Distribuirani napad uskraćivanjem usluga

Dario Šincek, Tedo Vrbanec
Učiteljski fakultet Sveučilišta u Zagrebu, Odsjek u Čakovcu
Ulica dr. Ante Starčevića 55, Čakovec, Hrvatska
Telefon: (040) 37 00 00 Fax: (040) 37 00 25 E-mail: {dario.sincek; tedo.vrbanec}@gmail.com

Sažetak – Iskustvo je autora da je u Hrvatskoj postotak korisnika računalno-komunikacijske tehnologije sa znanjem i iskustvom, ili čak samo sa željom za učenjem o sigurnosnim pitanjima korištenja Interneta, njegovih usluga i općenito računalnih mreža, zanemariv. Laicima, čak i prosječnim korisnicima broj i opseg prijetnji koje dolaze s Interneta i ostalih mrežnih resursa najčešće je nepoznat. Mnogo je razloga: od nedovoljnog obrazovanja, ignoriranja prijetnji, nezainteresiranosti krajnjih korisnika, ... Tema rada je jedan mali segment tih prijetnji koji se naziva distribuirani napadi uskraćivanjem usluga (engl. *Distributed Denial of Service*, DDoS), a koji predstavljaju povelik problem sistem i/ili mrežnim administratorima.

I. UVOD

DDoS napad jedan je od problema s kojima se s vremena na vrijeme susreću mnoga popularna web ali i druga sjedišta na Internetu. U apsolutnom broju korisnika Interneta koji se neprestano povećava, nisu problem oni dobronamjerni, već se, iako relativno slabo zastupljeni, povećava apsolutan broj onih koji ga nastoje zloupotrijebiti na razne načine. Oni se sve više udružuju – stoga je opasnost to veća. K tome, u današnje vrijeme nije potrebno biti vrhunski programer da bi se izveo napad, posebno ove vrste. Naime, brojni programi osmišljeni su upravo za tu svrhu, a nekima su opće poznati propusti u radu koji omogućuju DDoS. Oni sadrže visoki stupanj automatizacije omogućavajući izvođenje DDoS napada prosječnim korisnicima računala i Interneta. Nedužni korisnici Interneta mogu biti nesvjesno upleteni u mrežu DDoS napada. Obasipaju nas vijesti u javnim medijima koji govore da su desetine i stotine tisuća računala, bez znanja njihovih korisnika dio *botnet* mreža. *Botnet* je mreža računala inficiranih crvima, virusima, trojancima ili drugom malicioznom programskom podrškom koja se na računalo korisnika instalirala zbog neznanja, nemara, neodgovornosti, neopreznosti, naivnosti ili perfidnosti prevarantskih umova koji nudeći besplatne sadržaje na posebno pripremljenim web stranicama ili neku besplatnu programsku podršku, žrtvi podmeću „kukavičje jaje“. *Botovi* ili tzv. *zombie* računala koja su pod pritajenom vlašću kriminalaca koji ih, u za njih pogodnom trenutku, aktiviraju te vrše nelegalne aktivnosti, vrlo često DDoS napade na njima zanimljive ciljeve. Oni te *botnet* mreže čak i iznajmljuju. DDoS napade je, ponajviše zbog nemogućnosti predviđanja ishodišta napada (sva su računala potencijalno opasna u rukama neodgovornog i/ili needuciranog korisnika), gotovo nemoguće spriječiti. Jedino što preostaje sistem inženjerima i mrežnim administratorima, kada napad već započne, je mukotrpna borba za održavanje sustava kojeg se napada u koliko-toliko radnom stanju, te suradnja s represivnim sustavom i pružateljima Internet usluga radi dolaska do pravih izvora napada te njihovih vinovnika. U današnje vrijeme stoga se užurbano radi na izradi sustava detekcije i prevencije DDoS napada.

II. SIGURNOST

Sigurnost se kao tema provlači kroz čitav ovaj rad. Stoga je pokušajmo definirati: „Sigurnost je proces održavanja prihvatljivog nivoa rizika“. [1] Kad kažemo da je sigurnost proces, mislimo na to da njegova implementacija zahtjeva naporan trud, odricanje, upozoravanje, edukaciju, brojna programska i sklopovska rješenja i usluge koje nam omogućavaju „biti u toku“ s najnovijim prijetnjama koje se svakodnevno javljaju. Prema [1] kada se govori o sigurnosti i zaštiti informacijskih sustava i mreža uvriježeno je nekoliko principa koji danas vrijede kao osnovni postulati:

1. Sigurnost je proces. Sigurnost nije proizvod, usluga ili procedura, već skup koji ih sadrži - uz još mnogo elemenata i mjera koje se stalno sprovode.
2. Ne postoji apsolutna sigurnost.
3. Uz različite metode zaštite, treba imati u vidu i ljudski faktor, sa svim slabostima.

Ta načela vrijede kako za kućnog korisnika tako i za organizacije bez obzira na njihov opseg djelatnosti.

Nadalje, proces sigurnosti zasniva se na četiri osnovna koraka: procjena, zaštita, otkrivanje i odgovor.[1] Mnogi napadi usmjereni su na uništenje informacija, manipulaciju, prisluškivanje, onemogućavanje dostupnosti zajedno s ostalim nepopularnim radnjama koje uključuju informacije pa su stoga povjerljivost, cjelovitost i raspoloživost sastavni elementi sigurnosti.[1]

Područje metoda zaštite veoma je složeno te stoga nije potrebno ulaziti u dublje analize i specijalizacije tih metoda, jer klasifikacija metoda zaštite od DDoS napada sadrži na desetke principa i rješenja. Metode zaštite ovise o napadima i prijetnjama, pa one evoluiraju zajedno s njima. Iako se mišljenja razilaze, većina autora smatra da postoje četiri osnovne grupe metoda zaštita:

- kriptografske metode,
- programske metode,
- organizacijske metode i
- fizičke metode.

II. INTERNET

Internet je neraskidivo povezan s DDoS napadima. Česta je zabluda korisnika poistovjećivanje Interneta i World Wide Weba (WWW). Kao što znamo, WWW ili skraćeno web, tek je jedna od usluga koje nam nudi Internet. Pored weba, tu su i telnet, Usenet, FTP, e-mail, chat, IM, IRC, spomenimo najpoznatije. ISO/OSI [2]

(teorija) i TCP/IP (praksa) referentni modeli predstavljaju način na koji funkcioniraju mreže i Internet. Oni se razlikuju, ali je prednost u tome što ih možemo dovesti u vezu. Oni su apstraktni i praktični opis dizajna protokola komunikacijskih i računalnih mreža, predstavljeni u obliku sedam odnosno četiri sloja.

Osim najvažnijih usluga i protokola na kojima Internet počiva, u njegovo funkcioniranje uključuju se i *portovi* ili komunikacijska vrata. Najjednostavnije rečeno, *portovi* definiraju način održavanja veze između računala, poslužitelja, klijenata, itd. *Port* je broj na koji se pojedina aplikacija poziva prilikom početka/trajanja komunikacije te omogućava istovremenu komunikaciju različitih aplikacija između dvaju (ili više) računala. Bez koncepta *porta* bilo bi teže utvrditi kojoj aplikaciji pripada neki paket koji stiže s Interneta.

III. NAPADI

Gleda li se Internet kroz prizmu korisnosti i prijetnji, mnogima je jasno da je ovo osjetljivo područje podložno relativizmu. Naime, mnogi bi Internet definirali kao sredstvo olakšanog pristupa i razmjene informacija te međusobne komunikacije. Navedeno bismo mogli okarakterizirati kao pozitivnu stranu Interneta no sada ćemo govoriti o negativnim stranama Interneta tj. o vrstama napada.

Osoba koja inicira napad naziva se napadač. Napadač mora posjedovati najmanje tri svojstva:

- metodu,
- priliku i
- motiv.

Kako bi se mogle poduzeti efikasne mjere zaštite važno je razumjeti osnovni princip i metode koje napadači koriste da „osvoje“ računalni sustav ili mrežu. „U osnovi, napadi su akcije usmjerene na ugrožavanje sigurnosti informacija, računalnih sustava i mreža“. [1] Postoje razne vrste napada, no one se općenito mogu klasificirati u četiri osnovne kategorije: prekidanje, presretanje, izmjena i generiranje nepostojećeg sadržaja. Najčešće vrste napada su napadi krađe identiteta, TCP i UDP napadi te napadi na aplikacije i usluge aplikacijskog sloja.

IV. NAPADI USKRAĆIVANJEM USLUGA (DoS)

Prije definiranja distribuiranog napada uskraćivanjem usluga, potrebno je prikazati osnovne informacije o „običnom“ napadu uskraćivanjem usluga (DoS, engl. *Denial of Service*) i njegovoj strukturi. DoS su aktivnosti poduzete od strane zlonamjernih korisnika s ciljem onemogućavanja ispravnog funkcioniranja različitih računalnih i/ili mrežnih resursa čime određene usluge postaju nedostupne drugim (legalnim) korisnicima, na način da se opetovano i u najkraćim mogućim razmacima traži neka (najčešće legalna) usluga, ne dozvoljavajući, ne čekajući i ne očekujući od poslužitelja ili mreže da uzvrati odgovor, već se svjesno opterećuje snaga poslužitelja od kojeg se nešto traži kao i komunikacijski kanal kojim je napadana infrastruktura povezana na Internet, a s posljedicom „izgladnjivanja“ resursa (CPU ciklusi, memorija i komunikacijski kanal). [3]

Činjenica da je Internet izgrađen od konačnog broja mrežnih komponenata te da računalni sustavi ne raspolažu s neograničenim količinama procesne moći, pridonosi ishodima ovakvih napada. Iako je najčešće razlog zlonamjeran, napadi uskraćivanjem usluga nisu orijentirani prema stjecanju pristupa nedozvoljenim informacijama i podatcima ili drugim sigurnosnim te financijskim iskorištavanjima. Napadači DoS napade izvršavaju prvenstveno kako bi se međusobno dokazali ili kako bi nanijeli štetu napadnutim organizacijama. Iz tih napada oni nemaju nikakvu financijsku korist, ali napadnute organizacije često mogu imati velike štete. Štete se mjere u financijskim brojkama kao rezultat nemogućnosti poslovanja i potrebe za ulaganjem u sigurnosnu zaštitu, ali i u nefinancijskim mjerama pri čemu se prvenstveno misli na gubitak ugleda među klijentima i partnerima. [3]

Napadi uskraćivanjem usluga najčešće se obavljaju od strane udaljenih napadača pa se globalno dijele na dvije skupine prema sloju, odnosno, nivou sedmo-slojnog ISO/OSI modela na kojeg su usmjereni. Na taj način obično ih se dijeli u dvije skupine:

- napadi usmjereni na aplikacijski sloj i
- napadi usmjereni na mrežne resurse, odnosno mrežni sloj. [3]

V. DISTRIBUIRANI NAPADI USKRAĆIVANJEM USLUGA (DDoS)

Ovaj napad predstavlja jedan od najkontroverznijih, najkompleksnijih te najozbiljnijih napada. Izraz DDoS označava oblik napada uskraćivanjem usluga u kojem su izvori mrežnog prometa (napada) distribuirani na više mjesta diljem Interneta. Ta računala iz kojih se obavlja napad nisu u vlasništvu napadača, već žrtava koja, u pravilu, nisu svjesne da se njeno računalo koristi za napade protiv drugih računala i sustava. Najčešće se radi o računalima koja sadrže neku ranjivost što omogućuje napadaču razbijanje sustava zaštite te širenje zlonamjernog koda. Nakon toga računalo je u vlasti napadača koji jednom naredbom pokreće DDoS napad s mnogih provaljenih računala na ciljano računalo. [4]

DDoS napad uključuje mnoge strane - dobavljače programske podrške koji požuruju plasiranje nesigurne programske podrške na tržište, korisnika koji ne primjenjuje zakrpe koje se izdaju kao odgovor na eventualne propuste u programima i operacijskim sustavima, te ne ažurira antivirusne programe i ne koristi vatrozid, ISP-ovi (ISP = engl. *Internet Service Provider*, pružatelj Internet usluga) koji automatski ne pregledavaju dodatke e-pošte kako bi otkrili zloćudan kôd ili blokirali komunikacijska vrata (engl. *port*) na računalima klijenata, osobe koje iskorištavaju nakupljenu ranjivost u sustavu tako da pišu i šire zloćudni kôd i na kraju ga koriste za pokretanje DDoS napada (glavni mozak) i žrtve DDoS napada. Svaka od ovih strana bi mogla poduzeti određene korake i smanjiti vjerojatnost DDoS napada. [5]

DDoS napadi uključuju prvotno provaljivanje u stotine ili tisuće računala putem Interneta. Nakon toga, napadač instalira DDoS program na sve njih, čime zadobije

kontrolu nad njima za pokretanje koordiniranog napada na krajnju žrtvu. Ti napadi obično iskorištavaju kapacitet usmjerivača ili mrežne resurse što prekida povezanost mreže i korisnika. Da bi pokrenuo DDoS napad, zlonamjerni korisnik prvo mora izgraditi mrežu računala koja će se koristiti za stvaranje velikog prometa koji je potreban da bi se onemogućila usluga legitimnim korisnicima. Da bi stvorili ovu mrežu, napadači otkrivaju ranjive aplikacije (kao što su npr. web stranice) ili poslužitelje. Ranjivi poslužitelji su oni koji sadrže sistemsku programsku podršku s poznatim ranjivostima, ne sadrže antivirusne programe, sadrže antivirusne programe starijih inačica ili oni koji nisu ispravno konfigurirani. Napadači iskorištavaju takve ranjivosti poslužitelja kako bi dobili pristup. Sljedeći korak napadača je instaliranje novih programa (alati za izvršavanje napada) na ugrožene poslužitelje. Poslužitelji u kojima su pokrenuti takvi alati za izvršavanje napada nazivaju se *zombi* računala (engl. *zombies*), a mogu obaviti svaki napad koji im naredi napadač. Mnoštvo zombi računala naziva se „vojska zombija“ (engl. *zombi army*). Pored poslužitelja, napadač još više, ali po skoro istom principu preuzima kontrolu nad tisućama osobnih računala, njihove korisnike dodatno mameći raznim sadržajima na opasna web sjedišta ili na instaliranje maligne programske podrške prikrivenih funkcija.

Napad počinje probijanjem u slabo osigurana računala, koristeći poznate greške u standardnim mrežnim uslužnim programima te slabu konfiguraciju u operacijskim sustavima. Na svakom sustavu, nakon provale, napadač obavlja neke dodatne korake. Prvi korak je instaliranje programa kako bi se prikrila provala u sustav te kako bi se sakrili svi tragovi njegovih naknadnih aktivnosti. Na primjer, standardne naredbe za prikazivanje procesa koji su pokrenuti, zamijenjeni su inačicom koja ne prikazuje procese napadača. Svi ti alati imaju zajednički naziv „*rootkit*“, jer nakon instalacije preuzimaju administratorske ovlasti. Tada se instalira poseban proces koji se koristi za udaljenu kontrolu računala. Ovaj proces prima naredbe preko Interneta i kao odgovor na ove naredbe pokreće napad putem Interneta prema određenoj žrtvi. Rezultat ovoga automatiziranog procesa je stvaranje mreže koja se sastoji od rukovoditeljskih (engl. *master*) i posredničkih (engl. *slave*, *daemon*) strojeva. Svaki napadač mora raditi s adrese koja se najčešće ipak može povezati s njegovim identitetom. Stoga će oprezni napadač početi razbijanje sa samo nekoliko računala, a zatim ih koristiti za razbijanje više novih računala te ponavljanjem ovog ciklusa smanjiti mogućnost da bude otkriven. Vrijeme napada za napadača traje samo jednu naredbu koja pokreće pakete naredbi da svi zarobljeni strojevi pokrenu određeni napad na određeni cilj. [4]

V. TAKSONOMIJA DDoS NAPADA

Kako bi raščlanili taksonomiju distribuiranog napada uskraćivanjem usluga, promatramo sredstva koja se koriste za pripremu napada, karakteristike napada i učinak napada na žrtvu [6]. Ukupnost taksonomije vidljiva je na sl. 1.

Klasifikacija prema stupnju automatizacije

Tijekom priprema za napad, napadač mora pronaći potencijalno računalo - *agenta* i zaraziti ga zlokobnim kôdom. Oslanjajući se na stupanj automatizacije prilikom napada, razlikujemo: ručni, polu-automatizirani i automatizirani DDoS napad.

Ručni napad

Samo rani DDoS napadi su spadali u ovu kategoriju. Napadač je skenirao udaljena računala kako bi pronašao ranjivost, provalio u njih i instalirao zlokoban kôd. Zatim bi upravljao računalom i izvršio napad.

Polu-automatizirani napad

DDoS mreža se ovdje sastoji od rukovoditelja i agenata – posredničkih računala. Napadač postavlja automatizirane skripte za skeniranje i kompromitiranje tih računala i instalaciju malicioznog kôda. Tada koristi računala - rukovoditelje kako bi odredio vrstu napada i žrtvinu adresu i kako bi zapovijedao napad svojim agentima (posredničkim računalima) koji šalju pakete žrtvi. Oslanjajući se na mehanizam komunikacije koji se uspostavlja između računala - agenta i računala - rukovoditelja, poluautomatizirane napade dijelimo na napade s direktnom komunikacijom i napade s indirektnom komunikacijom.

Napadi s direktnom komunikacijom

Tijekom napada s direktnom komunikacijom, računalo - agent i računalo - rukovoditelj međusobno moraju znati identitet jedan drugog kako bi mogli komunicirati. To se postiže tako da se IP adresa računala - rukovoditelja kôdira (engl. *hard-coding*) u maliciozan kôd koji se kasnije instalira računalu - agentu. Svako računalo - agent tada javlja spremnost računalima - rukovoditeljima koja zatim spremaju IP adrese agenata u datoteku za buduću upotrebu. Nedostatak ovog pristupa je to što pronalazak jednog kompromitiranog računala može dovesti do razotkrivanja cijele DDoS mreže. Pošto agenti i rukovoditelji slušaju mrežne veze, podložni su identifikaciji mrežnih skenera.

Napadi s indirektnom komunikacijom

Napadi s indirektnom komunikacijom postavljaju nivo neizravnosti kako bi se povećalo preživljavanje DDoS mreže. Nedavni napadi prikazuju primjer napada koji koriste IRC kanale za komunikaciju agent/rukovoditelj. Korištenje IRC usluga zamjenjuje funkciju rukovoditelja jer IRC kanal nudi dostatnu anonimnost za napadača. DDoS agenti uspostavljaju vanjske veze sa standardnim uslužnim portovima koje koriste legalne mrežne usluge. Zbog toga se komunikacija agenta s kontrolnom točkom teško može razlikovati od legalnog mrežnog prometa. Agenti ne sadrže slušni port koji se inače lako otkriva pomoću mrežnih skenera. Napadač kontrolira agente pomoću IRC komunikacijskih kanala. Dakle, otkrivanje jednog agenta ne može voditi nikamo dalje, već samo do identifikacije jednog ili više IRC poslužitelja i imena kanala koje koristi DDoS mreža. Daljnje otkrivanje agenata od ove točke ovisi o mogućnosti praćenja agenata koji su trenutno spojeni na IRC poslužitelj. Pored IRC poslužitelja, i usluge trenutnih poruka IM (engl. *Instant Messaging*) podložne su tim zlouporabama. Ne postoji vidljiv razlog zašto napadači ne bi mogli koristiti/prenamijeniti i druge legitimne usluge za slične svrhe.

Automatizirani napadi

Automatizirani DDoS napadi dodatno automatiziraju fazu napada te tako izbjegavaju potrebu za komuniciranjem između računala - napadača i računala - agenata. Vrijeme početka napada, vrsta napada, trajanje

napada i adresa žrtve su pred-programirane u malicioznom kôdu. Očito je da takva postava mehanizama napada nudi minimalno izlaganje napadača, jer je napadač uključen samo u pokretanju jedne naredbe - početak napada. Specifikacija kôdiranog napada podrazumijeva samo jednu svrhu DDoS mreže. No, mehanizmi širenja obično ostavljaju stražnji ulaz (engl. *backdoor*) na uključenom računalu te tako omogućavaju lak pristup u budućnosti i eventualnu promjenu malicioznog koda. Polu-automatizirani i automatizirani napadi uključuju računala - agente koristeći automatske tehnike skeniranja i širenja.

Prema strategijama skeniranja razlikujemo napade koji se temelje na slučajnom skeniranju, skeniranju popisa podataka (engl. *hitlist*), topološkom skeniranju, razmjernom skeniranju i skeniranju lokalne podmreže. Napadači obično kombiniraju faze skeniranja i iskorištavanja te tako dobivaju veću populaciju agenata.

Prema mehanizmu širenja u malicioznom kodu razlikujemo napade koji postavljaju širenje iz središnjeg izvora, potajno širenje i autonomno širenje. Tijekom napada sa širenjem iz središnjeg izvora maliciozan kod je smješten na središnjem poslužitelju ili nekoliko njih. Nakon kompromitiranja računala - agenta šifra se preuzima sa središnjeg izvora kroz mehanizam za prijenos datoteka. Tijekom napada sa potajnim širenjem, šifra za napad se preuzima sa računala koje se koristilo za iskorištavanje sustava. Zaraženo računalo tada postaje izvor za sljedeći korak širenja. Potajno širenje lakše opstaje od napada sa širenjem iz središnjeg izvora jer koristi više točaka te tako izbjegava samo jednu točku koja može značiti neuspjeh. Napadi sa autonomnim širenjem izbjegavaju korak povratka datoteka tako što šalju upute za napad direktno u metu domaćina tijekom faze iskorištavanja.

Klasifikacija prema iskorištenoj ranjivosti

Distribuirani napadi uskraćivanjem usluge iskorištavaju različite strategije kako bi uskratili uslugu žrtvi ili žrtvinim klijentima. Prema ranjivosti na koju se cilja tokom napada razlikujemo protokolarne napade i napade grubom silom.

Protokolarni napadi

Protokolarni napadi iskorištavaju specifičnu značajku ili implementacijski „bug“ nekog protokola koji se instalira na žrtvino računalo kako bi se dobio pristup njegovim izvorima. Primjeri uključuju TCP SYN napad, CGI zahtjev za napad i autentifikacijski napad na poslužitelju. U TCP SYN napadu značajka koja se iskorištava jest dodjeljivanje veće količine prostora u redu za vezu odmah nakon što primatelj da zahtjev za TCP SYN. Napadač inicira višestruke veze koje nikada nisu završene te tako ispunjava red za vezu u beskonačnost. U napadu CGI zahtjeva, napadač troši vrijeme CPU-a žrtve tako što izdaje višestruke CGI zahtjeve. Kod napada sa ustanovljivanjem vjerodostojnosti poslužitelja, napadač iskorištava činjenicu da proces provjere vjerodostojnosti potpisa troši značajno više resursa nego generiranje lažnog potpisa. On šalje mnogobrojne lažne zahtjeve za provjerom vjerodostojnosti poslužitelju te tako veže njegove resurse.

Napadi grubom silom

Napadi grubom silom (engl. *Brute Force*) izvode se tako da se pokreće velika količina prividno legitimnih transakcija. Kako „*upstream*“ mreža može donijeti veći promet nego žrtvina mreža može podnijeti, ona iscrpljuje žrtvine resurse. Napade grubom silom dalje dijelimo s obzirom na sadržaje paketa i žrtvine usluge na napade s mogućnošću filtriranja i na napade bez mogućnosti filtriranja. Napadi s mogućnošću filtriranja su lažni paketi i paketi za nekritične službe/usluge žrtvinog rada, te se mogu filtrirati u vatrozidu (engl. *firewall*). Napadi bez mogućnosti filtriranja koriste pakete koji šalju zahtjeve legitimnim uslugama od strane žrtve. Tako se filtriraju svi paketi koji odgovaraju potpisu napada što vodi trenutnoj zabrani pristupa određenoj službi i za napadače, ali i za žrtve. Primjeri takvih napada su HTTP zahtjev za poplavom Web poslužitelja ili DNS zahtjev za poplavom imeničkih poslužitelja.

Granica između protokolarnog napada i napada grubom silom vrlo je tanka. Protokolarni napadi preplavljuju žrtvine resurse zahtjevima za suvišnim prometom, a loše dizajnirane odrednice protokola na domaćinima se često koriste za „odbijene“ napade sirovom snagom poput DNS napada ili *Smurf* napada. Razlika je u tome što žrtva može umanjiti učinke protokolarnih napada mijenjajući postavljene protokole za njegovu stranicu, ali je zato bespomoćna kod napada grubom silom, jer oni zloupotrebljavaju legalne i legitimne usluge (napadi bez mogućnosti filtriranja) ili zbog svojih vlastitih ograničenih resursa (žrtva ne može ništa protiv napada koji zamjenjuje širokopojasnu mrežu). Napadi sirovom snagom moraju stvoriti mnogo veći opseg paketa za napad nego protokolarni napadi kako bi mogli žrtvi nanijeti štetu. Promjenom postavljenih protokola žrtva podiže granicu otpornosti.

Klasifikacija prema dinamici mjera napada

Prema dinamici mjera napada razlikujemo neprekidne i promjenjive mjere napada.

Neprekidne mjere napada

Većina poznatih napada postavlja neprekidne mjere napada. Računala-agenti generiraju pakete za napad punom snagom. Ova neočekivana poplava ometa žrtvine usluge vrlo brzo te vodi k otkrivanju napada.

Promjenjive mjere napada

Promjenjive mjere napada su opreznije u svojem namještanju i mijenjaju mjere napada kako bi izbjegle otkrivanje i odgovor. Prema mehanizmu promjene mjera napada razlikujemo napade sa rastućim mjerama i napade sa nestalnim mjerama. Kod napada čije mjere postepeno rastu sporije se iskorištavaju žrtvini resursi. Promjena stanja žrtve može biti tako spora i postupna da se ni nakon dužeg perioda napad ne može otkriti. Napadi s nestalnim mjerama prilagođavaju mjere napada prema žrtvinom ponašanju, ponekad smanjujući učinak kako bi se izbjeglo otkrivanje napada. Na krajnjem mjestu je ekstremni slučaj pulsnih napada. Tijekom pulsnih napada agenti - domaćini u vremenskim intervalima prekidaju napad kako bi ga nastavili kasnije. Ako je ta akcija simultana za sve agente, tada žrtva doživljava povremene prekide veze sa službama. Ako su agenti podijeljeni na grupe koje su koordinirane tako da je jedna grupa uvijek aktivna, tada žrtva doživljava stalno uskraćivanje usluge.

Klasifikacija prema utjecaju

Ovisno o utjecaju DDoS napada na žrtvu razlikujemo raskidajuće i oduzimajuće napade

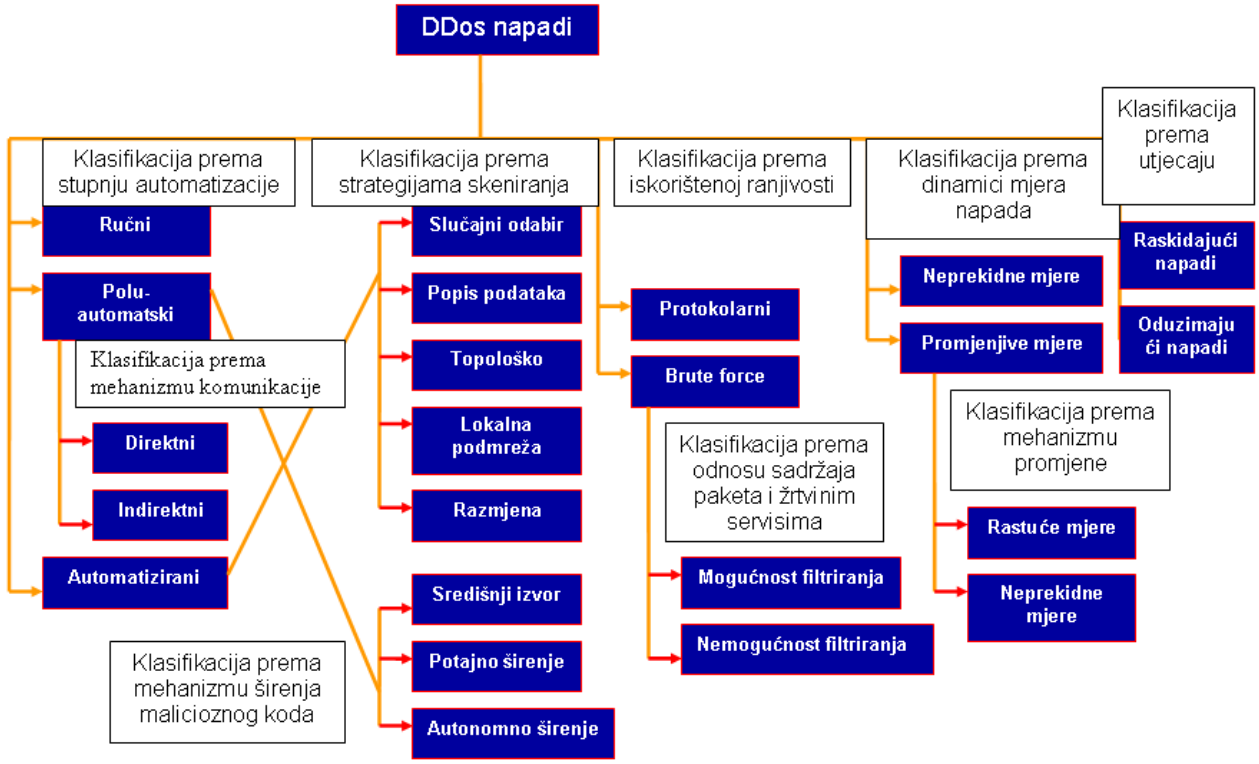
Raskidajući napadi

Cilj ovih napada je da se žrtvine usluge potpuno uskrate njezinim klijentima. Svi do sada poznati napadi spadaju u ovu skupinu napada.

Oduzimajući napadi

Cilj ovih napada bila bi potrošnja nekih (pretpostavimo konstantna) dijelova žrtvinih resursa. Kako ovi napadi ne vode potpunom uskraćivanju usluge, mogu ostati neotkriveni veći dio vremena. S druge strane, šteta nanesena žrtvi može biti ogromna. Npr., napad koji uzima 30 % žrtvinih resursa mogao bi dovesti do uskraćivanja usluge određenom postotku klijenata ili bi joj pala kvaliteta.

Neki klijenti, nezadovoljni kvalitetom, mogu promijeniti svog dobavljača usluge i žrtva gubi prihod.



Sl. 1. Taksonomija DDoS napada

VI. ZAKLJUČAK

U hrvatskom govornom području, u postojećoj ICT literaturi, tema DDoS je vrlo slabo zastupljena, kao i sigurnosti ICT uopće. S obzirom na prisutnost i posljedice pojave DDoS, autori smatraju da joj se posvećuje premalo pažnje. Štetnost ovih napada, posebno u gospodarstvu, državnim uslugama i uslužnom sektoru općenito, nalaže nužnost osvješćivanja korisnika o posljedicama istih, te edukacije o načinima smanjenja mogućnosti da i sami (nenamjerno i nesvjesno) ne postanu dio sustava koji provodi distribuirane napade uskraćivanjem usluga.

LITERATURA

[1] Pleskonjić, D. i dr., *Sigurnost računarskih sistema i mreža*, Mikro knjiga, Beograd, 2007.

[2] -, *OSI model*, Wikipedeia, 29. ožujak 2010., <http://en.wikipedia.org/wiki/OSI_model>, veljača 2009.

[3] -, *Napadi uskraćivanjem resursa*, +CERT.hr, 17. kolovoz 2006. < http://www.cert.hr/documents.php?id=253>, veljača 2009.

[4] -, *DDoS napad*, +CERT.hr, 26. rujan 2008. <http://www.cert.hr/documents.php?id=347>, veljača 2009.

[5] Chandler, J., *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, University of Ottawa, <http://www.uoltj.ca/articles/vol1.1-2/2003-2004.1.1-2.uoltj.Chandler.231-261.pdf>, veljača 2009.

[6] Mirkovic, J., Martin, J., Reiher, P., *A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms - UCLA CSD Technical Report no. 020018*, D-WARD Project Home Page, <http://www.lasr.cs.ucla.edu/ddos/>, veljača 2009.