DDoS напади и DDoS напади врз DNS

Александар Николоски[1], Митко Богдановски[2]

[1] Европски Универзитет – Скопје, Р. Македонија, nikoloski.aleksandar11@live.eurm.edu.mk

[2] Воена академија – Скопје, Р. Македонија, mitko.bogdanoski@eurm.edu.mk

Апстракт

Одликата на денешното модерно општество и иско ристеноста на информатиката во општествениот поре док и информациските системи во општествените сфе ри за дистрибуиран транспорт на податоци и добива ње на дистрибуирани информации дава можност за уживање на благодетите на новата комуникациска ера. Дистрибуираните системи се користат во електро нското банкарство, услужни компјутерски сервиси, ко муникациски, информативни сервиси, трговски серви си, берзански севиси и ред други кои работат врз прин ципот на дистрибуирана достава и обработка на бара ња за податоци. Според своето име претставуваат сино ним за системи кои бараат високо ниво на заштита и голема мамка за проневери, и злоупотреби вклучува јќи и различни видови на дистрибуирани напади. DDoS нападите за кои се повеќе слушаме и читаме од информативните средства го земаат трендот на моде рен начин на изразување на незадоволство. Аноним ната хактивистична група Anonymous која се појави 2003 година, своето незадоволство од спроведените политики кон интернет услугата и слободите го изра зува со изведување на ваков тип напади врз виталните структури на повеќе држави.Каков што беше случајот со нивните реакции против донесувањето на ACTA (Anti-Counterfeiting Trade Agreement).Но што во суштина се тие DDoS напади и нивните постулати се извор на идеи и потреби од нови истражувања, справување со проблеми и системска заштита

***Клучни зборови*—Зомби , ботнет , пингирање , напаѓачки агенти, компромитиран систем.**

I. Вовед

"This page cannot be dispayed". Замислете дека се задржувате на гледање на оваа порака, додека се обидувате да пристапите до вашата e-banking, e-mail или друга социјална мрежна сметка безнадежно. Замислете дека оваа состојба на "одрекување" не е само во секунди или минути, тоа трае неколку часа или дена! Ова е типичен Distributed Denial of Service (DDoS) напад.
DDoS нападот е дефиниран како напад во кој мноштво на компромитирани системи се напаѓа една цел, а со тоа се предизвикува негирање на услуга за корисниците на насочен систем. Протокот на дојдовни пораки до целниот систем во суштина присилува тоа да го исклучи, а со тоа негира услуга на системот за легитимните корисници [1].
Да се биде во можност да се спроведе успешен DDoS напад, хакерите мора да искористат она што се нарекува "ботнет". Ботнет е жаргон термин за колекција на софтвер роботи, или ботови, кои работат автономно и автоматски. Терминот често се поврзува со малициозен софтвер, но исто така, може да се однесува на мрежа на компјутери со користење на дистрибуиран компјутерски софтвер[2].
Ботнет е контролиран од страна на основоположник или "botmaster". Botmaster-от, за да се здобие со нови жртви (зомби), користи автономен малициозен ширечки софтвер (агент). Овие зомби се јадрото на било каков DDoS напад. Зомби се обично машини на невини корисници, машини кои не се свесни дека тие се дел од злонамерен напад. Агентите се извршуваат на зомби машини, botmaster-от само иницира напад-команда и ја избира целта. Командата е предадена на зомбите и зомби извршувачите. Несвесната цел се наоѓа себеси бомбардирана со „тони“ на пакети кои протекуваат низ нивнната мрежа и предизвикуваат одбивање на услуга [2]. Во подетална содржина ќе ги разработиме DDoS нападите според методологијата на комуникација, според начинот на ширење на нападот и според подвигот, исто така ќе разработиме и DDoS напад врз DNS (Domain Name Server), последиците од таков напад како и превенција од такви напади.

II. Видови DDoS напади

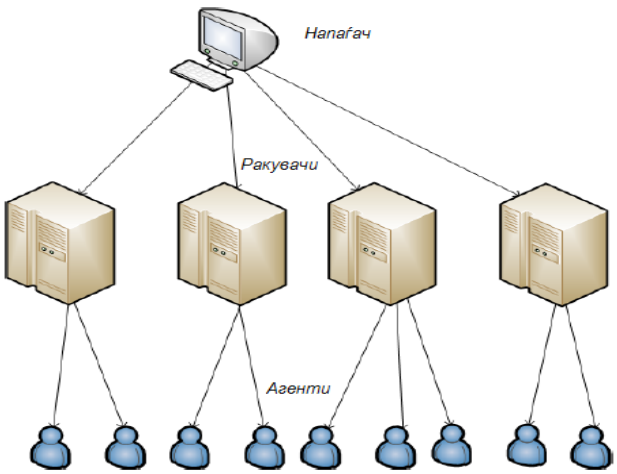
Постојат три главни класификации за DDoS нападите. Едната е врз основа на методологијата на комуникација помеѓу на паѓачот и жртвата. Втората класификација е врз основа на техниката на ширење. И последната во согласност со механизмот на експлоатација. Овие класификации не може да изгледаат многу очигледни. Сепак, тие се одличен начин да се разберат сите аспекти на botnets од различни перспективи.

II .1 *Поделба на DDoS според методологијата на комуникација*

Согласно методологијата на комуникација со жртвата постојат два вида на DDoS напади: базирани на агент-управувач и IRC (Internet Realy Chat)-базиран модел.

II .1.1 *DDoS напади базирани на агент-управувач*

DDoS нападот базиран на агент-управувач се состои од клиенти, секунданти и агенти. Клиентската платформа е местото каде што напаѓачот комуницира со остатокот од системот за DDoS напад (Слика 1). Управувачите се софтверски пакети кои се наоѓаат на компјутерски системи лоцирани преку Интернет кои клиентот напаѓачот ги користи за да комуницира директно со агентите. Агентски софтвер постои на компромитираниот систем кој на крајот ќе го спроведе нападот врз системот-жртва. Напаѓачот комуницира со одреден број ракувачи за да ги идентификува активните агенти, кога треба да се закаже напад, или кога треба да се надополнат агенти. Во зависност од тоа како напаѓачот го конфигурира DDoS нападот на мрежата, на агентите може да им е наложено да комуницираат со еден управувач или повеќе управувачи. Обично, напаѓачите ќе се обидат да го сместат управувачкиот софтвер на компромитиран рутер или мрежен сервер кој се справува со големи количини сообраќај. Ова ја отежнува идентификацијата на пораките помеѓу клиентот и управувачот и помеѓу управувачот и агентите. Комуникацијата помеѓу напаѓачот и управувачот и помеѓу управувачот и агентите може да биде преку TCP, UDP, ICMP протоколи. Сопствениците и корисниците на агентите обично не знаат дека нивниот систем е компромитиран и дека ќе биде искористен за учество во DDoS напад. Кога учествуваат во DDoS напад, секој агент користи само мала количина на ресурси (како на пример меморијата и пропусниот опсег), така што корисниците на овие компјутери ќе доживеат минимална промена во перформансите [3].

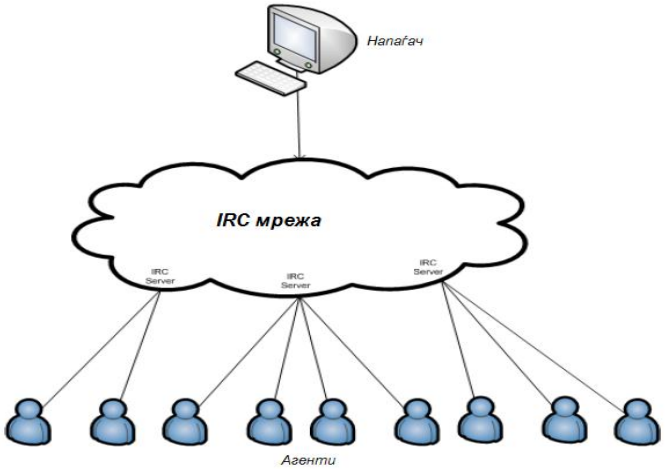


Слика 1. DDoS напад базиран на агент-управувач

II .1.2 *DDoS напади базирани на IRC*

IRC е мулти-кориснички, on-line разговорен систем. Овој систем им овозможува на корисниците да креираат две-партии или мулти-партиски интерконекции и тип на пораки во реално време помеѓу нив. IRC мрежните архитектури се состојат од IRC сервери кои се лоцирани на различни локации поврзани со канали, за да комуницираат едни со други преку интернет. IRC разговорните мрежи им овозможуваат на своите корисници да создадат јавни, приватни и тајни канали. Јавни канали се канали каде што повеќе корисници може да разговараат и да споделат пораки и датотеки. Јавните канали им овозможуваат на корисниците на каналот да ги видат сите IRC називи и пораките на корисниците на каналот. Приватните и тајните канали се поставени од страна на корисниците за да комуницираат само со други определени корисници. Приватните и тајни канали ги заштитуваат називите и пораките на корисниците кои се најавени од корисници кои немаат пристап на каналот. Иако содржината на приватните канали е скриена, одредени команди за лоцирање на каналот им овозможуваат на оние кои не се корисници на одреден канал да го идентификуваат неговото постоење, додека тајните канали е многу потешко да се лоцираат, освен ако корисникот е член на каналот.

IRC DDoS нападот е сличен на моделот на DDoS нападот базиран на агент-управувач, освен што наместо да се користи програмата на управувачот инсталирана на мрежата на серверот, за да се поврзе клиентот со агентите за комуникација се користи IRC каналот (Слика 2). Со употребата на IRC каналот, напаѓачите кои го користат овој тип на DDoS напад имаат дополнителни бенефиции. На пример, напаѓачите можат да користат "легитимен" IRC канал за испраќање на команди кон агентите. Ова го прави следењето на DDoS командните пакети многу потешко. Покрај тоа, IRC серверите имаат тенденција да дистрибуираат големи количини на сообраќај што го олеснува сокривањето на напаѓачот позади овој сообраќај. Трета предност е тоа што напаѓачот не мора да одржува листа на агенти, бидејќи тој, едноставно, може да се логира на IRC серверот и да ја види листата на сите достапни агенти. Агентот инсталиран во IRC мрежата обично комуницира со IRC каналот и го известува напаѓачот кога агентот е активен. Четврта предност е тоа што IRC мрежите, исто така, обезбедуваат корист со лесно споделување на датотеки. Споделувањето на датотеки е еден од пасивните методи на дистрибуција на агентскиот код. Оваа функција им олеснува на напаѓачите да ги обезбедат жртвите кои треба да учествуваат во нивните напади. Многу заеднички пристапи имаат со дистрибуцијата на кластери. Со други зборови, секоја група на агенти се поврзува со IRC серверот. Кога напаѓачот сака да комуницира со сите агенти, тој се поврзува со сите сервери со очекувани зомби и барања за команда. Со овој пристап, многу е потешко да се пратат сите зомби од ботнетот и да се исклучат. Регулаторот ќе биде во можност да ги прати само зомбите поврзани со серверот, не сите зомби [3].



Слика 2. *DDoS напад базиран на IRC*

II .2 *Поделба на DDoS нападите според подвигот*

Друга класификација за DDoS нападите е според типот на подвигот за напад. Што ќе искористи напаѓачот при самиот напад, е клучна точка што влијае на успехот или неуспехот на нападот. Искористувањето на ранливости не мора да бара силна техничка позадина во некои случаи, но во некои случаи напаѓачот мора да биде кодски гуру кој преку системот знае да чита податоци во хексадецимален формат.

II .2.1 DDoS *напади со осиромашување на пропусниот опсег*

Постојат две главни класи на DDoS напади со осиромашување на пропусниот опсег. Flood DDoS напад кој вклучува голем број на зомбија кои испраќаат голема количина на сообраќај кон системот-жртва, за да го стесни пропусниот опсег на системот-жртва. Во Flood DDoS нападот, зомбите го поплавуваат системот-жртва со IP сообраќај. Големиот обем на пакети испратени од страна на зомбијата, системот жртва го успоруваат, до пад на системот или стеснување на мрежниот пропусен опсег. Ова го загрозува легитимниот пристап на корисниците. Слика 1 и Слика 2 укажуваат на Flood DDoS напад од страна на агент-управувач на нападот на мрежата и напад врз IRC.

UDP (User Datagram Protocol) Flood напади: UDP е конектирачки протокол. Кога податочните пакети се праќаат преку UDP, не постои барање за ракување помеѓу испраќачот и примачот. Системот примач само ќе добие пакети кои е потребно само да ги обработи. Големиот број на UDP пакети испратени до системот-жртва може да ја засити мрежата, осиромашувајќи го пропусниот опсег достапен за легитимни барања за услуги од жртвениот систем.

Во DDoS UDP Flood нападот, UDP пакетите се праќаат или на случајни или на одредени порти на жртвениот систем. Типично, UDP flood нападите се дизајнирани за да оневозможат избран пристап до жртвата. Ова го предизвикува жртвениот систем да ги обработува влезните податоци и да се обидува да утврди кои провајдери ги имаат бараните податоци. Доколку жртвениот систем не ги вклучи сите апликации на целните порти, системот жртва ќе испрати ICMP (Интернет протокол за контрола на порака) пакет на испраќачкиот систем со содржина на порака "дестинација на недостижен порт"[4].

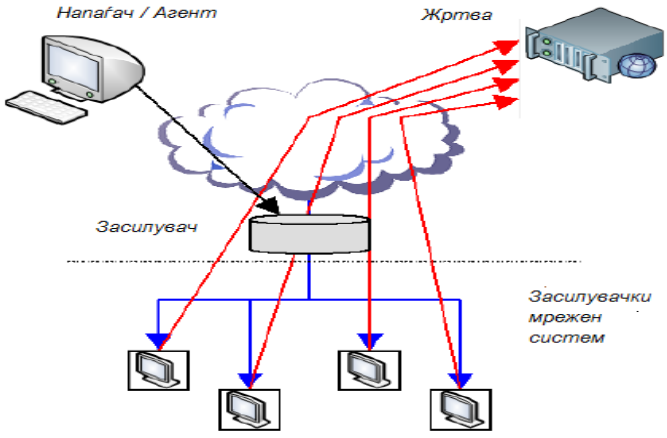
Често, напаѓачката DDoS алатка, исто така, измислува нов извор на IP адресата од каде што доаѓаат напаѓачките пакети. Ова помага да се скрие идентитетот на напаѓачот и гарантира дека враќањето на пакетите од жртвениот систем се вратени преку зомбијата, како друг компјутер со маскирана адреса.

ICMP Flood напади: ICMP е наменет за управување со мрежните карактеристики како што се: пронаоѓање на мрежна опрема и одредување на бројот на хостови или приближното време за да се дојде од локацијата на изворот до дестинацијата.

Засилувачкиот напад вклучува испраќање на пораки од напаѓачот или зомбито до емитувачката IP адреса, користејќи го ова за да ги предизвика сите системи во подмрежата од страна на емитувачката IP адреса да испратат порака до системот-жртва. Овој метод го засилува малициозниот сообраќај со кој се намалува брзината на пренос од жртвениот систем.

Smurf напади: Во DdoS Smurf нападот, напаѓачот испраќа пакети до мрежниот засилувач (Системот за поддршка на емитување и обраќање) (Слика3), со повратна адреса маскирана во IP адреса на жртвата [5][6].

Fraggle напади: Fraggle DDoS напад е сличен на Smurf нападот во тоа што напаѓачот испраќа пакети до мрежниот засилувач. Fraggle е различен од Smurf во тоа што Fraggle користи UDP_ECHO пакети наместо ICMP_ECHO пакети [7] [8].



Слика 3. Fagge и Smurf DDoS напади со засилувачки мрежен систем

II 2.2 DDoS *напади со осиромашување на ресурси*

DDoS нападите со осиромашување на ресурси го вклучуваат испраќачот на напаѓачки пакети што го злоупотребува мрежниот комуникациски протокол за испраќање на неправилни пакети со кои се преоптоваруваат мрежните ресурси, така што не можат да бидат на располагање за легитимните корисници.

Тука се вклучуваат нападите со подвиг на протокол кои се засноваат врз синхронизација на преносот и признанието дека пакетот е примен за потоа да се одговори на тоа признание, како и нападите со испраќање на барање каде пакетите се чуваат во магацин кој е отворен за пребарување во секој момент.

Напад со погрешен пакет е напад, каде напаѓачот им наредува на зомбијата да испратат неправилно формирани IP пакети на системот-жртва со цел да се сруши системот на жртвата. Постојат два вида на напади со погрешен пакет: напади на IP адресата на пакетот која ги содржи изворните и дестинациски IP адреси. Ова може да го збуни оперативниот систем на системот-жртва и да предизвика негов пад. Во нападот на IP пакетните опции, погрешниот пакет може да ги рандромизира опционалните полиња во рамките на еден IP пакети да ги постави сите услужни битови така што системот-жртва мора да користи дополнително обработувачко време за да го анализира сообраќајот. Ако овој напад е размножен со користење на дополнителни агенти, може да ја загрози обработувачката способност на системот-жртва[3].

II .3 *Поделба на DDoS нападите според техниката на ширење*

Претходните две класификации покажаа јасно колку DDoS нападот може да биде сериозен. Уште повеќе, треба да биде споменато расчистувањето со класификацијата. Класификацијата, според техниката на ширење е класификација што оди длабоко во внатрешната структура на агентите. Се дискутира за тоа како агентите се поставени на компромитираните компјутери, какви методи на комуникација се користат, и какви платформи се таргетирани.

II .3.1 *Подесување на DDoS Агентите*

Постојат активни и пасивни методи кои напаѓачите ги користат за да инсталираат злонамерен код на секундарен жртвен систем со цел да се подесат врз основа на обработувачот или IRC DDoS нападите на мрежа. Активните методи обично го вклучуваат напаѓачот преку скенирање на мрежата за системите со познати слабости. По идентификувањето на ранливите системи, напаѓачот работи на скриптите за да може да се пробие во системот. Откако напаѓачот има најдено дупка во системот, тој тајно може да се инсталира на DDoS агентен софтвер. Така системот се компромитира како секундарна жртва и може да се користи како зомби во DDoS напад. Пасивните методи обично вклучуваат споделување на напаѓачките корумпирани фајлови или градење на веб-сајтови кои ги искористуваат предностите на познати пропусти во веб прелистувачот како секундарна жртва. По пристапот до датотеката или веб-сајтот со вграден DDoS агент, секундарната жртва се компромитира, и агентот со DDoS код може да се инсталира.

Скенирање: Пред започнување на DDoS нападот, напаѓачите прво мора да го подесат DDoS нападот на мрежата. Тие често употребуваат алатка за скенирање за да се идентификуваат потенцијалните жртвени системи. Една заедничка алатка напаѓачите користат за скенирање на портови во софтверска програма наречена nmap. Напаѓачите можат да го симнат nmap од различни локации на интернет. Оваа алатка овозможува напаѓачите да изберат опсег на IP адреси за да се скенираат. Алатката потоа ќе продолжи да пребарува на Интернет за секоја од добиените IP адреси. Nmap враќа информации за секоја IP адреса која е емитувана низ различни порти со протоколи, како што се TCP и UDP кои се отворени, и специфичниот оперативен систем на скенираниот корисник. Напаѓачот тогаш може да ја испита добиената листа со потенцијални секундарни жртвени системи [9].

***Софтверска ранливост/Задна врата*:** Откако напаѓачот ја скенирал листата со ранливите системи, тој ќе треба да ја искористи ранливоста за да добие пристап до секундарната жртва на системот и да го инсталира DDoS агент-кодот. Постојат многу извори на Интернет, како што е CVE (Заеднички пропусти и експозиции) организацијата, која јавно ја има објавено листата на сите познати пропусти на различни системи. CVE категоризира повеќе од 2.000 различни типови на пропусти и тие имаат над 2.000 повеќе чекања за разгледување [10].

***Тројански коњ*:** Тројанскиот коњ е програма која се појавува за вршење на корисна функција, но во реалноста содржи скриен код, кој или извршува злонамерни акти или обезбедува неовластен пристап до некоја привилегирана системска функција [3]. Тројанските коњи се инсталираат на системот-жртва од страна на напаѓачот со што му се дозволува на напаѓачот да се здобие со контрола на компјутерот на корисникот, без корисникот да знае. Во случај на користење на алатката за DDoS напад, тројанскиот коњ веќе е инсталиран на системот-жртва и може да се користи од страна на напаѓачот за да добие пристап до системот на секундарната жртва, со тоа му се овозможува на напаѓачот да го инсталира DDoS агент-кодот. Тројанскиот коњ самиот по себе, обично се инсталира на системот на секундарната жртвата со користење на техники за пасивно подесување.

***Buffer overflow*:** Бафер е континуиран блок од меморија (со конечна големина) кој служи за привремено складирање на податочна област во рамките на компјутерот. Buffer overflow е напад против бафер кој испраќа повеќе податоци во баферот од големината на баферот. Ова предизвикува дополнителните податоци да избришат други информации во непосредна близина на баферот во меморијата за складирање од магацинот, како што е постапката за враќање адреса [11]. Ова може да го предизвика компјутерот да врати повик од постапката на малициозен код вклучен во податоците што се презапишани во баферот. Овој малициозен код може да се користи за да се почне активност на избор на напаѓачот (како DDoS агент) или да се обезбеди пристап до компјутерот на жртвата, така што напаѓачот може да го инсталира DDoS агент-кодот.

II .3.2 *Пасивна DDoS Инсталација*

Озвучени веб-страници: Овој метод напаѓачите можат да го користат за пасивно инфилтрирање во компјутерски систем на секундарна жртва, преку ранливите страни на веб прелистувачите. Овој метод му овозможува на напаѓачот да создаде веб-страни со код или команди на веб прелистувачот за да фатат жртва. Кога веб прелистувачот на жртвата отвара некоја веб-страница или се обидува да пристапи до содржината на веб-страницата индиректно презема инсталација на малициозен код (на пример, агент на DDoS). Еден пример за овој тип на напад е врз база на грешка во Мајкрософт Internet Explorer (IE) верзиите 5.5 и 6.0. Овие верзии на IE содржат ActiveX, технологијата развиена од страна на Microsoft за да се овозможи контрола во рамките на IE за гледање одредени plug-in-апликации кои се вградени во рамките веб-сајт кодот[12].

***Оштетена датотека*:** Друг метод за пасивен напад кој најчесто се користи е употреба на датотеки кои вклучуваат малициозен код вграден во нив. Кога системот-жртва се обидува да ги види или изврши овие фајлови, тој станува инфициран со злонамерен код.
Постојат многу трикови за создавање на инфицирани фајлови. Повеќето напаѓачи се доволно квалификувани да го вградат DDoS агентот или друг вирусен софтвер во рамките на легитимен фајл. Напаѓачите ги редизајнираат десктоп иконите како такви фајлови, се избираат долги имиња на датотеки со легитимни екстензии испреплетени во името на датотеката, така што, прикажувањето на нецелосно име на датотека е само пример за такви оштетени датотеки [13].

III АНАТОМИЈА НА DDoS НАПАД ВРЗ DNS

Во последно време, извршенаи се серии на DDoS напади на жртви со DNS корен и TLD (Top Level Domain) име на серверските оператори. Овие напади заслужуваат внимателна анализа, бидејќи тие комбинираат неколку алатки за напад и методи за зголемување на нивната ефикасност. Нападите, исто така, го свртуваат вниманието како оперативен проблем кој беше решен одамна, но сепак, повеќето ИТ администратори не го прифаќаат одговорот. При ваквите напади се користат следните пристапи:

***Системски компромис*:** Напаѓачот не сака да го користи својот сопствен систем за да нападне други системи и да ризикува да биде откриен, па затоа тој го започнува нападот од системи на кои тој има стекнато неовластена административна контрола. Постојат многу начини да се здобие со контрола на системите. Еден метод користи масовен е-маил црв за да заразат голем број на системи[14]. Кога црвот инфицира еден систем, се инсталира на далечинскиот управувач на софтверски агент или зомби, така што напаѓачите од далечина можат да ги контролираат, насочуваат и да ги иницираат DDoS нападите.

Дистрибуција на извори на DDoS напад: Во нападите, целта на напаѓачот е да ја именува комуникациската инфраструктура насочена кон името на серверскиот оператор, наместо да се именува себеси. Именуваните серверски оператори обично имаат големи пристапи, па почнувањето на нападот од еден извор е со мала веројатност да ја постигне целта. Но, со искористување на вистинска армија од нападни извори на напаѓачот може да се пополни пристап дури и од Gigabit во секунда. Botnets, колекцијата на зомби хостови најчесто служи како војска на напаѓачот [14].

***Засилување*:** Напаѓачите користат засилување за да се зголеми обемот на сообраќај во нападот. Во DNS нападите, напаѓачот засилувањето го користи за продолжување на DNS протоколот (EDNS0) кој овозможува големи DNS пораки. Напаѓачот составува барање во DNS порака од околу 60 бајти за да се активира доставување на одговор на пораката од околу 4.000 бајти до целта. Како резултат на факторот на засилување, околу 70:1, значително се зголемува обемот на сообраќајот за постигнување на целта, забрзувајќи ја постапката по која ресурсите на целта ќе бидат исцрпени [15].

Корупција на DNS податоци: За да се постигне ефект на засилување, напаѓачот издава DNS барање со податок дека има информации за евоцирање на многу голем одговор [13]. Постојат многу начини за напаѓачот однапред да знае кој DNS ресурс запис да го побара.

***Присвојување*:** Во DNS нападите, секој напаѓачки хост ја користи IP адресата на таргетираниот сервер како своја изворна IP адреса. Ефектот на измама на IP адреси на овој начин е тоа што одговара на DNS барања кои ќе бидат вратени до целта откако ќе бидат измамени домаќините.

III .1 *Извршување на нападот*

Кога ги знаеме сите елементи на нападот, можеме да погледнеме како се изведува нападот. Напаѓачот ја врбува неговата војска за напад на изворот (ботнетот). Пишува евиденција на големите засилувања (на пример, запис на 4000 бајтен DNS TXT ресурс) во зонскиот фајл на името на серверот каде има компромитација. Тој ја тестира и ја составува листата на отворени рекурзивни именувани сервери кои ќе бараат компромитиран именуван сервер со име на измамениот хост. Со овие елементи, напаѓачот заповеда неговата војска да го нападне насоченият именуван сервер преку отворени рекурзивни сервери.
Да претпоставиме дека напаѓачот е насочен кон именуваниот сервер во IP адресата 10.10.1.1. Со даден сигнал на напаѓачот, сите зомби во неговиот ботнет со DNS барање прашуваат за засилување на рекордот преку отворени рекурзивни сервери. Ботнетот е домаќин на измислен насочен именуван сервер со запис во изворната

IP адреса 10.10.1.1 од областа на IP пакетите кои ги содржат нивните DNS барања. Отворениот рекурзивен именуван сервер го прифаќа DNS барањето од ботнет хостовите. Ако отворениот рекурзивен именуван сервер не добил барање за овој рекорд предходно, и повеќе не го држи засиленият запис во неговата кеш меморија, тој обезбедува DNS барање за порака за самиот себе кон компромитираниот именуван сервер, и компромитираниот именуван сервер враќа засилен запис на софтверот од отворениот рекурзивен сервер. Отворениот рекурзивен сервер компонира DNS одговори кои содржат засилување на записот и ги враќаат на системот од кој потекнува барањето. Отворените рекурзивни сервери веруваат дека тие испраќаат DNS одговори на пораки до ботнет хостовите што го направиле почетното барање, но всушност IP измамата предизвикува одговорите да бидат проследени до целта, именуваниот сервер на 10.10.1.1.

Таргетираниот именуван сервер на 10.10.1.1 никогаш не издава DNS барања, но сега е бомбардиран со одговори. Одговорите содржат, на пример, 4000 бајтен DNS TXT рекорд. Една порака од оваа големина ја надминува максималната (Ethernet) преносна единица, па таа е поделена на повеќе IP пакетни фрагменти. Ова силно составување на одредиштето, со кое се зголемува обработката за оптоварување на целта ја подобрува измамата: бидејќи одговорот спојува неколку IP фрагменти, и само првиот фрагмент го содржи насловот на UDP, целта не може веднаш да се препознае бидејќи нападот е базиран на DNS.

Овој DDoS напад е најефикасен, кога започнува преку голем број на отворени рекурзивни сервери. Дистрибуцијата го зголемува сообраќајот и го намалува фокусот на изворите на нападот. Влијанието врз злоупотребениот отворен рекурзивен сервер е генерално ниска, така што оди неоткриено. Ефектите врз целта, сепак може да бидат сериозни [16].

III .2 *Преживување (ако вие сте целта)*

Постојат неколку мерки кои можат да се превземат за намалување на ефектите од DDoS нападот.

Изворните IP адреси не се маскирани во IP пакети вршејќи DNS одговори на пораки, па изворните адреси идентификуваат отворени рекурзивни сервери на зомби корисници. Во зависност од тежината на нападот и колку силно сакаме да одговориме на нападот, може да се ограничи стапката на сообраќај од овие изворни IP адреси или да се идкористи правило на филтрирање на DNS одговорите на пораки кои се сомнително големи (пример над 512 бајти). Во екстремност, може да се избере да се блокира сообраќајот од отворените рекурзивни сервери во целост (ова е прилично лесно да се направи, користејќи го блокирачкото ложиште на сајт листата.). Овие напори се со цел да се уништи изворот на нападот, и тие да не го редуцираат товарот на мрежите и префрлувањето помеѓу името на серверот и на отворениот рекурзивен сервер [17]. Може да се забележи дека, ако се блокира целиот сообраќај од овие отворени рекурзивни сервери може да се меша со сообраќајот од легитимните обиди за барања на корисниците на овие сервери. На пример, некои организации работат со отворени рекурзивни сервери, така што мобилните вработени може да се решат за ваков прекин, па корисниците можат да бидат погодени.

IV ПРЕВЕНЦИЈА ОД DDoS НАПАДИ

Многу институти и тимови истражуваат за DDoS нападите и како тие може да се спречат. Сепак, тоа не е во интерес на обичните корисниците, пред сè доколку е потребно да трошат повеќе пари и напор на тоа прашање. Во денешно време, по сè позачестените DDoS напади, многу е јасно дека голема е потреба за донесување одлуки за обид за да се намали тој ризик колку што е можно повеќе, со цел да се спречи или реши проблемот. Во моментов постојат неколку процедури/напори за намалување на DDoS нападите, кои се локални и не ефективни во случај на големи удари. Сепак, се случува силен истражувачки бран и се обидува да најде изводливо решение.

IV .1 *Тековните напори за да се спречат DDoS напади*

Тековните напори се пред сè локални, бидејќи нема координација помеѓу различните органи. Сегашниот модел е дистрибуиран авторизиран модел. Секој интернет провајдер, во секоја земја, има свој сет на правила/закони кои ја регулираат сајбер безбедноста. Во некои земји, дури и не постои орган кој ќе се грижи за безбедноста на сите корисници. Секој корисник е одговорен за своите постапки. Познато е дека дистрибуираните системи во целина се покомпликувани отколку централизираните системи. Иако реалниот свет е дистрибуиран, може да се тврди дека било кој аспект од животот треба да биде централизиран за да се дојде до една цел.

Некои од превземените активности се:

Филтрирање од страна на интернет провајдерите: Речиси сите интернет провајдери имаат IP филтри за да се постигне спречување на разни видови на напади. Ова всушност помага многу во спречување на некои од нападите како Smurf нападите, кои беа претходно споменати. Исто така, голем број на интернет провајдери детектираат малициозни пакети со познати потписи или лоши TCP/UDP опции. Оваа детекција, исто така, спречува некои векторски напади. Владите можат да спроведуваат политики за некои интернет провајдери за да ги блокираат одредени правци или подмрежи во случај на напади поврзани со политички прашања. Но, претходно споменатите напори се локални. Дури и интернет провајдерите во иста земја често не ги делат податоците за црната листа на IP адреси со злонамерни домаќини.

Мониторинг тимови: Постојат тимови кои ги следат интернет активностите за да се создаде една динамична

листа на адреси со метрики за нивното ниво на закана. Тим Кумру, како пример, следи одредена интернет критична инфраструктура, за обезбедување на резултати во овој дел. Со тоа се овозможува гледачот да го утврди обемот и времетраењето на реализирањето на испадот, и алокализираниот ефект на таквиот испад. Многу такви проекти за следење користат ICMP, но ова не е најдобра мерка за перформансите [18].

Податочни центри за итни случаи: Вообичаена практика за големите претпријатија е да постои податочен центар за опоравување или податочен центар за вонредна состојба. Иако некои корисници расправаат за овој метод како за техника за ублажување, сепак, ова не е техника за ублажување. И покрај тоа што овој метод е потребен, сепак, истиот мора да биде комбиниран со вистински техники за ублажување и превенција.

Алатки за лов: Постојат неколку алатки за ловење botnet-и кои не се јавно достапни, а се користат од страна на некои органи на прогонот. Microsoft има развиено една од овие алатки. Иако Microsoft не сака да даде детали за својот откривач на ботнет-компанијата вели дека истиот дури го открива нејзиното име со што би можело да се даде поим за сајбер криминалците ао што би се зголемил ефектот во нивно спречување. Алатката вклучува податоци и софтвер кој помага во спроведување на законот за да се добие подобра слика на податоците кои се обезбедени од страна на корисниците на Microsoft [19].

IV.2 *Препорачани методи за спречување DDoS напади*

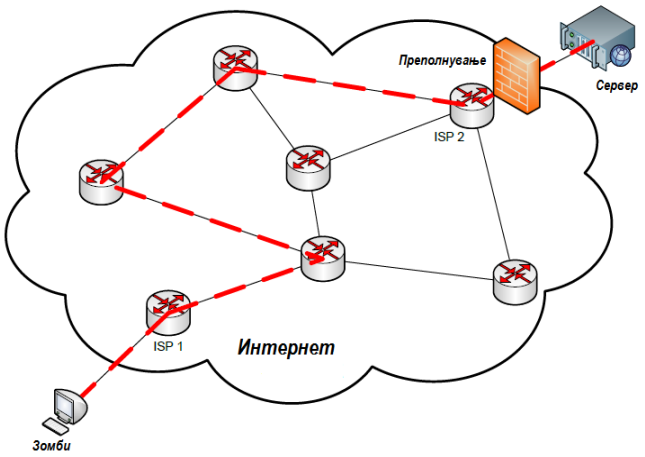
Сите претходни методи не се многу ефикасни. Веќе имаме видено премногу инциденти во изминатите неколку години со што можеме да кажеме дека има потреба од иновативни решенија. Решенија кои зависат од соработката помеѓу различните органи за да се обединат напорите против развојот на botnets.

Интернет-Интерпол: Овој термин сè уште не е валиден термин. Но, ова би можело да биде можно решение за проблемот со DDoS нападите. Во Интерпол постои правен оддел што се занимава со сајбер малициозни активности, кој е само за следење или за поддршка на тимови за тактички физички операции. Ако постои централизирана меѓународна сила која го регулира интернетот, принудувајќи стандарди и координирање меѓу земјите за "сајбер политички" прашања, тоа би можело да биде основа за едно ново и посоодветно решение за спротиставување против целокупниот компјутерски криминал. Можно решение на безбедносните проблеми кои постојат во сајбер просторот е постоењето на Интернет-интерпол, кој би функционирал на сличен начин како и Интерпол. Носителите на одлуки обично се плашат од зборот "пропис". Всушност главен проблем настанува доколку истиот се користи на лош начин. Сепак, со оглед на моменталната ситуација на современите закани, тоа стана секојдневие. Постојат клучни точки кои треба да се дискутираат во овој пристап за да се обезбеди ефикасност и транспарентност на оваа програма.

Опсег: Многу важна точка за дискусија е опсегот на оваа организирана сила (Интернет-интерпол). Ова решение е најпосакувано бидејќи Интернет-интерполот се занимава со сите сајбер закани за безбедноста. Сепак, овој труд ги разгледува само DDoS нападите и botnet-и, поради што во нашиот случај ќе се фокусираме на нашата студија за овие напади. Интернет-интерполот треба да биде поврзан со постоечките Интерпол власти. Тоа обезбедува непречен вовед во оваа организациска сила. Исто така, имајќи пристап до информациите кои Интерпол веќе ги има, ја прави работата полесна за аналитичарите. И, се разбира, постоењето на иста менаџерска структура, заштедува многу време, прави позадински проверки, деловна анализа и сите други правни прашања што треба да се испитаат пред осмислување на нова заштитна сила.

Врска: Интернет интерполот мора да биде поврзан со сите интернет провајдери. Ова осигурува оркестрација на комуникацијата помеѓу интернет провајдерите со што се овозможува интерно (во иста држава) и екстерно (во сите земји) спроведање на политики, споделување на информации за високата закана на IP адреси и подмрежи и агрегатна статистика за да се создадат математички и статистички модели. Со овозможувањето на поврзување со сите интернет провајдери се создава репутација на систем кој се базира на статистички податоци собрани од разни локации.

Улога: Како што споменавме претходно, Интернет-интерполот ќе има многу задачи и мисии. Сепак, ние сме само загрижени за неговата улога како превентивен систем за DDoS напади. Градење на репутацискиот систем е една од главните контрамерки што Интернет-интерпол ќе ги користи. Репутацискиот систем го обележува секој IP со нивото на закана, што укажува на веројатноста дека таа IP адреса е дел од ботнет. IP адресите над одреден праг се сметаат за висок ризик. Постојат неколку модели за справување со висок ризик кај домаќините.
Сигналите може да се праќаат во текот на домаќинскиот интернет провајдер кој може да ги блокира преку рутирање на снабдувањето, што е спротивно на тековниот блокиран систем, каде што е блокиран сообраќајот на крајот од синџирот, каде што е откриен нападот.
Слика 4 ја покажува оригиналната метода што во моментов се користи од страна на интернет провајдерите. Поради недостаток на комуникација помеѓу интернет провајдерите, лошиот сообраќај всушност е рутиран од зомби целиот пат во текот на патот до последниот интернет провајдер во синџирот. Овој интернет провајдер (ISP 2) открива дека серверот е под DDoS напад и со одржување своја IP црна листа, со својот заштитен sид го блокираа сообраќајот. Ова сценарио е начин кој е далеку од совршен.



Слика 4. Работа на Интернет-Интерпол

Хетерогеност на оперативни системи: Се смета дека во ова сценарио постои само еден оперативен систем што сите го користат. Со ова се олеснува работата на напаѓачите, кои можат да ја завршат својата задача со пишување на само еден програм кој работи на секоја машина на земјата! Напротив, ако секоја машина има свој оперативен систем, тогаш напаѓачот мора да пишува малициозен софтвер за секој одреден корисник. Во ова сценарио, botnet-от не би постоел сигурно. Тоа бара голем вложен труд од страна на потенцијален иот напаѓач.

Точката од овој аргумент е дека хетерогеноста на платформите му отежнува за напаѓачот да се приклучи на malware-от кој се шири. Проблемот е што повеќето од персоналните компјутери на земјата имаат софтвер на Microsoft. Неодамна, серверите исто така мигрираа на Microsoft. Овој факт ја прави одлуката прилично лесна за напаѓачот кога тој ја избира платформата под која ќе работат неговите агенти. Интернет-интерполот не може да помогне во оваа ситуација. Меѓутоа, националните масовни комуникациски методи можат да ја шират таа пропаганда за да се зголеми безбедносното знаење на јавноста.

Cloud computing*: Во денешно време забележан е значителен напредок на* cloud computing-от. EC2 Амазон и Гугл облаците се прилично големи и се користат во разни начини. За жал, cloud computing, исто така, се користи и за лоши цели. Брз-флукс од ловечки сајтови користат брза DNS ротација низ голем број на крајни точки што им помага на компјутерските измамници да ги избегнат повеќето од филтрите.

Зошто не се користи истата техника за да се обезбеди стабилноста против DDoS напади? Со резервните веб-сајтови на облакот и добар план за ротација, може да се направи употреба на повеќе мали сервери низ повеќе облаци на продавачите и можат да преживуваат силни DDoS напади. Овој метод е добар за приспособливост и робустност и бара многу за финансирање што е надвор од опсегот на ова истражување. Сепак, тоа и понатаму останува многу ветувачко решение.

***Спроведување на законот*:** Иако ова истражување е техничко истражување, вреди да се спомене дека тука во прашање не е само техничката страна. Сето она што ние го зборуваме за да се спречат DDoS нападите нема никаква врска со вистинските криминалци. Сајбер криминалот е многу лесно да се изврши и многу примамлив, затоа што казната не е неминовна. Обично, кога напаѓачите ги извршуваат нивните напади тие имаат чувство дека се безбедни, бидејќи на физички начин се далеку од местото каде што е извршен злонамерниот акт. Зошто бројот на извршени компјутерски криминални дејствија драстично се зголемува, додека за физички кривични дела се доаѓа до решение? Одговорот на ова прашање не може да се одговори директно. Сепак, може да се тврди дека обично сајбер криминалците немаат визуелизација на она што може да се случи со нив ако тие бидат фатени и обично тие мислат дека не постои моност да бидат лоцирани! Мора да постојат построги закони кои ги дефинираат сајбер криминалот и казните. На глобално ниво, во некои држави постоиат одреедни закони, во некои бројот на овие закони е многу мал, а во трети пак и воопшто не постојат закони против овој вид на крим инал! Дури и во земјите во кои има закони, не се вложува многу напор во следење и лов за одредување на напаѓачите. Исто така, испитувањата за сајбер криминалот мора да бидат повеќе публицирани.

V . ЗАКЛУЧОК

"This page cannot be displayed" сценариото повеќе не е научна фантастика. Без сериозни напори и детални истражувања за да се спречат овие индексирани чудовишта, ние ќе се пронајдеме себеси дисконектирани и назад во времето кога за испраќање на обично писмо ги користевме поштенските услуги! Се разбира, не постои „сребрен куршум“ во безбедноста. Ништо не е целосно безбедно. Сепак, со предложените техники, ризиците можат да се сведат на многу пониско ниво, отколку што е случајот во моментов.

Со Интернет-интерпол, имаме регулиран Интернет. Хетерогените платформи прават статистичка магија. Cloud computing е исто така добар систем кога се разгледува од безбедносен аспект. Има печат од планот Б во случај на фатална штета, што е многу важно. Дополнително на ова, потребно е фер применување на законите за да бидеме сигурни дека не само што корисниците си ги добиваат своите права, туку исто така дека и злонамерните корисници нема да се извлечат неказнето за извршените злонамерни дејствија. Инкорпорирањето на сите овие предлог мерки во еден заеднички систем може значително да допринесе во зголемување на сајбер безбедноста.

БИБЛИОГРАФИЈА

[1] Information Security Magazine. (2006, Jul). *Distributed Denial of Service Attack*. Retrieved from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html

[2] Wikipedia. (2008, Feb). *Botnets*. Retrieved from http://en.wikipedia.org/wiki/Botnet

[3] Lee, R. B., & Specht, S. M. (2005, Jan). *Taxonomies of Distributed Denial of Service Networks, Attacks, Tools and Counter Measures.* Retrieved from Prinecton University.
[4] Distributed Denial of Service: Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht. (2000, Feb). CIAC: U.S. Department of Energy.
[5] TFreak. (2003). *fraggle.c*. Retrieved from phreak.org: http://www.phreak.org/archives/exploits/denial/fraggle.c
[6] Federal Computer Incident Response Center. (2000). *Defense Tactics for Distributed Denial of Service Attacks.*
[7] Martin, M. J. (2002, Oct). *Smurf/Fraggle Attack Defense Using SACLS*. Retrieved from www.searchnetwork.techtarget.com: http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci856112,00.html
[8] TFreak. (2003, May). *Smurf.c*. Retrieved from Phreak.org: http://www.phreak.org/archives/exploits/denial/smurf.com
[9] Insecure.org. (2002, Aug). *Nmap Stealth Port Scanner Introduction*. Retrieved from http://www.insecure.org/nmap/
[10] Homeland Security. (2002, Mar). *Common Vulnerabilities and Exposures (CVE)*. Retrieved from cve.mitre.org: http://cve.mitre.org/
[11] Cowan, C., Wagle, P., Pu, C., Beattie, S., & Walpole, J. (2000). *Buffer Overflows:Attacks and Defenses for the Vulnerability of the Decade*. Retrieved from Oregon Graduate Institute of Science & Technology: www.ece.cmu.edu/~adrian/630-f04/readings/cowan-vulnerability.pdf
[12] Microsoft. (1999, Jun). *How to Write Active X Controls for Microsoft Windows CE2.1*. Retrieved from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnce21/html/activexce.asp
[13] Danchev, D. (2002, Oct). *The Complete Windows Trojans Paper*. Retrieved from BCVG Network Security: http://www.ebcvg.com/articles.php?id=91
[14] The Continuing Denial of Service Threat Posed by DNS Recursion http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf
[15] Extension Mechanisms for DNS (EDNS0) http://www.rfc-editor.org/rfc/rfc2671.txt
[16] BCP 38, RFC 2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,http://www.ietf.org/rfc/rfc2827.txt
[17] AC004, "Securing the Edge" by Paul Vixie http://www.icann.org/committees/security/sac004.txt
[18] AC004, "Securing the Edge" by Paul Vixie http://www.icann.org/committees/security/sac004.txt
[19] PCworld. (2008, Apr). *Microsoft Botnet-hunting Tool Helps Bust Hackers*. Retrieved from http://pcworld.about.com/od/securit1/Microsoft-Botnet-hunting-Tool.html