigation appliances, and on-demand cloud DDoS mitigation services.

2. There is no one-size-fits-all solution for DDoS mitigation. Businesses should consider the nature of their operations including latency sensitivity, bandwidth requirements, in-house technical expertise, and associated costs prior to selecting a DDoS mitigation solution.

3. Businesses should consider DDoS attacks as a threat to data integrity and confidentiality. DDoS mitigation is often considered an operational or business continuity issue, but threat actors are increasingly leveraging DDoS attacks in combination with network intrusion and data theft and extortion attempts.