QUANTIFYING THE RISK OF DDOS ATTACKS FOR THE TRADITIONAL ENTERPRISE

March 2016

Aberdeen Group's simple Monte Carlo analysis leverages empirical data to show that an incremental investment in distributed denial of service (DDoS) protection services reduces the median risk of DDoS attacks for the traditional enterprise by about 50%. Stated another way, enterprises realize more than four times annual return on their investment in additional DDoS protection.

➔ **Derek E. Brink,** CISSP,
Vice President and Research Fellow
Information Security and IT GRC

The objective of a **denial of service (DoS)** attack is to make the computing resources that the attacker is targeting unavailable to their intended users.

A **distributed denial of service (DDoS) attack** is distinguished from a DoS attack by its use of multiple devices and network connections (e.g., in a botnet) to achieve the same basic objective: render the targeted resources unavailable.

For simplicity, Aberdeen uses the term DDoS generically throughout its research, unless the term DoS is explicitly more appropriate for a specific context.

Technical details about distributed denial of service (DDoS) attacks should not be confused with **risk**.

As Aberdeen described in its research report on *Understanding Your Risk (for Real) from Distributed Denial of Service Attacks* (June 2015), leading industry sources provide a wealth of interesting and useful information about DDoS attacks, including:

- ➔ What DDoS attacks are
- ➔ How they work, in significant technical detail
- ➔ What resources they target
- ➔ Who is executing them, and why
- ➔ How executing them is becoming even easier
- ➔ Examples of organizations that have been affected
- ➔ Detailed statistics and technical information about the latest trends in DDoS attacks, in multiple dimensions

The only problem is that this information about DDoS attacks doesn't really tell security professionals and business decision-makers very much about their actual **risk** — which must always be described in terms of both *likelihood*, and *business impact*.

Case in Point: The Risk of DDoS Attacks for the Enterprise

Enterprises rely on their **networks** for multiple **network services** (e.g., *high-speed internet*, *mobility*, *data*, *voice*, and *video*), across multiple **network infrastructures** (e.g., *fixed*, *mobile*, and *cloud*). As noted above, industry sources make it abundantly clear that increasingly sophisticated denial of service attacks can negatively impact both the *availability* and the *performance* of enterprise networks and network-based services.

To understand and give advice about the risk of DDoS attacks to the traditional enterprise, however, we need to estimate both the *likelihood* of such attacks occurring, and the *business impact* of these attacks when they do occur.

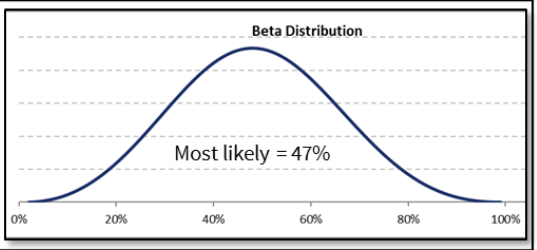
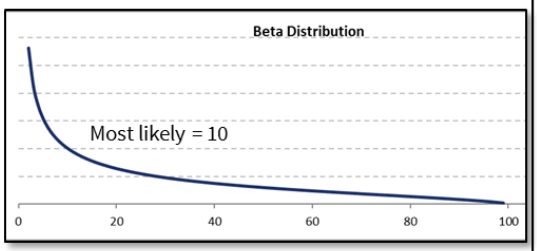
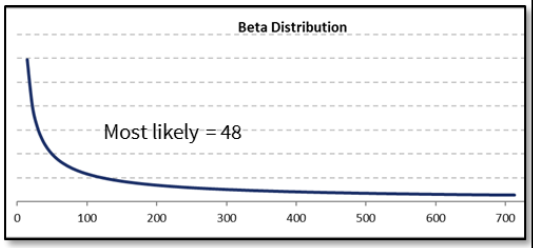
Step 1: What is the Likelihood of DDoS Attacks Occurring?

For the purposes of this analysis, Aberdeen leveraged findings from the Arbor Networks Worldwide Infrastructure Security Report (WISR, Volume X), which included detailed insights about the experiences of more than 110 enterprises, as well as those of more than 170 service providers. Based on this empirical data, Aberdeen modeled corresponding ranges and probability distributions for each of the following factors, as summarized in Table 1:

- ➔ The **likelihood** of experiencing a DDoS attack, within a 12-month period
- ➔ If attacked, the **number** of attacks experienced in a 12-month period

➔ The maximum **duration** of attacks experienced, in hours

Table 1: Empirical Data Shows the Likelihood, Frequency, and Duration of DDoS Attacks Against Traditional Enterprises

	Enterprises
Likelihood of experiencing a DDoS attack	
If attacked, number of attacks per year	
Maximum duration of attacks (hours)	

Source: Aberdeen Group, December 2015
adapted from Arbor Networks WISR

By using Monte Carlo modeling techniques to multiply these empirically based estimates for *likelihood* times *quantity* times *duration* over 10,000 independent scenarios, the result is a probability distribution for the total number of hours of DDoS attacks likely to be experienced per year. Selected characteristics of that distribution are summarized in Table 2.

Table 2: Enterprises Experience a Median of About 200 Hours of DDoS Attacks Per Year

	Enterprises
Likelihood of DDoS attacks > 0 hours / year	~ 53%
Median total hours of DDoS attacks	~ 200 hours / year
Likelihood of continuous DDoS attacks	< 5%

Source: Aberdeen Group, December 2015
modeled based on data adapted from Arbor Networks WISR

For traditional enterprises, the median value for the total hours of DDoS attacks likely to be experienced — that is, the value at which 50% of the 10,000 scenarios are above, and 50% are below — is about 200 hours per year. Assuming continuous 24x7x365 operations, this means that enterprises can expect their networks and applications to be under attack more than 2% of the time, as a median estimate. In addition, there's a non-trivial likelihood (a bit less than 5%) that enterprises will *continuously* be under attack.

Step 2: Modeling the Business Impact of DDoS Attacks Affecting the Traditional Enterprise

Most business decision-makers fully appreciate that when their networks and network-based services are down, or even hampered, time means money. To translate annual hours of DDoS attacks more fully into financial terms, Aberdeen estimated the annual business impact from DDoS attacks based on a simple Monte Carlo model of the following:

- The cost of full-time equivalent **responders** (e.g., the *incident response* team, *forensics* analysts, *IT* staff, *help desk* staff)

200

hours per year is the median total time that traditional enterprises experienced DDoS attacks against their networks and network-based resources.

- ➔ The percentage of revenue from network-based services that is lost (as opposed to merely deferred) **during the time of disruption**
- ➔ The present value of all expenses and / or lost future revenue that are **a result of disruptions** from DDoS attacks in the current year (e.g., as a result of *reputation damage*, *loss of trust*, *decrease in renewals*, *customer defection* to competitors, *legal fees*, *fines and penalties*, additional *marketing expenses*, and so on)

Not included in Aberdeen's model: the positive business impact that enterprises may gain from having networks and network-based services that are more secure, reliable, and high-performing as a result of better DDoS protection. After all, risks — like all uncertainties in life — can unquestionably be positive ("*rewarded*") as well as negative ("*unrewarded*"). In that sense, this analysis represents an understated, conservative estimate of the total risk.

The result is summarized in Table 3, which also addresses the important question of how an investment in additional DDoS protection services quantifiably reduces the organization's risk.

Table 3: Enterprises Realize a Significant (About 50%) Reduction in Risk — and a >4x Annual ROI — from an Investment in Additional DDoS Protection Services

Median (50% likelihood)	Enterprises
Median annual business impact of disruptions from DDoS attacks, under the status quo (network firewall, intrusion detection)	~ 2.2% of annual revenue ($2.2M / year, based on $100M annual revenue from network-based resources)
Median annual business impact of disruptions from DDoS attacks, after implementation of countermeasures (e.g., Arbor Networks DDoS Attack Protection)	~ 1.1% of annual revenue ($1.09M / year, including the annual cost of additional DDoS protection services)
Median reduction in the risk of DDoS attacks	about 50%
Median annual return on investment for additional DDoS protection services	about 4.2 times

Source: Aberdeen Group, December 2015
modeled based on data adapted from Arbor Networks WISR

Under the status quo — presumably deployments of traditional network firewalls, and intrusion detection / prevention systems — the median annual business impact of disruptions from DDoS attacks against traditional enterprises is about 2.2% of annual revenue. After the implementation of additional DDoS protection services, the median annual business impact is reduced to about 1.1% of annual revenue. This represents a reduction in risk of about 50%, *after* accounting for the incremental cost of the additional countermeasures. Another way to look at it: based on the median values, enterprises realize **an annual return on investment of about 4.2 times** for additional DDoS protection services.

4.2x

is the median annual ROI for enterprise investments in additional DDoS protection services.

Summary and Key Takeaways

- ➔ The *raison d'être* for security professionals is to help their respective organizations **manage risk**. *Subject matter expertise* about the technical details of DDoS attacks is important, but this kind of technical information should not be confused with risk.
- ➔ To be seen as a *trusted advisor* for the business decision-makers, security professionals must also learn to describe and communicate the risk of DDoS attacks properly. This means using the best available data to estimate the *likelihood* of such attacks occurring; the *business impact* of these attacks, when they do occur; and how an investment in additional countermeasures *quantifiably reduces* the organization's risk.
- ➔ As Aberdeen's simple Monte Carlo analysis shows, this is not as difficult as many security professionals may think.

Want to learn more?

Watch the webinar, The Latest Trends in DDoS – How They Can Help Answer the C-Suite's Questions About Risk and ROI, presented by Aberdeen Group and Arbor Networks.