CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# DDoS napad

## CCERT-PUBDOC-2008-09-240

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

## **CARNet CERT**, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

## **LS&S**, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

# 1. Uvod

Budući da u današnje vrijeme o Internetskim uslugama ovise razne tvrtke, djelatnosti, organizacije pa i obični korisnici, uskraćivanje usluga nekog poslužitelja dovodi do velikih gubitaka. Zbog toga možemo reći da su se Distribuirani Denial of Service [DDos] napadi pojavili kao jedna od najatraktivnijih, ako ne i najvećih slabosti Interneta.

Izraz DoS (eng. Denial of Service) označava napad uskraćivanja usluga. Takav napad karakterizira namjerno generiranje velike količine mrežnog prometa da bi se zasitili mrežni resursi i poslužitelji. Zbog prevelikog opterećenja oni više nisu u stanju pružati namijenjene usluge. Posljedica toga je nemogućnost legitimnih korisnika da koriste mrežne usluge poput: e-mail, weba i sl.

Izraz DDoS (eng. Distributed Denial of Service) 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 neka žrtva koja u pravilu i nije svjesna 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. Postoje razni alati koji omogućavaju automatizirano izvođenje napada, ali i alati koji služe u svrhu zaštite od takvih napada.

U ovom dokumentu ukratko je opisan DoS napad, kao i njegove osnovne vrste. Zatim je dan opis DDoS napada i nekih metoda tog napada. Slijedi usporedba DoS i DDoS napada prema načinu izvođena napada, prednostima te korištenim računalima. Također prikazan je kratak pregled poznatijih slučajeva DDoS napada u Hrvatskoj i svijetu. Na kraju su opisani osnovni alati za automatizaciju DDoS napada, kao i za zaštitu od napada.

# 2. DoS napad

DoS (eng. Denial of Service) napad ili napad uskraćivanja usluga je pokušaj napadača da učini nedostupnim računalo korisnicima kojima su namijenjene njegove usluge. Iako načini, motivi i ciljevi DOS napada mogu varirati, općenito napad se sastoji od napora jedne ili više osoba kako bi trajno ili privremeno spriječila efikasno funkcioniranje Internet stranice ili usluge. Počinitelji DoS napada obično ciljaju lokacije ili usluge web poslužitelja kao što su banke i DNS poslužitelji. Jedan od uobičajenih metoda napada uključuje zasićenje ciljanog uređaja s vanjskim komunikacijskim zahtjevima na način da uređaj ne može odgovoriti ili odgovara tako polako da postaje nedostupan. DoS napad je implementiran kako bi prisilio računalo da iskoristi resurse tako da ne može pružiti usluge namijenjene korisnicima.

Izvođenje denial-of-service napada smatra se kršenjem *Internet Proper Use Policy* pravila, ali također označava i kršenje zakona pojedinih nacija.

## *2.1. Osnovna obilježja*

*United States Computer Emergency Readiness Team* definira simptome DoS napada kao:

- neuobičajena sporost mreže (prilikom otvaranja datoteke ili pristupanja web stranicama),
- nedostupnost određene web stranice,
- nemogućnost pristupa bilo kojoj web stranici,
- drastično povećanje broja primljenih "*spam*" poruka elektroničke pošte (ovaj tip DoS napada se naziva "*Mail-Bomb*").

Važno je za napomenuti da ne spadaju svi gubici usluga, čak ni oni izazvani nedozvoljenim radnjama, u skupinu DoS napada. Neke metode napada mogu uključivati uskraćivanje usluga kao jednu komponentu cjelokupnog napada.

Denial-of-service napad također može dovesti do problema u granama (eng. branches) mreže oko napadnutog računala. Na primjer, komunikacijski kapacitet (eng. bandwidth) jednog usmjerivača između Interneta i LAN-a (eng. Local area network) može biti potpuno iskorišten prilikom napada kako bi se kompromitirala cijela mreža. Kada je napad proveden, cijela regija Interneta može biti ugrožena čak i bez znanja ili namjere napadača zbog nepravilne konfiguracije ili slabe mrežne infrastrukture.

DoS napad karakterizira eksplicitan pokušaj napadača da spriječi legitimnim korisnicima usluga korištenje tih usluga. Napadi mogu biti usmjereni na bilo koji mrežni uređaj, uključujući usmjerivače, poslužitelje elektroničke pošte ili DNS (eng. Domain Name System) poslužitelje.

DoS napad može biti počinjen na različite načine, a pet osnovnih tipova napada su:

1. Potrošnja računalnih resursa, kao što su komunikacijski kapacitet, diskovni prostor, ili procesorsko vrijeme.
2. Poremećaj konfiguracijskih podataka, kao što je usmjeravanje informacija.
3. Poremećaj informacija o stanju (eng. state information), kao što je neželjeno ponovno postavljanje (eng. reset) TCP veze.
4. Poremećaj fizičke komponente mreže.
5. Prekid komunikacije između legitimnih korisnika, tako da oni više ne mogu komunicirati na odgovarajući način.

DoS napad može uključivati izvršenje zlonamjernih programa namijenih za:

- maksimalno korištenje procesora kako bi se sprečavala bilo koja operacija,
- pokretanje pogreške u mikroprocesoru,
- pokretanje pogreške u redoslijedu naredbi kako bi računalo prešlo u nestabilno stanje,
- iskorištavanje pogreške u operacijskom sustavu da bi se uzrokovalo "izgladnjivanje" (eng. resource starvation) tj. korištenje svih dostupnih objekata tako da pravi posao ne može biti završen,
- rušenje samog operacijskog sustava,
- pokretanje posebno oblikovanih HTML datoteka koje navode korisnika da posjete web stranice mnogo puta sve dok se ne prekorači dopušteni komunikacijski kapacitet.

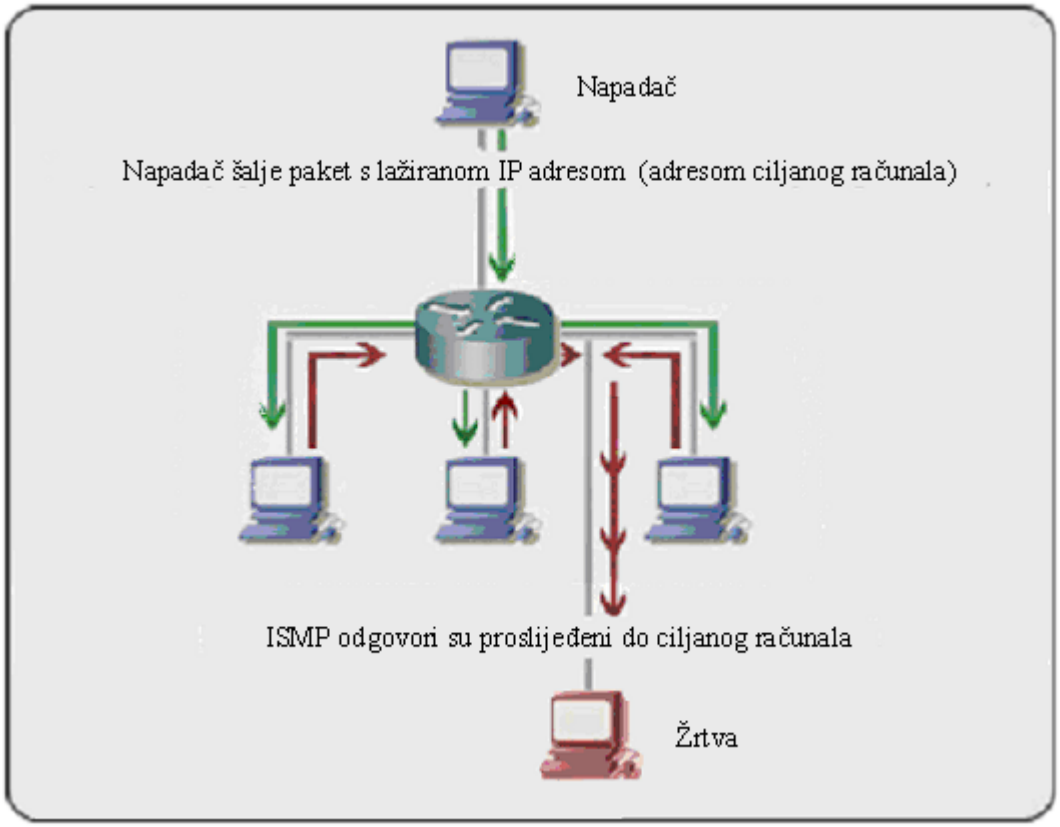
## 2.2. Metode DoS napada

Postoje razne metode izvođenja DoS napada, a najvažnije su ukratko opisane u nastavku.

### 2.2.1. ICMP fwuds

ICMP fwuds se odnosi na napade poplavljivanjem, slanjem velikog broja paketa na poslužitelje kako bi se iskoristili svi raspoloživi resursi.

**"Smurf" napad** je jedna posebna inačica poplavljujućih (eng. flooding) DoS napada na javni Internet. On iskorištava loše konfigurirane mrežne uređaje koji omogućuju slanje paketa na sve poslužitelje određene mreže putem adrese razašiljanja (eng. broadcast). Mreža tada služi kao "smurf" pojačalo. U tom napadu, počinitelji šalju veliki broj IP paketa s izvorišnih adresa koje su lažirane da bi izgledale kao adresa žrtve. Komunikacijski kapacitet mreže se brzo iskoristi što sprečava legitimne pakete da stižu do svog odredišta. Primjer takvog napada prikazan je na slici 1.




**Slika 1.** Scenarij "Smurf" napada

**Ping poplavljivanje** temelji se na slanju mnogo „ping" paketa, obično koristeći "ping -f" naredbu. Vrlo se jednostavno pokreće, a primarni uvjet je da napadač ima pristup većoj širini pojasa nego žrtva.

Prilikom **SYN poplavljivanja** šalje se niz TCP / SYN paketa, često s lažiranom adresom pošiljatelja. Svaki od tih zahtjeva žrtva tretira kao zahtjev za vezu, što uzrokuje napola otvorene veze slanjem natrag TCP / SYN-ACK paketa te čekanjem paketa s adrese pošiljatelja. Međutim, budući da je adresa pošiljatelja lažna, odgovor nikad ne dolazi.

### 2.2.2. Teardrop napad

"Teardrop" napad uključuje slanje oštećenih IP fragmenata s preklapanjem (eng. overlapping) na ciljano računalo. Nedostatak u kodu za TCP / IP fragmentaciju u brojnim operacijskim sustavima uzrokuje nepravilno rukovanje fragmentima te pad sustava kao rezultat toga. IP (eng. Internet

Protocol) paket koji je preveliki za usmjeritelj dijeli se na fragmente. U fragmente paketa upisuje se udaljenost od početka prvog paketa, što omogućuje ponovno sastavljanje paketa na drugoj strani. U ovom napadu napadač postavlja zbunjujuću udaljenost u jedan od fragmenata. Ako poslužitelj koji prima takav paket nema plan za takav slučaj rezultat će biti pad sustava. Ovim napadom ugroženi su Windows 3.1.x, Windows 95 i Windows NT operacijski sustavi, kao i inačice Linux operacijskog sustava s jezgrom (eng. kernel) starijom od 2.0.32 i 2.1.63.

### 2.2.3. Stalni DoS napadi

Stalni DoS napadi (PDoS – Permanent Denial of Service) je napad koji ošteti sustav tako jako da zahtijeva zamjenu ili ponovnu instalaciju fizičkih komponenti računala (eng. hardware). PDoS napad iskorištava sigurnosne nedostatke na udaljenim upravljačkim sučeljima bilo da su to usmjerivači, pisači ili drugo mrežno sklopovlje. Za razliku od DDoS napada, koji je usmjeren na uskraćivanje usluga ili rada web stranica, PDoS je usmjeren izravno na uništavanje računalnih komponenti.

Razvio ga je tim programera pod vodstvom jednog od zaposlenika Hewlett-Packard-Systems Security Lab-a Rich Smitha. Također, razvili su i alat PhlashDance koji se koristi za detekciju i prikaz PDoS ranjivosti.

### 2.2.4. Poplavljivanje na razini aplikacije

Razne ranjivosti koje omogućuju DoS stanja, kao što je prepisivanje spremnika (eng. buffer overflow), mogu uzrokovati zauzeće prostora na disku ili zauzimanje svih raspoloživih resursa memorije ili CPU vremena. Neke vrste DoS napada se oslanjaju prvenstveno na "brute force" napad, poplavljujući cilj s tokom paketa te zasićujući vezu ili preopterećujući resurse računala. Poplavljivanje zasićivanjem resursa oslanja se na činjenicu da napadač ima na raspolaganju veću širinu pojasa od žrtve. Čest način postizanja ovog napada danas je distribuirani DoS napad korištenjem *botnet*-a. „Botnet" je izraz koji se koristi za skupinu ugroženih računala (zvanih Zombi računala) na kojima je pokrenut zlonamjerni kod. Ostala poplavljivanja mogu koristiti određene vrste zahtjeva da bi zasitili resurse, na primjer, okupiranje maksimalnog broja otvorenih veza ili punjenje žrtvinog diskovnog prostora.

**"Banana" napad** je još jedan posebni tip DoS napada, a uključuje preusmjeravanje odlaznih korisničinih poruka natrag klijentu, sprečavanje vanjskog pristupa, kao i poplavljivanje klijenta poslanim paketima.

**'Pulsing zombie'** je izraz koji se odnosi na posebnu vrstu DoS napada kada je mreža podvrgnuta višestrukim *ping* porukama. Takvo stanje rezultira degradiranom kvalitetom usluga i povećanim korištenjem resursa. Ovu vrstu napada je teško otkriti.

### 2.2.5. Nuke

"Nuke" je stari DoS napad računalnih mreža koji se sastoji od slanja fragmentiranih ili oštećenih ICMP paketa na cilj. Postiže se pomoću modificiranog ping alata za višekratno slanje tih paketa čime usporavaju zahvaćeno računalo sve dok ne dođe do potpunog prekida.

Poseban primjer "nuke" napada je WinNuke, koja iskorištava ranjivosti u NetBIOS modulu u operacijskom sustavu Windows 95. Slanjem niza *out-of-band* podataka na TCP priključak (eng. port) 139 ciljanog uređaja uzrokuje zaključavanje računala i prikaz "Blue Screen of Death" poruke (tj. prestanak rada operacijskog sustava računala).

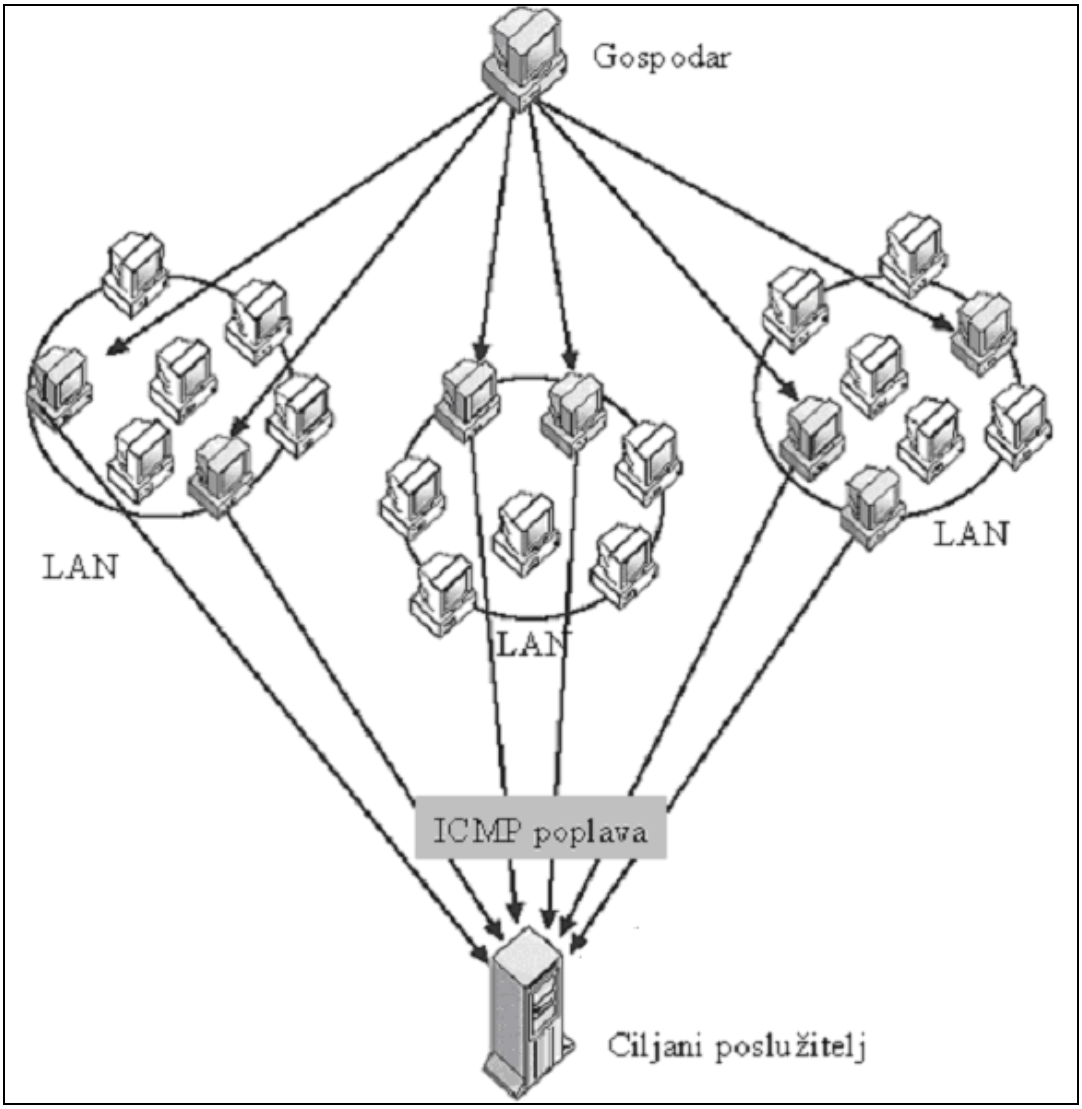
# 3. DDoS napad

Distribuirani napad uskraćivanja usluga (DDoS - distributed denial of service) nastaje kada više (prethodno) kompromitiranih sustava poplavljuje resurse ciljanih sustava, obično jednog ili više web poslužitelja. Napadač počinje DDoS napad iskorištavanjem ranjivosti jednog sustava te stvara DDoS „gospodara“ (eng. master). Zatim komunicira s ostalim sustavima koji su ranjivi te učitava posebne alate na mnoge, a ponekad i tisuće, sustava čiju je ranjivost uspio iskoristiti. Jednom naredbom napadač pokreće brojne napade poplavljivanja paketima na ciljano računalo što uzrokuje uskraćivanje usluga.

Razni zlonamjerni programi mogu u sebi nositi mehanizme DDoS napada, a jedan od poznatih primjera za to je računalni virus „MyDoom“ čiji se mehanizam pokreće u određeno vrijeme određenog datuma. Korisnički sustav, žrtva, može također biti ugrožen zlonamjernim programom iz vrste trojanaca (eng. trojan), koji od napadača preuzima *Zombi* agenta.

## *3.1. Opća obilježja*

DDoS napadi uključuju provaljivanje u stotine ili tisuće računala putem Interneta. Nakon toga, napadač instalira DDoS program na sve njih, čime dobije 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. Scenarij jednog DDoS napada prikazuje slika2.




**Slika 2.** DDoS napad

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 operacijske sustave i sistemske programe 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 (eng. zombies), a mogu obaviti svaki napad koji im naredi napadač. Mnogo zombi računala naziva se vojska zombija (eng. zombi army).

Znači, 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 su zamijenjeni 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 (eng. master) i posredničkih (eng. 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. Također, i kada napadač odluči prekinuti napad on treba poslati samo jednu naredbu.

### 3.1.1. Otkrivanje ranjivih poslužitelja

Napadači mogu koristiti razne tehnike kako bi pronašli ranjive poslužitelje:

- Skeniranje slučajnim odabirom (eng. Random scanning) – uređaj na kojem je pokrenut zlonamjerni kod proizvoljno odabire neku IP adresu iz zadanog adresnog prostoga te provjerava ranjivost. Ako pronađe ranjivi poslužitelj pokreće na njemu isti zlonamjerni kod koji je pokrenut na njemu. Prednost ove tehnike je mogućnost brzog širenja zlonamjernog koda, a nedostatak stvaranje velike količine prometa (lakše ga je otkriti).
- Skeniranje pomoću popisa pogodaka (eng. hit-list scanning) – prije početka skeniranja napadač radi popis velikog broja potencijalno ugroženih računala. Skeniranje se obavlja po popisu, a kada se nađe ranjivi uređaj na njemu se pokreće zlonamjerni kod. Popis se dijeli na dva djela i jedna se polovica prepušta novom ugroženom računalu. Prednost ove metode je da se u vrlo kratkom vremenu zlonamjerni kod pokrene na svim ranjivim uređajima na popisu, jer se popis podijeli i smanjuje svaki put kad se pronađe novi ranjivi uređaj.
- Topološko skeniranje (eng. Topological scanning) – pri izvođenju napada ova metoda koristi informacije (URL adrese) pohranjene na otkrivenom ranjivom računalu kako bi pronašla nove ciljeve. Prednost ove tehnike je velika točnost te velika brzina stvaranja vojske.
- Skeniranje lokalne podmreže (eng. Local subnet scanning) – ova vrsta skeniranja djeluje u području iza vatrozida, dijelu koji se smatra zaštićenim od skeniranja. Poslužitelj traži ugrožena računala u svojoj lokalnoj mreži. Prednosti metode su u tome što se može koristiti u kombinaciji s drugim metodama te postiže velike brzine.
- Skeniranje razmjene (eng. Permutation scanning) – sva računala dijele zajednički popis IP adresa. Nakon što je otkriveno i napadnuto novo ranjivo računalo, ono počinje skeniranje s proizvoljnog mjesta u popisu. Može se koristiti u kombinaciji s drugim metodama te postiže velike brzine.

### 3.1.2. Širenje zlonamjernog koda

Metode za širenje zlonamjernog koda te izgradnju mreže za napad možemo podijeliti u tri osnovne skupine:

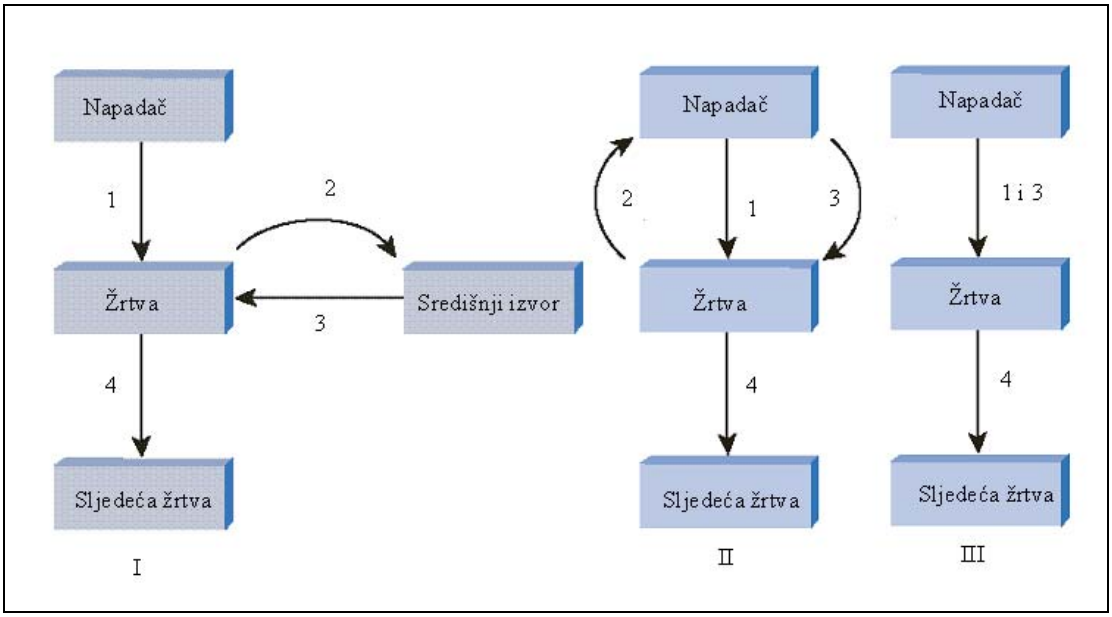
I. Širenje središnjeg izvora (eng. Central source propagation) – nakon otkrivanja ranjivog sustava informacije o tome su prenesene do središnjeg izvora pa se zlonamjerni kod prenosi do novog kompromitiranog sustava.

II. Širenje ulančavanjem unazad (eng. Back-chaining propagation) – u ovoj metodi napadač sam prenosi alat za izvođenje napada do novog ranjivog sustava.

III. Autonomno širenje (eng. Autonomous propagation) – poslužitelj prenosi alat za napad do novo otkrivenog ranjivog sustava u trenutku kada razbije sustav.

Slika 3 daje grafički prikaz metoda širenja zlonamjernog koda. Uz slike naznačeni su koraci koji se izvode prilikom toga:

1. iskorištavanje ranjivosti,
2. prijenos povratnih informacija,
3. širenje koda na ciljano računalo tj. prenošenje alata za napad,
4. ponavljanje radnje s sljedećim ranjivim računalom.




**Slika 3.** Metode širenja zlonamjernog koda

## *3.2. Metode DDoS napada*

DDoS napad možemo podijeliti u dvije osnovne grupe: tipični i reflektirani DDoS napad. Osim toga, postoje još neki oblici napada koji su posebno istaknuti u nastavku.

### 3.2.1. Peer-to-peer napad

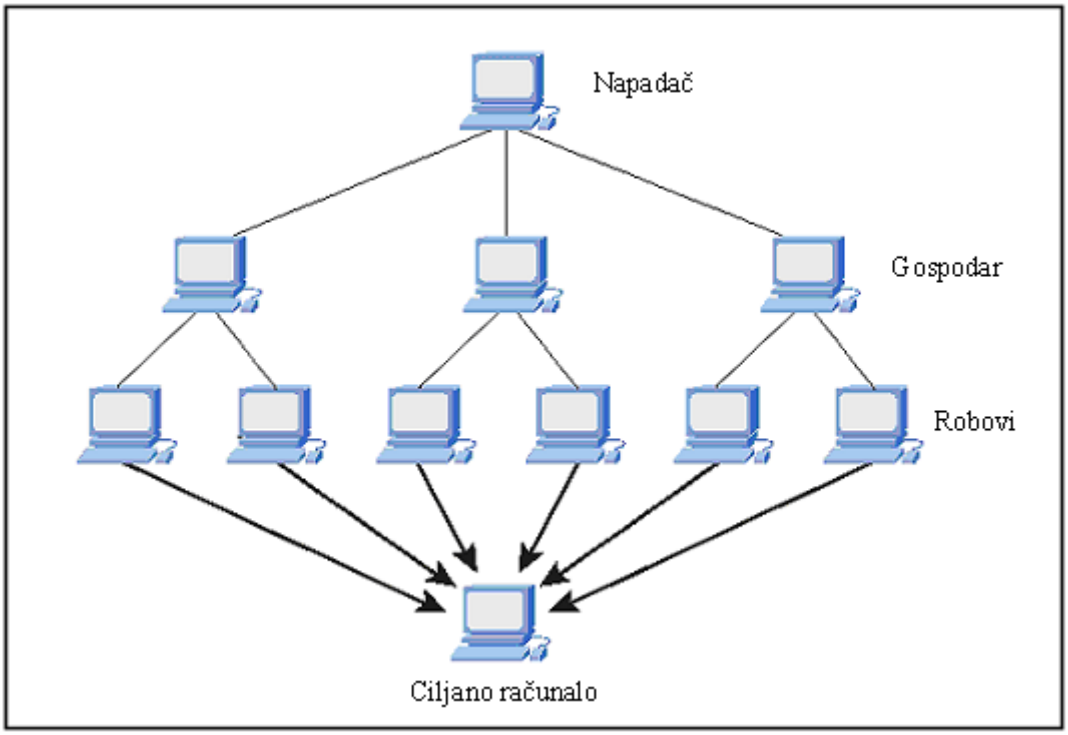
Napadači su otkrili način iskorištavanja nekoliko nedostataka u *peer-to-peer* (veza jedan-na-jedan) poslužiteljima za pokretanje DDoS napada. Prilikom izvođenja napada, napadač nalaže klijentima velikih *peer-to-peer* čvorišta za dijeljenje datoteka da se isključe iz svojih *peer-to-peer* mreža i spoje na žrtvino računalo. Kao rezultat toga, nekoliko tisuća računala može se agresivno pokušati povezati s ciljanim računalom. Iako tipični web poslužitelj može obrađivati nekoliko stotina veza u sekundi prije nego što mu performanse počnu opadati, većina web poslužitelja pada gotovo odmah pri pet ili šest tisuća veza / sec. Prilikom *peer-to-peer* napada web stranica može biti pogođena sa 750.000 veza u kratkom vremenu.

### 3.2.2. DNS Backbone DDoS napad

DNS Backbone DDoS napad je napad u kojem se zlonamjerni korisnik koristi DDoS napadom kako bi razbio jedan ili više DNS poslužitelja. DNS (eng. Domain Name System) poslužitelj služi za prevođenje tekstualnih imena poslužitelja u IP adrese. Izvođenje ovog napada može biti vrlo štetno jer dolazi do velikog gubitka prometa. Napad se izvodi kao i obični DDoS napad samo što se usmjerava protiv DNS poslužitelja.

### 3.2.3. Tipični DDoS napad

U tipičnom DDoS napadu vojska napadača se sastoji od zombi gospodara i zombi robova. Poslužitelji su komprimirani uređaji koji su nastali tijekom procesa skeniranja i sadrže zlonamjerni kod. Napadač koordinira i naređuje gospodaru koji zatim proslijedi naredbu robovima. Konkretnije, napadač šalje naredbu za napad gospodaru i aktivira sve procese napada na tim uređajima, koji su u stanju hibernacije, čekanja na odgovarajuću naredbu da se probude i počnu napad. Zatim gospodari, potaknuti ovim procesima, šalju naredbe za napad robovima naređujući im da počnu DDoS napad na ciljani uređaj. Na taj način, robovi počinju slati veliki obujam paketa na ciljani uređaj, poplavljujući svoje sustave beskorisnim opterećenjem i iskorištavaju svoje resurse. Slika 4 prikazuje ovu vrstu DDoS napada.




**Slika 4.** Tipični DDoS napad

U slučajevima DDoS napada, koriste se lažirane IP adrese izvora u paketima. Napadači preferiraju korištenje takvih krivotvorenih izvornih IP adresa iz dva glavna razloga. Prvi je skrivanje identiteta zombi strojeva da bi napadači sakrili svoj identitet. Drugi razlog odnosi se na izvođenje napada, kada napadači žele onemogućiti bilo koji pokušaj filtriranja prometa na računalu žrtvi.

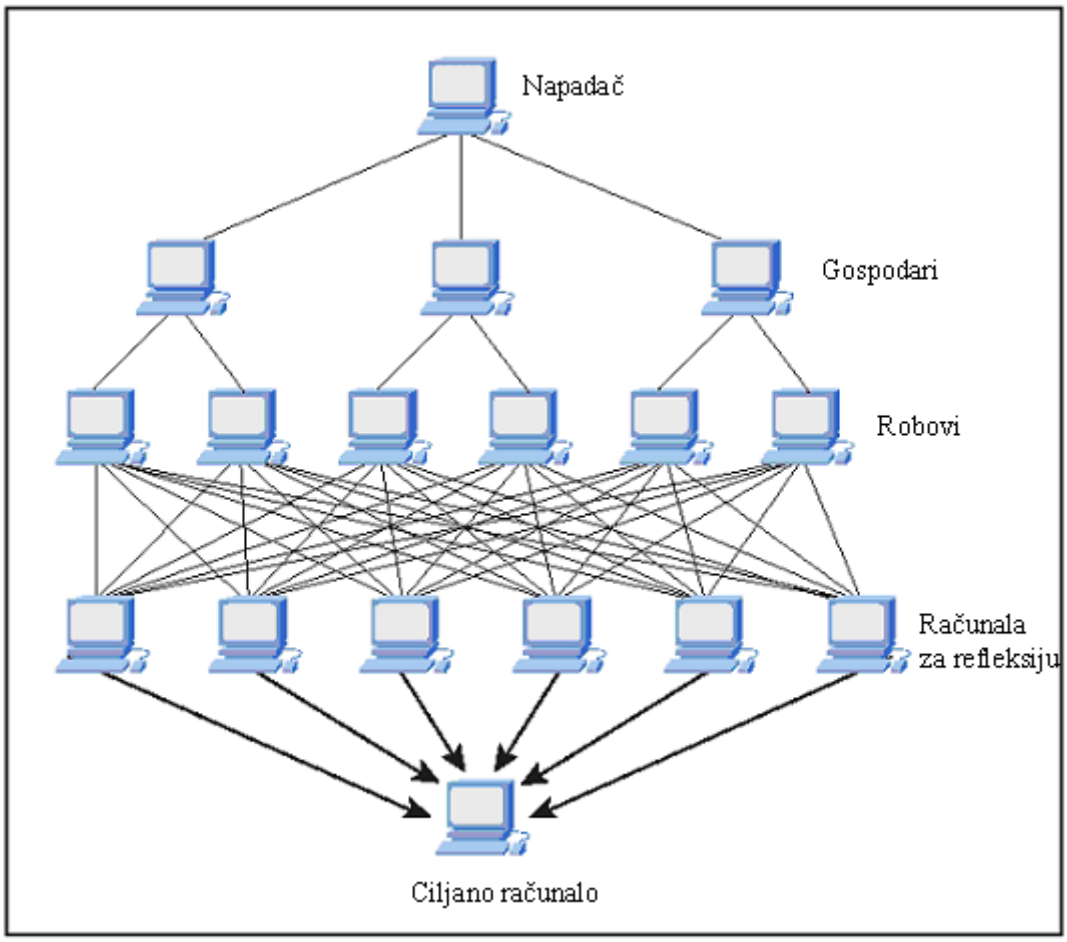
### 3.2.4. DRDoS napad

DRDoS (eng. distributed reflected denial of service) uključuje slanje lažnih zahtjeva na vrlo velik broj računala koja odgovaraju na njih. Izvorišna adresa unutar zahtjeva postavljena je tako da svi odgovori idu na ciljano računalo. Time dolazi do iskorištavanja resursa te uskraćivanja usluga.

DRDoS napad generira istu količinu prometa kao i DDoS napad, ali koristi efikasniju metodu za postizanje toga. Slika 5 prikazuje korake DRDoS napada. Kada poslužitelj prima SYN paket odgovora SYN / ACK paketom – to su prva dva koraka za uspostavu veze. Pri napadu šalje se SYN

paket bilo kojem od javno dostupnih poslužitelja s lažiranom izvornom IP adresom koja pokazuje na ciljanu žrtvu napada. Primatelj SYN paketa generira SYN / ACK i šalje ga žrtvi. Na ovaj način poslužitelj se koristi da bi odražavao pakete na ciljanu mrežu, a ne za slanje paketa izravno na cilj kao što je slučaj u DDoS.

Slično kao i kod DDoS napada koristi se velik broj poslužitelja za slanje SYN paketa koji zatim generiraju veliku količinu prometa. U odnosu na DDoS napad, DRDoS je napad koji može uzrokovati više štete s manjim brojem poslužitelja. Poslužitelji koji reflektiraju ne moraju biti ranjivi, tj. na njih ne treba provaljivati pa se za napad može koristiti veliki broj poslužitelja koji su inače dobro zaštićeni.




**Slika 5.** DRDoS napad

Jedna od mogućnosti zaštite sustava od DRDoS napada je filtriranje SYN/ACK paketa. Ako se pretpostavi da je ciljano računalo zapravo poslužitelj ono nema razloga primati SYN/ACK pakete (poslužitelji primaju samo SYN i ACK pakete). Ipak takvim postupkom filtriranja paketa moguće je odbaciti neke korisne pakete.

## *3.3. Usporedba DoS i DDoS napada*

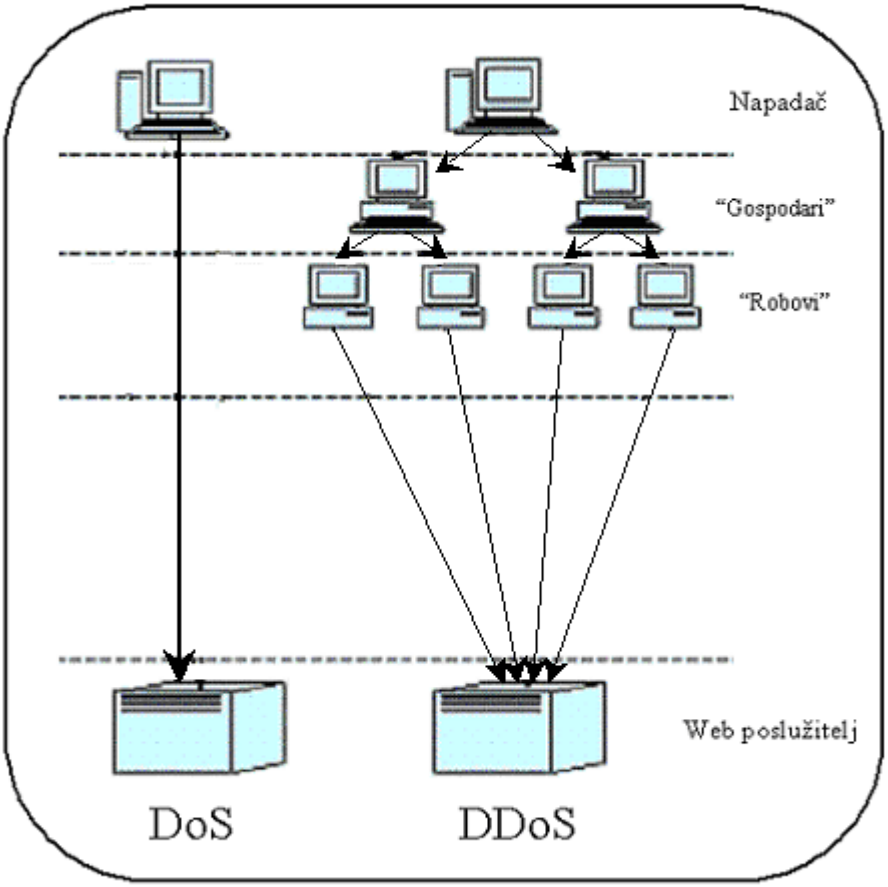
Vrlo je važno primijetiti razliku između DoS i DDoS napada. Ako napadač izvodi napad iz jednog poslužitelja taj napad će biti klasificiran kao DoS napad. U stvari, bilo koji napad na uporabljivost bi se trebao klasificirati kao Denial of Service napad. S druge strane, ako je jedan napadač koristi tisuću zombi sustava za istovremeno pokretanje napada taj napad će biti klasificiran kao DDoS napad. Znači, DoS napad se provodi s jedne te iste IP adrese, dok pri DDoS napadu radi se o više IP adresa.

Još jedna važna razlika između DoS i DDoS napada je u tome što kod DDoS napada postoji mogućnost da vlasnik nekog računala ne zna da sudjeluje u napadu. Takva računala nazivamo gospodari, a oni upravljaju robovima. Razlike između DoS i DDoS napada prikazuje slika 6.

DDoS napad može napraviti daleko više štete mrežnim operatorima, davateljima usluga, ali i običnim korisnicima Internet usluga. Svakim novim priključivanjem računala na Internet javlja se mogućnost stvaranja novog gospodara ili roba.

Glavne prednosti napadača koji koristi DDoS napad su:

- više računala može generirati više prometa od jednog,
- više napada raznih računala teže je otkloniti od napada jednog računala,
- ponašanje svakog računala koje napada može biti upravljano sa nekim od alata za automatizaciju napada što je teže pronaći i otkloniti.




**Slika 6.** Razlika između DoS i DDoS napada

U sigurnosti računalnih mreža, „povratni radarski signal" je neželjeni efekt napada uskraćivanja usluga. U ovoj vrsti napada, napadač lažira izvorišnu adresu u IP paketima poslanim na žrtve. U većini slučajeva, žrtva ne može razlikovati lažirane i legitimne pakete, tako da žrtva odgovara na lažirani paket kao što bi i inače. Ovi paketi su odgovor poznat kao povratni radarski signal.

# 4. Poznati DDoS napadi

Od prve pojave DDoS napada izvedeni su brojni napadi ove vrste koji su ugrozili gotovo sve poslužitelje priključene na Internet. Pregled nekih ozbiljnijih i poznatijih napada dan je u nastavku.

## *4.1. DDoS napadi u svijetu*

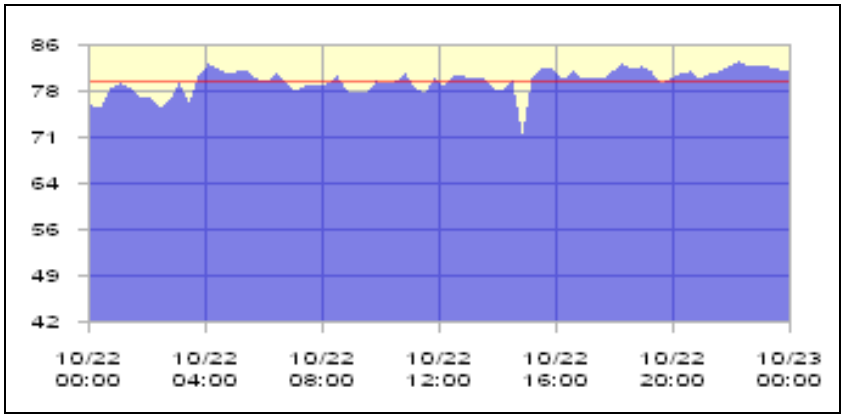
Prvi veliki DRDoS napad koji uključuje DNS poslužitelje kao reflektore se dogodio u siječnju 2001. Cilj napada bio je Register.com, a izveden je lažiranjem zahtjeva za MX zapise od AOL.com (DNS adresom mail poslužitelja). Trajao je oko tjedan dana prije nego je mogao biti praćen do napadačkog poslužitelja i isključen. Koristio je popis nekoliko desetaka tisuća DNS zapisa koji su nastali godinu dana ranije.

U veljači, 2001, grupa studenata NUI Maynooth sveučilišta napala je poslužitelj irskog vladinog odjela za financije (Government's Department of Finance) .

U srpnju 2002, analizom je utvrđeno da je iskorištena ranjivost poslužitelja projekta „Honeynet Project Reverse Challenge“ te je stvoren još jedan DDoS agent, koji provodi nekoliko srodnih DNS napada, uključujući i optimiziran oblik DRDoS napada.

U dva navrata do sada, napadači su obavili DNS Backbone DDoS Attacks na središnje DNS poslužitelje. Jedan od tih DDoS napada izveden je 21. listopada 2002. kada su napadnuti ključni DNS poslužitelji. Svih 13 DNS poslužitelja ciljani su istovremeno, a na 9 poslužitelja izazvano je stanje uskraćivanja usluga. Ovaj pokušaj je zabilježen kao prvi napad koji je usmjeren kako bi onemogućio funkcioniranje Interneta u cijelosti. Slika 7 prikazuje razinu prometa (eng. traffic index) u razdoblju od 24h u vrijeme ovog napada. Iskazan je preko ljestvice od 0, jako sporo, do 100, jako brzo. Računa se uspoređujući trenutne odgovore sa svim prijašnjim odgovorima tog usmjerivača u zadnjih 7 dana.

Drugi napad na DNS poslužitelje dogodio se 6. veljače 2007., ali ni na jednom od poslužitelja nije izazvano DoS stanje. Voditelj tehničkog odjela IANA-e John Crain izjavio je da je u utorak ujutro zabilježen nagli rast prometa prema središnjim DNS poslužiteljima.




**Slika 7.** Razina prometa u vrijeme DDoS napada na DNS poslužitelje

U kolovozu 2008. dogodio se još jedan ozbiljniji DDoS napad. U tjednima koji su vodili do petodnevnog gruzijsko-ruskog rata izveden je DDoS napad usmjeren na poslužitelje gruzijske vlade. Nosio je poruku: “win+love+in+Russia" ("osvojiti+ljubav+u+Rusiji"), a učinkovito je preopteretio i isključio više poslužitelja. Ciljane web stranice uključivale su i web stranicu gruzijskog predsjednika (Mikhail Saakashvili) i National Bank of Georgia. Iako su teške sumnje stavljene na rusku bandu RBN (eng. Russian Business Network), ruska vlada odbacila je tvrdnje, navodeći da je moguće da su pojedinci u Rusiji ili negdje drugdje sami pokrenuli napade.

## *4.2. DDoS napadi u Hrvatskoj*

21. travnja 2001. zabilježen je najveći napad na hrvatske Internet poslužitelje zbog kojeg je Hrvatska bila "odsječena" od Interneta. U subotu navečer oko 18 sati još nepoznati počinitelj ili počinitelji DDoS napadom na HT-ove usmjerivače otežali su pristup sadržajima web stranica izvan Hrvatske. Nakon što je

prvi napad zaustavljen, pola sata iza ponoći, kasnije je uslijedilo još nekoliko napada. Autor ili autori napada još nisu locirani, a prema istraživanjima napadi su pristigli iz 23 zemlje svijeta. Nakon što je u subotu napadnut HT, već u nedjelju je izvršen DDoS napad i na drugi najveći hrvatski ISP, Iskon. No, kako su tada i Iskon i ostali domaći ISP-ovi (osim CARNet-a) svoje Internet usluge pružali preko HT-ove veze svaki napad na HT-ov Hinet bio je na štetu i svim ISP-ovima.

Neki od poznatijih DDoS napada na hrvatske web stranice su napadi na dvije popularne web stranice: www.auti.hr i www.oglasnik.hr. Napade je navodno izvela grupa maloljetnika iz Tuzle tražeći određeni novčani iznos kako bi prestali s ometanjem rada web stranica.

# 5. Kako se braniti

Zbog toga što DDoS napada komunikacijsku infrastrukturu čak i ako je primarno usmjeren na poslužitelj, te zbog toga što u napad uključuje ogroman broj kompromitiranih računala, izuzetno je važno naći učinkovit način obrane od njega. U nastavku dokumenta opisne su neke osnovne metode tehničke zaštite, kao i zakonska regulativa.

## *5.1. Tehnička zaštita*

Prvo i najvažnije pravilo kojega se treba pridržavati kako bi se sustav zaštitio od napada je osigurati dovoljnu razinu sigurnosti poslužitelja. Pri tome postoje neke osnovne metode koje se trebaju provesti:

- napraviti popis svih procesa koji su pokrenuti na poslužitelju kao i popis svih mrežnih priključaka na kojima se pružaju usluge,
- onemogućiti sve procese osim onih koji su potrebni za normalan rad poslužitelja kako bi pružio predviđene usluge,
- uvesti filtriranje paketa (npr. pomoću programa IPFilter).

Filtriranje paketa ima mnoge prednosti, a jedna od njih je i izuzetno važna funkcija onemogućavanja lažiranja izvorne adrese (iznimno efikasno protiv DRDoS napada). Također je moguće blokirati pakete koji dolaze s nepoznatih odredišta kao i osigurati nadzor nad pristupom uslugama (definirati prava pristupa pojedinog korisnika uslugama).

Usmjerivači povezani na Internet mogu biti konfigurirani tako da skeniraju pakete (provjera IP adrese, porta) prije ulaska u interne mreže. Također se mogu koristiti kako bi se osigurala mreža nekog poduzeća kao potencijalnog izvora izvora DDoS napada. To se postiže filtriranjem odlaznih paketa te provjerom IP adrese svih paketa. Usmjerivač može također biti korišten kako bi se ograničio broj odlaznih TCP SYN paketa, ali ovu korištenje ove opcije preporuča se samo boljim poznavateljima mrežnih protokola jel nepravilna konfiguracija može dovesti do blokiranja legitimnog prometa.

Još jedan način zaštite je korištenje vatrozida (eng. firewall), koji radi na sličan način kao i usmjerivači za filtriranje prometa.

Opisani načini zaštite ne brane sustav od napada, ali osiguravaju da sustav ne sudjeluje u napadu (ne postane zombi, rob ili gospodar). Kako bi spriječili sam DDoS napad na sustav postoje također neke metode koje je potrebno provesti:

- distribuirati web stranicu preko višestrukih poslužitelja (vrlo skupo),
- povezivanje na Internet preko više pristupnih točaka,
- ugradnja alata za praćenje napada.

Do sada, programeri nisu uspjeli razviti 100% učinkovit obrambeni mehanizam. Svi mehanizmi koji su prezentirani mogu se suprotstaviti ili samo određenim DDoS napadima ili su na kraju ipak na neki način ugroženi od strane napadača. Stoga, brojne organizacije i pojedinci uporno rade na razvoju novih obrambenih mehanizama. Računala mamci (eng. Honeypots) su važna metoda za prepoznavanje, sprečavanje i obranu od DDoS napada.

## *5.2. Zakonska zaštita*

Konvencija o kibernetičkom kriminalu predstavlja oblik međunarodnog ugovora. Međunarodni ugovori važan su izvor međunarodnog prava kojim se uređuju međusobni odnosi između subjekata međunarodnog prava. Konvenciju o kibernetičkom kriminalu donijelo je Vijeće Europe 23. studenoga 2001. godine, a stupila je na snagu 1. srpnja 2004. godine. Konvenciju je potpisalo 38 država (među njima

i nečlanice Vijeća Europe: Kanada, Japan, Južna Afrika i Sjedinjene Države), a ratificiralo ju je 11 država: Albanija, Bugarska, Cipar, Danska, Estonija, Hrvatska, Luksemburg, Mađarska, Makedonija, Rumunjska i Slovenija.

Republika Hrvatska je ratificirala Konvenciju te njene odredbe unijela u svoj Kazneni zakon donošenjem Zakona o izmjenama i dopunama kaznenog zakona koji je stupio na snagu 1. listopada 2004. godine.

**Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava**

Članak 223.

(1) Tko ošteti, izmjeni, izbriše, uništi ili na drugi način učini neuporabljivim ili nedostupnim tuđe računalne podatke ili računalne programe, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(2) Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnim podacima ili programima ili neovlašteno presreće njihov prijenos, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(3) Tko onemogući ili oteža rad ili korištenje računalnog sustava, računalnih podataka ili programa ili računalnu komunikaciju, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(4) Ako je kazneno djelo iz stavka 1., 2. ili 3. ovog članka počinjeno u odnosu na računalni sustav, podatak ili program tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnog javnog interesa, ili je prouzročena znatna šteta, kaznit će se kaznom zatvora od tri mjeseca do pet godina.

(5) Tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne programe ili računalne podatke stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1., 2. ili 3. ovog članka, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(6) Posebne naprave, sredstva, računalni programi ili podaci stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1., 2. ili 3. ovog članka oduzet će se.

(7) Za pokušaj kaznenog djela iz stavka 1., 2. i 3. ovoga članka počinitelj će se kazniti.

# 6. Alati vezani uz DDoS napad

Kada se govori o alatima vezanim uz DDoS napad mora se napraviti podjela alata na one koji automatiziraju izvršavanje napada i one koji služe za otkrivanje napada. U nastavku je pregled nekih poznatijih alata koji služe u obje svrhe.

## *6.1. Izvršavanje napada*

Postoje brojni alati koji automatiziraju izvršavanje DDoS napada, a neki od najpoznatijih su:

1. Jedan od poznatijih programa za DDoS napade trinoo (**trin00**) je skup programskih paketa koji služe za izvođenje DDoS napada. Osnovni dio programa ima zadaću razašiljati veliki broj UDP paketa na ciljano računalo, što znači da radi na principu UDP poplavljivanja. Kako računalo pokušava odgovoriti na te brojne lažne zahtjeve (porukom "ICMP port unreachable") dolazi do zasićenja resursa te na kraju do uskraćivanja usluga. Dostupan je za Windows i Linux operacijske sustave.
2. Nakon alata trinoo počeo je razvoj alata **Tribe Flood Network** (TFN) koji radi na principu ICMP, UDP i SYN poplavljivanja te "Smurf" napada. Nedostatak alata je u tome što je dostupan samo za operacijske sustave Linux i Solaris.
3. Kombiniranjem karakteristika programa trinoo i TFN nastaje novi alat za izvođenje DDoS napada nazvan **Stacheldraht**. Prednost alata je u tome što omogućuje automatsko lažiranje izvorne adrese. Stacheldraht ima implementirane iste tehnike napada kao i alat TFN, a dostupan je za operacijske sustave Linux i Solaris.
4. Program **Trinity** omogućuje pokretanje više tipova poplavljivanja na ciljanu web stranicu, uključujući UDP i SYN.
5. Vrlo sličan programu trinoo razvijen je i program **Shaft** koji omogućava izvođenje raznih napada poplavljivanjem. Također ima mogućnost kontrole veličine paketa te trajanja napada.

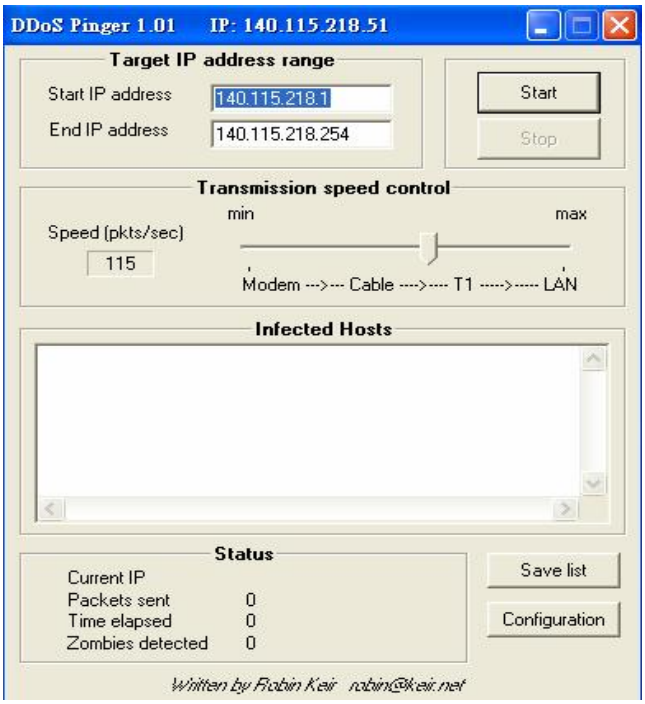
6. Alat **Tribe Flood Network 2K** (TFN2K) je složenija inačica alata TFN dizajnirana kako bi onemogućila filtriranje paketa, omogućila udaljeno pokretanje naredbi i skrivanje izvorne IP adrese s koje dolazi napad.

Postoje i mnogi noviji alati za izvršavanje napada kao što su: Mstream, Omega, Trinity, Derivatives, myServer i Plague.

## *6.2. Obrana od napada*

Budući da su razvijeni razni programi koji olakšavaju izvođenje DDoS napada postoje i mnogi koji služe za obranu. Neki alati koji se mogu iskoristit kao oružje u borbi protiv DDoS napada su:

1. Program **DdoSPing** je skener koji može otkriti rad programa trinoo, Stacheldraht i TFN. Nedostatak programa je u tome što otkriva rad navedenih programa samo ako imaju izvorno namještene postavke (eng. default) što se vrlo lako može promijeniti.




**Slika 8.** Sučelje programa DdoSPing

2. Program **find_ddos** također se koristi za skeniranje sustava kako bi pronašao trinoo, Stacheldraht, TFN2K i TFN programe.
3. Program **dds** (eng. Distributed DoS Scanner) omogućava otkrivanje aktivnosti programa trinoo, Stacheldraht i TFN. Dostupan je za sljedeće operacijske sustave: Linux (kernel inačica 2.2.x), Solaris (inačice 2.6 i veće), Digital Unix 4.0d, IMB AIX 4.2, FreeBSD 3.3. i OpenBSD 2.6.
4. Program **gag** skenira sustav kako bi otkrio Stacheldraht program, dok ostale programe ne može detektirati. Navedeni alat dostupan je za iste operacijske sustave kao i alat dds.
5. Alat **RID** je još jedan od skenera koji otkriva prisutnost trinoo, Stacheldraht i TFN programa.

Kao što je prikazano, većina alata za obranu od DDoS napada radi na jednakom principu: skeniraju sustav kako bi otkrili aktivnosti nekog od alata za automatiziranje DDoS napada.

# 7. Zaključak

DDoS napad jedna je od poteškoća s kojima se susreću gotovo sve web stranice i poslužitelji spojeni na Internet. Izvođenje napada u današnje vrijeme vrlo je jednostavno i nije potrebno veliko stručno znanje, zbog mnogih alata koji automatiziraju cijeli proces pripreme i napada. Zahvaljujući tome, u vrlo kratkom vremenu, moguće je stvoriti ogromnu mrežu računala koji čekaju jednu naredbu kako bi započeli napad.

Budući da je opasnost od DDoS napada velika potrebno je provesti odgovarajuće mjere zaštite računalnog i komunikacijskog sustava. Veliki problem stvara činjenica da korisnik nehotice ili bez svog znanja može sudjelovati u izvršavaju DDoS napada. Tomu pridonose programi koji imaju zadatak prekivanja zlonamjernog koda koji će pokrenuti napad s ranjivog računala.

Kako bi se sustav zaštitio i kako bi se spriječilo sudjelovanje u DDoS napadu, potrebno je provesti mjere zaštite poput filtriranja prometa te korištenja vatrozida. Ipak te mjere nisu dovoljna zaštita kako bi se sustav zaštitio i od toga da postane cilj nekog DDoS napada. Ne postoji nikakva sigurna zaštita, ali razvijeni su brojni alati koji mogu otkriti napad. Stoga se dopunska zaštita sastoji od prepoznavanja napada i brze reakcije na njega.

# 8. Reference


[1] DoS napad, http://en.wikipedia.org/wiki/Denial-of-service_attack, rujan 2008

[2] DDoS napad, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html, rujan 2008

[3] DDoS napad, http://www.cert.org/homeusers/ddos.html, rujan 2008

[4] DDoS Attack tools, http://staff.washington.edu/dittrich/misc/ddos/, rujan 2008

[5] KONVENCIJA O KIBERNETIČKOM KRIMINALU I KAZNENI ZAKON REPUBLIKE HRVATSKE, http://www.vojkovic.info/PDF/zbpdf_zb200601_123-136.pdf