MAZEBOLT

2018

# The Hidden Costs of DDoS Attacks

## Table of Contents

## MazeBolt Introduction

MazeBolt is an Israeli Cyber Security threat assessment company that strengthens enterprises' resistance to cyber-attacks. MazeBolt's pioneering DDoS Testing & Phishing Simulation & Awareness solutions are used by Fortune 1000 & NASDAQ-listed companies in more than 50 countries operating in 20 languages.

MazeBolt's BaseLine DDoS Testing Methodology – the ***de-facto*** industry standard – was developed on the basis of years of in-depth experience and understanding of how DDoS attacks and DDoS mitigation work.

## Executive Summary

Based on DDoS testing data MazeBolt has accumulated since 2014, DDoS mitigation systems, regardless of DDoS mitigation vendor, either On-premise Devices (CPE), Cloud Scrubbing services, or hybrid solutions of both fail to mitigate approximately 45% of DDoS tests, on average, when tested for the **first time** against the most common attack vectors (BaseLine DDoS testing). This means that the consistent increase in the number and average size of DDoS attacks translates directly to a growing number of companies that are left to deal with the aftermath of highly disruptive and costly DDoS attacks.

Beyond the financial loss of sales and reputational damage that DDoS attacks cause by rendering websites and services unavailable, MazeBolt identifies another 13 risks that DDoS attacks pose for companies.

This document takes an in-depth look at these risks and analyses them to provide companies with a comprehensive understanding of the DDoS risk landscape and suggests pre-emptive measures that companies can take to minimize the impact of DDoS attacks.

***"…it's clear that companies are buying [DDoS Mitigation] solutions that aren't working""***

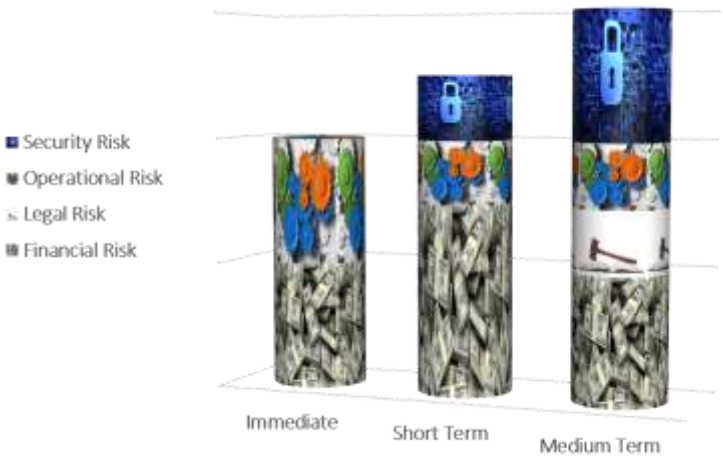
Barrett Lyon, Head Research and Development of Security Solutions @ Neustar

The analysis views these risks through two main dimensions as illustrated in Figure 1:

**Time of Impact**: Immediate, Short-term & Medium-term

**Type of Impact**: Financial Risks, Security Risks, Legal Risks & Operational Risks

Figure 1: DDoS Attack Risks by Type of Impact



The three sections that follow correspond to the (i) Immediate, (ii) Short-term & (iii) Medium-term phases within which the relevant risks and the pre-emptive measures companies can take are described.

## The 3 Pillars of DDoS Risk Management

Validating a company's DDoS Mitigation posture generally has three main aspects that need to be addressed:

### Verify Your DDoS Mitigation Works as Expected

MazeBolt's findings from hundreds of DDoS tests conducted over the past years consistently highlight the fact that DDoS mitigation solutions, be it CPE, Cloud Scrubbing services or hybrid solutions of both are very often misconfigured and will not provide the protection expected. The only way to identify these vulnerabilities is to test the DDoS mitigation against the most common DDoS attack vectors.

### Ensure Your Vendors Live Up to Their SLAs

Cloud Scrubbing services will typically commit to mitigating DDoS attacks within a certain timeframe. We've had a number of cases in which DDoS Tests we conducted in the middle of the night could not be handled by the Cloud Scrubbing services team on call and escalating the issue at 02:00 to get someone on deck took valuable time.

### Does Your DDoS Response Play-book Hold Water?

Coming under attack in any circumstance takes people from theory to practice in unexpected ways, and results are very often not what was planned for.

> *"Everybody has a plan until they get punched in the face."*
>
> Mike Tyson.

Having a DDoS response play book is a necessity nowadays. Equally as important is running drills that allow the different teams involved in DDoS mitigation to make sure communication paths are clear, roles and responsibilities are defined, and tasks are preformed adequately.

# Immediate Risks

## Loss of Revenue from Site Inaccessibility

This is the first risk that usually comes to mind when thinking of a "DDoS Attack" and rightfully so. Neustar's most recent study indicates that nearly half of the enterprises (49%) estimated their hourly revenue risk at US$250,000 or higher. When taking into account that mitigating DDoS attacks takes 45% of enterprises between 3 hours to more than one day that amounts to significant financial loss.

## Session Disruption

Beyond ecommerce, DDoS attacks create session interruptions, where the customer is right in the middle of a transaction or game, and the system suddenly goes down. What kind of customer experience are you promoting?

## Productivity Losses

What if your site serves as the gateway for remote employees? The longer it takes to get the site back up, the less work gets done by all employees in the organization.

## IT Staff Time & Its Impact on Security

While your 15 employees are fighting the DDoS attack, who is doing their regular jobs? Who is watching all the other systems not connected to the DDoS attack?

# Short-term Risks

## Customer Loss

Consider all the potential long-term customers you've lost because your site was down when they began their shopping process. Instead of buying from you, they have chosen to make their purchase from a competing vendor. The price is reasonable, the delivery gets to them on time, and the products are at an acceptable quality. The potential lifetime value of the customer has now been gifted to one of your competitors.

## Losing Your Reputation

When a technology website is rife with spelling and grammatical errors, customers are less likely to buy because they take the attitude that if a company cannot be bothered with the small stuff here, they aren't going to be bothered about the small stuff that's wrong with their technology.

Potential customers have a similar attitude about a company whose DDoS attack has been generally reported. If they cannot be bothered to protect their own systems, what kind of care are they going to take with the security infrastructure of the technology they're selling?

## Price of Distraction

As your technology gets increasingly more sophisticated, so does the technology of cybercriminals. According to recent DDoS surveys, it takes as many as 15 people to mitigate a DDoS attack. While these 15 people are fighting the attack, they don't have time to focus on the rest of the network. This creates an opportunity for the cybercriminals to exfiltrate thousands to millions of customer records or proprietary corporate or governmental information they can use for financial or political gain.

> *"Nine in every ten organizations acknowledged some form of breach or associated activity with DDoS attacks with an average of two breaches per attacked company per year."*
>
> Neustar Oct. 2017: Global DDoS Attacks & Cyber Security Insights Report

### Consulting Fees

You need to bring in a forensics team to determine what happened instead of preparing yourself against the attack. This type of consulting may be an external DDoS firm who advises you on what went wrong and why you had downtime. This last-minute consulting is expensive in terms of time and money.

### Customer Service Overload

This relates to the cost of the help-line personnel required to step in and answer the frantic customers calling to see if their bank transfers or bill payments went through? What if you are an online gaming site, and customers were in the process of loading money into their accounts? Or in the middle of a tournament?

## Medium-term Risks

### SLA Noncompliance May Entail Penalties

DDoS attacks automatically invalidate any type of SLAs you're committed to meeting. If your back-end system must be accessible 24/7 and you're down, your unhappy clients can demand refunds, sue you, or simply wait until the contract expires and go elsewhere because they know you aren't going to be able to fulfill their requirements.

### The Threatening Remains

Some of the attackers may be using the DDoS distraction to leave APTs, e.g. backdoors installed through a normally unexploitable vulnerability but because certain protections are down during a DDoS attack, those vulnerabilities are now available to exploit within your network. How long and how many resources will it take you before you find them?

### Breaking the Law May Result in Potential Fines

Regulatory requirements may demand that certain information must always be accessible. GDPR for example has two requirements that directly discuss availability in Article 32 and Recitals 49.

GDPR fines can reach up to 20 million Euros or 4 percent of annual global turnover, whichever of both is highest.

> *"…shall implement appropriate technical and organisational measures to ensure… the ongoing confidentiality, integrity, availability and resilience of processing systems and services"*
>
> Art. 32 GDPR Security of processing

### The Blame Game

Look around you. Who within the IT team or senior management will get blamed if the system is inadequate to prevent against a major DDoS attack? Even though the IT security team has put in budget after budget request to replace the aging network infrastructure, that manager may be the first to go. If a DDoS attack leads to a significant exfiltration or extended outage, a member of senior management may need to take the fall – even though she had made cybersecurity a priority and systems were already in the process of being upgraded.

### Budget Reallocation

The excessive cost of recovery from a DDoS attack may require budget cuts to other departments, affecting marketing, R&D, HR, and more. All the various internal realignment in the organization may be quite painful in terms of time and arguments, depending on the organization and the size of the problem.

### Blackmail

What if your systems are overwhelmed, and you just cannot stop the attack? Maybe the hackers will – for a price.

## Conclusion

The longer your website or IT services are down due to a DDoS attack, the more it costs you. It isn't just "time is money." It's reputation, customer loss, long-term budget allocation, penalties for non-compliance, income lost on transactions that couldn't be completed, and a lot more.

If you're prepared with a hardened and robust DDoS defense system coupled with a response procedure, you'll have a quick, lower-cost recovery. If you aren't, it will cost much more than you thought possible.

## References

1. https://www.computerweekly.com/news/252439254/DDoS-attacks-cost-up-to-35000
2. https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report
   https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/
3. http://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm
4. http://www.privacy-regulation.eu/en/r49.htm
5. https://hello.neustar.biz/201710-Security-Solutions-Siteprotect-DDoS-2H2017-Report-LP.html