DEGREE PROJECT IN COMMUNICATION SYSTEMS, FIRST LEVEL
STOCKHOLM, SWEDEN 2015

Distributed denial of service attacks

Protection, Mitigation, and Economic Consequences

MARTIN EKLUND and PATRIK STÅHLBERG

KTH ROYAL INSTITUTE OF TECHNOLOGY
INFORMATION AND COMMUNICATION TECHNOLOGY

Distributed denial of service attacks

Protection, Mitigation, and Economic Consequences

Martin Eklund and Patrik Ståhlberg

2015-07-14

Bachelor's Thesis

Examiner and Academic adviser
Gerald Q. Maguire Jr.

Industrial adviser
Björn Fredriksson (Nordea)

KTH Royal Institute of Technology
School of Information and Communication Technology (ICT)
Department of Communication Systems
SE-100 44 Stockholm, Sweden

Abstract

Distributed Denial of Service attacks is a problem that constantly threatens companies that rely on the internet for major parts of their business. A successful DDoS attack that manages to penetrate a company's network can lead to devastating damages in the form of lost income, reduced productivity, increase in costs, and damage to the company's image and reputation.

The different DDoS attacks are many and of different character and often Offer different parts of the network, which makes it very difficult to defend against. It is also very clear that DDoS attacks are increasing in both numbers and size every year. From our experiments we have proven that anyone with little knowledge and limited resources can perform DDoS attacks that will make a website unavailable. This fact should cause companies that base their business on the internet, aware that they are likely to someday be subject to a DDoS attack.

From our research we have found a variety of different DDoS solutions on the market that promise to offer protection. Many of which claim to protect against all different types of DDoS attacks. In practice it is impossible to find something that guarantees 100% safety. According to earlier research in the field, there are many different ways of protecting a network against DDoS attacks, e.g. via Software Defined Networking, Hop-Count Filtering, or Kill-bots.

Our own tests show that a virtual firewall can offer protection against DDoS attacks on a low scale, but that such a solution has a number of weaknesses. If the firewall does protect the website, the attacker could instead shift to attacking the firewall itself.

Our research also shows that the most common motives behind DDoS attacks are criminal purposes. Criminals use DDoS attacks to earn money by offering directed DDoS attacks against websites or by trying to blackmail companies into paying a fee for not being attacked.

We have also seen that the economic consequence of DDoS attacks are devastating if not handled with a sufficiently fast response. After investigating the e-commerce company CDON.com we learned that they could potentially lose roughly 36 410 SEK per minute when a DDoS attack is underway against them.

In today's business climate it is important for companies to be able to rely on the internet for their activity and for customers to have easy access to the company's products and services. However, companies' websites are being attacked and thus these companies need an explicit plan of how to mitigate such attacks.

Keywords

DDoS, Zombie, Botnet, Botmaster, Spoofing

Sammanfattning

Distributed Denial of Service (DDoS) attacker är ett problem som ständigt hotar företag, som förlitar sig till internet för centrala delar av sin verksamhet. En DDoS-attack som lyckas penetrerar ett företags nätverk kan medföra förödande skador i form av förlorade intäkter, minskad produktivitet, ökade kostnader samt skada på företagets rykte/varumärke.

DDoS-attackerna är många och av olika karaktär, som attackerar olika delar av ett företags nätverk, vilket leder till att det är svårt att effektivt skydda sig mot DDoS-attacker. Det står också klart att DDoS-attacker ökar både till antalet och storleksmässigt för varje år som går. Utifrån våra egna experiment har vi kunnat bevisa att vem som helst med små medel och begränsade kunskaper kan utföra en DDoS-attack som sänker en webbsida. Ett faktum som gör att alla företag vars verksamhet är baserad på internet bör räkna med att de någon gång bli utsatta för en DDoS-attack.

Utifrån våra undersökningar kan vi se att det finns en uppsjö av olika DDoS-skydd på marknaden, skydd som hanterar några problem som DDoS-attacker medför, men det finns inga kompletta skydd som kan garantera 100 % säkerhet. Utifrån tidigare forskning på området framgår det att det finns många olika sätt att skydda sig mot DDoS-attacker, t.ex. genom Software Defined Networks, Hop-Count Filtering eller Kill-bots.

Våra egna tester visar på att en virtuell brandvägg kan vara ett sätt att skydda sig mot DDoS-attacker, men testerna visar också att en sådan lösning inte heller är säker då man kan förstöra åtkomsten till webbsidan genom att överbelasta brandväggen.

Undersökningen visar också att ett av de vanligaste motiven bakom DDoS-attacker är kriminella ändamål. Kriminella som använder DDoS-attacker för att tjäna pengar genom att erbjuda riktade DDoS-attacker mot websidor eller genom försök att utpressa till betalning med DDoS-attacker som ett hot.

Vi har kommit fram till att de ekonomiska konsekvenserna av DDoS-attacker kan vara ödestigna för företag om det inte hanteras i tid. Genom våra egna beräkningar har vi visat att e-handelsföretaget CDON.com riskerar att förlora ca 36 415,90 kr per minut som en DDoS-attack pågår mot företaget.

Anledningen till av vi valt att ägnad denna uppsats åt DDoS-problemet, är den skrämmande ökningen av DDoS-attacker som man kan se sker årligen. Attackerna blir flera, de ökar storleksmässigt och de blir allt mer sofistikerade. Attackerna utförs också tillsynes omotiverat i vissa fall, men också välplanerade attacker utförs för att skada företag ekonomiskt.

I dagens företagsklimat är det viktigt att företaget har möjlighet att använda sig av internet för att driva verksamheten och göra det enkelt för kunder att ta del av företagets produkter/tjänster. Att företags webbsidor blir utslagen på grund av en DDoS-attacker är idag en verklighet, och en tydlig plan för att hur man ska hantera en sådan incident bör finns på plats inom företag.

Nyckelord

DDoS, Zombie, Botnet, Botmaster, Spoofing

Acknowledgments

We would like to thank Gerald Q. Maguire Jr. for his support, help and for letting us use his equipment and lab. We would also like to thank Björn Fredriksson at Nordea for giving us helpful tips along the way.

Stockholm, June, 2015
Martin Eklund and Patrik Ståhlberg

Innehållsförteckning

Lista över figurer

Lista över tabeller

Lista över förkortningar

C&C	Command-and-Control
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name System
Gbps	Gigabits per second
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
PCAP	Packet Capture
PPS	packets per second
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
THC	The Hacker's Choice
TLS	Transport Layer Security
UDP	User Datagram Protocol

1 Introduktion

Detta kapitel ger en kort bakgrund till projektet och leder vidare till problemställningen som motiverar detta examensarbete. Här presenteras också uppsatsens mål, syfte, avgränsningar, och vilken vetenskaplig metod vi använt oss av. Kapitlet avslutas med en disposition som beskriver rapportens struktur.

1.1 Bakgrund

Enligt Arbor Networks, Inc. är distribuerade överbelastningsattacker(DDoS-attacker) ett växande problem för företag världen över [1]. Ett företag som blir dabbat av en DDoS-attack riskerar att belastas med stora kostnader, samtidigt som de riskerar att förlora marknadsandelar [2].

I och med att kostnaderna kopplade till en DDoS-attack kan bli omfattande har det lett till att det finns ett stort utbud av tjänster som skyddar mot just DDoS-attacker. Många av leverantörerna av DDoS-skydd marknadsför sig som att det skyddar mot alla typer av DDoS-hot [3], men kan man verkligen skydda sig mot alla DDoS-hot?

Ett problem som företag ställs inför när det väljer att förlägga stora delar av sin verksamhet på internet är hur de ska skydda sig mot DDoS-attacker [1], [4]. Vilken typ av skydd kan företaget investerar i, som samtidigt är ekonomiskt försvarbart? Kommer skyddet att minska företagets kostnader eller kommer det bidra till ökade kostnader?

1.2 Problem definition

Den årliga trenden man kan se av DDoS-attacker är att de både ökar i antal, samt att de även ökar storleksmässigt. Attackerna blir även mer sofistikerade och utvecklas för att attackera flera delar av företagets infrastruktur, vilket gör det svårare för företag att skydda sig mot attackerna [1].

Med ökningen av antalet DDoS-attacker är det längre inte en fråga om ett företag ska bli utsatt för en DDoS-attack utan snarare när [1], [4]. När väl ett företag blir drabbat en DDoS-attack riskerar de att drabbas av förödande konsekvenser, såväl ekonomiska som varumärkesmässiga.

Det underliggande problemet som vi avser att lösa med denna rapport är att många företag är dåligt förberedda mot DDoS-attacker. Genom att åskodliggöra de ekonomiska konsekvenserna av DDoS-attacker och genom att utföra egna DDoS-attacker i en kontrollerad miljö, med begränsade förkunskaper, har vi förhoppningen att företag som inte har en handlingsplan färdig för hur de ska hantera DDoS-attacker ska ta tag i problemet och på så sätt rusta sig bättre inför framtiden.

1.3 Syfte

Syftet med denna uppsats är att ta reda på hur vanligt förekommande DDoS-attacker är på internet idag, vilka olika typer av DDoS-attacker det finns och hur de fungerar? Vi har också för avsikt att ta reda på vilka ekonomiska konsekvenserna en DDoS-attack kan leda till för utsatta företag, samt ta reda på vilka möjligheter det finns för de utsatta företagen att skydda sig mot DDoS-attacker. Frågeställningar:

1. Vad kan en DDoS-attack få för ekonomiskakonsekvenser för ett företag?
2. Hur kan kriminella använda sig av DDoS-attacker för att tjäna pengar?
3. Vad är de vanligaste motiven bakom en DDoS-attack?
4. Hur ser utvecklingen ut för DDoS-attacker?
5. Vilka olika typer av DDoS-attacker finns det?

6. Vilka typer av DDoS-skydd finns det?
7. Hur svårt är det att utföra en DDoS-attack?

1.4 Mål

Målet för uppsatsen är att få en tydlig bild av hur utvecklingen ser ut kring DDoS-attacker och öka våra kunskaper i området. Genom att belysa utvecklingen tillsammans med de ekonomiska konsekvenserna av DDoS-attacker, samt genom att visa hur lätt det är att genomföra en DDoS-attack har vi förhoppningen att kunna påverka företag att överväga att investera i DDoS-skydd.

De övergripande målet har brutits ner i följande delmål:

1. Genomföra en litteraturstudie av tidigare forskning i ämnet
2. Genomföra en litteraturstudie av utvecklingen av DDoS-attacker
3. Genomför en litteraturstudie av de ekonomiska konsekvenserna av DDoS-attacker
4. Undersöka vilka typer av DDoS-skydd som finns på marknaden idag.
5. Genomför egna DDoS-attacker i en kontrollerad miljö.
6. Presentera resultatet av litteraturstudien och experimenten

1.5 Vetenskaplig metod

Efter att ha övervägt olika alternativ av forskningsmetodiker valde vi slutligen att genomföra en litteraturstudie samt egna experiment där vi i en kontrollerad miljö utför DDoS-attacker utifrån olika scenarion.

1.5.1 Ekonomisk och tekniskt perspektiv

Vi har valt att tillämpa två perspektiv för vår undersökning, ett ekonomiskt – och ett tekniskt perspektiv. I litteraturstudien utgår vi utifrån ett rent ekonomiskt perspektiv och undersöker de olika konsekvenserna av DDoS-attacker. När vi sedan kommer till de egna experimenten utgår vi ifrån ett tekniskt perspektiv. Experiment där vi konstruerar en egen testmiljö och simulerar DDoS-attacker. Dels för att visa att det är relativt lätt att utföra, men också för att visa hur man kan försvara sig mot en DDoS-attack samt hur man kan identifiera en DDoS-attack genom att studera trafikflödet.

Anledningen till att vi valt att göra en två delad undersökning med fokus på både ekonomi och teknik. Grundar sig i det faktum att vi tillhör högskoleingenjörsprogrammet i Teknik och ekonomi. Ett program där man kombinerar kurser inom ekonomi och ett valt teknik område (datateknik i vårt fall). För att kunna ta examen ut en högskoleingenjörsexamen inom teknik och ekonomi krävs det att man genomför ett examensarbete som innehåller både ekonomiska och tekniska aspekter.

1.5.2 Litteraturstudie

Att företag skulle avslöja några detaljer angående sitt DDoS-skydd och hur mycket resurser företaget spenderar för att bekämpa DDoS-attacker, bedömer vi som högst osannolikt, då det är ofördelaktigt för företaget. Vilket skulle innebära att vi skulle spendera mycket tid på en undersökning som i slutändan inte ger några tillförlitliga resultat. Om vi mot förmodan skulle få ut någon information utifrån en intervjustudie eller en enkätundersökning tror vi att mycket av informationen skulle anses som hemlighetsstämplad, med avseende till företagenssäkerhet. Sedan

att företag skulle lägga resurser på att besvara våra frågor med vetskapen att det inte gynnar företaget på något sätt, utan enbart riskerar att skada företaget om informationen skulle komma på villovägar, tror vi återigen är osannolikt.

För att få information angående de ekonomiska konsekvenserna av DDoS-attacker, samt för att få en bild av utvecklingen kring DDoS-attacker, har vi istället använt oss av undersökningar som stora DDoS-skydds leverantörer genomfört (Arbor Networks och Kaspersky Lab) , under 2014. Vi har även granskat årsredovisningar från ett svenskt e-handelsföretag (CDON.com) för att beräkna vilken typ av skada en DDoS-attack skulle kunna göra på företagets nettoomsättning.

1.5.3 Experiment

Anledningen till att vi valt att utföra våra egna experiment är dels för att bredda våra egna kunskaper kring DDoS-attacker, hur man kan utföra dem och hur man kan skydda sig mot dem. Vi har också en förhoppning att våra experiment ska bevisa den hypotesen som vi hade när vi påbörjade detta arbete, d.v.s. DDoS-attacker är väldigt lätt att utföra utan någon tidigare kunskap. Genom att bevisa den hypotesen hoppas vi kunna motivera företag till att investera i DDoS-skydd.

Förutsättningen för att vi ska anse att vår hypotes är bevisad är att vi lyckas utföra tillräckligt kraftfulla attacker så att en testwebbsida blir otillgänlig för anvädnare.

1.6 Avgränsningar

På grund av den snäva tidsramen av 10 veckors arbetstid samt komplexiteten av ämnet, anser vi att det är lämpligast att avgränsa oss till enbart litteraturstudier och egna tester/experiment.

1.6.1 Avgränsning av litteraturstudier

Litteraturstudierna som ligger till grund för resultatet är avgränsade till Kaspersky labs "Global IT security risks survey 2014 – Distributed Denial pf Service(DDoS) attacks"[2], en världsomfattande undersökning kring utvecklingen av DDoS-attacker och dess ekonomiska effekt och 2014 års årsredovisning för det svenska e-handelsföretaget CDON.com[5].

1.6.2 Avgränsning av eget experiment

Vi har valt att begränsa oss till att utföra endast HTTP Get – och SYN flood attacker. Samt att testa att skydda oss mot DDoS-attacker, enbart genom att använda oss av en virtuell brandvägg.

1.7 Disposition

Kapitel 2 presenterar relevant bakgrundsinformation kring DDoS-attacker, hur utvecklingen ser ut, vilken tidigare forskning som gjorts inom området samt exempel på hur DDoS-attacker använts på internet idag för att uppnå olika syften. Kapitel 3 presenterar de vetenskapliga metoderna som vi valt att använda, vilka mål vi har för avsikt att uppnå. I kapitlet presenteras också processen bakom de olika insamlingsmetoderna samt de etiska aspekter som vi tagit hänsyn till. Kapitel 4 presenterar designen av testbädden vi använt för våra tester/experiment. Kapitel 5 presenterar resultatet av litteraturstudien och våra egna tester. Resultaten disskuteras även utifrån olika perspektiv. Kapitel 6 presenterar slutsatserna vi dragit av undersökningen och hur resultatet påverkats beroende på förutsättningarna. Vi presenterar också förslag för hur man skulle kunna gå vidare och utöka studien. Och slutligen avslutas kapitlet med vår egen reflektion av undersökningen, utifrån olika perspektiv.

2 Bakgrund

Det här avsnittet bidrar med grundläggand kunskaper om DDoS-attacker, vilket vi anser är nödvändigt för läsaren att kunna ta till sig innehållet i rapporten. Avsnittet innehåller också relevant information om utvecklingen av DDoS-attacker, tidigare forskning och skydd som finns tillgängliga på marknaden idag. Bakgrundsavsnittet disponeras på följande sätt.

2.1 Bagrundens disposition

Eftersom bakgrundskapitlet är det längsta kapitlet av rapporten har vi valt att göra en separat disposition för att underlätta för läsaren att särskilja de olika sektionerna av bakgrunden.

2.1.1 Begrepp

För att få en bättre förståelse av vad DDoS-attacker är och innebörden av de olika begreppen som frekvent förekommer i texten har vi gjort detta bakgrundsavsnitt där de olika beståndsdelarna av DDoS behandlas med korta beskrivningar och förklarande bilder.

2.1.2 Motiv

Vi behandlar också vilka motiv som är vanligt förekommande bakom DDoS-attacker, vilket vi tror kan ge läsaren en förklaring till varför antalet DDoS-attacker ökar. Vi går också in i detalj på hur kriminella utnyttjar DDoS-attacker för att tjäna pengar.

2.1.3 Angripare

Vidare förklarar vi vilka olika typer av DDoS-attacker som förekommer på internet idag. Vi förklara också kort hur varje attack fungerar rent tekniskt för att läsaren ska få en förståelse av den bakomliggande tekniken av DDoS-attacker och för att få en bättre förståelse för vad DDoS-attacker är.

2.1.4 Utvecklingen av DDoS

För att få en bättre bild av hur utvecklingen har sett ut av DDoS sedan det först dök upp på internet till idag, presenterar vi resultatet av en årlig världsomfattande undersökning utförd av Arbor Networks som syftar till att följa utvecklingen av DDoS-attacker mot företag och myndigheter världen över.

2.1.5 En känd DDoS-attack

För att ge läsaren ett riktigt exempel på hur en DDoS-attack kan påverka ett företag, presenterar vi delar ur Teliasoneras egen incidentrapport angående DDoS-attacken som företaget utsattes för 2014.

2.1.6 DDoS-skydd

Efter att lagt mycket fokus på DDoS-attacker har vi valt att också ta med ett avsnitt där vi presenterar olika företag som tillhandahåller DDoS-skydd. Några av de största aktöreran på marknaden samt ett par mindre som kan tänkas vara intressanta för svenska företag.

2.1.7 Tidigare forskning

För att visa hur brett området är har vi valt att presentera tidigare forskning inom området DDoS. Bestående av utvalda rapporter vi anser vara relevanta för området eller som är lik vår egen forskning.

2.1.8 Sammanfattning

Slutligen avslutar vi bakgrundsavsnittet med att sammanfatta avsnittet och lyfta tillbaka de central delarna som vi anser att läsaren behöver ha med sig när de fortsätter till nästa del av rapporten.

2.2 Vad är DoS- och DDoS-attacker

Denial of service (DoS) är en attack vars mål är att delvis begränsa eller helt begränsa offrets möjlighet att utföra nyttigt arbete, genom att överrösa offret med massiva mängder trafik i form av "requests" eller data. Offren kan vara allt ifrån serverar, klienter, routrar, en nätvärkslänk, ett helt nätverk, en internetanvändare, en internetleverantör, ett land eller ett företag som använder sig av internet för att förmedla sina tjänster [6].

T ex när ett e-företag som säljer produkter/tjänster över internet blir utsatt för en DoS-attack begränsas delvis företagets legitima kunders möjlighet att logga in på webbsidan och genomföra köp av företagets produkter/tjänster, eller i värsta fall kan kunderna inte logga in på webbsidan överhuvudtaget på grund av attacken. Vilket innebär att försäljningen stoppas.

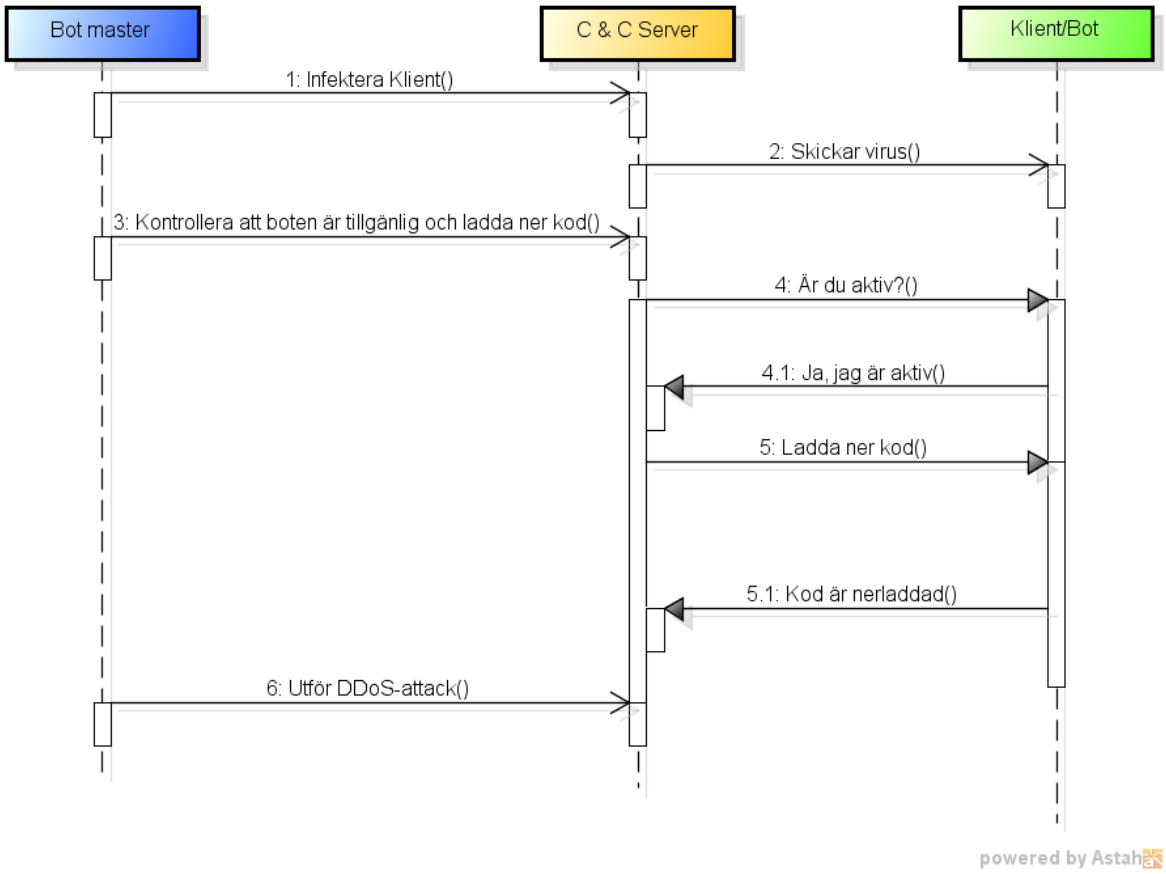
Fallet när det handlar om en DoS-attack initieras attacken av en ensam värd. Däremot när det handlar om en Distributed Denial of Service-attack (DDoS-attack) är det istället en grupp skadliga värdar som utför attacken.

2.3 Vad är ett botnät?

Ett botnät är ett nätverk av infekterade datorer (bots/zombies). Datorerna är infekterade av ett virus (Trojan), som sedan kriminella kan använda för att ta kontroll över datorerna. Genom att ta kontroll av varje individuell dator och sedan organisera dem i ett nätverk av infekterade datorer(botnät) [7]. De kriminella kan sedan styra nätverket från distans och använda dem t.ex. för att utföra DDoS-attacker, skicka spam, utföra nätbedrägerier, sälja piratkopierade spel/program, utföra hacker attacker, etc [8].

2.3.1 Hur fungerar det?

Det första som händer när ett botnät skapas är att datorer blir infekterade av ett virus. Nästa som händer är att de infekterade datorerna blir kontaktade av en kommando och kontroll server (C & C). När kontakten sker berättar boten/klienten om den är aktiv och redo för tjänstgöring. Servern gör då ett avgörande om vilken ytterligare kod klienten/boten ska ladda ner och exekvera [9]. Bakom C & C servern finns administratören för botnätet, bot mastern/bot- herden. Bot mastern styr C & C servern och anger vilken typ av verksamhet den ska bedriva [9].



Figur 1: **Sekvensdiagram skapandet av ett botnät**

2.4 Motivation bakom DDoS-attacker

Det finns många bakomliggande motiv när det kommer till DDoS-attacker, allt ifrån ekonomisk vinning, politiska -/religiösa mål, kriminella ändamål etc [1][10]. Kriminella ändamål är en av motivationerna som placerar sig högt upp på listan av de vanligaste motiven till DDoS-attacker [1]. På grund av att det är ett så vanligt motiv kan det vara lönt att titta närmare på hur det visar sig på internet idag. Det är också speciellt intressant ur företagssynpunkt då det ofta är de som blir offren för attacker som är kriminellt motiverade [1].

2.5 DDoS-attacker på en affärsverksamhet

Allt eftersom att utevecklingen av DDoS-Attacker gått framåt, har det dykt upp en ny marknad för försäljning av DDoS-attacker. Det är en marknad där ljusskygga aktörer erbjuder tjänster som möjliggör för en kund att lätt genomföra en egen DDoS-attack mot ett önskat mål [1]. Det finns också maffia-liknande utpressningsmetoder där man med hot om att utföra en DDoS-attack försöker förmå ett offer att betala en avgift för att slippa attacken. [Bilaga A]

2.5.1 Uthyrning av botnät

Uthyrning av botnät för att genomföra DDoS-attacker är en växande marknad. Tjänsten fungerar som följer: mot betalning får kunden tillgång till ett färdigt botnät av infekterade datorer som är redo att utnyttjas för att utföra DDoS-Attacker mot önskade offer [11–13].

Utbudet av botnät har växt sig så stort att kunderna har många alternativ att välja mellan, vilket har lätt till att det uppstått en konkurrenssituation mellan de olika leverantörerna av botnät. Ett sätt man kan se att det har uppstått konkurrens bland leverantörerna är att de börjat använda sig av marknadsföringstaktiket i form av gratistester för att differentiera sig från sina konkurrenter, för att locka potentiella kunder. Genom att kunden får gratis tillgång till botnätet i t.ex. en 10 minutersperiod får kunden möjlighet att testa botnätets kapacitet för att bilda sig en uppfattning av vad de kan tänkas åsdakomma för DDoS-attacker, vilket sedan leverantören hoppas ska leda till att kunden väljer att betala för att hyra botnätet [12].

Ett annat marknadsföringsknep som botnät leverantörerna använder sig av är demonstrationer, dvs. leverantören väljer ut ett offer som de sedan utför en riktad DDoS-attack emot för att visa botnätets kapacitet [1].

Utifrån resultatet framgår det att man med väldigt små medel, endast $35, kan få tillgång till ett botnät innehållande 1000 datorer, som är redo att utföra DDoS-Attacker mot önskade mål. Attacker som potentiellet kan medföra avsevärda kostnader för drabbade företag.

Tabell 1: Kostnad för att hyra ett botnät bestående av 1000 datorer

Position av botnät	Pris
Kanada	$270
Storbritannien	$240
Ryssland	$200
Frankrike	$200
USA	$180
Världsomfattande	$35

2.5.2 Beställning av riktade DDoS-attacker

En annan tjänst som finns tillgänglig är att beställa en riktad DDoS-attack. Det enda kunden behöver göra är att betala för tjänsten och ange vilken webbsida som de vill att leverantören ska attackera [14][Bilaga B]. Sedan sköter leverantören resten.

I Bilaga B kan man se ett tydligt exempel av en webbsida tillhörande en aktör som specialiserat sig på att genomföra riktade DDoS-Attacker mot betalning. Leverantören riktar sig till bl.a. företag som önskar få konkurrensfördelar genom att leverantören utför en DDoS-attack mot en eller flera av företagets konkurrenter, vilket framgår av nedanstående citat från leverantörens webbsida.

"It seems that all is well and business have long gained its momentum, but has recently appeared a number of competitors with whom you just can not cope? Our company offers a ddoS attack order, by which time your competitors go out of control due to off and hang on their sites." [Bilaga B]

Utöver ovanstående citat förklarar också levernatören vilka negativa effekter en riktad DDoS-attack kommer att få för konkurrenterna, samtidigt som leverantören framhäver kundens möjlighet att tjäna mera pengar medan konkurrenterna är upptagna med att försöka hantera effekterna av DDoS-attacken [14]. Leverantören erbjuder flera olika typer av attacker och de erbjuder också ett 10-15 minuters långt gratistest av tjänsten[15].

2.5.2.1 Priser

Leverantören baserar sin prissättning utifrån hur lång tid kunden vill att attacken ska pågå. De erbjuder också en rad olika rabatter om man väljer Attacker som varar längre än en vecka. Här nedan är en prislista, där minimum priserna är angivna för de olika tidsintervallen DDoS-attacken

ska pågå, priset kan dock skilja sig från minimum priset beroende på vem som är det tilltänkta offret[15].

Aktören erbjuder fyra olika typer av priser beroende på hur länge man vill att attackerna ska pågå. Aktören uppger också att det är minimum priserna, då priserna kan skilja beroende på vad målet för attacken är [14].

Tabell 2: Priser TOP- DDOS Service (Support)

Pris	Längd av attack
$5	1 timmes lång attack
$40	24 timmars lång attack
$260	1 veckas ihållande attack
$900	1 månads ihållande attack

2.5.3 Utpressning

Ett tredje sätt för kriminella att tjäna pengar på DDoS-attacker är utpressning, vilket fungerar på följande sätt. De kriminella skickar ett mail till ett företag där de förklara att om företaget inte betalar en angiven summa pengar, kommer företagets webbsida att bli utsatt för en DDoS-attack, vilket kommer att göra sidan obrukbar till dess att summan har betalats. Samma summa ska sedan betalas ut varje månad för att företaget ska undvika DDoS-attacker. Eventuella förseningar av betalningen resulterar i att avgiften höjs för varje dag den är försenad [16][Bilaga A].

2.6 DDoS Attacker

Ofta brukar DDoS-attacker delas upp i tre olika kategorier:

- Volymbaserade attacker,
- Protokollattacker, och
- Applikationslagerattacker.

2.6.1 Volymbaserade attacker

Attacker som baseras på volym fokuserar på att försöka överbelasta offrets nätverksresurser genom att skicka stora mängder data som mättar offrets anslutning till internet. Attacker av denna typ kallas på engelska för "floods", vilket ger en bra bild av vad som faktiskt sker. Offret blir översvämmat av data. En typisk översvämnings attack är distribuerad mellan tusentals frivilliga datorer och/eller zombies även kallat botnät, som alla skickar stora mängder data till offret vars nätverk blir överbelastat. En legitim användare, som under tiden av en sådan attack, försöker anropa offrets webbsida kommer märka att det går extremt långsamt eller till och med inte lyckas nå sidan alls. Några vanliga volymbaserade attacker är UDP översvämning och ICMP/Ping översvämning [17], [18].

2.6.1.1 UDP översvämning

User Datagram Protocol (UDP) är ett anslutningslöst protokoll som skickar datagram till andra värdar på ett IP-nätverk utan att tidigare behövt upprätta någon typ av session mellan enheterna (ingen handslagsprocess behövs). En UDP översvämnings attack utnyttjar ingen specifik svaghet, utan missbrukar istället UDPs normala beteende i en sådan hög grad att det orsakar trängsel på

offrets nätverk. Attacken går till på så sätt att ett mycket stort antal UDP datagram skickas, ofta från spoofade IP adresser, till slumpvis valda portar på offrets server. Servern som tar emot denna trafik klarar inte av att bearbeta all data, utan använder istället hela sin bandbredd till att försöka skicka Internet Control Message Protocol (ICMP) “destination unreachable" paket som svar på att ingen applikation lyssnar på de valda portarna. Eftersom en UDP översvämnings attack är volymbaserad mäts attacken ofta i Gbps (bandbredd) och paket per sekund (PPS) [17], [18].

2.6.1.2 ICMP/Ping översvämning

Internet Control Message Protocol (ICMP) är också ett anslutningslöst protokoll som användas för IP operationer, diagnostik och felmeddelanden. En ICMP/Ping Översvämnings attack är relativt lik en UDP Översvämnings attack på så sätt att ICMP Översvämning inte heller utnyttjar någon specifik svaghet för att uppnå denial-of-service. ICMP Översvämning överbelastar servern med ICMP Echo Requests (Ping) paket genom att skicka tillräckligt många tillräckligt snabbt utan att vänta på svar. Detta leder till att servern använder en stor del av både sin utgående och ingående bandbredd till att försöka svara med ICMP Echo Reply paket, vilket resulterar i att servern/systemet blir betydligt långsammare [17], [18].

2.6.2 Protokollattacker

Protokollattacker inriktar sig på en servers resurser, i ett försök att förbruka serverns beräkningskapacitet eller minne, för att uppnå ett tillstånd av denial-of-service. Tanken bakom attacken är att angriparen utnyttjar existerande svagheter på servern eller i kommunikationsprotokollen så att servern blir för upptagen med att hantera de falska förfrågningarna och på så sätt inte har tillräckligt med resurser för att hantera de legitima förfrågningarna.

TCP/IP är till skillnad från UDP ett anslutningsorienterat protokoll. Med det menas att sändaren av ett paket måste upprätta en komplett anslutning med mottagaren innan några paket kan skickas. TCP/IP gör det genom en mekanism som kallas för "three-way handshake", där sändaren skickar ett SYN meddelande, får ett SYN-ACK meddelande som svar och avslutar handslaget med att skicka tillbaka ett ACK meddelande. Dessa meddelanden skapar en halvöppen anslutning. Ofta missbrukar angripare TCP/IP protokollet genom att skicka dessa TCP paket i fel ordning vilket resulterar i att serverns beräkningskapacitet tar slut i ett försök att förstå den onormala trafiken [17].

2.6.2.1 TCP SYN översvämning

Under en SYN översvämnings attack får angriparna servern att tro att de vill upprätta legitima anslutningar genom en mängd TCP förfrågningar med TCP flaggan satt till SYN, från spoofade IP adresser. På grund av tre-vägs handskakning måste servern då allokera buffers för att förbereda anslutningarna och sedan skicka ett SYN-ACK meddelande som svar, men eftersom angriparnas IP adresser är spoofade skickas aldrig ett ACK meddelande tillbaka till servern. Servern måste hålla dessa anslutningar öppna och skicka om dessa SYN-ACK meddelande som inte besvaras, tills en time-out uppstår. Serverns resurser är dock begränsade och en SYN översvämnings attack skapar så många anslutningsförfrågningar att den inte hinner få time-out på anslutningar innan mängder av nya kommit in. På så sätt uppstår lätt ett denial-of-service tillstånd [18].

Figur 2: **SYN översvämning och TCP handskakning**

2.6.2.2 SSL baserade attacker

Eftersom Secure Socket Layer (SSL), en krypteringsmetod som används av ett flertal kommunikationsprotokoll, blivit allt mer populärt, har angripare börjat inrikta sig mot det. SSL körs konceptuellt ovanför TCP/IP och ger säkerhet åt användare som kommunicerar genom andra protokoll genom att kryptera deras trafik och autentisera parterna som kommunicerar.

Attacker baserade på SSL kan användas på många olika sätt, bl.a. skicka skräpdata till SSL servern, missbruka funktionen som styr krypteringsnyckelns förhandlingsprocess eller inrikta sig på handslags mekanismen.

Ett av de värsta problemen med SSL attacker, som även gör det så populärt för en angripare, är att krävs väldigt mycket mer resurser av en server att hantera en sådan attack jämfört med att utföra den. Detta på grund av att en SSL attack kan skickas över SSL-krypterad trafik, vilket gör det väldigt svårt att identifiera attacken [17].

2.6.2.3 Krypteringsbaserad HTTP attack (HTTPS översvämning)

Företag världen över börjar mer och mer att använda sig av SSL/TLS (Transport Layer Security) i deras applikationer för att kryptera och säkra deras trafik. Attacker mot krypterad trafik blir på så sätt även allt mer populära, för att det är så svårt att stoppa. DDoS-skydden som finns idag inspekterar inte SSL trafiken eftersom det skulle kräva att den krypterade datan dekrypterades. HTTPS översvämning är en typ av attack som blivit väldigt framgångsrik, där massiva mängder krypterad HTTP trafik skickas. Detta på grund av att den krypterade HTTP attacken för med sig utmaningar som kräver krypterings- och dekrypterings mekanismer för försvararen [18].

2.6.2.4 THC-SSL-DOS

Detta är ett verktyg som togs fram av hackergruppen The Hacker's Choice (THC) för att bevisa och uppmuntra en förbättring av SSLs sårbarhet. THC-SSL-DOS är en väldigt effektiv DoS attack då det bara kräver ett litet antal paket för att åstadkomma en denial-of-service för en server. Vad som händer är att attacken missbrukar SSLs handslagsprocess genom att omförhandla krypteringsnycklen, om och om igen ändå tills serverns resurser är förbrukade. Den är så effektiv på grund av att serverns resurser förbrukas 15 gånger snabbare än klientens. Det påstås även att en enda hemPC kan ta ner en hel SSL baserad web server. Då förstår man även vad flera maskiner tillsammans kan åstadkomma med en DDoS attack [17].

2.6.3 Applikationslagerattacker

Attacker mot applikationslagret är idag bland det vanligaste en angripare fokuserar på och attackerna ökar för varje år. Dessa attacker riktar sig inte enbart mot HTTP utan även mot HTTPS, Domain Name System (DNS), Voice over IP(VOIP), Simple Mail Transfer Protocol (SMTP) och andra applikationsprokoll som har någon typ av svaghet som kan utnyttjas eller missbrukar för att uppnå ett tillstånd av överbelastning. Eftersom HTTP är det mest använda applikationsprotokollet på internet idag är det väldigt populärt att angripa för en person/grupp som vill åstadkomma skada på en webbsida [17].

2.6.3.1 DNS översvämning

DNS Översvämning är baserat på samma sätt som de andra flood attackerna, genom att skicka stora mängder DNS förfrågningar. DNS är ett protokoll som används för att översätta domännamn till IP adresser och använder sig av det underliggande UDP protokollet. DNS utnyttjar på så sätt den snabba begär- och svarstiden utan att behöva ta hänsyn till att skapa någon anslutning först, som TCP behöver. Under en DNS Översvämnings attack missbrukas detta för att skicka stora mängder DNS förfrågningar, via botnets eller direkt. Målet är då att få DNS server så pass överbelastad att den inte kan hantera fler DNS förfrågningar, och så småningom krascha [17].

2.6.3.2 DNS Amplification

DNS Amplification är en typ av DDoS attack som utnyttjar DNS serverns beteende för att amplifiera attacken. För att utföra attacken behöver angriparen först och främst spoofa IP adressen av DNS resolvern och byta ut den mot offrets IP adress. Detta gör så att svaren från DNS servern skickas till offret istället.

Angriparen behöver även hitta en internet domän som är registrerad med många DNS records. Under attacken skickas DNS frågor som begär hela listan av DNS records för den domänen. Detta görs för att svaren som skickas till offret ska vara så stora som möjligt, ofta så stora att de behöver delas upp i flera paket.

Med hjälp av väldigt få datorer kan angriparen alltså skicka en stor mängd korta DNS frågor till alla DNS servrar och fråga efter deras DNS records listor. DNS servern letar efter svaren och ger dessa till DNS resolvern. Eftersom angriparen spoofade IP adressen för DNS resolvern och ersatte den med offrets IP adress kommer alla DNS svar skickas till offret istället.

Angriparen uppnår på detta sätt en amplifikations effekt eftersom varje kort DNS fråga, genererar ett svar som ibland är upp till 100 gånger så stort som frågan. Skulle t.ex. angriparen generera 3Mbps av DNS frågor, amplifieras detta till 300Mbps av trafik till offret.

Offret blir utsatt för en enorm mängd DNS svar där varje svar även är uppdelat i flera paket. Detta kräver att offret även måste återmontera paketen vilket är en resurskrävande uppgift

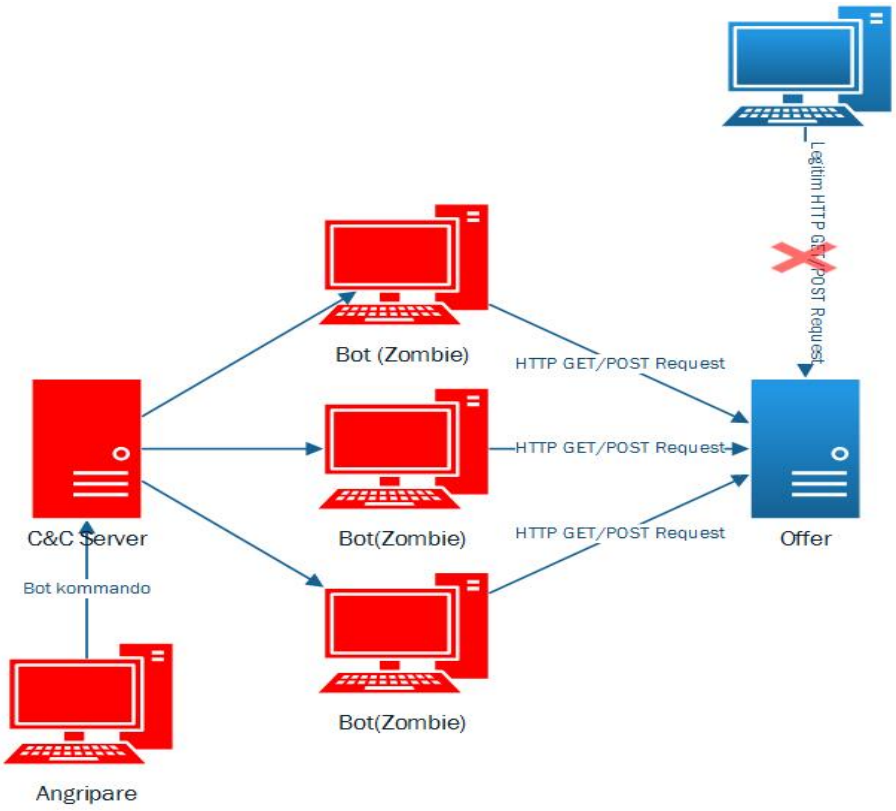
samtidigt som den hanterar resten av angriparens trafik. Snart nog är offret så pass upptagen med att hantera angriparens trafik att offret inte längre kan serva någon legitim användare och angriparen har uppnått ett denial of service tillstånd [19].

2.6.3.3 HTTP Översvämning

HTTP översvämning är den absolut vanligaste DDoS attacken mot applikationslagret. Attacken fungerar på så sätt att det skickas, vad man kan tro är legitima sessionsbaserade HTTP GET eller POST förfrågningar till offrets web server. Attacken sker ofta synkroniserat från flera datorer samtidigt som kontinuerligt ber om att få ladda ned offrets webbsida. Detta görs i syfte att dränka applikationens resurser i så många förfrågningar att ett denial-of-service tillstånd uppstår. Skillnaden på GET och POST förfrågningar är:

POST förfrågningar innehåller parametrar (som ofta tas ifrån input fälten på en sida) som kan sätta igång komplexa processer på en server (då servern t.ex. behöver kontakta någon databas) som kräver mer av dess resurser än en vanlig GET förfrågning. POST översvämning anses därför vara effektivare än GET översvämning eftersom det kräver färre förfrågningar för att sänka en server.

GET översvämning å andra sidan är betydligt vanligare än POST översvämning, då det är mycket enklare att utföra. GET förfrågningar sker så fort man öppnar en “vanlig länk" och inkluderar t.ex. bilder, generellt sett statisk data [17].



Figur 3: HTTP översvämnings attack

2.7 Utvecklingen av DDoS-attacker

Detta avsnitt visar hur utvecklingen av DDoS-attacker ser ut i världen, baserat på Arbor Networks årliga undersökning [1].

2.7.1 Arbor Networks

2014 utförde säkerhetsföretaget Arbor Networks en undersökning där internetleverantörer och representanter från regeringar, företag och utbildningsinstitut, runtom i världen får besvara 182 frågor, bestående av friformsfrågor och flervalsfrågor. Utifrån svaren (287 svarande) har Arbor Networks sammanställt en rapport, "Worldwide Infrastructure Security Report X", som visar på hur utvecklingen av DDoS-attacker ser ut i världen. Hur antalet attacker ökat, hur storleken på attackerna förändrats över tid och i hur stor utsträckning olika typer av DDoS-attacker förekommer. Det är ett årligt återkommande arbete som Arbor Networks gör och 2014 års upplaga är nummer 10 av rapporten [1].

Vi har valt att använda oss av Arbor Networks rapport för att visa på hur trenden ser ut kring DDoS-attacker. Anledningen till att vi valt att använda oss av just den rapporten är för att det är baserat på en världsomfattande undersökning, som vi känner stor tillförlitlighet till.

2.7.2 Resultat av “Worldwide Infrastructure Security Report X"

Resultatet av Arbor Networks Worldwide Infrastructure Security Report X visar på en utveckling där DDoS-attacker ökar i antal och ökar storleksmässigt [1].

2.7.2.1 Förekomsten av DDoS-attacker

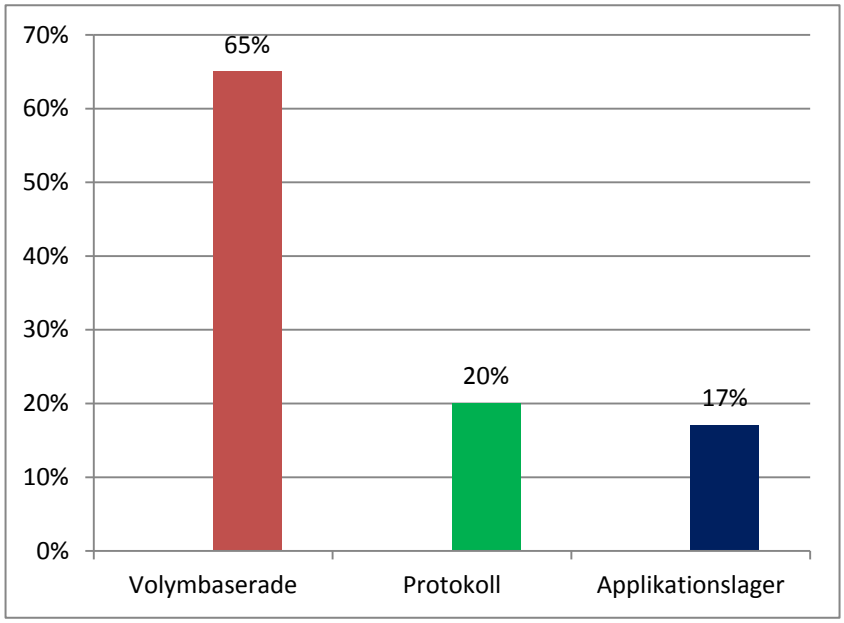
DDoS-Attacker har sedan de först uppkom för drygt 15 år sedan växt till att bli ett ständigt hot mot företag och operatörer över hela världen som utnyttjar internet för sin verksamhet. Det man kan se är att DDoS-attackerna är under ständig utveckling och blir allt mer sofistikerade för varje år som går [3] [20]. Hur många som blir utsatta för DDoS-attacker är väldigt svårt att avgöra då det finns ett stort mörkertal över antalet attacker. Företag(t.ex. en bank) som ofta blir utsatta för DDoS-attacker löper risken att bli stämplade som osäkra och riskerar då att förlorar kunder pga. av en osmickrande image [2]. Således är det fördelaktigt att hemlighetsstämpla information om att företaget blivit utsatta för en DDoS-attack, för att minimera risken att informationen ska nå befintliga eller potentiella kunder. Resultatet av Worldwide Infrastructure Security Report X visar dock, att av de 287 svarande angav 42 % att de blivit utsatta för mer än 21 attacker i månaden, under 2014 [1].

2.7.2.2 Ökning av olika DDoS-attacker

Dagens DDoS-skydd som erbjuds på marknaden idag är välanpassade för att hantera stora datamängder, vilket förekommer vid volymbaserade attacker. Det har i sin tur lätt till en utveckling där attacker som är riktade mot applikationslagret har ökat kraftigt, vilket är svåra att skydda sig mot. Med en ökning av attacker som riktar sig mot applikationslagret vore ett rimligt antagande vara att antalet volymbaserade attacker skulle ha minskat, men så är inte fallet. Antalet volymbaserade attacker har även de ökat i antal och även storleksmässigt. [20]

Arbor Networks undersökning visar på en ökning på hela 86 % i antalet attacker som var riktade mot applikationslagret, från 2013 – 2014. Undersökningen visar också på att volymbaserade attacker fortfarande dominerar ifråga om antal, ca 65 % av de tillfrågade angav att de blivit utsatt

för volymbaserade attacker under 2014, medan bara 17 % angav att de blivit utsatta för attacker riktade mot applikationslagret [1].

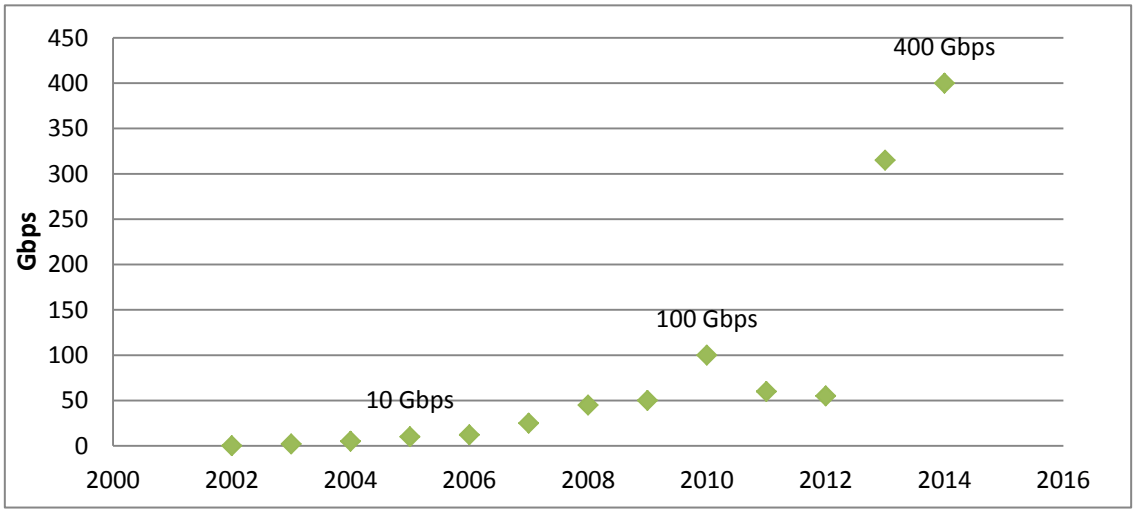


Figur 4: **Andel tillfrågade som blivit utsatta för DDoS attacker (data från Arbor Networks)**

2.7.2.3 Storleksökningen av volymbaserade attacker

Om man går tillbaka i tiden så långt som till 2005 kan man se att den största rapporterade attacken befann sig i storleksordningen 10 Gbps. Följer man sedan utvecklingskurvan fem år framåt i tiden till 2010 kan man se att storleken på de största rapporterade attackerna växer för varje år som går. År 2010 hade storleken 10 dubblats i jämförelse med 2005, 10 Gbps → 100 Gbps [1].

2011 och 2012 skede dock ett trendbrott och storleken på de största attackerna minskade i storlek, till ca 50 Gbps, vilket är en halvering från 2010 års toppresultat på 100 Gbps. Under år 2013 vände trenden dock åter igen och seglade upp på nya rekordnivåer, när den störta attacken noterades på nivåer strax ovanför 300 Gbps. För att sedan 2014 växa igen till hela 400 Gbps [1].

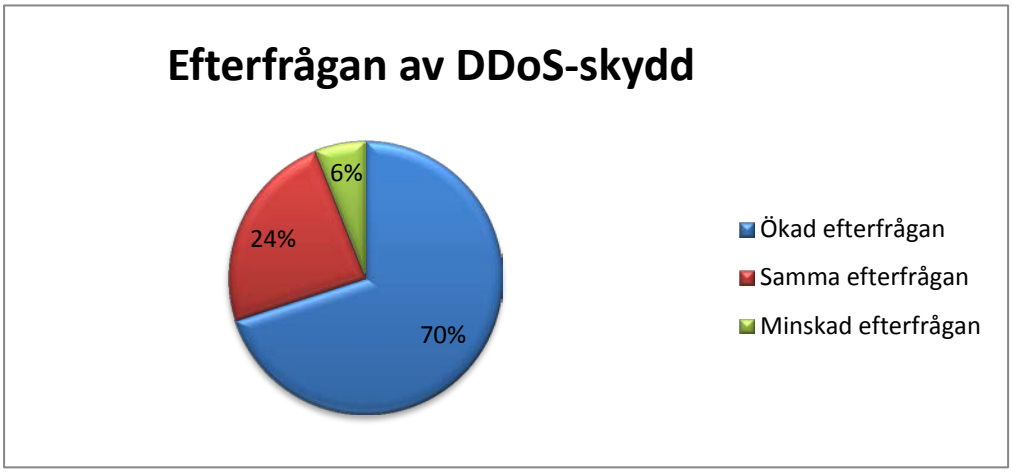


Figur 5: **Storleksmässig förändring av Volymbaserade attacker**

Toppnoteringen från 2014 på 400 Gbps motsvarar en storleksökning på hela 4000 % om man jämför med nivåerna som de största attackerna låg på 2005, 10 Gbps. Det finns en tydlig trend att de största attackernas storlek växer med tiden, men utifrån utredningen kan man också se att antalet attacker med storleksordningen över 100 Gbps växer till antalet. För bara några år sedan var en attack med storleksordningen över 100 Gbps väldigt ovanligt, men så är inte längre fallet idag [1].

2.7.2.4 Ökad efterfrågan av DDoS-skydd

Ett annat tecken på att antalet DDoS-attacker ökat från 2013-2014 är den ökade efterfrågan på DDoS-skydd som leverantörerna har noterat [1].



Figur 6: Förändring av efterfrågan av DDoS-skydd 2014

I undersökningen uppger 70 % av de tillfrågade leverantörerna av DDoS-skydd att de har en ökad efterfrågan [1]. Det bör tolkas som att antalet DDoS-attacker har ökat, eventuellt att företag har blivit mer säkerhetsmedvetna och ser en större hotbild när det kommer till DDoS-attacker.

2.8 En känd DDoS-attack

Som tidigare nämnts förekommer det en trend där antalet DDoS-attacker ökar och de växer storleksmässigt. Men eftersom det ur marknadsföringssynpunkt är ofördelaktigt för företag att tillkännage att de blivit utsatt för en DDoS-attack är det sannolikt att det finns ett stort mörkertal av attacker som inte rapporteras. I detta avsnitt tar vi dock upp en känd attack, som har rapporterats om i media.

2.8.1 2014 Telia

I december 2014 blev Telia utsatt för en massiv DDoS-attack vilket fick effekten att internetåtkomsten i Telias nät helt slogs ut. Det ledde till att Telias internettjänster inte fungerade, inklusive tv och IP-telefoni. IP-telefoni blev så pass begränsad så att kunder inte ens kunde ringa 112 [21], [22]. Det innebar att kunder med Telia abonnemang varken kunde surfa på internet eller se på tv.

Utifrån den incidentrapport som Teliasonera lämnat ifrån sig till Post- och telestyrelsen(PTS) framgår det att avbrottet orsakades av återkommande DDoS-attacker, vilket ledde till stor inverkan på internetbaserade tjänster. Teliasonera hävdar att attacken genomfördes genom att kunders

utrustning blev kapade och anledningen till att kapningen var möjlig, berodde på felaktiga inställningar i utrustningen [21][22].

2.8.1.1 Händelseförlopp

Med hjälp av den kapade utrustningen kunde angriparna sedan skapa en förstärkt attack, av skadelystna DNS-förfrågningar [21],[22]. Det ledde till att lastbalanseraren i Teliasoneras nätverk blev överbelastad, vilket resulterade i att tjänsterna delvis kraschade [21], [22].

Hela förloppet bestod av attacker i tre omgångar. Först en kortare attack som startade klock 22 den 9 december, följt av en längre attack den 10 december, en attack som pågick mellan 09:44 och 20:00. Den avlutande attacken utfördes den 12 december och pågick mellan 02:00 och 05:00[21].

För att lösa problemen som attacken medförde sattes ett antal åtgärder in, men exakt vad dess åtgärder var är sekretessbelagt. Det framgår i incidentrapporten att åtgärderna var framgångsrika - attacker som var riktade mot företaget senare dagar gav inte samma effekt som tidigare [21], [22]. Det förblir fortfarande okänt vem som låg bakom attacken. Dock har den ryska hackargruppen Lizard Squad tagit på sig ansvaret för attacken, via Twitter. De hävdar att målet för attacken var spelföretaget EA. Huruvida det stämmer har ännu inte gått att bekräfta [21].

2.9 DDoS-skydd på marknaden

Det finns många olika leverantörer av DDoS-skydd på marknaden. För att få en bättre förståelse av hur de olika skydden fungerar har vi granskat leverantörerans produktbeskrivning. Leverantörerna är, Telia, Arbor Networks, Kaspersky lab, Cisco Systems och Juniper Networks. För att få en detaljerad beskring av varje produkt se [Bilaga C].

Det finns också sätt att upptäcka planerade DDoS-attacker, innan de utförs. Netflix har släppt tre opensoucre verktyg(Scrumbler och sketchy) för att upptäcka planerade DDoS-attacker [23].

Med hjälp av fördefinierade(görs av en administratör) nyckelord söker "Scrumbler" igenom forum på social media nätverk för att hitta diskussioner om potentiella hack eller DDoS-attacker mot organisationer. "Sketch" tar sedan en skärmdump av innehållet för att sedan ta bort texten från sidan [23].

2.10 Tidigare forskning

I detta avsnitt behandlas tidigare forskning inom området olika sätt att upptäcka DDoS-attacker och skydda sig mot dem. Samt begrepp som kan vara relevant för läsaren när de fortsätter igenom rapporten.

2.10.1 Software Defined Networking

DDoS-attacker har studerats i ett flertal år nu, men man kan ändå se en ökning av attackerna i både antal och styrka för varje år som går. UDP, TCP SYN, och ICMP översvämnings attacker dominerar ökningen och målet för dessa volymbaserade attacker är att utarma offrets beräkningsresurser såsom CPU, minne och nätverkets bandbredd genom att skicka en enorm mängd skräpdata. Under senare år har man även lagt märke till en stor ökning av multi-vector DDoS-attacker [24]. Till exempel då en UDP översvämning kombineras med en slow HTTP GET översvämning, vilket vilseleder offret att försöka hantera den onormala UDP trafiken, medan HTTP översvämningen sakta men säkert utarmar HTTP serverns beräkningsresurser.

Många förslag för att hantera DDoS-attacker har tagits fram av både akademin och industrin. Få av dessa tekniker har dock tagits i bruk på grund av komplexiteten i deras implementation, där antaganden görs som inte stämmer överens med dagens verklighet och skulle kräva stora ändringar för en utbredd "deployment" [25].

Den snabba utvecklingen av Software Defined Networking (SDN) ger dock en möjlighet att ompröva och förbättra DDoS-skydden tack vare frikopplingen av nätverkets control plane och data plane samt controllern's programerbarhet. SDN controllern får en global överblick av nätverkets tillstånd och kan på ett centraliserat sätt skydda nätverket [25].

2.10.1.1 Komponenter

Nedan förklaras de olika komponenterna som föreslås i författarnas ramverk.

2.10.1.1.1 OpenFlow Switch

OpenFlow switchar håller tabeller över olika flöden för att utföra lookups och forwarding av paket. "Flow entries" består av "match fields", counters, och actions som appliceras på matchande flöden.

När en OpenFlow switchar tar emot ett flöde, utför den en lookup operation i flödestabellen, finns inte det flödet med, skickas informationen om flödet vidare till controllern [25].

2.10.1.1.2 Middlebox

En middlebox är en enhet som säkerställer säkerhets policies för att mildra attacker. I författarnas ramverk föreslås att middleboxen lagrar och driver olika typer av säkerhets policies för att hantera olika klasser av DDoS attacker. De rekommenderar även specialiserade middleboxes som endast driver en typ av säkerhets policy för att hanterar en viss speciell typ av DDoS attack [25].

2.10.1.1.3 Monitoring plane

Består av två olika moduler:

Flow Statistics Collector, samlar flödesinformation från OpenFlow switcher och skickar vidare informationen till *detection engine*. OpenFlow switchar upprätthåller counters för varje flödestabell och "flödesentry". Kundens controller kan även välja att hämta denna flödesstatistik från switcharna.

Detection Engine, tar flödesstatistiken från Collectorn som input och genererar säkerhetsvarningar om onormala flöden identifieras. Varningarna triggar sedan *Policy Engine* att hantera inkommande flöden på respektive sätt [25].

2.10.1.1.4 Policy Engine

Vid mottagandet av en varning från Detection Engine, genererar den regler för att hantera de onormala flödena som identifieras. Dessa regler sparas i lookup tabellen för att senare kunna verkställas. Controllern är sedan den som distribuerar reglerna till OpenFlow switcharna [25].

2.10.1.1.5 Security APIs

Ramverket tillåter ISPs att tillhandahålla säkerhetsfunktioner till sina kunder via APIs hos controllern, vilket möjliggör skydd/säkerhet vid behov som en service. Förfrågningar inkluderar t.ex. distribuering av middleboxes för att filtrera misstänksam trafik eller stoppa skadlig trafik. Kunden kan också, via dessa APIs, tilldela olika prioriter till flöden, för att hantera legitim trafik på respektive sätt. Denna säkerhetstjänst är något som bara skulle vara tillgängligt för abonnerande

kunder. Detta är även något som IETF gruppen I2NSF försöker standardisera för ett utbrett användande de kommande åren [25].

2.10.1.1.6 Path lookup

Ramverket antar också att alla vägar är beräknade I förväg av ISPn. Vägarna kan beräknas genom en "all-pairs shortest path algorithm". Om en länk bryts kan vägarna beräknas igen. Path lookup komponenten behåller en tabel av möjliga vägar sorterade enligt kvaliteten på service de erbjuder, vilket associeras med unika etiketter. Vägarna associeras sedan med olika flöden baserade på vilken trafikklass de tillhör. Legitima flöden blir t.ex. tilldelade högprioriterade vägar medan misstänksamma flöden tilldelas vägar som innehåller middleboxes. Till sist blir elaka flöden skickade genom vägar som leder till "sinkholes". I författarnas ramverk tar path lookup modulen input från policy engine och returnerar vägen som matchar [25].

2.10.1.1.7 Flow Label API

Flöden som inte finns med i flödestabellen hos switcharna blir forwardade till controllern, på ett sätt som beskrivs av OpenFlow specifikationen i [26] och de läggs till i flödestabellerna enligt controllerns centraliserade nätverks policy. Flödena blir tilldelade en etikett som bestämmer vägen för flödena, från ingress switchen till egress switchen. Etiketten används för att snabba upp switching och rerouting, eftersom switcharna då bara behöver kontrollera etiketten och skicka vidare flödet till nästa hop, istället för att inspektera hela paketets header. Det lättar även belastningen för OpenFlow switcharna genom att reducera antalet entries in deras flödestabeller, till antalet etikett entries. I praktiken kan etiketterna tilldelas genom att skriva om VLAN ID fältet, som beskrivs i [26].

2.10.1.1.8 Attack Mitigation

Baserat på de förberäknade vägarna som associeras med de onormal flödena, distribuerar denna modul middleboxes vid specifika punker längs vägen, innan trafiken når kundens nätverk. Baserat på märken som ges av kundens controllers detection engine, kan ISPns controller modifiera etiketterna för flödenas entries, så att dessa flödens kan processas av middelboxarna. Se exempel på en mitigation algorithm i [25].

2.10.1.1.9 Tag API

Denna modul genererar en unik hash etikett. APIn fungerar som en applikation som blir distribuerad till switcharna genom ett "configuration apply" kommando. APIn extraherar paketets header och använder IP-4 tuplen (käll adress, destinations adress, käll port, destinations port) som input och genererar en unik etikett att lägga in i paketets käll MAC adressfält genom användandet av en Push Tag handling [26]. Se algoritm för att generera en etikett i [25]. Etiketten säkerställer en konsistent "end-to-end" nätverks policy och identifierar även flöden på ett effektivt sätt. Etikettfunktionen utförs vid edge switcharna och flöden som kommer dit får en etikett av edge switchen själv [25].

2.10.2 Hop count filtering

För att dölja vart en flood attack kommer ifrån är det vanligt att angriparen använder en spoofad IP adress genom att sätta in en slumpvis vald 32-bits käll adress i IP headern. Vissa kända DDoS attacker, som smurf och Distributed Reflection Denial of Service (DRDoS) attacker kan inte ens utföras utan spoofade IP adresser. Dessa döljer käll adressen av varje spoofat paket med offrets IP adress. Internet är i allmänhet sårbart för IP spoofing på grund av IP protokollets statelessness och destinations-baserade routing. IP protokollet saknar också en kontroll för att förhindra en

avsändare att dölja var paketet kommer ifrån. Destinations-baserad routing vidhåller heller inte någon information om avsändarna utan skickar bara varje paket till sin destination utan att autentisera paketets käll IP adress. I allmänhet bidrar IP spoofing till att göra DDoS attacker väldigt svåra att upptäcka och motverka [27].

Författarna tar här upp ett förslag baserat på hop count filtrering, som i deras experiment implementerades i en Linux kernel, för att sålla bort spoofade IP paket. Idén bakom hop count filtrering är att de flesta spoofade IP paket, när de når sitt mål, inte har något hop-count värde som är konsistent med ett legitimt IP paket från den avsändaren som blivit spoofat [27].

Hop-Count Filtering (HCF) bygger således upp ett IP to hop-count (IP2HC) mapping table, samtidigt som den använder en måttlig mängd lagring för att samla adress prefixer baserat på hop-counts. För att fånga ändringar av hop-count under dynamiska nätverks förhållanden, utvecklar även författarna en "säker" uppdateringsprocedur för att förhindra IP2HC mapping table att förstöras av HCF-medvetna angripare [27].

HCF använder sig av två olika tillstånd, *alert* och *action*, för att inspektera IP headern av varje IP paket. Under normala förhållanden befinner sig HFC i *alert*, där den väntar på onormala TTL beteenden utan att kasta bort några paket. När den upptäcker en attack byter HCF tillstånd till *action*, där den kostar bort IP paketen med missmitchande hop-counts. Författarna till HCF visar i sin rapport att de kan känna igen nära 90% av alla spoofade IP paket och att deras false positive är så pass låg att de kan slänga bort spoofade IP paket med väldigt få indirekta skador [27].

2.10.2.1 Beräkning av TTL baserad Hop-Count

Eftersom hop-count information inte är direkt lagrad i IP headern måste den beräknas baserat på TTL fältet i IP headern. Det sista TTL värdet när ett paket når sin destination är det initiala värdet subraherat med antalet mellanliggande hop. Ett problem som uppstår här, är att en destination bara ser det slutgiltiga TTL värdet. De flesta moderna operativ systemet använder dock bara ett fåtal olika TTL värden, 30, 32, 60, 64, 128, och 255. Eftersom man generellt tror att väldigt få Internet hops är längre ifrån varandra än 30 hops, kan man bestämma det initiala TTL värdet av ett paket genom att välja det lägsta initiala värdet i det set som är större än det slutgiltiga TTL värdet. Till exempel, om det slutgiltiga TTL värdet är 112 är det initiala värdet antagligen 128, alltså det mindre av två möjliga värden, 128 och 255 [27].

2.10.2.2 Inspektions algoritm

Inspektionsalgoritmen extraherar käll IP adressen och det slutgiltiga TTL värdet från varje IP paket. På samma sätt som beskrevs ovan får algoritmen reda på det initiala TTL värdet och subtraherar det med det slutgiltiga TTL värdet för att få fram en hop-count. Käll IP adressen fungerar sedan som ett index i IP2HC mapping tabellen för att få fram ett korrekt hop-count för den IP adressen. Matchar dessa hop-counts blir paketet autentiserat, annars klassificerat som spoofed. Värt att tänka på här är att en spoofad IP adress kan ha samma hop-count som den från en zombie till ett offer. HCF kommer alltså inte kunna identifiera alla spoofade paket, men författarna visar ändå i sin rapport att de, med ett begränsat antal hop-counts, på ett väldigt effektivt sätt identifierar spoofade IP adresser [27].

2.10.2.3 Hop-Count Distribuering

För att HCF ska fungera så effektivt som möjligt måste distribueringen av hop-counts från klienters IP adresser vid en server anta en mängd olika värden. Eftersom HCF inte känner igen falska paket vars IP adress har samma hop-count som en angripare, är det viktigt att undersöka hop-count distribueringar på olika platser i Internet för att försäkra sig om att hop-count distribueringen inte

är samlad kring ett enda värde. Om 90% av klienternas IP adresser är tio hops ifrån en server skulle man inte kunna skilja på spoofade paket och legitima enbart med hjälp av hop-count filtering. Författarna har således även använt sig av ren traceroute data från 50 olika traceroute gateways för att få fram en mer exakt hop-count distribuering, där de flesta traceroute gateways observerade fler än 40,000 klienter. För att få en mer detaljerad bild av författarnas hop-count distribuering, se [27].

2.10.2.4 Konstruktion av HCF tabellen

Att ha en noggrann HCF tabell (dvs, IP2HC mapping table) är väldigt viktigt för att kunna upptäcka maximalt antal spoofade IP paket. Målet med konstruktionen av HCF tabellen är att ha en noggrann IP2HC mappning, uppdaterad IP2HC mappning och ett krav på en måttlig mängd lagring. Genom att klustra adressprefixen baserat på hop-counts kan man bygga en noggrann IP2HC mapping table som maximerar HCFs effektivitet utan att lagra hop-counten för varje IP adress. Författarna designar även en säker uppdateringsprocedur som fångar ändringar hos legitima hop-counts medan det förhindrar angripare att förorena HCF tabellen [27].

2.10.2.5 IP Adress Aggregering

Genom att aggregera IP adresserna kan man signifikant reducera kravet på lagring för IP2HC mappningen. IP adress aggregering täcker även de IP adresser som är samlokaliserade med IP adresserna som redan finns i HCF tabellen. Att gruppera värdar efter de första 24 bitarna i IP adressen är en vanlig aggregeringsmetod. Dock så kan värdar ha nätverksprefixar längre än 24 bitar och således finnas i andra fysiska nätverk, trots att de har samma 24 första bitar. Detta leder till att författarna ytterligare delar upp IP adresserna inom dessa 24-bitars aggregat, till mindre kluster baserat på hop-counts [27].

Eftersom 24-bits aggregering inte ger rätt hop-count för alla IP adresser testar författarna tre olika filter: "Strict Filtering" droppar paket som inte exakt matchar det i tabellen, "+1 Filtering" droppar paket vars hop-count skiljer med mer än 1 jämfört med tabellen och "+2 Filtering" droppar paket som skiljer sig med mer än 2. Deras experiment visar att "+1 Filtering" är en bra kompromiss mellan false negatives och false positives [27].

2.10.2.6 Föroreningssäker Initialisering och Uppdatering

För att initialt populera HCF tabellen, bör en internet server samla information från klienterna som innehåller både IP adressen och motsvarande TTL värden. Beroende på mängden trafik servern tar emot kan denna insamlingsperiod pågå olika lång tid. Att hålla IP2HC tabellen uppdaterad är även väldigt viktigt då hop-counts kan ändras på grund av t.ex. routing instabilitet eller att nätverk går ner. IP2HC tabellen måste även skyddas från angripare som kan tänkas förorena den. Ett sätt att se till att enbart legitima paket används under initieringsfaser och under uppdateringar är via TCPs handslagsprocess. IP2HC tabellen bör enbart uppdateras om TCP anslutningen är i fasen *established*. En spoofad IP adress som skickar ett SYN paket kommer inte få ett SYN/ACK svar från servern och kan således inte slutföra handslaget. Denna metod ger en bra säkerhet, men det blir för kostsamt att uppdatera IP2HC tabellen med varje ny TCP anslutning. Författarna har därför lagt till en parameter som kan konfigureras för att bestämma hur ofta denna uppdatering ska ske [27].

2.10.2.7 HCFs två tillstånd

HCF bör inte vara aktivt hela tiden, då det orsakar en delay i den kritiska vägen av paketets bearbetning. Därför introducerar HCF två olika tillstånd: *alert* upptäcker spoofade paket, och *action* slänger spoofade paket. HCFs normala tillstånd är *alert*, där den håller koll på ändringar av hop-

counts utan att slänga paket. Så fort den upptäcker ett flöde av spoofade paket byter den tillstånd till *action* för att börja undersöka varje paket och slänga spoofade paket [27].

I tillståndet *alert*, utför HCF följande uppgifter: inspekterar hop-counts för en delmängd av alla inkommande paket, beräknar spoofade pakets counter, uppdaterar IP2HC mapping table om legitima hop-counts har ändrats. För en mer detaljerad beskrivning med exempelalgoritm, se [27].

Tillståndet *action* utför liknande beräknar som *alert* men istället för att undersöka en delmängd av paketen inspekterar detta tillstånd varje enskilt paket och slänger paketet om det är spoofat. HCF stannar i detta tillstånd så länge spoofade paket upptäcks. För en mer detaljerad beskrivning med exempelalgoritm, se [27].

2.10.2.8 Skydd mot DRDoS attacker

HCF skyddar även mot DRDoS attacker, där en angripare förfalskar IP paket som innehåller legitima förfrågningar, så som DNS queries, genom att sätta käll IP adressen av de spoofade paketen till offrets IP adress. Angriparen skickar sedan dessa spoofade paket till ett stort antal reflektorer. Varje reflektor tar bara emot en liten mängd spoofade IP paket så den inte upptäcker något onormalt mönster och alltså inte orsakar något alarm. Vanliga intrusion detection metoder baserade på pågående trafik eller åtkomstmönster är ofta inte känsliga nog att upptäcka dessa spoofade paket. HCF letar dock specifikt efter IP spoofing och gör det möjligt att upptäcka dessa försök att lura servrarna att agera som reflektorer. Författarna säger dock att HCF inte är perfekt och att några spoofade paket alltid kommer igenom, men HCF kan ändå upptäcka tillräckligt många för att undvika DRDoS Angripare [27].

2.10.3 SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks

DDoS flooding attacker är särskilt svåra att försvara emot, eftersom själva arkitekturen som bidragit till att Internet växt så våldsamt – intelligenta end-värdar sammankopplade med ett relativt enkelt nätverk (end-to-end principle)- används till angriparnas fördel. I denna arkitektur kan vem som helst skicka paket till vilken destination som helst. Mottagaren har heller inget sätt att stoppa paketen innan den mottager dom [28].

Detta stycke presenterar "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks", vilket är ett förslag där offret av en översvämningsattack får möjlighet att välja individuella trafikflöden som den vill stoppa, utan att behöva något per-flow state i nätverket, eller kontakt med någon router eller ISP, medan den samtidigt tillåter legacy klienter och servrar att kommunicera med uppdaterade klienter och servrar [28].

SIFF erbjuder ett flertal egenskaper:

- **Priviligierad kommunikation mellan klient/server:** SIFF tillåter klienter och servrar etablera en priviligierad kanal över IP där paketen får företräde framför icke-priviligierade paket [28].
- **Mottagaren kontrollerar priviligierade flöden:** SIFF tillåter den mottagande värden att avsluta en priviligierad kanal och på så sätt stoppa flödet av paket på den kanalen från att nå mottagarens nätverk. Paketen kommer med hög sannolikhet att droppas av en närliggande router och på så sätt inte ta upp någon bandbredd på länken närmast mottagaren [28].
- **Begränsar spoofing av käll adresser:** Likt ingress filtrering, är den mottagande värden av en priviligierad kanal, med hög sannolikhet, säker på att inkommande paket verkligen kommer ifrån en värd på samma nätverk som käll IP adressen i paketet [28].

- **Litet, konstant tillstånd vid routrarna:** Routrar som implementerar SIFF behöver bara hålla en konstant mängd tillstånd per routers interface, oberoende antalet priviligierade kanaler genom routern. *Detta är enligt författarna huvudegenskapen av SIFF, då andra liknande lösningar kräver ett tillstånd per flow i routrarna* [28].
- **Små bearbetningar per paket vid routrarna:** En SIFF router behöver bara utföra två likhetskontroller för varje priviligierat paket, eller en hashberäkning för varje oprivilegierat paket, som den forwardar. Dessa beräkningar är oberoende antalet priviligierade eller oprivilegierade kanaler genom routern. Hashberäkningen och likhetskontrollen kan även göras parallellt med routerns table lookup [28].

2.10.3.1 Antaganden

Författarna av SIFF gör ett antal antaganden för att bygga upp systemet. De antar först att offret har möjligheten att avgöra att den är under attack och att den kan differentiera mellan legitima klienters flöden och elaka flöden. Differentieringen behöver inte vara per paket, bara att den existerar. *Författarna tar dock inte upp hur denna differentierings algoritm skulle kunna se ut då det kan bero på vilken applikation det handlar om, bara att den existerar.* De antar även att klienter, servrar och routrar är omdesignade att följa ett modifierat IP nätverk [28].

De antar att IP headern har tillräckligt med utrymme för att rymma informationen som routarna markerar i paketen. Följande fält antas finnas:

- **Flags field** (3-bitar). Innehåller följande 1-bits flaggor: Signalling flag (SF), indikerar om paketet är ett non-legacy paket; Packet type flag (PT): Indikerar att paketet antingen är ett DTA (set) eller EXP (unset) paket (Se förklaring av DTA och EXP paket nedan); och capability update flag (CU): Indikierar om capability reply field är närvarande i headern [28].
- **Capability field.** Används av routrarna för att lägga till sina markeringar på paketen på väg till destinationen [28].
- **(Optional) Capability reply field.** Används av mottagaren av paket för att signalera sändaren om en ny/updaterad capability och är bara närvarande när capability update flag är satt [28].

Ingen specifik längd är antagen för capability eller capability reply field då det kan bero på andra parametrar.

De antar även att SIFF routrar är kapabla att utföra små ändringar av "marking field" för varje paket som forwardas. Dessa ändringar kan göras parallellt med routerns table lookup. Detta är ett mindre antagande eftersom routern ändå måste ändra varje pakets TTL och IP Header Checksum [28].

2.10.3.2 Ett övergripande perspektiv av hur SIFF fungerar

Klienter och servrar deltar i en handslagsprocess med hjälp av ett specifikt oprivilegierat paket kallat EXPLORER (EXP) paket. Routrar lägger till path specifik information i EXP paketen, vars aggregat mellan alla routrar längs vägen används som en capability token för en priviligierad kanal mellan klienten och servern. Efter handslagsprocessen kan klienten och servern kommunicera genom den priviligierade kanalen med hjälp av DATA (DTA) paket, där de lägger till capabilities från EXP paketen. När routern forwardar ett DTA paket, kollar den först att dess capability stämmer överens med informationen som skulle ha blivit tillagd om paketet hade varit ett EXP paket. Matchar informationen skickas paketet vidare, annars droppas det omedelbart [28].

2.10.3.3 Handshake protocol

För att en klient och en server ska kunna kommunicera över en priviligierad kanal måste de först genomgå ett handshake protocol för att få en capability att lägga till sina priviligierade paket.

Initieraren av handslaget måste först skicka ett EXP paket med dess *capability field* satt till 0. Paketet blir märkt som EXP paket genom att sätta *signalling flag (SF)* och lämna *packet type flag (PT)* osatt. Alla routrar längs vägen vänsterskiftar sedan *z* bitar in i *capability field* av EXP paketet, förutom första routern, som ser ett marking field där alla bitar är 0, lägger istället till 1 bit innan dess egen markering (så att capabilitien består av alla bitar upp till, men inkluderar inte, den mest signifikanta 1 biten). För en mer detaljerad beskrivning av hur det går till, se [28].

När EXP paketet når server skapar den ett svarspaket. Svarspaketet är också ett EXP paket, med *capability field* initiserat till 0, men med *capability update flaggan (CU*) satt och *capability reply field* initierad till innehållet av *capability field* av EXP paketet från klienten. När klienten mottager serverns EXP paket, undersöker klienten *capability reply* fältet, tar alla bitar upp till, men inkluderar inte, den mest signifikanta 1 biten, splittar dom i grupper av z bitar och vänder om deras ordning för att få fram capabilitien. Denna capability sätts sedan in i capability fältet av alla efterföljande priviligierade paket klienten skickar [28].

Routerns markering och forwarding av DTA paket skiljer sig något från EXP paketen. När en router mottager ett DTA paket, beräknar den markeringen som om paketet vore ett EXP paket, men verifierar sedan bara att den beräkningen stämmer överens med de minst signifikanta bitarna i capability fältet. Stämmer markeringen, högerskiftar routern den markeringen till dom mest signifikanta bitarna av capability fältet. Detta medför att markeringen för next-hop routern upptar de minst signifikanta bitarna. För en mer detaljerad beskrivning av hur det går till, se [1]. Ett DTA paket når bara sin destination om varje router längs vägen kan matcha sin markering mot dom minst signifikanta bitarna i capability fältet. När servern mottager klientens priviligierade paket, kan servern beräkna sin capability på samma sätt som klienten gjorde och handslaget är klart och de båda kan kommunicera med priviligierade DTA paket [28].

2.10.3.4 Router Marking Calculation

Varje router måste alltså beräkna en märkning för varje paket den forwardar; den vänsterskiftar märkningen in i paketet om det är ett EXP paket, eller verifierar och högerskiftar märkning om det är ett DTA paket. För varje specifikt paket beräknas märkningen genom the sista *z* bitarna av outputen av en keyed hash function med följande parametrar: IP adressen av interfacet dit paketet anlände vid aktuell router, IP adressen av sista hopp routerns utgående interface, källa och destinations IP adressen av paketet som forwardas [28].

För SIFF att effektivt stoppa falska priviligierade packet floods, måste routern beräkna sina märkningar snabbare än den kan utföra en table lookup. Skulle routern inte klara av detta kan angriparen överösa routern med illegitima DTA paket vilket resulterar i att routern antingen fyller sin buffer med DTA paket och börjar droppa möjligen legitima DTA paket, eller överbelastar sin route-lookup förmåga. Routern måste på grund av detta, klara av att beräkna hash funktionen i hårdvara [28].

2.10.4 Kill-Bots

Denial of service attacker sker i allt större utsträckning av professionella hackare som med sina botnets bestående av tusentals datorer utpressar företag för pengar eller blir hyrda för att slå ut konkurrenter. Dessa DDoS-attacker blir även smartare och smartare eftersom de, för att undvika att bli upptäckta, i större utsträckning går ifrån rena flooding attacker till DDoS-attacker som istället

försöker efterlikna flash crowd attacker. Detta för att vara så lik legitim trafik som möjligt, från en enorm mängd användare, vilket gör det väldigt svårt att urskilja vilka som är legitima användare och inte. Attackerna fokuserar även på högre lager av en servers resurser, såsom dess CPU, databaser, minne eller disk-bandbredd. Författarna kallar detta för CyberSlam attacker, efter ett känt FBI case där DDoS-for-hire var involverat[29], [30].

Problemet med att stoppa dessa CyberSlam attacker har sin grund i att trafiken från dessa elaka botnets är så pass lik det av en vanlig användare att det blir väldigt svårt att t.ex. filtrera trafiken baserat på IP prefixen. Många hemsidor använder sig heller inte av lösenord eller någon typ av login information och skulle hemsidorna göra det kan dessa lösenord ändå stjälas från äventyrade datorer. För att kontrollera lösenord vid inloggning krävs även att man upprättar en anslutning där man låter oautentiserade klientar komma åt socket buffers, Transmission Control Blocks (TCBs) och arbetsprocesser, vilket gör det enkelt att attackera själva autentiseringsmekanismen[30].

Ett förslag för att skydda sig mot attacker som efterliknar Flash Crowds har då tagits fram av några dataingenjörer från MIT som kallar det för Kill-Bots, vilket är en kernel utvidgning. Kill-bots inriktar sig mot små eller mellanstora onlineföretag och icke-kommersiella hemsidor.

Nedan ges en övergripande förklaring av Kill-bots. Vill läsaren ha en mer detaljerad förklaring om hur det exakt fungerar hänvisar vi till rapporten [30].

2.10.4.1 Autentisering och Admission control

Kill-bots kombinerar två olika funktioner: autentisering och admission control.

(i) **Autentisering:** Autentiseringsmekanismen tas i bruk så fort servern märker att den börjar bli överbelastad. Det finns två olika faser.

Fas_1: I denna fas har autentiseringsmekanismen satt igång och kräver då varje ny anslutning att lösa ett reverse Turing test. Detta är inget problem för människor men zombies från botnets klarar inte av det. Kill-bots fokuserar på grafiska testar, CAPTCHAS, men det funkar lika väl med andra typer av reverse Turing tester. Legitima användare kommer antingen klara testet, ladda om sidan ett antal gånger och kommer de fortfarande inte åt sidan kommer de antagligen tillbaka senare. Zombies å andra sidan, som vill överbelasta en server kommer fortsätta begära att få lösa testet utan att lyckas. Deras beteendemönster kommer på så sätt att skilja sig från en legitim användare, vilket ger Kill-bots en möjlighet att identifiera vilka IP adresser som tillhör zombies och droppa deras förfrågningar. Kill-bots använder SYN cookies för att förhindra spoofade IP adresser och ett Bloom filter för att räkna hur många gånger en IP adress har misslyckats med ett test. Överstiger antalet misslyckade test ett visst threshold kommer dess förfrågningar att droppas [30].

Efter att antalet upptäckta zombie IP adresser har stabiliserats (Bloom filtret lär sig inga nya IP adresser) går Kill-bots över till Fas_2. Under denna fas ges inte längre några tester ut. Här litar istället Kill-bots helt och hållet på att Bloom filtret droppar förfrågningar från IP adresserna den har lärt sig. Syftet med detta är att tillåta legitima användare som inte kan eller vill lösa de grafiska testarna att ansluta till servern oberoende den pågående attacken [30].

(ii) Admission control: Förutom autentisering tillämpar även Kill-bots admission control. En webbsida som skyddar sig mot DDoS genom autentisering stöter ofta på ett generellt problem. Den har endast en viss mängd resurser som den måste fördela på att autentisera nya användare och serva klienter som redan är autentiserade. För att kunna erbjuda bästa möjliga service till användare som redan är autentiserade och användare som vill autentiseras krävs en finfördelning av serverns resurser. Kill-bots försöker därför räkna ut "admission probabiliteten" α som bäst maximerar en servers "goodput" (den optimala probabiliteten för nya klienter att bli autentiserade). Den tillhandahåller även en "controller" som tillåter servern att konvergera till önskad "admission probabilitet" genom att enkelt mäta hur mycket av serverns kapacitet som utnyttjas [30].

Så fort en ny användare försöker ansluta kommer dess IP adress jämföras med en lista av kända zombie adresser. Är adressen inte redan känd kommer Kill-bots släppa igenom anslutningen med probabiliteten $\alpha = f(load)$. Insläppta anslutningar måste sedan under $steg_1$ besvara ett grafiskt pussel. Löser klienten pusslet får den en HTTP cookie som under en kort period tillåter klienten att ansluta till servern utan att gå igenom admission control och utan att besvara ytterligare pussel. Under $steg_2$ ges inte längre några pussel ut, utan insläppta anslutningar får genast en HTTP cookie [30].

Kill-bots har några få viktiga egenskaper:

- Den mest fundamentala egenskapen hos Kill-bots är det faktum att den skickar ett pussel utan att ge access till TCBs eller socket buffers, vilket man normalt skulle behöva göra. Ett DDoS skydd vill helst minimera resurserna som tas upp av oautentiserade klienter [30]. Därför modifierar Kill-bots serverns TCP stack så att den kan skicka ett 1-2 packet stort pussel i slutet av TCPs handslagsprocess utan att hålla någon anslutning öppen medan den samtidigt behåller TCPs congestion control [30].
- Kill-bots förbättrar prestandan oavsett om servern överbelastas av DDoS-attacker eller äkta Flash Crowds. Detta på grund av admission control som bara tillåter nya anslutningar om de kan hanteras [30].

2.10.4.2 Hotmodell

Syftet med Kill-bots är att öka prestandan under just CyberSlam attacker, som försöker efterlikna mönstret av legitim webtrafik och förbrukar resurser från högre lager av en server, som .t.ex. dess CPU, minne, databaser och disk-bandbredd.

Viktigt att tänka på gällande Kill-bots är att den inte tar hänsyn till bandbredds-flood attacker, attacker mot en servers DNS entry eller mot routing entries. Författarna av Kill-bots gör även ett antal antaganden där de antar att angriparen kontrollerar ett godtyckligt antal maskiner som kan vara fritt distribuerade över internet. Angriparen kan även ha godtyckligt stora CPU- och minnesresurser. Angriparen kan inte sniffa paket på serverns lokala nätverk eller på en huvudlänk som bär legitima användares trafik. Angriparen har inte heller fysisk tillgång till själva servern. Sista antagandet är att zombies från botnets inte kan lösa de grafiska testerna och att angriparen inte har tillgång till så pass många människor för att kontinuerligt lösa flera pussel.

2.10.4.3 Säkerhetsanalys

I denna sektion tar vi upp vad Kill-bots klarar av att hantera från en angripare.

(i) Socially-engineered attack: Angriparen syftar här till att lura en stor mängd människor att lösa dessa pussel för sin egen räkning. Detta har gjorts tidigare för att ta sig förbi grafiska testar från Yahoo och Hotmail där avsikten var att skapa nya epost konton [2]. Kill-bots kan hantera dessa attacker på ett bättre sätt eftersom det pussel en Kill-bots erbjuder upphör att gälla efter 4 minuter, till skillnad från att skapa ett epost konto, där man har betydligt längre tid på sig att besvara pusslet. Detta betyder att angriparen inte får chansen att samla på sig tillräckligt många svar för att förbereda en attack. En viktig poäng att tänka på här är även att attacken redan blivit svårare att utföra eftersom angriparen tvingats till en socially engineered attack [30].

(ii) "Förorena" Bloom filtret: Angriparen kanske försöker spoofa IP adresser och sedan "förorena" Bloom filtret så att Kill-bots misstar legitima användare som elaka. Detta ska inte gå eftersom SYN cookies används för att förhindra spoofade IP adresser och Bloom filtrets poster modifieras efter att SYN cookie kontrollen lyckats [30].

(iii) Copy attacker: Under en copy attack löser angriparen ett grafisk pussel, erhåller motsvarande HTTP cookie och distribuerar sedan den till ett stort antal zombies som på så sätt kan komma åt webbsidan. För att vara skonsam mot proxies och mobilanvändare, använder sig Kill-bots av en nedre gräns av in-progress förfrågningar per pussel. Författarnas implementation satte denna gräns till 8 [30].

(iv) Replay attacker: En session cookie inkluderar en säker hash av tiden då den blev skapad och är bara giltig under en viss tidsperiod. Om en angripare försöker spela upp en cookie utanför detta tidsintervall kommer den bli nekad. En angripare kanske också löser pusslet för att sedan spela upp "lösningspaketet" för att få flera Kill-bots cookies. När Kill-bots ger ut en cookie för ett korrekt svar är dock cookien i form av en Token (Se en mer detaljerad beskrivning i [30]). Detta betyder att uppspelningen av "svaret" resulterar i samma cookie igen [30].

(v) Databas attack: En angripare kan även försöka samla på sig alla möjliga pussel och deras motsvarande svar. När en zombie sedan mottager ett pussel kan den leta i sin databas efter motsvarande svar och skicka tillbaka det till servern. För att förhindra detta använder sig Kill-bots av en väldigt stor mängd pussel samtidigt som periodiskt byts ut mot ett nytt set. För en angripare att bygga upp en databas med så pass många pussel, distribuera den till alla zombies och sedan låta alla zombies söka i denna databas för att hitta svaret inom 4 minuter, blir väldigt svårt [30].

2.10.5 Mindre relaterat arbete 1

I rapporten *Analys av DDoS*-attacker *för identifiering och prevention* skriver författarna om hur de med hjälp av pcap-filer analyserar trafikflödet och på så sätt identifierar DDoS-attacker [31].

Författarna har skapat en kontrollerad labbmiljö med hjälp av simulering. De är dock kritiska till att använda simulering då de anser att de simulerade komponenterna inte alltid beter sig som fysiska komponenter skulle göra i verkligheten [31].

2.10.6 Mindre relaterat arbete 2

I rapporten *Överbelastningsattacker mot nätverk och hur man skyddar sig mot dem*, gör författaren en genomgång av 25 olika sorters överbelastningsattacker, men till skillnad från många andra rapporter vi har läst har författaren också valt att belysa de ekonomiska konsekvenseran av DDoS-attacker [32].

Författaren nämner kostnader som drabbar företagen i form av förlorade affärsmöjligheter och ökade driftkostnader [32]. Författaren går dock inte in i detalj och visar vad som utgör de olika kostnaderna.

2.11 Sammanfattning

Vi summerar avsnittet med en tillbakablick på vad vi har lärt oss. Vi har redogjort att DoS- och DDoS-attacker är attacker vars syfte är att göra ett företags tjänster/webbsida obrukbar för legitima användare. Vi har också förklarat begreppet botnät, vilket är ett nät av infekterade datorer som används för att utföra DDoS-attacker.

Vi har också visat att det är idag är väldigt billigt att få tag i ett botnät för att utföra DDoS-attacker. Det finns också aktörer vars affärsidé bygger på att utföra riktade DDoS-attacker mot betalning. Olika former av kriminella aktiviteter kopplade till DDoS-attacker, vilket är en av de vanligaste motivationer till att DDoS-attacker utförs.

Det finns tre typ av DDoS-attacker, Volymbaserade-, Protokoll- och Applikationslagerattacker. Och som utvecklingen i världen ser ut de senaste åren ökar antalet attacker både till antal och storleksmässigt, vilket har lett till en ökad efterfrågan för DDoS-skydd.

2.11.1 Tidigare forskning

Eftersom DDoS-attacker blivit så vanligt och så framgångsrikt har det pågått mycket forskning kring hur man på bästa sätt skyddar sig mot dessa attacker. Avsnittet tar upp huvudpunkterna av ett flertal forskningsförslag där olika lösningar inriktar sig mot olika specifika problem för att ge inspiration och en inblick i hur forskare ser på problemet.

Hop Count Filtering försöker förhindra spoofade IP adresser genom att beräkna Hop Counts för att se om de är trovärdiga, är de inte trovärdiga är det stor sannoliket att de är spoofade. Spoofade IP adresser skyddar angriparens identitet och möjliggör ytterligare typer av attacker.

SIFF försöker förhindra flooding attacker genom att använda priviligierade kanaler för kommunikation mellan legitima användare och servern.

Kill-bots försöker förhindra flooding attacker och äkta flash crowds genom användandet av CAPTCHAS då servern märker att den blir överbelastad.

Software Defined Networking försöker skapa ett programerbart nätverk som erbjuder full kontroll av nätverket via en controller för att på så sätt ha möjlighet att sätta in snabba skyddsmekanismer som kan hantera DDoS attacker.

Under detta avsnitt ser vi även att många av lösningarna baseras på antaganden som inte stämmer med dagens arkitektur av internet. Förslagen är även inriktade mot ett specifikt problem men man kan lätt se att lösningarna skulle kunna kombineras för att ge ett mer heltäckande skydd.

3 Metodik

Avsnittet avser beskriva vilka metoder vi använt och motivationen bakom valen.

3.1 Vetenskaplig metodik

Vi har valt att använda oss av litteraturstudier och experiment som vår vetenskapliga metodik. I följande avsnitt kommer vi att motivera varför vi använde de metoderna och varför vi valde att inte använda oss av andra metoder.

3.1.1 Litteraturstudie

För att få en bättre bild av de ekonomiska konsekvenserna av en DDoS-attack har vi använt oss av Kasperksy labs "Global it security risks survey 2014 – Distributed Denial of Service (DDoS) attacks [2]. Undersökningen består av svaren från 3900 svarande från 27 olika länder. Undersökningen är en årlig undersökning där de svarande består av medelstora, stora och väldigt stora företag [2]. En stor del av undersökningen kretsar kring att identifiera de kostnader som är vanligast förekommande i samband med DDoS-attacker mot företag [2].

För att ge ett konkret exempel på hur en DDoS-attack skulle påverka ett e-handelsföretag har vi granskat årredovisningen för CDON.com och gjort beräkningar utifrån den nettoomsättning som företaget fick under 2014 [5]. Årsredovisningen är en offentlig handling och därför kan vi fritt använda oss av materialet.

3.1.2 Experiment

För att tillföra en ytterligare nivå till rapporten valde vi att utföra egna experiment, i en sluten labb miljö. Eftersom vi vid starten av arbetet skapat oss en hypotes om att DDoS-attacker är väldigt lätt att utföra, med hjälp av dagens teknik. Skulle vi lyckas att utföra en lyckad DDoS-attack, trots att vi inte besitter de kunskaperna sedan tidigare, skulle det bevisa vår hypotes. Detta tror vi gör att företag blir extra benägna att stärka sig mot eventuella DDoS-angrepp.

3.1.3 Enkätundersökning

Anledningen till att vi valt att inte utföra en egen enkätundersökning är för att vi tror att litteraturstudier kommer att medföra en större tillförlitlighet än enkätundersökningar, då vi bedömer att vi kommer få ett stort bortfall om vi skulle genomföra en egen enkätundersökning. Genom att istället använda oss av resultatet från världsomfattande undersökningar, utförda av två av de största aktörerna på marknaden för DDoS-skydd (Arbor Networks och Kaspersky Lab) tror vi att vi får en mer tillförlitligt bild av utvecklingen av DDoS-attacker.

3.1.4 Intervjustudie

Anledningen till att vi valt att inte genomföra en intervjustudie är för att vi upplever det som att det är svårt att få respondenter som vill svara på frågor angående DDoS-attacker, då mycket av den informationen är hemlighetsstämplad. Den enda informationen som respondenterna får ge berör händelser som redan är offentliga, vilket innebär att vi inte behöver utföra intervjuer för att ta del av den informationen.

3.2 Målet

I avsnittet presenterar vi målen för de olika delarna av undersökningen.

3.2.1 Litteraturstudier

Målet för studien var att visa hur utvecklingen av DDoS-attacker ser ut och vilka typer av kostnader som kan uppkomma i samband med DDoS-attacker. Anledningen till att vi gör det är för att öka vetskapen om DDoS och för att få företag att inse vilket hot DDoS-attacker verkligen är och för att ge företag ett incitament att investera i ett DDoS-skydd.

Med hjälp av den informationen ska man sedan kunna ta fram en affärsplan för ett företag vars verksamhet riktar sig till att hjälpa andra företag som blir utsatta för DDoS-attacker. Inte bara genom att hantera attacken utan också bidra med kunskap och handlingsplaner som kan bemöta eventuella skador som DDoS-attacken har gjort på företagets varumärke och eventuella förluster av marknadsandelar.

3.2.2 Granskning av årsredovisning

Målet för den studien var att åskodliggöra hur mycket ett e-handelsföretag riskerar att förlora om de blir utsatt för en DDoS-attack.

3.2.3 Experiment

Målet med de egna experimenten var att bevisa vår hypotes om att det är väldigt lätt att utföra en DDoS-attack, utan några tidigare kunskaper. Efter att vi har lyckats med att utföra en DDoS-attack har vi också för avsikt att hitta ett sätt att skydda oss mot DDoS-attacken.

3.3 Vad ska vi göra?

I detta avsnitt går vi igenom de olika typerna av undersökningar vi ska göra, litteraturstudier och egen experiment.

3.3.1 Litteraturstudie

Vi ska genomföra en litteraturstudie av en årlig världsomfattande undersökning om DDoS-attacker, som genomförs av en av världens största leverantörer av DDoS-skydd, Kaspersky Lab. Med hjälp av resultatet planerar vi åskådliggöra de vanligaste förekommande ekonomiska konsekvenserna som uppstår i samband med DDoS-attacker. För att sedan diskutera hur dessa konsekvenser kan hanteras och hållas till ett minimum.

Genom att granska ett svenskt E-handelsföretag(CDONE.com) och dess årsredovisning planerar vi att beräkna vad en DDoS-attack kan medföra för tänkbara intäktsförluster, beroende på hur länge attacken varar. Genom att utgå ifrån nettoomsättningen kan vi beräkna den förväntade minskningen av nettoomsättningen beroende på vilket tidsintervall som företagets webbsida blir obrukbar. Detta är möjligt då CDONE.com är ett företag som baserar hela sin försäljning på internet, d.v.s. företaget har inga fysiska butiker och kan inte bedriva någon försäljning om webbsidan skulle bli onåbar pga. av en DDoS-attack.

3.3.2 Experiment

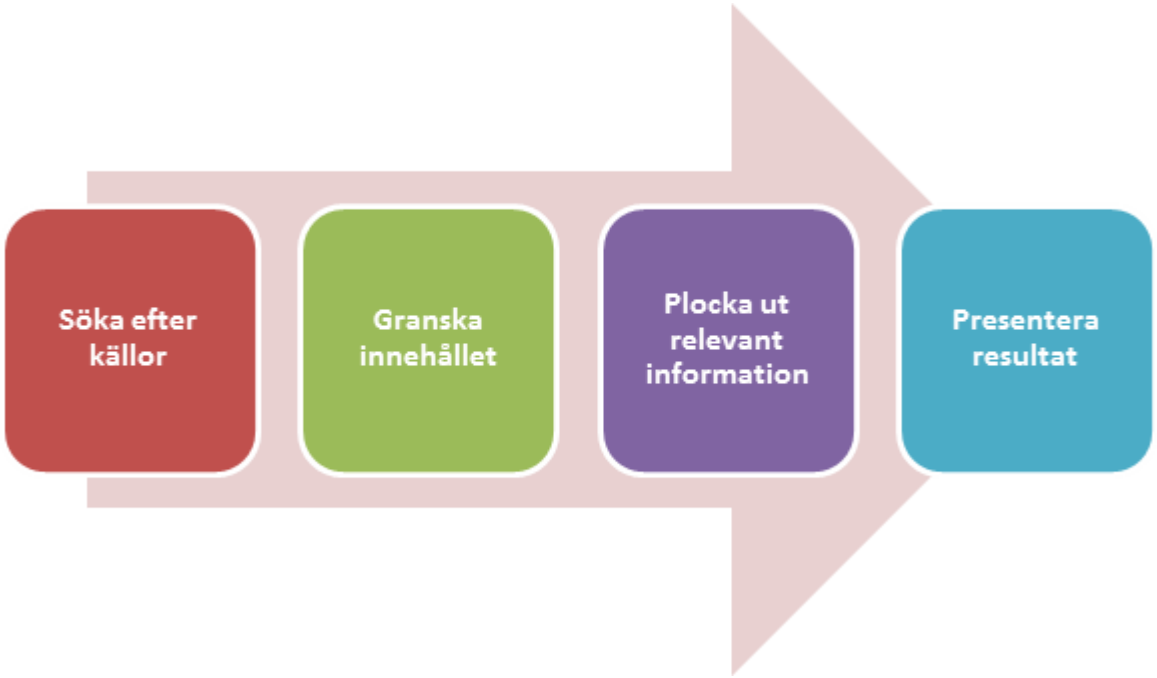
Vi ska även utföra egna tester där vi försöker genomföra DoS- och DDoS-attacker mot två olika webbservrar och en Brandvägg. Efter att ha genomfört lyckade attacker planerar vi också att ändra utformningen av nätverket för att försöka skydda webbservern från attackerna genom att sätta en virtuell brandvägg mellan servrarna och angriparna.

3.4 Forskningsprocess

I följande avsnitt åskådliggör vi hur vi har gott till väga för att genomföra våra olika studier, litteraturstudie och experiment.

3.4.1 Litteraturstudie

Processen för litteraturstudien var uppdelad i fyra olika steg, vilket illustreras i Figur 7.



Figur 7: **Forskningsprocess (Litteraturstudie)**

3.4.1.1 Söka efter källor

Litteraturstudien började med att vi letade efter källor som kunde passa ämnet för vår undersökning. Till en början begränsade vi vår sökning till databaserna KTHB Primo [33]och Digitala Vetenskapliga Arkivet (DiVA) [34]. Databaser som innehåller:

- "*vetenskapliga artiklar*
- *tryckta tidskrifter och e-tidskrifter*
- *tryckta böcker och e-böcker*
- *konferensbidrag*
- *examensarbeten och avhandlingar, med mera*" [33].

Vi utökade sedan våra källor i forma av, rapporter från industrin, multinationella företag som specialerat sig på hanteringen av DDoS-attacker, produkt-/tjänsteinformation från företag som säljer DDoS-skydd, årsredovisningar från E-handelsföretag och Webbsidor om DDoS-attacker och DDoS-skydd.

3.4.1.2 Granska innehållet

Efter att ha tagit fram ett stor underlag av källor började vi granska innehållet. Webbsidor och rapporter som vi inte ansåg relevanta för vår forskning plockades bort, och kvar var då bara de källor vi ansåg var lämpliga för vår undersökning.

3.4.1.3 Plocka ut relevant information

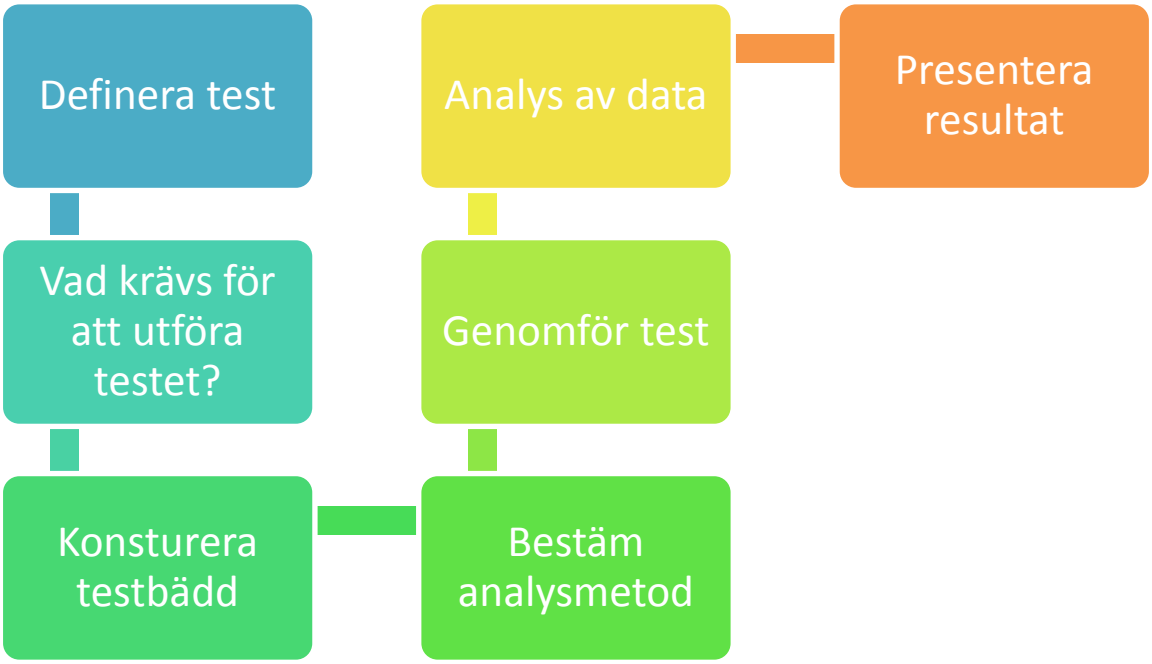
Efter att ha avgränsat oss till en speciell uppsättning källor började vi med att leta plocka ut den information som vi ansåg var relevant för att besvara vår frågeställning.

3.4.1.4 Presentera resultat

Den utvalda informationen presenterade vi sedan i form av ett resultat, som besvara våra tidigare frågeställningar.

3.4.2 Experiment

Processen för experimenten/testen var uppdelad i sju olika steg, vilket illustreras i Figur 8.



Figur 8: **Forskningsprocess för egna experiment/test**

3.4.2.1 Definiera test

Det första steget i processen var att definiera testet, dvs. avgöra vilken typ av attack vi skulle utföra samt bestämma målet för testet, utföra en lyckad attack för att rendera en websida obrukbar, eller utföra en attack för att sedan försöka avvärja den utan att websidan blir obrukbar.

3.4.2.2 Vad krävs för att utföra testet?

Nästa steg gick ut på att undersöka hur ett sådant test skulle kunna utföras. Leta efter relevant information på internet, undersök hur andra har genomfört liknande test tidigare. Fastställ vilka komponenter som behövs för att utföra testet, i form av hårdvara och mjukvara.

3.4.2.3 Bestäm analysmetod

Steg 3 bestäm hur vi ska analysera data som samlas in i samband med testet. Vad exakt är det vi ska titta på?

3.4.2.4 Konstruera testbädd

Efter all nödvändig hårdvara och mjukvara är införskaffad och analysmetoderna fastställda, återstår det att konsturera testbädden innan vi kan utföra testet. Sammankoppla alla komponeter som ska ingå i testbädden och konfigurera dem för testet.

3.4.2.5 Genomför test

Efter testbädden är färdigställd utförde vi testet.

3.4.2.6 Analys av data

Med hjälp av förbestämda analysmetoder granskade och analyserade vi insamlad data.

3.4.2.7 Presentera resultat

Efter dataanalys sammanställde vi data och redovisade den i rapporten.

3.5 Datainsamling

Den etiska aspekten har till stor del styrt datainsamlingen. Då DDoS är ett komplext ämne i sig, där mycket av informationen är hemlighetsstämplad, har man frestats med tanken att ta till mindre etiska metoder för att få tag på den information vi eftersökte. T.ex. lekte vi med tanken att utge oss för att vara ett företag som var intresserad av att köpa DDoS-skydd från olika leverantörer för att på så sätt få redan på mer information. Vi valde dock att inte fullfölja den idén då den bryter mot de forskningsetiska principerna:

Tabell 3: Forskningsetiska principer

Konfidentialitetskravet	Uppgifter om alla deltagare i en undersökning skall ges största möjliga konfidentialitet. Personuppgifter skall förvaras på ett sådant sätt att obehöriga inte kan ta del av dem [35].
Informationskravet	Forskaren ska informerade om den aktuella forskningsuppgiftens syfte till de som berörda av forskningen [35].
Samtycketskravet	Vi en undersökning har deltagare rätt att själv bestämma över sin medverkan [35].
Nyttjandekravet	Uppgifterna som samlas in om enskilda personer får enbart användas för forskningsändamål [35].

3.5.1 Slutsats

Genom att basera vår undersökning kring litteratur och offentliga handlingar behöver vi inte ta hänsyn till ovanstående forskningsetiska principer.

3.5.2 Experiment

Vi har valt att avgränsa våra experiment till att endast undersöka DDoS-attacken HTTP GET och SYN översvämning. Vi har också begränsat oss till att attackera två olika typer av servrar, Apache, Windows server, samt en Astaro brandvägg.

3.5.3 Urval

Tidigare forskning är hämtad från källor från databaserna KTHB Primo[33]och DiVA [34]. Undersökningarna som ligger till grund för bilden av den framtida utvecklingen av DDoS-attacker och de ekonomiska konsekvenserna av attackerna är Arbor Networks " Worldwide Infrastructure Security Report X"[1] och Kaspersky Labs "B2B-International-2014-Survey-DDoS-Summary-Report"[2].

För att kunna genomföra beräkningar för minskad nettoomsättning av vi använt oss av Qliro Group AB årsredovisning för 2014 och specifikt för dotterbolaget CDON.com [5].

3.1 Experimentdesign & genomförande

Experimenten som vi utförde byggde på två olika testbäddar som vi kommer att presentera i det här avsnittet. Vi presenterar även vilken typ av Mjukvara som vi har använt för våra tester.

3.1.1 Testbädd 1 (http Get Attack)

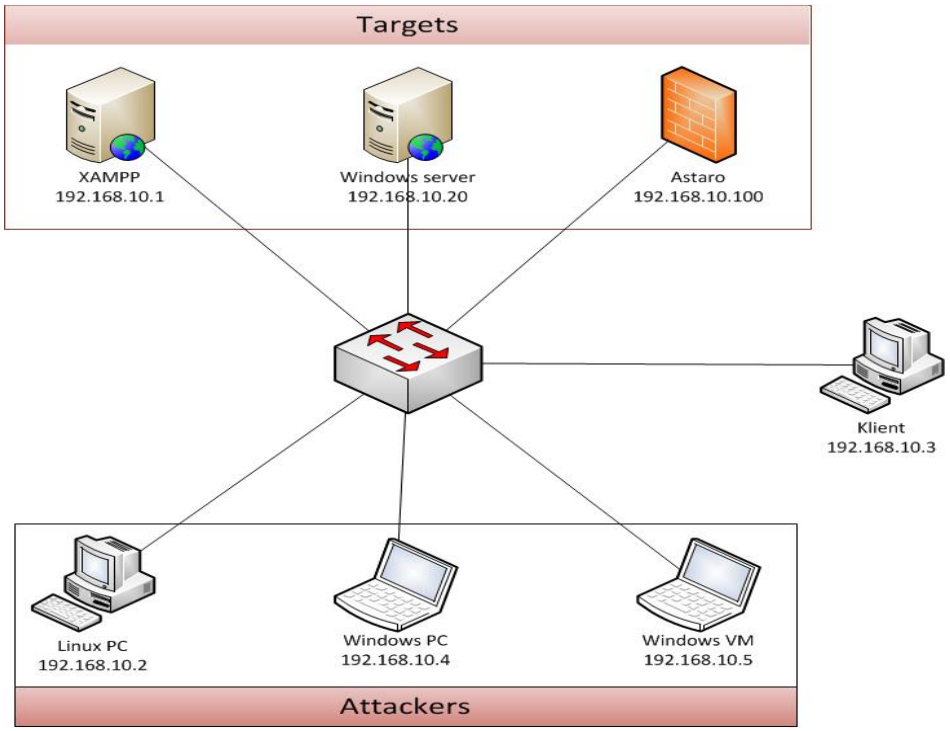
För att bygga upp tesbädd 1 och kunna utföra våra expreminent gjorde vi följande:

1. Två Webbserverar sätts upp med en testwebbsida.
2. En Klient skapas och ansluts till nätverket för att kontrollera att webbsidan är på plats.
3. En brandvägg ansluts till nätverket.
4. En Windows PC och en Windows VM ansluts till nätverket.
5. På komponenterna i steg 4 installeras HOIC.
6. En Linux PC ansluts till nätverket och på den installeras GoldenEye.
7. Kontrollerar att alla komponenter i nätverket har åtkomst till varandra.
8. En riktad DDoS-attack genomförs med hjälp av tre maskiner (HOIC och GoldenEye).
9. Med hjälp av klienten försöker vi komma åt webbsidan.
10. Kontrollera Wireshark för att se vilken trafik som servern tar emot.

Uppbyggnaden av tesbädd 1 såg ut på följande sätt:

Tabell 4: Komponenter testbädd 1

Värd	IP Adress	Maskin	Programvara
Webbserver(Apache)	192.168.10.1	Windows PC	XAMPP
Attacker	192.168.10.2	Linux PC	Golden eye
Klient	192.168.10.3	Linux PC	Firefox
Angripare	192.168.10.4	Windows PC	HOIC
Angripare	192.168.10.5	Windows VM	HOIC
Webbserver(ISS)	192.168.10.20	Windows VM	Windows server
Brandvägg	192.168.10.100	Astaro VM	Astaro
Switch	-	-	-



Figur 9: **Nätverksuppbyggnad testbädd 1**

3.1.2 Testbädd 2 (http Get Attack)

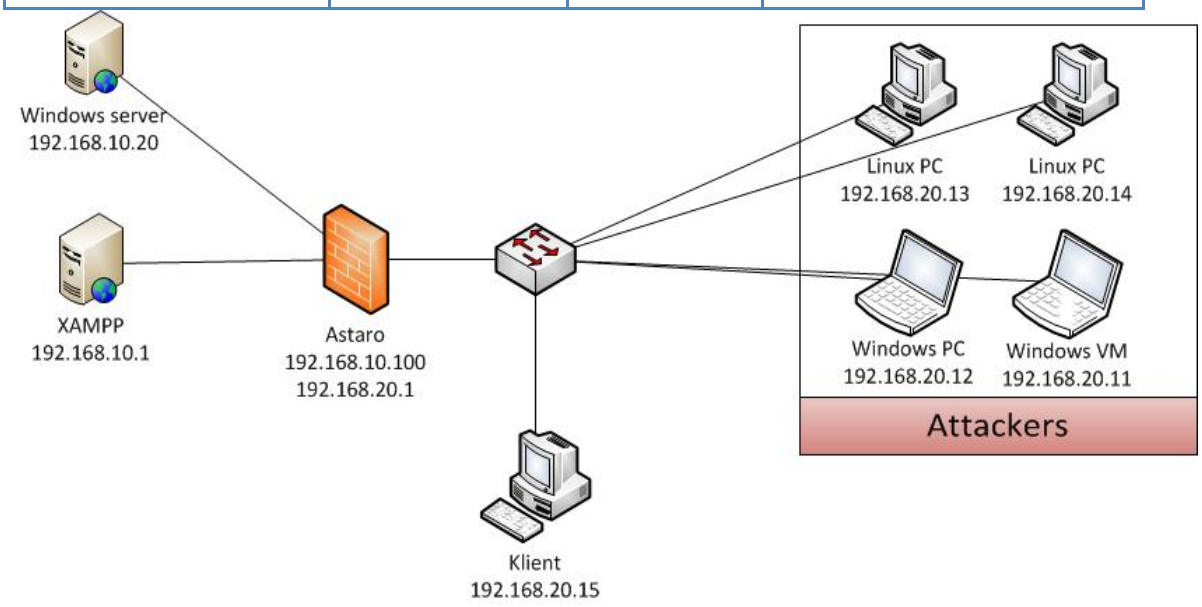
För att bygga upp tesbädd 2 och kunna utföra våra expreminent gjorde vi följande:

1. Sätt upp Astaro brandväggen och konfigurerar den så att den har ett interface i varje subnät (192.168.10.100 & 192.168.20.1)
2. Två Webbserverar sätts upp med en testwebbsida på 192.168.10.0/24 subnätet, konfigurerar dem så att de använder Astaro som standard gateway (192.168.10.100).
3. På 192.168.20.0/24 subnätet skapas fyra "Attackers" och en Klient, som alla använder Astaro som standard gateway (192.168.20.1).
4. Installera HOIC på Windows maskinerna (192.168.20.11 & 192.168.20.12).
5. Installera GoldenEye på Linux maskinerna (192.168.20.13 & 192.168.20.14).
6. Kontrollera att alla komponenter i nätverket har åtkomst till varandra.
7. En riktad DDoS-attack genomförs med hjälp av fyra maskiner (HOIC och GoldenEye).
8. Med hjälp av klienten försöker vi komma åt webbsidan och Astaro.
9. Kontrollera Wireshark för att se vilken trafik som servern tar emot.

Uppbyggnaden av tesbädd 2 såg ut på följande sätt:

Tabell 5: Komponenter testbädd 2

192.168.10.0/24			
Värd	IP Adress	Maskin	**Programvara**
Webbserver(Apache)	192.168.10.1	Windows PC	XAMPP
Webbserver(ISS)	192.168.10.20	Windows VM	Windows server
Brandvägg	192.168.10.100	Astaro VM	Astaro
192.168.20.0/24			
Brandvägg	192.168.20.1	Astaro VM	Astaro
Angripare	192.168.20.11	Windows VM	HOIC
Angripare	192.168.20.12	Windows PC	HOIC
Angripare	192.168.20.13	Linux PC	Golden eye
Angripare	192.168.20.14	Linux PC	Golden eye
Klient	192.168.20.15	Linux PC	Firefox
Switch	-	-	-



Figur 10: Nätverksuppbyggnad testbädd 2

3.1.3 Hårdvara/Mjukvara som används

För att genomföra våra tester behövde vi både hårdvara och mjukvara. Detta avsnitt avser att åskodliggöra de olika program oc maskiner som vi använde för att utföra testen.

3.1.3.1 Hårdvara

Vi har valt att använda oss av datorer med två olika operativsystem, Linux och Windows. Fördelningen såg ut på följande sätt:

- Linux PC x 3
- Windows PC x 2

3.1.3.2 Mjukvara

För att kunna utföra testerna har vi varit tvungna att installera olika sorters mjukvara. I det här avsnittet kommer vi ge en kort förklaring av de olika programmen som vi har använt oss av.

3.1.3.2.1 Astaro

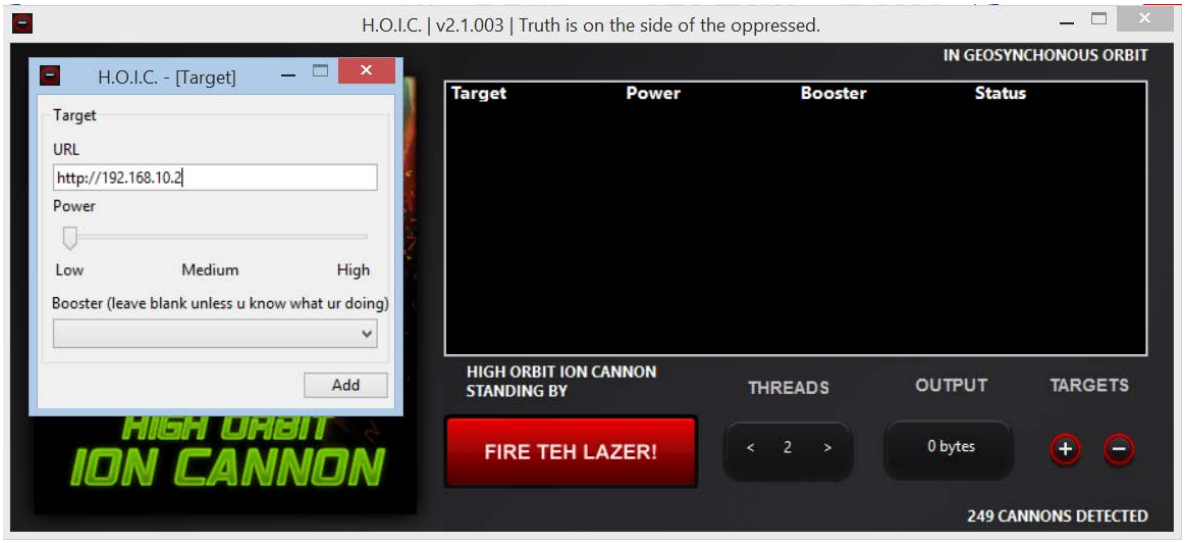
Astaros Unified Threat Management (UTM) brandvägg för hemanvändare är ett eget dedikerat operativsystem på en dedikerad hårdvara. Används som brandvägg för att hantera trafik som går både in och ut ur nätverket, för att skydda mot scanners, bots, diverse Angripare och andra farliga bedrifter ett nätverk kan råka ut för [36].

3.1.3.2.2 GoldenEye

GoldenEye är ett python script för säkerhetstester av DDoS attacker. Scriptet skapar ett antal workers med ett antal sockets vardera. Dessa skickar sedan antingen HTTP GET eller HTTP POST requests till valt offer [37].

3.1.3.2.3 HOIC

High Orbit Ion Cannon är en lättanvänd mjukvara för windows (Finns en sämre variant för Linux också) som används för att skicka HTTP GET floods till ett valt offer [38]. Nedan beskrivs hur det går till.



Figur 11: High Orbit Ion Canon

- Tryck på "+" tecknet i nedre högra hörnet, som man ser på Figur 11.
- Välj sedan ditt mål och skriv in dess URL under "URL" i popup rutan som öppnas.
- Välj önskad styrka (högre styrka kräver mer prestanda).
  - Low ~ 2 requests / sek och tråd
  - Medium ~ 4 requests / sek och tråd
  - High ~ 8 requests / sek och tråd
- Avancerade användare kan även välja att tillföra Booster scripts för att göra attacken ännu mer kraftfull.

- Tryck på "Add" och ditt mål kommer nu synas på huvudskärmen.
- På huvudskärmen kan man nu även välja hur många trådar HOIC ska använda sig av. Ju fler desto kraftfullare attack. Här rekommenderas upp till 20-30 trådar, då fler än så ofta får programmet att krascha.
- Slutligen, för att starta attacken, tryck på "FIRE TEH LAZER!"

3.1.3.2.4 Hping3

Hping3 är ett nätverksverktyg som skickar anpassade TCP/IP paket för att t.tex. testa brandväggars regler, port scanning eller testa nätverkets prestanda med olika protokoll m.m [39].

3.1.3.2.5 IIS

Internet Information Services (IIS) är en web server skapad av Microsoft [40].

3.1.3.2.6 Oracle VM VirtualBox

VirtualBox är en mjukvara för att skapa separata virtuella maskiner [41].

3.1.3.2.7 Windows Server 2008

Microsofts operativsystem för Windows Server 2008 [42].

3.1.3.2.8 Wireshark

Wireshark är en mjukvara som analyserar paket och används ofta för att felsöka nätverk, analysera nätverk och utveckling av kommunikationsprotokoll [43].

3.1.3.2.9 XAMPP

XAMPP är en öppen käll cross-plattform web server bestående av Apache HTTP Server, MySQL, PHP och Pearl [44].

3.2 Bedömning av reliabiliteten och validiteten av insamlad data

I följande avsnitt bedömer vi reabiliteten och validitetet av insamlad data.

3.2.1 Reliabilitet

Hur kan vi veta att våra resultat är tillförlitliga?

3.2.1.1 Litteraturstudie

Vi bedömer att resultatet vi kommer att få från litteraturstudien är tillförlitligt. Vi grundar det i att Kaspersky Lab är en av de största leverantörerna av DDoS-skydd på marknaden och deras undersökning *Global IT security risks survey 2014 – Distributed Denial of Service (DDoS)Attacks*" är en årlig undersökning och resultaten grundar sig på svaren från 3900 respondenter från 27 olika länder [2].

Årredovisningen från CDONE.com måste vara korrekt enligt bokföringslagen och har således granskats av revisorer, vilket gör att den kan anses som tillförlitlig.

3.2.1.2 Experiment

Vi bedömer att data vi samlar in vid våra tester är tillförlitligt. Det grundar sig i att vi innan starten av testen kontrollerar att all trafik når de tilltänkta målen. Under testet kontrollerar vi också trafikens flöde med hjälp av Wireshark och på så sätt kan vi upptäcka i realtid om trafiken inte skickas genom nätverket på det sätt vi har tänkt.

3.2.2 Validitet av experiment

Vi anser att resultatet från våra testar kommer ha hög validitet. Det grundas i den simpla kontrollen vi gör för att bedöma resultatet, är webbsidan tillgänglig eller inte?

Genom att kontrollera webbsidans tillgänglighet innan vi utför testet kan vi fastställa att om webbsidan går ner är det på grund av DDoS-attacken vi utfört.

3.3 Planerad data analys

För att kunan se analysera våra tester var vi tvungna att definiera exakt vad vi skulle titta på. Samt bestämma vilka verktyg vi skulle använda oss av.

3.3.1 Teknik för data analys

Vi bevakar trafiken i realtid för att se när DDoS-attacken startar, när den stoppas och för att kontrollera så att DDoS-trafiken når fram till det tänkta målet, webbservern.

3.3.2 Mjukvara

För att kunna bevaka trafiken använder vi oss av Wireshark.

3.4 Utvärdering

De frågeställningar som vi tar hänsyn till när vi utvärderar resultatet är följande:

- Når DDoS-trafiken fram till det tilltänkta målet, om inte, varför?
- Är webbsidan tillgänglig eller inte?
- Om hemisdan är uppe, hur är prestandan? Tar det långt tid att ladda nya sidor?

4 Analys

Vi har alltid börjat varje experiment med att försöka göra vår webbsida obrukbar utan att använda oss av någon brandvägg. Web servern har alltså varit helt exponerad i nätverket. Innan varje attack startat har vi självklart lyckats komma åt webbsidan och under varje attack har vi sedan försökt få åtkomst till webbsidan via en legitim klient. Under attacken har vi även analyserat mängden trafik genom Wireshark. Vi har sedan observerat om vi lyckats nå webbsidan under attacken eller inte. Lyckades vi inte nå webbsidan gjorde vi om samma test fast med brandväggen mellan angriparna och web servern. Genom att både analysera Wireshark och samtidigt observera statusen av web servern kunde vi enkelt se, via Wireshark, att web servern tog emot betydligt mindre trafik. Brandväggen droppade/blockade alltså en stor del av HTTP trafiken från angriparna. Vi kunde även enkelt observera att vi under attackens gång även hade åtkomst till webbsidan utan problem. Vi har alltså på ett enkelt sätt kunnat kolla om webbsidan är "Up" eller "Down".

4.1 Resultat

I detta avsnitt redovisar vi resultatet av vår studie och diskuterar dem utifrån ett ekonomiskt- och säkerhetsmässigt perspektiv.

Resultatavsnittet är uppdelat i två avsnitt:

- Litteraturstudier
- Experiment

I avsnittet litteraturstudier presenteras resultatet från granskningen av Kasper labs "Global IT Security risks survey 2014 – Distributed Denial of service (DDoS) Attacks" [2]. Avsnittet innehåller också resultatet av våra beräkningar på vilken inverkan en DDoS-attack skulle göra på företaget CDON.com, i form av minskad nettoomsättning.

4.1.1 Litteraturstudier

Resultatet av Kaspersky labs undersökning är som följer.

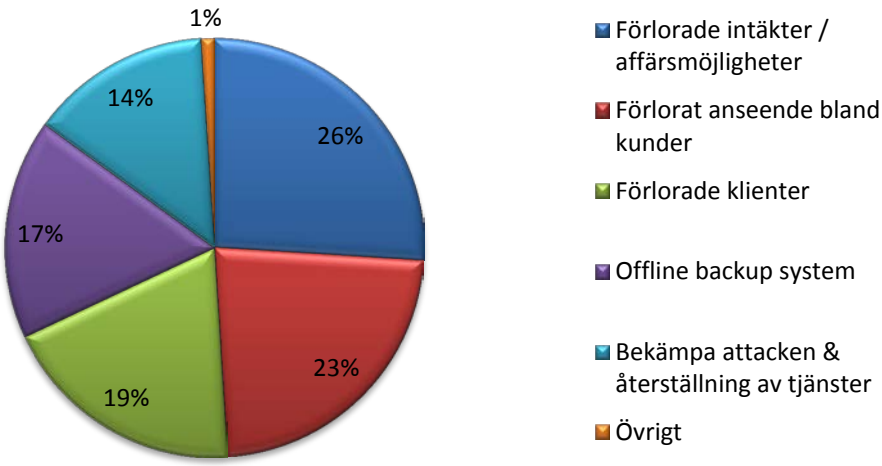
4.1.1.1 Ekonomiska konsekvenser av DDoS-attacker

Kaspersky labs undersökningen visar på att den genomsnittliga kostnaden för en DDoS-attack är $52,000, för små och medelstora företag, medan för större företag ligger kostnaden på $444,000 [2]. Kostnader bestående av förlorade affärmöjligheter och IT utgifter.

De två konsekvenserna av DDoS-attacker som IT chefer fruktar mest är:

- Förlorade intäkter,
- Förlusten av kunders förtroende.

Och det visar sig att det är just de två konsekvenserna som är de vanligaste förekommande i samband med en DDoS-attack [2].



Figur 12: **Kostnader av DDoS-attacker (Kaspersky lab)**

Kostnaderna som är anslutna till DDoS-attacker kan brytas ner till fyra huvudområden [1].

1. Skadat förtroende
2. Ökad personalomsättning & investeringskostnader
3. Professionella tjänster
4. Affärsstörningar

Till varje huvudområde hör sedan en rad olika kostnadsposter.

Skadat förtroende

- Förlust av affärsmöjligheter
- Skador på företagets rykte/varumärke
- Skadad kreditvärdering
- Ökade försäkringspremier

Ökad personalomsättning & investeringskostnader

- Kostnader för programvara eller infrastruktur
- Utbildningskostnader
- Personalkostnader

Professionella tjänster

- IT-säkerhetskonsulter
- Juridiska ombud
- Ledningskonsulter

Affärsstörningar

- PR/ Företagsimage konsulter

- Tillfällig förlust av åtkoms till kritisk/viktigt företagsinformation
- Tillfällig förlust av försäljningsmöjligheter

4.1.1.2 Case Tillfällig förlust av försäljningsmöjligheter (CDON.com)

CDON.com hade en Nettomsättning av 1.887,8 Mkr år 2014 [5].

Tabell 6 Nettoomsättning CDON.com 2014

Nettoomsättning	
År	1 878 000 000,00 kr
Månad	1 573 166 66,67 kr
Dag	52 438 888,89 kr
Timme	2 184 953,70 kr
Minut	36 415,90 kr
Sekund	606,93 kr

Om CDON.com skulle bli utsatt för en DDoS-attack som medförde en tillfällig förlust av försäljningsmöjligheter skulle det resulterat i en minskad nettoomsättning på 36 416 kr per minut (Om kunderna väljer att avstå från sitt inköp eller väljer att vända sig till ett konkurrerande företag).

4.1.2 Experiment

I detta avsnitt kommer visa inställningarna för våra experiment samt vad som resultatet blev i varje test.

4.1.2.1 Testbädd 1

4.1.2.1.1 Test 1, (HTTP Get) Offer Apache server (XAMPP)

Test 1 HTTP Get attack mot XAMPP Apache server, inställnignarna såg ut som följer:

Tabell 7: Angripare test 1 testbädd 1

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	160	1280

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	20	700

Resultatet blev:

Tabell 8: **Offer test 1 testbädd 1**

Offer – Windows PC

Programvara	Webbserver	Status efter attack
XAMPP	Apache	Down

4.1.2.1.2 Test 2, (HTTP Get) Offer Brandvägg (Astaro)

Test 1 HTTP Get attack mot Astaro brandvägg, inställnignarna såg ut som följer:

Tabell 9: **Angripare test 4 testbädd 1**

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	80	640

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	60	480

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Resultatet blev:

Tabell 10: **Offer test 4 testbädd 1**

Offer – Astaro VM

Programvara	Brandvägg	Status efter attack
Astaro	Astaro	Down

4.1.2.1.3 Test 2, (HTTP Get) Offer Windows server (ISS)

Test 1 HTTP Get attack mot Windows server (ISS), inställnignarna såg ut som följer:

Tabell 11: Angripare test 4 testbädd 1

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	160	1280

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	20	700

Resultatet blev:

Tabell 12: Offer test 4 testbädd 1

Offer – Windows server (ISS)

Programvara	**Webbserver**	**Status efter attack**
Windows	ISS	Up/Service unavailable.

4.1.2.2 Testbädd 2

4.1.2.2.1 Test 1, (HTTP Get) Offer Apache server (XAMPP)

Test 1 HTTP Get attack mot XAMPP Apache server, inställnignarna såg ut som följer:

Tabell 13: Angripare test 1 testbädd 2

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	160	1280

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Angripare 4 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Resultatet blev:

Tabell 14: Offer test 1 testbädd 2

Offer– Windows PC

Programvara	**Webbserver**	**Status efter attack**
XAMPP	Apache	Up
Programvara	**Brandvägg**	**Status efter attack**
Astaro	Astaro	Up

4.1.2.2.2 Test 2, (HTTP Get) Offer Brandvägg (Astaro)

Test 1 HTTP Get attack mot Astaro brandvägg, inställnignarna såg ut som följer:

Tabell 15: Angripare test 3 testbädd 2

Angripare 1 - Windows PC

Programvara	**Inställningar**	
HOIC	**Threads**	**Http get/s**
	100	800

Angripare 2 - Windows VM

Programvara	**Inställningar**	
HOIC	**Threads**	**Http get/s**
	80	640

Angripare 3 – Linux PC

Programvara	**Inställningar**	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Angripare 4 – Linux PC

Programvara	**Inställningar**	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Resultatet blev:

Tabell 16: Offer test 3 testbädd 2 - HTTP Get) Offer Brandvägg (Astaro)

Offer – Windows PC

Programvara	**Webbserver**	**Status efter attack**
XAMPP	Apache	Up
Programvara	**Brandvägg**	**Status efter attack**
Astaro	Astaro	Up/Slow

Under sista experimentet använde vi oss av två Linux maskiner som körde Hping3 för att skapa en SYN översvämnings attack, där stora mängder SYN meddelanden skickades från slumpartade käll IP adresser, för att upprätta så många TCP anslutningar som möjligt. Detta försök lyckades inte ta ner våra web servrar men attacken gjorde vår web servers konfigurationssida obrukbar.

4.2 Reliabilitets analys

Resultaten anser vi är tillförlitliga. Eftersom vi genomför flera tester och får samma resultat. Vi bevakar också trafiken med Wireshark och kunde då bekräfta att angriparnas trafik når målet i testbädd 1, och i testbädd 2 fastnar trafiken i Astaro brandväggen, vilket var tanken.

4.3 Validitets analys

Eftersom vårt resultat baseras på statusen på webbservern och brandväggen efter en utförd attack, är servern och brandväggen uppe eller ner? Är det svårt att misstolka och ingen risk för att vi skulle fokusera på fel mätvärden vid testen. Med det sagt anser vi att vi har hög validitet i vår undersökning.

4.4 Diskussion

Avsnittet avser att diskuttera resultaten av litteraturstudien samt expremimenten. Och eventuellet ge en djupare bild av DDoS-Attacekr och de problem de medför.

4.4.1 Litteraturstudier

I detta avsitt kommer vi diskuttera resultatet av litteraturstudien.

4.4.2 Ekonomiska konsekvenser av DDoS-attacker

Som nämnts i resultat delen kan man dela upp de ekonomiska konsekvenserna i fyra huvudområden. I det här avsnittet kommer vi att diskutera dessa områden och åskådliggöra vad varje rubrik står för, enligt oss.

4.4.2.1 Skadat förtroende

Kundernas förtroende för ett företag är något som byggs upp över tid. Ett företag som vårdar sina kundrelationer och möjliggör för kunderna att få sina behov tillfredställda har stor chans att bilda långtgående kundrelationer som kan resultera i återkommande intäkter. Ett företag vars förtroende blivit skadat i följd av en DDoS-attack riskerar att förlora mycket.

4.4.2.1.1 Förlust av affärsmöjligheter

När ett företag blir utsatt för en DDoS-attack kan de bli tvungna att omfördela personalresurser för att lösa problemet. Det i sin tur leder till att företagets möjligheter att hantera de befintliga kundernas behov blir reducerad. Kunder som har uppdrag som är tidskänsliga eller kunder som helt enkelt är missnöjda på företaget (på grund av problem som uppstår i samband med DDoS-attacker) kanske väljer att gå till ett konkurrerande företag, som kan tillgodose deras behov.

4.4.2.1.2 Skador på företagets rykte/varumärke

För ett företag som profilerar sig som ett säkert företag, t.ex. banker, är det skadligt att bli förknippad med DDoS-attacker. Kunder som vill placera sina pengar på en säker plats kan i sin tur tänkas placera sina pengar i en annan bank, som inte har ett rykte av att bli utsatt för DDoS-attacker. Det är en av anledningarna till att många företag hemlighetsstämplar uppgifterna kring DDoS-attacker som drabbat företaget. För att informationen inte ska nå potentiella kunder, som i sin tur väljer en konkurrerande bank som upplevs som säkrare.

Samma sak gäller tillgänglighet och användarvänlighet. Ett företag vars webbsida ständigt krånglar/ligger nere på grund av att de blir utsatta för DDoS-attacker riskerar att förlora många kunder. Ett varumärke kan ta flera år att bygga upp, men bara ett ögonblick att rasera.

4.4.2.1.3 Skadad kreditvärdering

Ett företag som spenderar mycket tid på att bekämpa DDoS-attacker och försummar den dagliga verksamheten, vilket i sin tur leder till att företagets betalningsmöjligheter kan försämras på grund likviditetsbrist. För att förbättre livkiditeten i företaget är det tänkbart att företag blir tvungen att ta till nyupplåning. Faktorer som sedan ligger till grund för när företagets kreditvärdering sätts.

En sänkt/skadad kreditvärdering leder till att banker kommer att ta ut en högra ränta vid upplåning, på grund av att företagets betalningsmöjligheter anses vara sämre än tidigare. Det kan till och med gå så långt att företagets värdering är så dåligt att det inte får något låneerbjudanden från banken överhuvudtaget.

4.4.2.1.4 Ökade försäkringspremier

Ett företag som har tecknat en försäkring som täcker några av de skador som förekommer vid DDoS-attacker riskerar att få en ökad kostnad i form av en höjd försäkringspremie om företaget blir utsatt för en attack. Ett företag som en gång har blivit utsatt för en attack anses bära en högre risknivå och således måste försäkringsbolaget justera försäkringspremien för att kompensera för eventuella framtida kostnader.

4.4.2.2 Ökad personalomsättning & investeringskostnader

För att hantera en DDoS-attack krävs det att företaget tillför resurser för att hantera problemet. Antigen genom att tillsätta personal eller investera i lösningar.

4.4.2.2.1 Kostnader för programvara eller infrastruktur

Efter att företaget har blivit drabbat av en DDoS-attack är det vanligt att företaget investerar i ny programvara eller ny infrastruktur, som bättre kan hantera framtida DDoS-attacker [2].

4.4.2.2.2 Utbildningskostnader

Till följd av en DDoS-attack kan ett företag bli tvunget att investera i utbildning av den egna personalen för att kunna hantera framtida DDoS-attacker, utbildning i användningen av nya programvaror samt nya rutiner.

4.4.2.2.3 Personalkostnader

Ökade personalkostnader är en kostnad som kan förekomma när ett företag blir utsatt för en DDoS-attack. Har man kunskapen inom företaget kan de ske i form av att It-tekniker tvingas arbeta övertid för att lösa problemet, vilket som tidigare nämnts, resulterar att dessa personer inte är tillgängliga för att utföra andra arbetsuppgifter, vilket kan resultera i företaget förlorar kunder [2][45].

4.4.2.3 Professionella tjänster

En annan kostnad som kan uppstå vid DDoS-attacker är konsultkostnader.

4.4.2.3.1 IT-säkerhetskonsulter

IT-rådgivning i form av IT-säkerhetskonsulter måste anlitats för att hantera DDoS-attacken, vilket är en följd av att kunskapen för att lösa problemet inte finns hos den befintliga personalen [45].

4.4.2.3.2 Juridiska ombud

Till följd av DDoS-attacken kan det vara aktuellt att driva en juridisk process mot de ansvariga för attacken. Det leder till att advokater/juridiska ombud måste anlitas, vilket medför extra kostnader.

4.4.2.3.3 Ledningskonsulter

För att bättre kunna hantera framtida angrepp på företaget är det nödvändigt för företaget att ta fram nya rutiner och en handlingsplan för hur man hanterar situationen i framtiden. För att ta fram en sådan handlingsplan kan det krävas spetskompetens, som företaget kan få genom att ta in en managmentkonsult, vilket medför en kostnad.

4.4.2.4 Affärsstörningar

När ett företag blir utsatt för en DDoS-attack är det nästintill ofrånkomligt att det blir störningar i företagets affärer.

4.4.2.4.1 PR/ Företagsimage konsulter

Som vi nämnt tidigare kan företagets anseende/image skadas vid en DDoS-attack och ett skadat anseende kan vara svårt att återställa. Därför är det fullt tänkbart att det första steget som företaget tar för att återställa sitt rykte är att hyra in en PR konsult som kan hjälpa till med arbetet [2].

4.4.2.4.2 Tillfällig förslust av åtkoms till kritisk/viktigt företags information

För ett företag vars verksamhet är basserad på internet kan det bli svårt att komma åt viktigt information vid en attack. T.ex. ett företag som använder sig av en extern tjänster eller servrar med olika funktioner och som lagrar information för företagets räkning.

4.4.2.4.3 Tillfällig förlust av försäljningsmöjligheter

Ett företag vars försäljning helt är baserad på företagets webbsida riskerar att förlora sina försäljningsmöjligheter om det blir utsatta för en DDoS-attack. Även företag som har försäljning via telefon eller i butik riskerar att försämra sina försäljningsmöjligheter då det har svårare att nå ut till alla kunder.

4.4.3 Case CDON.com

Utifrån våra beräkningar kan vi se att CDON.com potentiellt skulle kunnat förlora/minska omsättningen med 36 416 kr(2014) för varje minut som webbsidan var otillgänglig på grund av en DDoS-attack. Förutsatt att kunden valde att vända sig till ett annat företag för att göra sin order.

Koncernen har identifierat driftstörningar som en stor risk för verksamheten. Vilket framgår av följande utklipp ur årsredovisningen [5].

Möjligheten finns att företaget(CDON.com) har blivit utsatt för DDoS-attacker under 2014 och att det var just en sådan händelse som har föranletts för att skriva in ovanstående stycke i årsredovisningen. Det är bara något vi kan spekulera i, men det viktigaste menar vi är att företaget är medvetet om riskerna och arbetar aktivt för att minska dem. Vilket framgår av företagets års redovisning.

4.4.4 Experiment

I detta avsitt kommer vi diskuttera resultatet av experimentet.

4.4.4.1 Testbädd 1, Offer XAMPP (HTTP Get)

Resultatet av testet är att webbsidan går ner efter mindre än 1 minut. Först efter att vi avslutat HOIC programmen är webbsidan tillgänglig igen. Webbsidan blir överbelastad av det stora antalet förfrågningar som skickas till webbsidan.

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
739	0.044800000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
740	0.044874000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
741	0.044911000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
742	0.044932000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
743	0.045750000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
744	0.045795000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
745	0.045825000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
746	0.045850000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
747	0.045858000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
748	0.045867000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
749	0.045875000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
750	0.045884000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
751	0.045892000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
752	0.045901000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
753	0.045909000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
754	0.045918000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
755	0.045926000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
756	0.045934000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
757	0.045942000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
758	0.045951000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
759	0.045959000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0
760	0.045967000	192.168.10.1	192.168.10.2	HTTP	131	GET /Test/ HTTP/1.0

Figur 13: HTTP Get översvämning (eget experiment)

4.4.4.2 Testbädd 1, Offer Astaro (HTTP Get)

Resultatet liknar det i tidigare test, sidan blev otillgänglig efter mindre än en minut. Till en början noterade man att sidan hade problem att ladda när man utförde någon aktion och sedan försvann tillgängligheten helt. Viktigt att skilja på här är att brandväggen fortfarande fungerade i bakgrunden. Det var endast Astarons konfigurationssida som blev otillgänglig p.g.a. HTTP trafiken. Brandväggen gjorde i praktiken fortfarande det den var konfigurerad att göra. För att få hela brandväggen att sluta fungera hade vi behövt överbelasta länken som var kopplad till brandväggen genom att skicka mer data än vad länken klarar av. Klarar t.ex. länken av 10Gbps och vi skickar 11Gps kommer ingenting att komma igenom brandväggen.

4.4.4.3 Testbädd 1, Offer ISS (HTTP Get)

I fallet med Windows server och ISS lyckades vi aldrig göra webbservern helt obrukbar, utan endast vid ett par tillfällen lyckades vi få felmeddelandet "http Error 503 – Service unavailable". Varför den servern klarade sig bättre mot angreppen vet vi inte, men det skulle vara intressant att undersöka det vidare. Rent generellt verkar det som att den dedikerade Windows servern klarade mer trafik än XAMPP. Hade vi haft ännu fler angripare skulle vi självklart kunnat göra Windows servern obrukbar också. I verkliga attacker är det ofta 100-tals eller 1000-tals angripare.

4.4.4.4 Testbädd 2, Offer XAMPP genom Astaro (HTTP Get)

Genom att konstruera ett nytt nätverk där trafiken mellan webbservern och angriparna var tvungen att passera genom en brandvägg (Astaro) kunde vi effektiv avvärja DDoS-attacken. Brandväggen hjälpte således till att blocka/droppa en stor del av HTTP trafiken som den upptäckte, innan den nådde webbserven. Men som vi tidigare diskuterade skulle man i praktiken istället för att angripa själva webbservern, istället angripa brandväggen, genom att skicka tillräckligt mycket volymbaserad trafik. Genom att inse att det är otroligt svårt att motverka volymbaserade attacker, där t.ex. 11Gbps skickas över en 10Gbps länk förstår man att det spelar stor roll vart i nätverket dessa brandväggar placeras. För att ha störst chans att motverka dessa volymbaserade attacker bör således brandväggarna placeras så långt ut i nätverket som möjligt, gärna redan hos ISPn, för att då ha möjlighet att routa om trafiken till t.ex. ett Scrubbing center, innan det når ens eget nätverk.

5 Slutsats och framtida/vidare forskning

Som vi tidigare nämnt är DDoS-attacker ett stort hot mot företag som använder sig av internet för stora delar av sin verksamhet. Det vi menar med att det är et stort hot är att DDoS-attacker kan medföra både ökade kostnader och minskade intäkter för ett drabbat företag[1], vilket är direkt kopplat till företagets framtida kokurransmöjligheter. Kostnaderna som är anslutna till DDoS-attacker kan brytas ner till fyra huvudområden [1].

Antalet DDoS-attacker har en ökande trend och det kan vara ett säkert antagande att antalet personer som har utfört en DDoS-attack ökar. Men vad är då den bakomliggande orsaken till att någon utför en DDoS-attack?

5.1 Slutsats

Mål som vi hade satt upp för litteraturstudien var att ta reda på hur utvecklingen ser ut i världen kring DDoS-attacker, samt ta reda på vilka som är det vanligaste ekonomiska konsekvenserna av en DDoS-attack. Genom att gett en tydlig bild av att DOS-attacker ökar både till antal och storleksmässigt årligen, anser vi att vi uppnått den delen av målet. Vi har också identifierat de vanligaset konskevenser av DDoS-attacker för att sedan vidare utveckla och ge konkreta exempel på hur det kan se ut för utsatta företag. Genom att genomföra egna beräkningar baserade på den redovisade nettoomsättningen för CDON.com lyckades vi också sätta exakta siffror för hur mycket ett e-handelsföretag kan förlora per minut deras webbsida inte är tillgänglig för kunderna. Med det anser vi att vi visat de ekonomiska konsekvenserna av DDoS-attacker.

Efter att genomfört våra egna tester har vi kommit till insikten att det är väldigt lätt att utföra DDoS-attacker. Vi har också förstått att det inte finns några säkra lösningar, även om man investerar i de dyraste DDoS-skydden på marknaden så garanterar det inte att man inte blir påverkad av DDoS-attacker.

Från undersökning kan vi se att kriminell aktivitet utgör stor del av de DDoS-attacker som förekommer i världen idag. I och med att man har hittat sätt att tjäna pengar på DDoS-attacker kommer det fortsätta att vara en attraktiv attackform. Vilket får oss att tro att antalet DDoS-attacker kommer att fortsätta öka även i framtiden.

Om vi hade möjlighet att göra om forskningen skulle vi ha utökat experiment delen av undersökning- börja tidigare och utöka testen med flera datorer för att skapa ett större nätverk.

5.2 Begränsningar

Eftersom mycket information om företags DDoS-skydd och attacker de blivit utsatta för är hemlighetsstämplade, vilket har gjort det svårt att få relevant information från Svenska företag. Vi hade gärna sett att vi fick inblicken i vilken typ av DDoS-skydd som används av olika företag och hur de är uppbyggda. Vi skulle också ha velat veta hur vanligt förekommande DDoS-attacker är för svenska företag och hur de valt att hantera det.

Ytterligare begränsningar som vi har känt av är tidsramen av 10 veckor. I och med att ämnet är så komplext skulle det lämpas att undersökas vidare på en högre nivå. En undersökning som skulle omfatta mer omfattande experiment.

Vi hade också sätt att vi hade fått mer tid att arbeta enbart med våra experiment och utökat vår testbädd med flera datorer/nätverksinterface för att simulera ett verkligt botnät(storleksmässigt).

5.3 Framtida forskning

Det som inte rymdes under tidsrammen för examensarbetet är följande:

Tabell 17: Framtida foskning

Intervjustudie	Intervjua personer som arbetar med att förhindra DDoS attacker.
Enkätundersökning	Undersöka DDoS-klimatet på den svenska markanden.
Utökade experiment	Genomföra flera experiment: testa markandens DDoS-skydd, Konstruera ett eget DDoS-skydd och genomföra DDoS-attacker med hjälp av pktgen.

5.3.1 Intervjustudie

Genomföra en intervjustudie med personer som jobbar med att förhindra DDoS-attacker, leverantörer av DDoS-skydd och företag som använder sig av deras tjänster.

Genom att utföra dess intervjuer har vi en förhoppning att man ska få en bättre förståelse för hur olika DDoS-skydd fungerar(en bättre förklaring än den som DDoS-skydds leverantörerna presenterar på sina Webbsidor). Genom intervjuerna kan man också få en tydligare bild av hur stora resurserna är som företag spenderar på DDoS-skydd/förhindra DDoS-attacker.

5.3.2 Enkätundersökning

Genomföra en egen enkätundersökning(likt Arbor Networks och Kaspersky lab) för att ta reda på hur vanligt det är att Svenska företag blir utsatt för DDoS-attacker, och hur mycket pengar det lägger ner på att skydda sig mot DDoS-attacker.

5.3.3 Experiment

Utöver de experiment som vi har utfört med DDoS, finns det annat som vi skulle velat test.

5.3.3.1 Testa befintliga DDoS-skydd

Något som framtida forskning kan vara centrerad kring är att testa de olika DDoS-skydden som vi har presenterat i uppsatsen. Genom att konstruera en egen testmiljö och sedan sätta upp olika testscenarion där olika DDoS-attacker testas mot de olika DDoS-skydden. När man sedan fått resultaten av testet kan man sammanställa en jämförelse(Benchmarking) av de olika DDoS-skydden. Och på så sätt se vilka som skyddar mot vad.

Det är också tänkbart att man genomför tester där man kombinerar olika former av DDoS-skydd tillsammans för att hitta en så optimal lösning som möjligt.

Det finns dock en rad problem som man måste lösa för att kunna genomföra experimenten.

- Man måste kunna konstruera en test miljö som är jämförelsebar med internet, utan att riskera att omedvetet avfyra en DDoS-attack på internet.
- Man måste ha tillgång till olika DDoS-skydd för att kunna implementera dem i testmiljön, vilket kan vara svårt att få till.

5.3.3.2 Konstruera ett eget DDoS-skydd

Ett ytterligare steg kan vara att konstruera ett eget DDoS-skydd. Ett projekt som kräver lång tid och förmodligen omfattande resurser om det behövs investeringar i både hård- och mjukvara.

På grund av den satta tidsramen för examensarbetet (10 veckor) är det inte möjligt för oss att genomföra en undersökning i samma omfattning

5.3.3.3 DDoS-attack med pktgen

Då vi enbart hade 10 veckor på oss att utföra detta arbete hann vi aldrig försöka göra Astaro brandväggen obrukbar. Vi skulle ha kunnat åstadkomma det genom att skapa en volymbaserad attack via en mjukvara i linux som heter pktgen. Pktgen dedikerar en eller flera kärnor i maskinen till att enbart skicka så mycket paket som bara möjligt. Detta skulle kunna resultera i att länken som externt kopplas till brandväggen tar emot så mycket trafik att ingen annan, legitim trafik, kan komma igenom.

5.4 Reflektion

Efter att ha genomfört vår studie har det förstärkt vår bild av DDoS-attacker, som vi hade när vi startade studien. DDoS-attacker är vanligt förekommande och det är väldigt lätt att utföra dem även om man inte besitter några egna kunskaper.

Med denna studie har vi lyckats belysa de många olika ekonomiska konsekvenserna som DDoS-attacker kan ha för ett företag. Det står klart att DDoS är ett stort hot mot alla företag med verksamhet förlagd på internet. Ett företag som ständigt blir utsatt för DDoS-attacker löper risken att hamna i en framtida svår ekonomisk sits.

Vi har också lyft fram det faktum att det finns en omfattande marknad för DDoS-skydd. Vi har inte angivit några priser i denna rapport då vi saknar en komplett lista, men kostnaden för att endast skydda en enda IP-adress är avsevärd och en kostnad som alla företag helst skulle vilja undvika. Trots de höga priserna så finns det inga kompletta skydd som skyddar mot alla typer av DDoS-attacker, vilket gör att företag som har investerat i dyra DDoS-skydd ändå riskerar att falla offer för DDoS-attackerna.

I efterhand känner vi oss nöjda med resultatet av studien. Vi har uppnått alla de mål vi satt upp för studien, både visa de ekonomiska konsekvenserna av DDoS-attacker, samt att vi har visat hur lätt det är att genomföra DDoS-attacker utan tidigare kunskaper.

Referenser

[1] Arbor Networks, Inc., “Worldwide Infrastructure Security Report,” Volume X, 2014.

[2] Kaspersky Lab, “B2B-International-2014-Survey-DDoS-Summary-Report,” 2014.

[3] “Telia DDoS Protection - Säkerhet - Företag - Telia.se.” [Online]. Tillgänglig vid: https://www.telia.se/foretag/katalog/VisaProdukt.do?productRef=/foretag/natverksakerhet/sakerhet/ddos-protection/ddos-protection.product#1. [Accessed: 23-Apr-2015].

[4] “Ddos-attackerna blir fler och större,” *Computer Sweden*. [Online]. Tillgänglig vid: http://computersweden.idg.se/2.2683/1.546231/ddos-attackerna-blir-fler-och-storre. [Accessed: 15-Apr-2015].

[5] Qliro Group AB, “Qliro Group AB Årsredovisning 2014.” 2015.

[6] M. Hadley och E. Rescorla, “RFC 4732 - Internet Denial-of-Service Considerations,” 2006. [Online]. Tillgänglig vid: https://tools.ietf.org/html/rfc4732. [Accessed: 27-Apr-2015].

[7] “Botnet Attacks | Internet Security Threats | Kaspersky Lab.” [Online]. Tillgänglig vid: http://www.kaspersky.com/internet-security-center/threats/botnet-attacks. [Accessed: 27-Apr-2015].

[8] “Har din dator kapats till ett botnät?” [Online]. Tillgänglig vid: http://www.kaspersky.com/se/about/news/press/2013/Har_din_dator_kapats_till_ett_botna_. [Accessed: 28-Apr-2015].

[9] “Så fungerar botnäten - TechWorld.” [Online]. Tillgänglig vid: http://techworld.idg.se/2.2524/1.415852/sa-fungerar-botnaten. [Accessed: 28-Apr-2015].

[10] S. Mansfield-Devine, “DDoS: treats and mitigation.” Network Security (12):5-12, 2011.

[11] “Enkelt att köpa cyberbrottstjänster,” *TechWorld*. [Online]. Tillgänglig vid: http://techworld.idg.se/2.2524/1.498387/enkelt-att-kopa-cyberbrottstjanster. [Accessed: 15-Apr-2015].

[12] Kent Olofsson, “Ddos-attackerna blir fler och större,” *Comput. Swed.*, Feb. 2014.

[13] Ponemon, "*Cybercrime report*," [Online]. Tillgänglig vid: http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime. [Accessed:15-Apr-2015]

[14] “DDoS for hire services offering to ‘take down your competitor’s web sites’ going mainstream,” *Webroot Threat Blog*. [Online]. Tillgänglig vid: http://www.webroot.com/blog/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-sites-going-mainstream/. [Accessed: 15-Apr-2015].

[15] Dancho Danchev, “DDoS for hire services offering to ‘take down your competitor’s web sites’ going mainstream,” *Webroot Threat Blog*, 02-Jun-2012.

[16] “Dancho Danchev’s Blog - Mind Streams of Information Security Knowledge: Pricing Scheme for a DDoS Extortion Attack.” [Online]. Tillgänglig vid: http://ddanchev.blogspot.se/2009/11/pricing-scheme-for-ddos-extortion.html. [Accessed: 27-Apr-2015].

[17] Radware, “DDoS Survival Handbook,” 2013.[Online] Tillgänglig vid: http://security.radware.com/uploadedFiles/Resources_and_Content/DDoS_Handbook/DDoS_Handbook.pdf Accesed: 27-Apr-2015]

[18] Incapsula, Inc., “DDoS Attack Types & Mitigation Methods,” 31-Mar-2015. [Online]. Tillgänglig vid: http://www.incapsula.com/ddos/ddos-attacks/. [Accessed: 06-Apr-2015].

[19] “DNS Amplification Attack - Targets & Consequences.” [Online]. Tillgänglig vid: http://security.radware.com/knowledge-center/DDoSPedia/dns-amplification-attack/. [Accessed: 21-May-2015].

[20] Kent Olofsson, “Ddos-attackerna blir fler och större,” *Computer Sweden*, Stockholm, Sweden, 10-Feb-2014.
[21] “Kapade routrar bakom ödleattacken - IDG.se.” [Online]. Tillgänglig vid: http://www.idg.se/2.1085/1.603231/kapade-routrar-bakom-odleattacken. [Accessed: 21-Apr-2015].
[22] P.-O. Wibron, “Incident rappor Teliasonera,” 2.0, Dec. 2014.
[23] “Netflix releases home-grown DDoS detectors • The Register.” [Online]. Tillgänglig vid: http://www.theregister.co.uk/2014/08/28/netflix_releases_homegrown_web_detective_tools/. [Accessed: 21-May-2015].
[24] Akamai, “Prolexic Quarterly Global DDoS Attack Report Q1 2014,” 2014.
[25] R. Sahay, G. Blanc, Z. Zhang, och H. Debar, “Towards Autonomic DDoS Mitigation using Software Defined Networking,” NDSS Symposium 2015, San Diego, 2015. [Online] Tillgänglig vid: http://www.internetsociety.org/sites/default/files/01_3_2.pdf
[26] Open Networking Foundation, “OpenFlow Switch Specification.”
[27] Cheng Jin, Haining Wang, och Kang G. Shin, ‘Hop-count filtering: an effective defense against spoofed DDoS traffic’, 2003, p. 30 [Online]. DOI: 10.1145/948109.948116
[28] A. Yaar, A. Perrig, och D. Song, ‘SIFF: a stateless internet flow filter to mitigate DDoS flooding attacks’, IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, pp. 130–143 [Online]. DOI: 10.1109/SECPRI.2004.1301320.
[29] K. Poulsen, “FBI busts alleged DDoS Mafia,” 26-Aug-2014.
[30] S. Kandula, M. Katabi, M. Jacob, och A. W. Berger, “Botz-4-sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds,” 2nd Symposium on Networked Systems Design and Implementation (NSDI), 2005. Tillgänglig vid: https://www.usenix.org/legacy/event/nsdi05/tech/kandula/kandula.pdf
[31] P. Genestig och Joel Gustafsson, “Analys av DDoS-attacker för identifiering och prevention,” Kandidatuppsats, Högskolan i Halmstad, Sektionen för informationsvetenskap, data-och elektroteknik, 2014. [Online] Tillgänglig vid: http://www.diva-portal.se/smash/get/diva2:747357/FULLTEXT01.pdf
[32] M. Kjellman, “Överbelastningsattacker mot nätverk och hur man skyddar sig mot dem,” VASA YRKESHÖGSKOLA, 2013. [Online] Tillgänglig vid: https://www.theseus.fi/bitstream/handle/10024/74128/VAMK_LP_e0900745.pdf?sequence=1
[33] “Primo by Ex Libris.” [Online]. Tillgänglig vid: http://kth-primo.hosted.exlibrisgroup.com/primo_library/libweb/action/search.do. [Accessed: 05-May-2015].
[34] “Enkel sökning.” [Online]. Tillgänglig vid: http://www.diva-portal.org/smash/search.jsf?dswid=-896. [Accessed: 05-May-2015].
[35] “Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning.” Vetenskapsrådet, 2002.
[36] “UTM & Next-Gen Firewall | Network Firewall Appliances | Sophos UTM.” [Online]. Tillgänglig vid: https://www.sophos.com/en-us/products/unified-threat-management.aspx. [Accessed: 14-Jun-2015].
[37] “jseidl/GoldenEye · GitHub.” [Online]. Tillgänglig vid: https://github.com/jseidl/GoldenEye. [Accessed: 14-Jun-2015].
[38] “HOIC Attacks - High Orbit Ion Cannon Attacks.” [Online]. Tillgänglig vid: http://security.radware.com/knowledge-center/DDoSPedia/hoic-high-orbit-ion-cannon/. [Accessed: 14-Jun-2015].
[39] “hping3(8) - Linux man page.” [Online]. Tillgänglig vid: http://linux.die.net/man/8/hping3. [Accessed: 14-Jun-2015].

[40] “Home : The Official Microsoft IIS Site.” [Online]. Tillgänglig vid: https://www.iis.net/. [Accessed: 14-Jun-2015].
[41] “Oracle VM VirtualBox.” [Online]. Tillgänglig vid: https://www.virtualbox.org/. [Accessed: 14-Jun-2015].
[42] “Windows Server 2008 R2 and Windows Server 2008.” [Online]. Tillgänglig vid: https://technet.microsoft.com/en-us/library/dd349801(v=ws.10).aspx. [Accessed: 14-Jun-2015].
[43] “Wireshark · Go Deep.” [Online]. Tillgänglig vid: https://www.wireshark.org/. [Accessed: 14-Jun-2015].
[44] “XAMPP Installers and Downloads for Apache Friends.” [Online]. Tillgänglig vid: https://www.apachefriends.org/index.html. [Accessed: 14-Jun-2015].
[45] TDC Sverige, “DDoS-attackerna kostar samhället miljoner – så här skyddar du dig,” 21-2013. [Online]. Tillgänglig vid: http://www.mynewsdesk.com/se/tdcsverige/pressreleases/ddos-attackerna-kostar-samhaellet-miljoner-saa-haer-skyddar-du-dig-847657. [Accessed: 06-Apr-2015].
[46] “DDosProtection_Tjanstebeskrivning-150127.” Telia.
[47] “DDoS Attacks - Arbor Networks.” [Online]. Tillgänglig vid: http://www.arbornetworks.com/ddos-attacks. [Accessed: 23-Apr-2015].
[48] “Cloud-based DDoS Protection for Enterprises.” [Online]. Tillgänglig vid: http://www.arbornetworks.com/products/arbor-cloud/for-enterprises. [Accessed: 23-Apr-2015].
[49] “DDoS Attacks Protection with Pravail APS.” [Online]. Tillgänglig vid: http://www.arbornetworks.com/products/pravail/aps. [Accessed: 24-Apr-2015].
[50] “Threat Management System with Peakflow SP.” [Online]. Available: http://www.arbornetworks.com/products/peakflow/tms. [Accessed: 24-Apr-2015].
[51] “DDoS Protection | DDoS Attack Prevention | Kaspersky Lab.” [Online]. Tillgänglig vid: http://www.kaspersky.com/business-security/ddos-protection. [Accessed: 23-Apr-2015].
[52] “DDoS Secure – Juniper Networks.” [Online]. Tillgänglig vid: http://www.juniper.net/us/en/products-services/security/ddos/. [Accessed: 23-Apr-2015].
[53] “Defeating DDOS Attacks - Cisco.” [Online]. Tillgänglig vid: http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.html. [Accessed: 29-Apr-2015].

Bilaga A: Utpressningsbrev

Sample DDOS extortion letter:

"Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us.

The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.

1-st payment (10 000 rubles) Must be made no later than DATE. All subsequent payments (10 000 rubles) Must be committed no later than 31 (30) day of each month starting from August 31. Late payment penalties will be charged 100% for each day of delay.

For example, if you do not have time to make payment on the last day of the month, then 1 day of you will have to pay a fine 100%, for instance 20 000 rubles. If you pay only the 2 nd date of the month, it will be for 30 000 rubles etc. Please pay on time, and then the initial 10 000 rubles offer will not change. Penalty fees apply to your first payment - no later than DATE"

You will also receive several bonuses.
1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value ddos attacks a simple site is about $ 100 per night, for you it will cost only 70 $ per day.
2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.

Payment must be done on our purse Yandex-money number 41001474323733. Every month the number will be a new purse, be careful. About how to use Yandex-money read on www.money.yandex.ru. If you want to apply to law enforcement agencies, we will not discourage you. We even give you their contacts: www.fsb.ru, www.mvd.ru"

Bilaga B: Leverantör av riktade DDoS-attacker

Bilaga C: DDoS-skydd

Telia DDoS Protection

Telia erbjuder en molntjänst som bygger på att den skadliga trafiken som försöker nå ett företags nätverks genom deras internetanslutning tvättas bort. Det i sin tur leder till att attackernas effekt blir minimerade och den legitima trafiken kan passeras så ostört som möjligt [3].

- "*Skydd mot alla typer av DDoS-hot*
- *Paketeringar för stora och mindre organisationer*
- *Bevakning dygnet runt av Telia*
- *Endast en molntjänst ger fullgott skydd*
- *Motåtgärder som slås på och av automatiskt*
- *Uppgraderingar och utrustning ingår"* [3]

Hur går det till?

Telia DDoS Protection fungerar på så sätt att det finns en grundkonfiguration som startar tvätten av trafiken automatiskt(Auto Mitigation), vilket sker när Telias övervakningsplatsform registrerar en attack mot något av de bestämda skyddsobjekten [46].

Under tvättningsprocessen dirigeras trafiken, riktade mot skyddsobjekten, genom Telias tjänsteplattform, där sedan den legitima trafiken slussas vidare till skyddsobjektet [46].

Krav & förutsättningar

Kunden får själv definiera vilka servrar och applikationer i den egna IT-miljön som ska skyddas av Telia. Alla servrar och applikationer som använder sig av IP för sin kommunikation kan ingå i skyddsobjektet. Det kan ingå upp till 254 värdar i varje skyddsobjekt [46]. Ett krav för att en skyddsobjektgrupp ska omfattas av Telia DDoS Protection är att den är ansluten till någon av Telias följande kommunikationslösningar:

- Telia Bredband Pro (Tidigare Telia ProLane).
- TeliaSonera Datanet med internetkonnektivitet [46].

Paketering

Telia erbjuder två olika paket av Telia DDoS Protection, Small och Standard. Paketen har olika specifikationer vilket illusteras i följande bild:

Paketeringar

Bra att veta

		Small	Standard
Access	Begränsad högsta bandbredd	300 Mbit/s	10 Gbit/s
Kundkommunikation	Telia ringer upp under attackhantering	Ingår ej	Ingår
Skyddsobjekt	Inkluderade tvättimmar/år	20	300
	Inkluderade MO:s	2	5
	Max antal IP-adresser/MO	5	254
	Max antal IP-adresser i tvätt (samtidigt)	10	32
	Använda blandade (kundspecifika) templates	Ingår ej	Ingår
Funktioner	Learning mitigation	Ingår ej	Ingår
	Blackholing	Tillval	Ingår
	Max antal IP-adresser för vitlistning	3	5
Rapportering	Omfattning	Begränsad	Full
	Periodicitet	Per månad	Per vecka

Figur 14: Telia DDoS Protection paket

Arbor Networks

Arbor Networks har skyddat många av väldens störta och mest krävande nätverk i mer än ett decennium [47]. För att skydda företagsresurser från dagens DDoS-attacker förespråkar Arbor Networks en flerskikts lösning av DDoS riskreducerande lösningar(multi-layer DDoS mitigation solutions) [47].

Hur går det till?

För att kunna skydda sig mot dagens stora volymbaserade attacker, som överskrider 300 GB/s , behöver företag skydd i molnet, vilket Arbor Networks erbjuder med sin flerskitslösning. Förutom skydd i molnet behövs också skydd på plats (on-premise protection) för att hantera attacker mot applikationslagret och attacker riktade mot befintliga "stateful infrastructure devices", som brandväggar, Intrusion Prevention Systems(IPS) och ADCs [47].

Produkter

Arbor Networks erbjuder tre olika typer av skydd Arbor Cload, Pravail Availiability Protection Solution och Peakflow Threat Management System.

Arbor Cload

Arbor Cloud är en lösning som skyddar mot hela spektrumet av moderna DDoS-attacker genom att kombinera skydd på plats och molnbaserade metoder för att lindra attackerna [48] .På plats skydd mot state-exhausting attacker riktade mot företagets säkerhetsinfrastruktur. Det hjälper också till att förhindra smygande attacker som kring går både brandväggar och IPS för att sikta in sig på applikationer som är kritiska för företagets affärer [48].

Samtidigt skyddar den globala, multi-terabit, "on-demand traffic Scrubbing service" mot volymetriska DDoS-attacker, som är förstora för att hanteras på plats [48].

Pravail Availiability Protection Solution

Pravail Availiability Protection system mitigerar hot mot applikationslagret innan de påverkar företagets nätverk och servicetillgängligheten [49]. Pravail Availiability Protection system on-premise/på plats DDoS-skydd, som ständigt förbättras av automatiska säkerhetsuppdateringar levererade av Arbor Security Engineering and Response Team (ASERT). Pravail Availiability Protection system skyddar mot både kända och nya hot mot företags tillgänglighet [49].

Peakflow Threat Management System

Peakflow Threat Management System ser till företags tjänster är tillgängliga och vid behåller sin prestanda, genom att leverera automatiskt 24/7 DDoS-mitigation and realtids insyn i nätverksapplikationer [50]. Peakflow Threat Management System avlägsnar DDoS-attack trafik med kirurgisk precision från företagets nätverk, utan att störa viktiga nättjänster. Systemet ger också en omfattande realtidsinsyn i företagets nätverksapplikationer så att företaget proaktivt kan övervaka och underhålla tjänsters prestanda [50].

Kaspersky lab

Kaspersky lab erbjuder en total, integrerad lösning som innehåller allt ett företag behöver för att försvara sig mot en DDoS-attack [51]. Vilket innefatta följande:

- Speciell sensor mjukvara för installation på företagets webbsida.
- Tillgång till distribuerade nätverk av "Cleaning centers"
- Avancerad intelligens om de senaste DDoS-attacker
- Tillgång till Kaspaersky lab's "Security Operation Center"
- Omfattande support – samt direkt tillgång till DDoS-skydds experter.
- Tidigare attack rapporter och analyser [51].

Hur går det till?

Kaspersky DDoS Protection tar hand om alla steg som krävs för att försvara ett företag, från löpande 24x7 analys av företagets trafik, för att sedan varna för eventuella attacker och sedan omdirigera trafiken, rengöra trafiken, återföra den legitima "rena" trafiken till företaget och sedan slutligen ge företaget en attack rapport och en analys [51].

Kaspersky lab hävdar att tillskillnad från andra DDoS leverantörer bekämpar Kaspersky lab´s DDoS- attacker på två fronter:

- **Speciell försvars infrastruktur** – inklusive Kaspersky lab´s senors programvara, som körs på företagets webbplats och system som kör på ett nätverk av Kaspersky lab sajter.
- **Kaspersky Lab DDoS intelligens** – för att tidigt upptäcka DDoS-attacker [51].

Special Sensor

Kasparsky lab´s tillhandahåller en speciell sensor programvara som sedan körs på kundens webbsida. Direkt efter att sensor programvaran har installerats börjar den samla statistik och bygger användarprofiler som hjälper till att skydda företaget [51].

Genom att hela tiden övervaka trafiken och kontinuerligt bygga upp statistik och analysera beteendemönster ökar sensorn kontinuerligt sin förmåga att upptäcka de subtila avvikelserna som är karakteristiska för starten av en DDoS-attack [51].

Cleaning Centers

Vi händelsen av en DDoS-attack blir företaget varnat av Kaspersky lab, vilket gör det möjlighet att omdirigera trafiken till ett av Kaspersky lab´s "Cleaning centers". Kaspersky lab skickar sedan enbart vidare den legitima/ren trafiken till företaget [51].

Eftersom Kaspersky lab har investerat i distribuerade Cleaning centers kan de leverera både slitstark och skalbar trafikrengöringsförmåga [51].

DDoS attack intelligens

Kaspersky labs malware experter använder sofistikerade metoder för att övervaka hotbilden för DDoS-attacker och på så sätt ligga före hackare – för att försöka nå tidigare upptäckt av DDos-attacker. [51]Efter som traditionella DDoS-skydds leverantöre inte har en säkerhetsunderrättelse avdelning kan de inte leverera de proaktiva skyddslager som Kaspersky lab erbjuder [51].

Juniper Networks

Juniper Networks erbjuder DDoS-skydd, DDoS Secure, för företag mot volymbaserade attacker och application-layer attacks [52].

Hur går det till?

Genom att kontinuerligt inspektera ingående och utgående nätverkstrafik stoppas DDoS-attacken innan den kan påverka tillgängligheten för företagets skyddade resurser [52].

För att angöra vilka inkommande förfrågningar som går att lita på använder DDoS Secure av en avancerad CHARM algoritm. På så sätt kan man droppa misstänkta icke-kompatibla paket så snart den optimala prestandan hos de kritiska resurserna börjar minska [52].

Några världens mest trafikerade webbservrar, DNS och affärskritiska applikationerna använder sig just av DDoS Secure för att skydda sig mot ett stort urval av DDoS-attacker [52].

Egenskaper av DDoS Secure

- Dynamisk och självlärande
- Effektiv mot de senaste application-layer- och multivector attacker.
- Extremt låg fördröjning
- Upp till 40 Gbps genomströmningskapacitet
- Fullt IPv6 kompatibel
- Plug-and-play, enkelt att installera och konfigurera
- Felsäker och hög tillgänglighet alternativ
- Helautomatisk för snabbast svar och lägsta ägandekostnader
- Integrerade på plats och monbaserad hybridlösning för hantering av den vidaste uppsättningen av attacker [52].

Cisco Systems

Cisco erbjuder en komplett DDoS-skydds lösning baserat på principerna: detektering, avledning, verifikation och forwarding. Så fort en DDoS attack startas mot ett offer skyddat av Ciscos lösning händer följande:

- *Detekterar* DDoS attacken
- *Avleder* trafiken mot offret till en Cisco apparat för behandling
- *Analyserar och filtrerar* det elaka trafikflödet från det normala flödet av paket
- *Forwardar* enbart den normala trafiken

Cisco påstår att de kan erbjuda ett komplett skydd mot alla typer av DDoS attacker, till och med dom som inte har påträffats förut [53].

Ciscos lösning består av två distinkta komponenter – Cisco Traffic Anomaly Detector (TAD) XT och Cisco Guard XT – som arbetar tillsammans för att erbjuda ett komplett DDoS skydd.

- Cisco Traffic Anomaly Detector XT – Fungerar som ett tidigt varningssystem som erbjuder en djupgående analys av DDoS attackerna. Passivt övervakar den trafiken i nätverket för att hitta avvikelser från det "normala" eller grundläggande mönster som indikerar en DDoS attack. Så fort TAD XT identifierar en attack varnar den Cisco Guard XT med detaljerade rapporter och specifika varningar för att snabbt reagera mot hotet [53].
- Cisco Guard XT – Är hörnstenen av Ciscos DDoS lösning. Den fungerar som en högpresterande maskin för att lindra DDoS attacker, implementerad uppströms vid antingen ISPns data center eller vid yttersta gränsen av ett stort företag för att skydda både nätverket och data centrets resurser [53].

När Cisco Guard XT blir notifierad att ett mål är under attack, blir trafik avsett för det målet omdirigerat till Guarden (eller Guardsen) som är associerad med målet under attack. Trafiken blir då

utsatt för en fem-stegs analys och filtreringsprocess avsedd att ta bort all elak trafik medan den tillåter normal trafik att passera oavbrutet [53].

Cisco Guard XT finns alltid närgränsande till en router eller switch på ett serparat nätverks interface, vilket ger ett on-demand skydd utan att påverka trafikflöden från andra system. Beroende på dess läge kan Cisco Guard XT skydda flera potentialla mål samtidigt, så som routers, web servrar, DNS servrar samt LAN och WAN bandbredd [53].

Cisco's MVP Arkitektur

För att separerar elak trafik från legitim trafik används en arkitektur som Cisco kallar för Multiverification Process (MVP) som består av fem olika moduler eller steg.

Filtering – Modulen inkluderar bade statiska och dynamiska DDoS filter. Det statiska filtret blockerar oviktig trafik avsedd till ett offer under attack och kommer med standard värden från Cisco, men kan konfigureras av användaren själv. De dynamiska filtrena införs av de andra modulerna baserat på observerade mönster och detaljerade analyser av trafikflödena och skickar ut realtids uppdateringar som antingen ökar nivån av verifikation för misstänkta flöden eller blockerar flöden som blivit verifierade som elaka [53].

Active verification – Modulen verifierar att paketen som kommer in i systemet inte har blivit spoofade. Cisco Guard XT har enligt Cisco en unik käll-autentiserings mekanism för att förhindra att spoofade paket når offret. Den aktiva verifikationen har även fler mekanismer som bidrar med att identifiera legitim trafik, så att dessa paket inte blir discardade [53].

Anomaly recognition – Modulen undersöker all trafik som inte blev stopped av de två tidigare stegen och jämför dess monster med monster som registrerats över tid och letar efter avvikelser som skulle kunna identifiera källan av de elaka paketen [53].

Protocol analysis – Modulen behandlar flöden som Anomaly recognition fann misstänksamma, för att identifier applikations-specifika attacker, som t.ex. HTTP error attacker. Den upptäcker även protokoll transaktioner som inte går korrekt till [53].

Rate limiting – Modulen förhindrar flöden från att överösa målet medan mer detaljerad undersökning pågår. Den formar trafiken per-flöde, där källor straffas som använder för mycket resurser under en för lång period [53].

Distribuering av systemet

Providers

Cisco Guard XT bör placeras vid strategiskt viktiga punkter i infrastrukturen, vid t.ex. peering points, för att skydda kärnroutrar, länkar och kunder. De kan även placeras vid edge routern för ett dedikerat kundskydd [53].

Företag och Data Centers

Gällande företag och data centers bör Cisco Guard XT placeras vid distributionslagret i data centret, för att skydda de långsamma länkarna nedströms och servrarna. Cisco Guard XT kan anslutas till en distributionsswitch and har stöd för redundant konfiguration [53].

Bilaga D: Detaljerat resultat

Testbädd 1

Test 1

Tabell 18: Angripare test 1 testbädd 1

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	160	1280

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	20	700

Tabell 19: Offer test 1 testbädd 1

Offer – Windows PC

Programvara	Webbserver	Status efter attack
XAMPP	Apache	Down

Test 2

Tabell 20: Angripare test 2 testbädd 1

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	150	1200

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Tabell 21: Bilaga, Offer test 2 testbädd 1

Offer – Windows PC

Programvara	**Webbserver**	**Status efter attack**
XAMPP	Apache	Down

Test 3

Tabell 22: Angripare test 3 testbädd 1

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	100	800

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Tabell 23: Offer test 3 testbädd 1

Offer – Windows PC

Programvara	**Webbserver**	**Status efter attack**
XAMPP	Apache	Down

Test 4

Tabell 24: Angripare test 4 testbädd 1

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	80	640

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	60	480

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Tabell 25: Offer test 4 testbädd 1

Offer – Astaro VM

Programvara	**Brandvägg**	**Status efter attack**
Astaro	Astaro	Down

Test 5

Tabell 26: Angripare test 4 testbädd 1

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	160	1280

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	20	700

Tabell 27: Offer test 4 testbädd 1

Offer – Astaro VM

Programvara	**Webbserver**	**Status efter attack**
Windows	ISS	Upp/Service unavailable.

Testbädd 2

Test 1

Tabell 28: Angripare test 1 testbädd 2

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	160	1280

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Angripare 4 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Tabell 29: Offer test 1 testbädd 2

Offer – Windows PC

Programvara	**Webbserver**	**Status efter attack**
XAMPP	Apache	Up
Programvara	**Brandvägg**	**Status efter attack**
Astaro	Astaro	Up

Test 2

Tabell 30: Angripare test 2 testbädd 2

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	200	1600

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	50	400

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Angripare 4 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Tabell 31: Offer test 2 testbädd 2

Offer – Windows PC

Programvara	**Webbserver**	**Status efter attack**
XAMPP	Apache	Up
Programvara	**Brandvägg**	**Status efter attack**
Astaro	Astaro	Up

Test 3

Tabell 32: Angripare test 3 testbädd 2

Angripare 1 - Windows PC

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	100	800

Angripare 2 - Windows VM

Programvara	Inställningar	
HOIC	**Threads**	**Http get/s**
	80	640

Angripare 3 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Angripare 4 – Linux PC

Programvara	Inställningar	
Golden eye	**Workers**	**Sockets per worker**
	10	500

Tabell 33: **Offer test 3 testbädd 2**

Offer – Windows PC		
Programvara	**Webbserver**	**Status efter attack**
XAMPP	Apache	Up
Programvara	**Brandvägg**	**Status efter attack**
Astaro	Astaro	Up/Slow

Test SYN flood

Tabell 34: **Attackers: 2 Linux VM som kör hping3**

Programvara	Brandvägg	Status efter attack
Astaro	Astaro	Down

TRITA-ICT-EX-2015:149