A BUSINESS WHITEPAPER FROM NSFOCUS

NSFOCUS

DISTRIBUTED DENIAL-OF-SERVICE (DDoS) ATTACKS: **AN ECONOMIC PERSPECTIVE**

Table of Contents

Introduction 3

A Distributed Denial-of-Service Primer 4
- *Volumetric based attacks* 4
- *Application based attacks* 4
- *Threat Actors, Attack Vectors and Motivations – What drives DDoS Attacks?* 4

The Financial Impact of Distributed Denial-of-Service Attacks 5
- *Direct Costs* 5
- *Indirect Costs* 7

A Closer Look At The Cost of Distributed Denial-of-Service Attacks 8
- *DDoS Attack Cost Model* 8
  - Example: Online Retail 9
  - Example: Software Development 12
- *Return on Investment: A Three Year Cost Analysis* 13
- *Conclusion* 14

The Economics of DDoS Attacks: A Macro View 15

Summary 15

Executive Summary

Senior executives are wisely paying attention to Distributed Denial-of-Service (DDoS) attacks, since the financial consequences can be significant. A comprehensive analysis of the financial impact of a DDoS attack should include both direct and indirect costs, bearing in mind that the cost of a DDoS attack is closely tied to the duration and type of attack itself.

This paper presents a model that can be used to estimate costs and return-on-investment (ROI) based on the specifics of each situation.

Payback for DDoS protection solutions can range from immediate to less than 6 months,, depending on the features, cost and performance of the chosen solution.

In light of the fact that macro trends point to a continuing rise in the frequency and damage from DDoS attacks, a model such as this becomes increasingly important.

Introduction

While network security experts disagree on when the first Distributed-Denial-of-Service (DDoS) attack occurred, it is generally conceded that the most visible series of attacks occurred in February of 2000 when Internet giants Yahoo, Amazon, eBay, E-trade and others were attacked intermittently over a period of several days. The Yankee Group estimated the total cumulative costs of these attacks at $1.2 Billion U.S. Dollars, and it was later discovered that the attacks were conducted by a 15-year old Canadian teenager using the alias “Mafiaboy”. The teenager had crafted the series of attacks using several publicly available hacker tools.[1]

More than fourteen years later, DDoS attacks are more frequent, complex and destructive than ever. The threat actor landscape has expanded from a single individual with a hobby and an agenda to include cyber-terrorists, professional hackers/crackers/phreakers, hostile nation states, rival companies and even unwitting employees, customers, partners and private citizens. Today, there has been an explosion in connectivity ushered in by mobile and cloud computing, coupled with the availability of sophisticated but easy-to-use DDoS tools and the rapid commoditization of network bandwidth. As a result, it has never been easier to launch a sustained attack designed to debilitate, humiliate or steal from any company or organization connected to the Internet. These attacks often threaten the availability of both network and application resources, and result in loss of revenue, loss of customers, damage to brand and theft of vital data.

Fortunately, DDoS mitigation techniques have also evolved; today, the DDoS mitigation market comprises dozens of companies who collectively invest billions of dollars in the research and development of advanced countermeasures. The accuracy and effectiveness of these solutions certainly differ, but there is no denying that specialized DDoS technology is being deployed by organizations of all sizes in order to insulate themselves against this growing threat.

This paper examines the financial impact of modern DDoS attacks by describing the costs typically incurred by the victims of these attacks. It summarizes publicly-available information and research about the scope and costs of recent high-profile attacks, and provides a model that can be used to measure the impact of a DDoS attack for your own organization. While all of the costs in the model may not directly apply to your specific business or organization, they are presented to provide a complete picture of the expenses to consider when evaluating the purchase of DDoS protection. Finally, this paper discusses the larger economic factors that will continue to fuel the proliferation of these types of attacks for the foreseeable future.

[1] SANS Institute, “The Changing Face of Distributed Denial-of-Service Mitigation, 2001

A Distributed Denial-of-Service Primer

DDoS attacks are an attempt to exhaust network, server or application resources so that they are no longer available to intended users. These attacks generally fall into two categories:

Volumetric based attacks

These attacks are characterized by the presence of an abnormal and overwhelming number of packets on the network. Threat actors attempt to consume all available network bandwidth and/or exhaust router, switch and server forwarding capacity by flooding these devices with malicious traffic so that legitimate user traffic is starved. Some examples of volumetric based attacks include UDP, ICMP and SYN flood attacks.

Application-based attacks

Application-based attacks are designed to exploit weaknesses or software defects that exist in the protocols and applications themselves. They attempt to disrupt service by consuming CPU, memory or storage resources in target servers that are running the application so that the application is no longer able to serve legitimate users. They may also attempt to crash the application by supplying malformed messages or unanticipated input to the application. Some examples of application attacks include HTTP GET/POST attacks, SIP header manipulation attacks and SQL injection attacks.

Hybrid attacks

Modern DDoS attacks are very sophisticated and often blend several volumetric and application based attacks in order to disrupt service. These so called “hybrid” attacks attempt to consume all network bandwidth while simultaneously exhausting server resources. Frequently these attacks are used to not only create a catastrophic denial of service condition but also distract security operations personnel from other malicious activity such as the installation of backdoors or other advanced persistent threats (APT) tools designed to steal vital data. Another common attack technique is to probe an organization’s DDoS response capabilities using a series of short duration attacks over a longer period of time in order to craft a site-specific plan designed to circumvent existing DDoS protection solutions.

Threat Actors, Attack Vectors and Motivations – What drives DDoS Attacks?

Who is performing these attacks (threat actors), what means do they use (threat vectors) and what is their motivation?

The answers to these questions are as varied as the attacks themselves. Threat actors can include ex-employees, current employees, hobbyists, political activists (hacktivists), professional hackers (hackers-for-hire), competitors, hostile nation states or vandals who simply enjoy creating chaos.

These attackers can use a seemingly infinite number of devices and protocols as a means to carry out their attacks. Sophisticated and large virtual networks of compromised computers, mobile phones, internet connected smart devices (IoT/home automation), infrastructure servers, home routers, Unified Communications systems and almost anything that is internet connected could be controlled by malicious attackers to launch directed and sustained attack campaigns. These so called "botnets" or "zombie armies" will use a diverse set of protocols typically found at layers 3, 4 and 7 of the Open Systems Interconnection Model (OSI) to carry out the attacks. A non-inclusive list of these protocols includes TCP, UDP, ICMP, NTP, SSDP, HTTP, DNS, SNMP, FTP and more. Attackers can exploit the manner in which the protocols work as well as software defects in their implementation to disrupt service delivery. These protocols and devices are the threat vectors to consider when designing an effective DDoS mitigation strategy.

Motivations for DDoS attacks tend to be financial, philosophical or political in nature. Typical motivations include blackmail/extortion, political or ideological disputes, revenge, vandalism, an attempt to gain a competitive advantage in a business rivalry or an attempt to cover up or distract from other exfiltration or theft of data activities. Regardless of the motivation, it is clear that if you are connected to the Internet or rely on the internet to conduct your business operations you can be a target. The significance of the DDoS threat has not gone unnoticed: a recent survey of more than 641 IT security and operations professionals revealed that 38% of respondents ranked Denial-of-Service attacks as their most significant IT security concern, placing this class of attack in the top 3 out of 10 overall IT security threats.[2]

The Financial Impact of Distributed Denial-of-Service Attacks

In any DDoS attack there are both direct and indirect costs to the victim. Direct costs, in general, are easier to measure and can be immediately associated with the attack. Indirect costs, on the other hand, are more difficult to identify and their effects are often not felt for weeks, months or in some cases years following the actual attack itself.

Direct Costs

Loss of revenue: This is usually the most straightforward metric to collect, particularly if your primary business is electronic commerce. Online retailers, streaming media services, online gaming, business to business hubs, online marketplaces, Internet based advertisers and internet commerce businesses are among those that experience direct revenue loss with any disruption of service. These companies typically measure revenue in clicks or impressions per minute or average revenue per minute or transaction. Revenue is completely lost for the duration of any attack that takes them completely offline, or can be severely reduced during periods when their online systems are performing outside of their normal operating level.

[2] Ponemon Institute, "The Cost of Denial-of-Services Attacks", March 2015

DDoS Attack Cost Categories

Direct

Loss of revenue
Loss of productivity
IT operations/security
Help desk
Consultants
Customer credits/SLA
Legal/Compliance
Public relations

Indirect

Damage to brand
Theft of vital data
Customer loss
Opportunity cost

Loss of productivity: Many companies and organizations use their network, online resources and publicly-available services to support their primary business. Any disruption to the availability of these important resources results in a loss of productivity. Whether employees are accessing the Internet, performing software tasks on remote servers, transferring or accessing valuable company data remotely, entering data into business systems, using cloud based services, e-mailing, printing, communicating or any number of other network related tasks they can be negatively impacted by DDoS attacks.

Personnel costs – IT operations/security teams: This cost includes the fully-burdened salary of any employees who are involved in eliminating the DDoS threat and restoring service to its normal levels. In some organizations, this can be a single person or two. In others, this can be a larger team comprised of both IT operations and security professionals and involve multiple, geographically diverse locations. Due to the severe impact of a DDoS attack most companies will involve all technical resources capable of helping to restore service until the threat has been eliminated. These costs can mount quickly over the minutes, hours, days and potentially even longer time it can take to recover from a DDoS attack.

Personnel costs – Help desk: In most DDoS attacks there is a surge of activity and calls to help desk support personnel. Calls can come from customers, partners and internal employees who contact the help desk for a variety of reasons: to report the current outage, to request the current status, to find out when service will be restored, to complain, to request a refund or service credit and more.

Specialized Consultants: In some instances it may be necessary to call in an emergency security consultant or hire a managed security services expert who specializes in DDoS attacks to restore service. These consultants can become involved in active mitigation to eliminate the threat, security incident and event management (SIEM) assistance, forensic or compliance reporting efforts or provide follow up analysis and recommendations to prevent future attacks.

Customer credits/Service level agreement enforcement: Some businesses offer service level agreements to their customers that guarantee a certain level of service availability. DDoS attacks can prevent these business from meeting these commitments and often result in finance penalties. Also, many companies and retailers are forced to refund purchases or credit back services in order to retain customers or improve loyalty and satisfaction after suffering the effects of DDoS attacks.

Legal/Compliance: Many industries have strict regulations regarding the handling of sensitive data and the reporting of any cyber security attacks and breaches. In these instances, detailed forensics and root-cause analysis must be performed. The activities can take an extended period of time to complete and their costs can be substantial. Also, legal costs can be incurred in order to defend against parties seeking compensation for the disruption of service.

Public relations: Some victims of DDoS attacks end up spending additional money with public relations firms in an effort to restore the goodwill and confidence of the general public or their customers after an outage. These firms will often help the victims create clear messaging about the incident and what is being done to prevent attacks of this type in the future. They can also help with press announcements, editorial calendars, contributed articles, speaking engagements or even televised interviews and advertising.

Indirect Costs

Damage to brand: Some companies spend a substantial portion of their operating budget to create and nurture their brand image through advertising, PR, direct-mail campaigns and other initiatives. Earning the trust and faith of customers and constituents often takes years of time, effort and money. Today's DDoS attacks can damage your brand and ruin your reputation in a shockingly short amount of time.

Customer loss: The effects of a DDoS attack including disruption of service and theft of customer information can cause a loss of confidence in your customer base. These customers can decide to move their business to a competitor or use social media to vent their anger and frustration. Clearly none of these outcomes is desirable and unfortunately it may take some time to realize the full extent of any customer losses.

Theft of vital data: A worrisome trend in recent DDoS attacks is for threat actors to use the DDoS attack as a smokescreen or distraction to hide other malicious activity. The DDoS attack itself is only a means to an end. The real goal of the attack is to steal critical data. In this style of attack, the threat actor directs a DDoS attack to a certain portion of the network while launching specially crafted attacks at other targets. The goal is to compromise these other targets and either steal critical data during the DDoS attack or install a backdoor that will grant future access to the network and its resources.

These attacks can be successful because IT staff are completely focused on mitigating the DDoS attack itself while other malicious activity goes unnoticed. There are many types of DDoS attacks that attempt to take servers off-line or crash applications while still leaving enough network bandwidth to compromise other targets. Additionally, if the victim does not have a dedicated DDoS protection system, the hackers may attempt to loosen firewall or IDS/IPS security rules to keep these systems online. This creates further holes in perimeter security that can be exploited. The sheer volume of logs generated during a DDoS attack makes discovering other malicious activity extremely difficult even after the DDoS attack is thwarted. Vital data can include credit cards, passwords, intellectual property, trade secrets, medical information, private customer records and banking information. One high profile example of this style of attack occurred when hackers launched a DDoS attack on Carphone Warehouse and stole the personal details of over 2 million customers.[3]

Opportunity cost: This category encompasses the set of projects, work or activity that is delayed or dropped because the company is occupied with repairing the damage of a DDoS attack as a priority. Priority activities associated with a DDoS attack can include forensic analysis, incident reporting to comply with relevant regulations, public relations and the deployment of new DDoS protection systems.

A Closer Look at The Cost of Distributed Denial-of-Service Attacks

There have been numerous surveys and studies conducted on the cost of DDoS attacks. While the results vary based on industry, company size, security operating budget and more, a common element of all of these estimates is that the cost is closely tied to the duration of the outage caused by the attack. Consider the following:

- For some financial and web-based business, DDoS attacks can result in millions of dollars of damages per hour.[4]

- The average amount of downtime following a DDoS attack is 54 minutes and the average cost for each minute of downtime is $22,000. However, the cost can range from as little as $1 to more than $100,000 per minute of downtime.[5]

- DDoS is no longer an annoyance threat. In fact, it hasn't been for several years. There is real loss and real cost, and companies of all industries and sizes are vulnerable.[6]

This information provides a general measure of the impact of these types of attacks and the findings demonstrate that there is a substantial financial risk to not being prepared for a DDoS attack. This paper provides a model that can be used as a template to better estimate the cost of an attack for your specific situation.

DDoS Attack Cost Model

[3] The Telegraph, "Carphone Warehouse hackers 'used traffic bombardment smokescreen'", August 2015

[4] Frost & Sullivan, "Global DDoS Mitigation Market Research Report", July 2014

[5] Ponemon Institute, "Cyber security on the offense: A study of IT security experts", November 2012

[6] IDC Research, "Breach Is a Foregone Conclusion: DDoS", October 2015

The model is introduced by describing the costs associated with a hypothetical attack for both an online retailer and a software development company. These businesses are fictional but the cost factors presented are representative of those that would be considered in any real-world DDoS attack.

Example: Online Retail

Company Profile: The company is an online retailer offering discounted name brand office furniture including chairs, desks, cabinets and artwork. They also offer bulk consumable office supplies and their current trailing 12-month revenue is $35,000,000. Their IT operations team consists of 4 engineers and they have a separate help desk staffed to receive calls from both internal employees and online customers. There are 2 full time employees staffing the help desk at any given time.

Scenario - A: The company was the victim of a DDoS attack that resulted in a complete outage of their online store. Customers were not able to browse the store or complete purchases for the duration of the outage.

Scenario A – Cost Table:

	Outage Duration						
	30 Minutes	**2 Hours**	**5 Hours**	**8 Hours**	**1 Day**	**3 Days**	**Notes**
Direct Costs							
Loss of revenue	3,600	14,400	36,000	57,600	172,800	518,400	1
Loss of productivity							
IT operations	108	430	1,076	1,721	5,163	15,490	2
Help desk	10	40	100	160	480	1,440	3
Consultants	1,600	2,000	2,400	3,000	4,000	8,000	4
Customer credits/SLA	3	11	27	43	128	383	5
Legal/compliance							
Public relations			1,200	1,200	2,400	3,000	6
Indirect Costs							
Damage to brand							
Theft of data							
Customer loss				35,000	87,500	175,000	7
Opportunity cost							
Total cost ($ USD)	5,320	16,881	40,802	98,724	272,471	721,713	

Notes:

1 – The company does 90% of their annual revenue during a 12-hour period (6am-6pm PST) with an average revenue per minute of $120. The outage occurred during this window.

2 – The model assumes a fully burdened average salary of $108,000 per IT operations staff and all 4 employees in this example were involved in detecting and mitigating the DDoS attack for the entire duration of the outage.

3 – The model assumes a fully burdened average salary of $42,000 per help desk employee with a total per cost call of $1. There were 2 employees at the help desk at the time of the incident fielding 20 total calls per hour. Each call to the help desk during the outage averaged 2 minutes in duration.

4 – The hourly cost for a specialized security consultant is $200 per hour. The consultant was hired for forensic analysis and to make recommendations improving perimeter security to prevent future DDoS attacks. The amount of time included in the model ranged from 8 hours of consulting for a 30-minute attack to 5 business days for a 3-day outage. This time includes all necessary activities for a full analysis including log collection and event correlation from affected networking devices and server systems.
5 – In an effort to build goodwill among those customers affected by the outage the company offered a $10 discount towards future purchases. The model assumed discounts were given to 1% of the total customers who were affected by the outage. The costs are based on an average margin of 15% per online purchase.
6 – The company pays an average of $15,000 per month to a public relations agency for press and analyst relations. The company begins to work with the PR firm when the duration of the outage is greater than 5 hours. The amount of additional hours billed by the PR agency ranges from 10 billable hours for a 5-hour outage to 40 billable hours for an outage lasting 3 days.
7 – The company's 12-month revenue was $35,000,000 from 152,174 online customers at an average purchase of $230 per customer. The financial impact of permanently losing customers to competitors due to the outage is examined over a three-year period. The number of customers the company lost is assumed to be 1/10th of 1% of total annual customers due to an 8-hour outage, ¼ of 1% of total annual customers due to a 24-hour outage and ½ of 1% of total annual customers for an outage duration of 3 days.

Scenario - B: The company was the victim of a hybrid volumetric and application-layer DDoS attack that resulted in a complete outage of their online store and the theft of vital customer account information. Customers were not able to browse the store or complete purchases for the duration of the outage. The stolen data included customer names, phone numbers, addresses, email addresses, account passwords and credit card numbers.

Scenario B – Cost Table:

	Outage Duration						
	30 Minutes	2 Hours	5 Hours	8 Hours	1 Day	3 Days	Notes
Direct Costs							
Loss of revenue	3,600	14,400	36,000	57,600	172,800	518,400	1
Loss of productivity							
IT operations	108	430	1,076	1,721	5,163	15,490	2
Help desk	15	60	150	240	720	2,160	3
Consultants	17,600	18,000	18,400	19,000	20,000	24,000	4
Customer credits/SLA	3	11	27	43	128	383	5
Legal/compliance							
Public relations	60,000	60,000	60,000	60,000	60,000	60,000	6
Indirect Costs							
Damage to brand	22,050,000	22,050,000	22,050,000	22,050,000	22,050,000	22,050,000	7
Theft of data							
Customer loss	3,500,002	3,500,002	3,500,002	3,500,002	3,500,002	3,500,002	8
Opportunity cost							
Total cost ($ USD)	25,631,327	25,642,903	25,665,654	25,688,606	25,808,813	26,170,435	

Notes:

1 – Ninety percent of the company’s annual revenue is realized during a 12-hour period (6am-6pm PST) with an average revenue per minute of $120. The outage occurred during this window.

2 – The model assumes a fully burdened average salary of $108,000 per IT operations staff and all 4 employees in this example were involved in detecting and mitigating the DDoS attack for the entire duration of the outage.

3 – The model assumes a fully burdened average salary of $42,000 per help desk employee with a total per cost call of $1. There were 2 employees at the help desk at the time of the incident fielding 30 total calls per hour. Each call to the help desk during the outage averaged 2 minutes in duration.

4 – The hourly cost for a specialized security consultant is $200 per hour. The consultant was hired for forensic analysis and to make recommendations improving perimeter security to prevent future DDoS attacks. The amount of time included in the model ranged from 88 hours of consulting for a 30-minute attack to 15 business days for a 3-day outage. There were 80 hours spent on the forensic analysis of the data theft alone. This time includes all necessary activities for a full analysis including log collection and event correlation from affected networking devices and server systems.

5 – In an effort to build goodwill among those customers affected by the outage the company offered a $10 discount towards future purchases. The model assumed discounts were given to 1% of the total customers who were affected by the outage. The costs are based on an average margin of 15% per online purchase.

6 – The company paid $20,000 per month to their PR agency for a period of 3 months to help minimize the damage caused by the theft of their customer’s personal data.

7 – According to a study conducted by the Ponemon Institute, the average diminished value of an organization’s brand involving the theft of 100,000 or more customer records was 21%.[7] The brand damage was calculated at more than $22,000,000 based on a total company valuation of 3 times trailing 12-month revenue or $105,000,000 USD.

8 – The company lost 10% of its customers due to the data theft.

[7] Ponemon Institute, Reputation Impact of a Data Breach”, November 2011

Example: Software Development

Company Profile: The company is a 500-person software development firm based in the San Francisco Bay Area. They are a global company with 8 locations connected using a private MPLS wide-area network (WAN). Their Internet data center, in San Francisco, supports their main internet connection as well as a virtualized server farm that is used by the company's 200 software engineers as their primary development environment for application development and testing.

Scenario - C: The company was the victim of a hybrid volumetric and application-layer DDoS attack that completely exhausted WAN bandwidth and brought down the company's development servers. This prevented access to the Internet for the entire company and disrupted software development activities.

Scenario C – Cost Table:

	Outage Duration						
	30 Minutes	**2 Hours**	**5 Hours**	**8 Hours**	**1 Day**	**3 Days**	**Notes**
Direct Costs							
Loss of revenue							
Loss of productivity	2,462	9,849	24,622	39,394	118,183	354,550	1
IT operations	81	323	807	1,291	3,873	11,618	2
Help desk	5	20	50	80	240	720	3
Consultants	1,600	2,000	2,400	3,000	4,000	8,000	4
Customer credits/SLA							
Legal/compliance							
Public relations							
Indirect Costs							
Damage to brand							
Theft of data							
Customer loss							
Opportunity cost			1,845	11,228	11,228	11,228	5
Total cost ($ USD)	4,148	12,191	29,723	54,993	137,523	386,115	

Notes:

1 – Loss of productivity costs during the outage are calculated using an average fully burdened salary of $123,600 per software developer. On average 40% of the company's developers are online and using the centralized development servers or the Internet for research.

2 – The model assumes a fully burdened average salary of $108,000 per IT operations staff and all 3 employees in this example were involved in detecting and mitigating the DDoS attack for the entire duration of the outage.

3 – The model assumes a fully burdened average salary of $42,000 per help desk employee with a total per cost call of $1. There were 10 total calls per hour to the help desk by internal employees to either report the outage and/or request a status update.

4 – The hourly cost for a specialized security consultant is $200 per hour. The consultant was hired for forensic analysis and to make recommendations improving perimeter security to thwart future DDoS attacks. The amount of time included in the model ranged from 8 hours of consulting for a 30-minute attack to 5 business days for a 3-day outage. This time includes all necessary activities for a full analysis including log collection and event correlation from affected networking devices and server systems.

5 – The opportunity cost was calculated assuming a delay to the implementation of other projects by the IT team due to the DDoS attack. At an outage duration of 5 hours, the attack was a distraction and only resulted in a 2-week delay to other projects. In the case of an 8 or

more-hour outage the company decided to evaluate and install a new DDoS protection solution which delayed other IT projects for a three-month period. In this particular example, the company had planned to replace its aging MPLS WAN infrastructure with a new, software-defined WAN solution that would save the company 66% in monthly bandwidth costs. At a monthly cost of $500 per MPLS WAN link, the company would save $2,640 monthly. In addition, the IT team had planned to implement a new, automated password recovery and management solution as well as convert to a new anti-virus solution for their host machines. It was estimated that these projects would save the IT department an average of $52.50 per day in eliminated help desk calls.

Return on Investment: A Three Year Cost Analysis

This paper has described the costs associated with a single DDoS attack using a variety of scenarios. It is useful to analyze the impact of multiple attacks over a longer period of time to obtain an accurate picture of the return-on-investment (ROI) of any DDoS protection solution.

A comprehensive security survey of over 370 networking and security managers from more than 14 industries reported that respondents experienced a weighted average of 4.5 DDoS attacks per year and an average attack duration of 8.7 hours.[8] The following table calculates the three year cost of the scenarios described in this paper using the information provided by the survey.

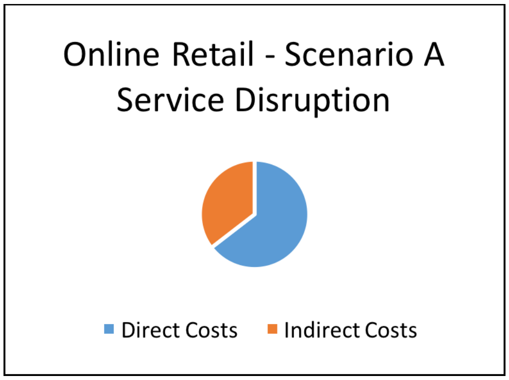
[8] SANS Institute, “DDoS Attacks Advancing and Enduring”, February 2014

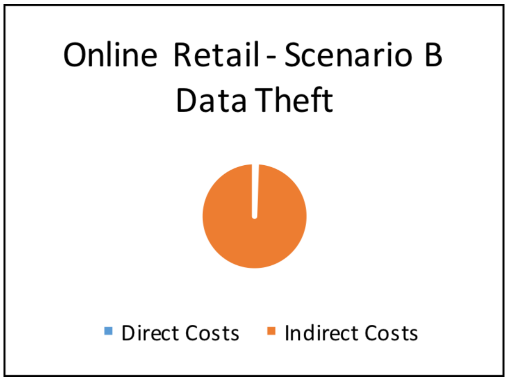
	Online Retailer - Scenario A DDoS Attack	Online Retailer - Scenario B Data Theft	Software Company DDoS Attack
Single incident cost (8 hour)	$98,724	$25,688,606	$54,993
Estimated Three year cost	Single incident cost x 13.5 = 1,332,770	(Single incident cost x 13.5) + Cost data theft = $33,471,156	Single incident cost x 13.5 = $742,402
Estimated Monthly cost	$36,743	$929,754	$20,622

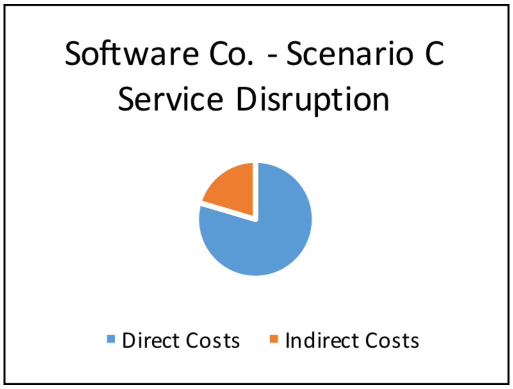
Using this analysis, we can see that the payback period for most DDoS protection solutions will range from immediate to less than 6 months depending on the cost, capability and performance of the particular solution.

Conclusion

In examining the direct and indirect costs of our three sample scenarios it becomes clear that the distribution of costs can vary widely depending on the results of the attack. While direct costs related to service disruption are relatively easy to identify, the indirect costs associated with either a data breach or the permanent loss of customers can quickly become the most expensive portion of a DDoS attack. As shown in Scenario B, the damage due to the theft of customer data and the loss of customers dwarfed the direct costs incurred as a result of the attack. It is imperative that any cost analysis include both direct and indirect costs in order to obtain a complete view of the financial impact of the attack. The charts below depict the cost distribution of an eight-hour outage for the three sample scenarios.







The Economics of DDoS Attacks: A Macro View

Unfortunately, it has never been easier or less expensive to launch a DDoS attack. The last decade has seen orders of magnitude increases in bandwidth, compute power and device connectivity that make it easy to quickly overwhelm the online activities of most companies and organizations. Compounding the problem is the fact that the technical barrier to entry for launching DDoS attacks has never been lower. The early days of hacking required some amount of technical skill and a detailed understanding of the underlying network and application protocols to create an attack. Today, there are massive, automated botnets available for rent ranging from $10 to $300 USD monthly and capable of generating up to 3 Gbps worth of attack traffic.[9]

They can be combined and used with other amplification techniques to generate an overwhelming amount of attack traffic. These botnets increasingly use sophisticated, complex, multi-layer attacks but can be controlled with a simple web GUI front-end. A single credit card number or PayPal account and the IP address (or addresses) of the victim are often all that is needed to launch massive attacks capable of disrupting critical online systems.

DDoS attacks are at an inflection point where the low cost and simplicity of launching an attack mean that their frequency will only increase. We saw the same thing a few years ago with spam, when the cost of sending bulk email dropped, and compute power, bandwidth and email software improved, and the amount of SPAM increased.

Similarly, trends in the cost, performance and availability of modern DDoS attacks point to the proliferation of these types of attacks for the foreseeable future.

Summary

This paper has detailed the cost factors to consider when evaluating the financial impact of DDoS attacks on any organization. It has also demonstrated how the costs can vary based on the nature of the threat, the type of business under attack and the vulnerabilities that are exploited. It provided a template that can be used to measure the impact of any potential attack for your specific situation and provides a cost model that is useful for evaluating the ROI of DDoS protection solutions. Finally, it described the wide landscape of threat actors, threat vectors, motivations and economic trends that will continue to drive the increased frequency and effectiveness of modern DDoS attacks for the foreseeable future.

[9] Karami, Park and McCoy, “Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services, August 2015

NSFOCUS

NSFOCUSGLOBAL.COM