DoS Napadi

Osnovna podjela

DoS napadi semogu podijeliti u dvije skupine. Kako se kod svih udaljenih DoS napada radi o napadima na sustave pomoću paketa razlikuju se obzirom na vrstu poruka odnosno paketa koji su upućeni prema žrtvi.

Napad iskorištavanja ranjivosti

Poruke mogu biti upućene ka specifičnoj aplikaciji ili određenom softverskom dijelu sustava koji sadrži neku slabost. Onda se specijalnim projektiranjem tih poruka iskorištava ranjivost i dovodi sustav u stanje obustavljanja posluživanja. U tom slučaju radi se o aplikacijskom DoS napadu, odnosno stručni termin je “iskorištavanje ranjivosti“ (eng. Vulnerability attack).

Flooding napad

Također, može se upućivati velik broj legalnih poruka samom sustavu tako da one kompromitiraju komunikacijski kanal ili zauzmu ključne resurse sustava (memorija, procesorski ciklusi, mrežni protok, itd.), te ga tako preopterete i onemoguće mu normalan rad. Da bi se to ostvarilo, napadačev stroj mora biti u mogućnosti generirati daleko veći broj poruka nego što napadnuti poslužitelj može obraditi u ograničenom vremenu. Takva vrsta napada naziva se Flooding attack (eng. Flood - poplava). Dakako komercijalni poslužitelji su građeni s velikim prometom na pameti, tako da bi napadač teško mogao preopteretiti stroj napadajući samo iz jednog smjera. U toj situaciji napadači se najčešće služe računalima koje su doveli pod svoju kontrolu probijanjem kroz sustav i krađom administratorskih ovlasti, najčešće pomoću rootkit alata. Zbirnim napadom sa svih računala koje imaju pod svojom kontrolom (eng. botnet) napadaju sustav s više strana te ga „izgladnjuju“ od njegovih resursa. Takav napad je izazov i za najbolje konstruirane mreže i poslužitelje, i naziva se distribuirani napad uskraćivanjem sigurnosti (eng. DDoS, distributed Denial of Service attack).

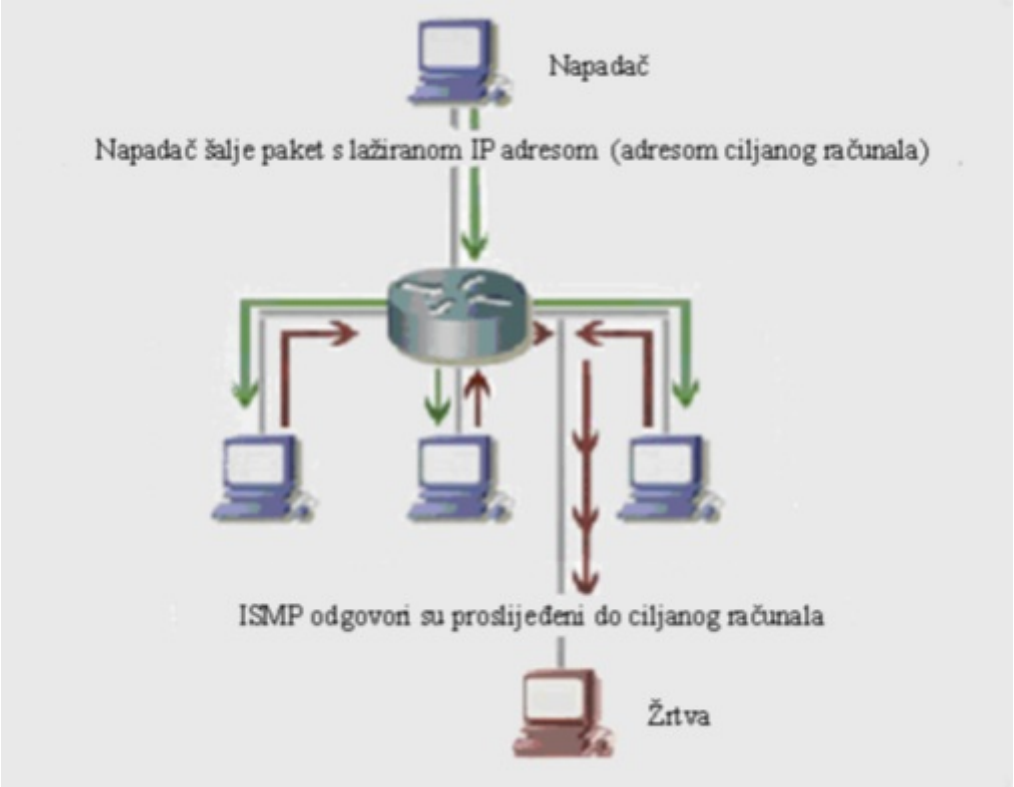
Vrste Napada

ICMP Flood napadi

U ovu kategoriju spadaju svi napadi koji temelje svojedjelovanje na ICMP protokolu (Internet Control Message Protocol), koji je jedan od temeljnih protokola unutar TCP/IP skupa protokola. Protokol služi primarno za slanje kontrolnih poruka unutar mreže, za razliku od primjerice UDP ili TCP protokola koji služe za prijenos podataka. Napadi zloupotrebljavaju način na koji protokol odgovara na određene kontrolne signale da preplave mrežu žrtve. U takve ubrajamo: smurf, ping flood, ping of deathi SYN napade. Postoje i drugi, ali su manje zastupljeni.

Smurf napad

Temelji se na krivo konfiguriranim mrežnim uređajima i koristi mogućnost slanja poruka svim uređajima na određenoj mreži pomoću broadcast adrese na mreži. U primjeni se šalje velik broj echo zahtjeva (ping) na usmjernik gdje je adresa pošiljatelja izmijenjena da odgovara adresi žrtve, najčešće samog usmjernika ali ne nužno. Usmjernik onda odašilje zahtjeve na cijelu podmrežu i sva računala odgovaraju na zahtjeve efektivno gušeći mrežu svojim odgovorima. U današnje vrijeme rijetko kad uspijevaju ovakvi napadi pošto je zaštita od istih jednostavna i ustvari je postala standardna postavka usmjerivača da onemogućavaju slanje na broadcast adrese.



Ping flood

Jednostavan tip napada gdje se koristi slanje velikog broja ping (echo request) zahtjeva na adresu žrtve, gdje je glavni uvjet za uspjeh napada da napadač posjeduje veću protočnost podataka od žrtve. Uspješnost napada je veća ukoliko žrtva odgovara s echo reply paketima.

Ping smrti (eng. Ping of Death)

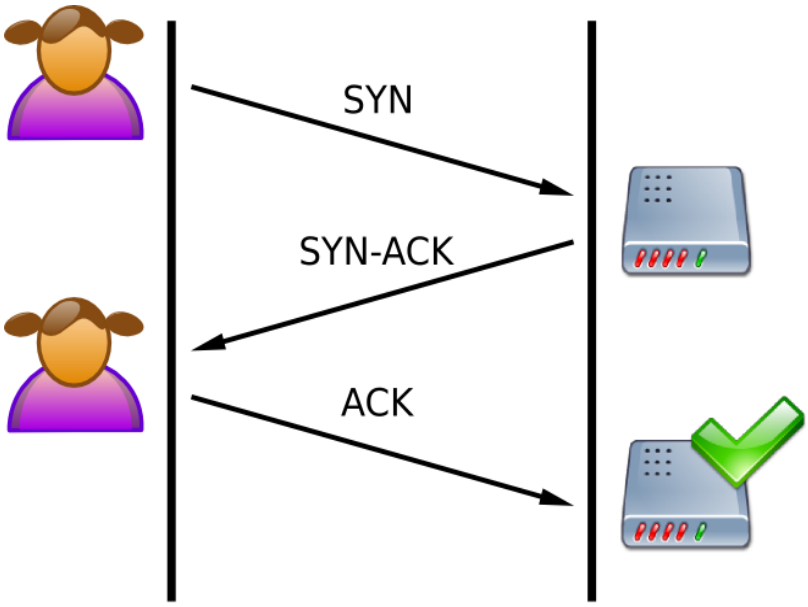
Usprkos zastrašujućem nazivu radi se o jednostavnijem tipu DoS napada gdje se iskorištava greška u implementaciji TCP/IP protokola. Temelji se na nemogućnosti obrade ping paketa veličine veće od najveće dopuštene veličine paketa unutar IPv4 definicije. Usporedbe radi, normalan ping request je duljine 32, odnosno 84 okteta s IP headerom, dok je najveći paket unutar IPv4 iznosio 65535 bajta. Ovaj napad je utjecao na većinu sustava uključujući Linux, Unix, Mac, Windows, printere i routere. Danas je jedino od povijesne važnosti jer je greška u implementaciji davno sanirana.

SYN flood

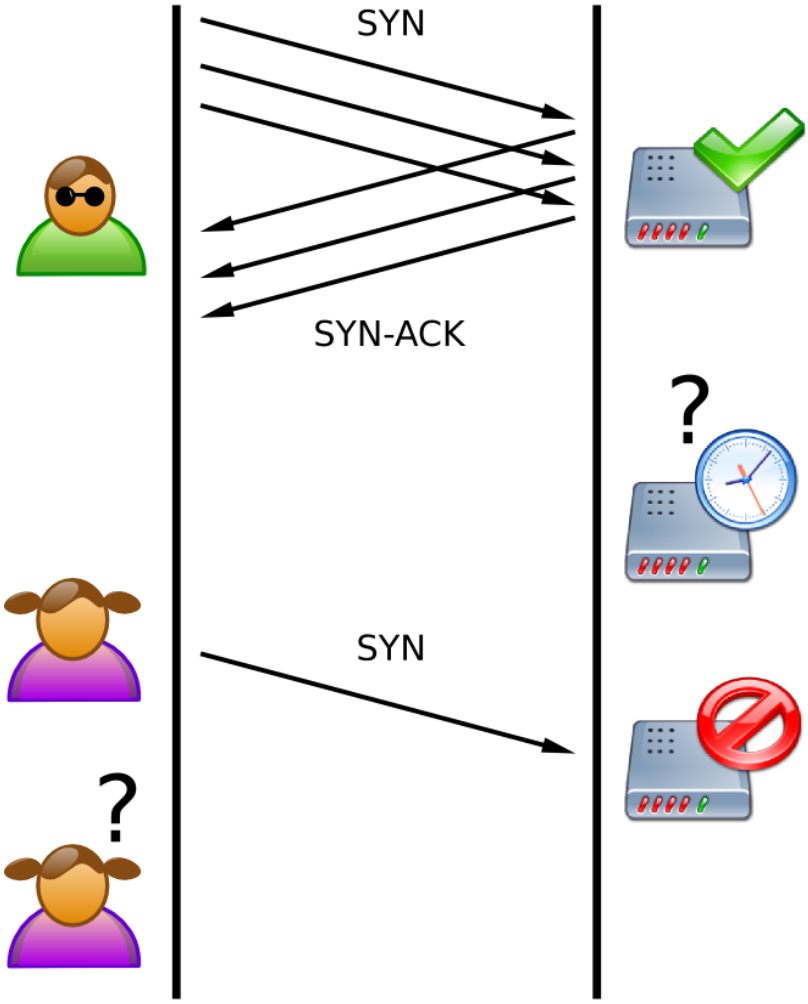
Vrsta DoS napada u kojem napadač šalje niz SYN (eng. synchronize) zahtjeva žrtvi. Uskraćivanje usluge se postiže korištenjem TCP protokola i načina na koji on uspostavlja vezu između dvaju sustava. Klijent i poslužitelj razmjenjuju niz poruka koje izgledaju ovako:

1. Klijent zahtjeva vezu slanjem SYN poruke poslužitelju.
2. Server odgovara i potvrđuje vezu slanjem SYN-ACK (synchronize- acknowledge) poruke klijentu.
3. Klijent potvrđuje slanjem ACK poruke i time je veza ostvarena.

Ovo je također prikazano na slici u nastavku.



Takva vrsta uspostavljanja komunikacije naziva se još i TCP three-way handshake, gdje je na slici legitimni korisnik prikazan lijevo,a desno poslužitelj kojemu on upućuje zahtjev za vezom. Ranjivost se temelji na dužnosti poslužitelja da zadrži i registrira sve SYN zahtjeve te ih drži u memoriji dok se ne ispuni konekcija. Napadač koristi to saznanje tako da šalje, s lažirane adrese ili s drugih računala, više SYN zahtjeva na koje dobiva odgovor u obliku SYN-ACK poruke, ali nikad ne odgovara na istu s ACK zahtjevom prisiljavajućiposlužitelja da zadržava takve polu otvorene veze u memoriji. Kada iskoristi sve resurse za takve poluotvorene veze poslužiteljviše ne može obraditi novopristigle legitimne SYN zahtjeve, te je time uskraćena usluga redovnim korisnicima. Konkretna implementacija napada se može izvesti tako da se izmjeni izvorišna adresa zahtjeva s nekom nepostojećom ili se klijent napadača postavi tako da ne šalje ACK pakete, uskraćujući odgovor poslužitelju. Primjer je dan na slici 4, gdje je napadač prikazan zelenom bojom. Danas se ta vrsta napada koristi iako postoje efektivne zaštitne mjere u obliku SYN Cookies-a o kojima će biti govora kasnije.

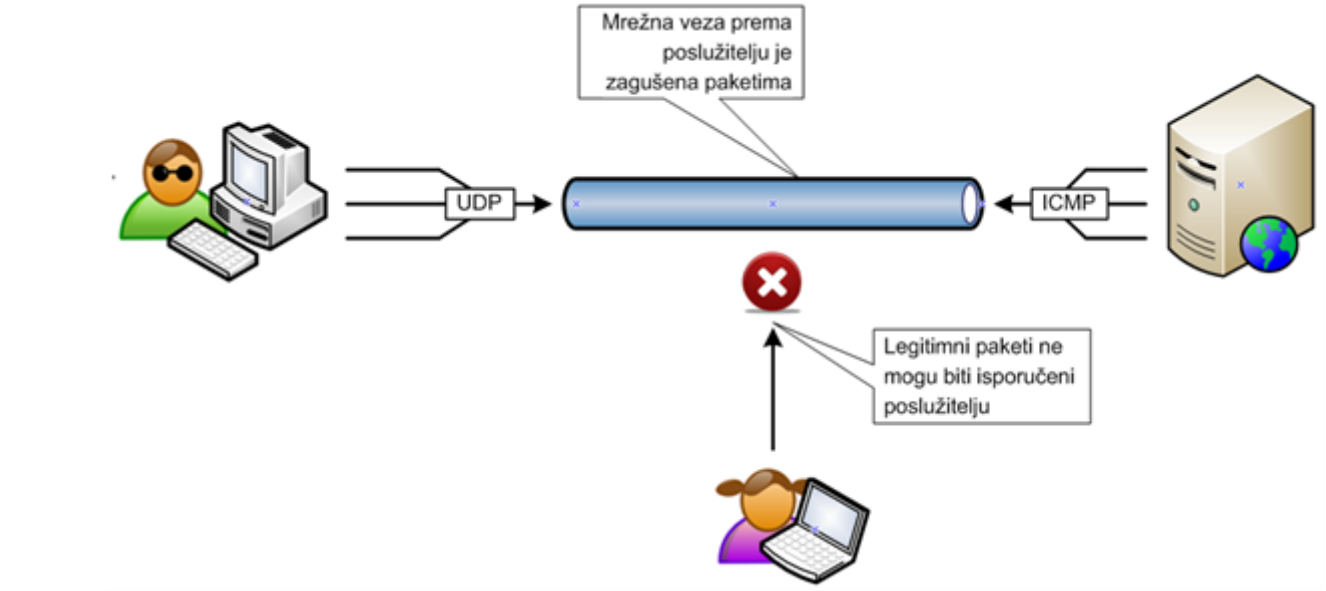


UDP Flood

Napad pomoću UDP protokola se uveliko razlikuje od napada TCP protokolom. Imajući na umu da UDP protokol ne garantira nikakvu isporuku niti očekuje uspostavljanje veze slanjem poruka potvrde (SYN, SYN-ACK, ACK), ova ranjivost se temelji na slanju velikog broja UDP paketa na slučajno odabrane priključke (eng. port) računalnog sustava. Nakon primitka poruka poslužitelj će:

1. provjeriti koja aplikacija osluškuje na odabranom portu,
2. uvidjeti da nema takve aplikacije te
3. odgovoriti na zahtjev ICMP Destination Unreachable paketom (nedostupna destinacija)

Takvim načinom obrade poslužitelj će sam sebi zagušiti konekciju odgovaranjem na velik broj lažnih UDP paketa. Taj scenarij je prikazan slijedečom slikom.



Teardrop napad

Napad u kojemu napadač koristi manjkavosti sastavljanja fragmenata unutar TCP/IP sustava. Slanjem oštećenog koda prevelike veličine prema žrtvi, moguće je da dođe do rušenja sustava zbog ranjivosti. Zbog veličine, poruka se fragmentira na manje pakete.U fragmente paketa upisuje se udaljenost od početka prvog paketa, što omogućuje ponovno sastavljanje paketa na drugoj strani. Napadač postavlja zbunjujuću udaljenost u jedan od fragmenata. Ako poslužitelj koji prima 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.

Nuke napad

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 paketa čime se usporava napadnuto računalo sve dok ne dođe do potpunog prekida. Poznatiji primjer nuke napada je WinNuke, koja iskorištava ranjivosti u NetBIOS modulu kod operacijskog sustava Windows 95. Slanje niza podataka van zacrtanih vrijednosti (eng. Out-of-band) na TCP priključak (eng. Port) 139 ciljanog uređaja uzrokuje zaključavanje računala i prikaz “Blue Screen of Death” poruke (tj. prestanak rada operacijskog sustava računala).
Postoje i druge vrste napada, ali su ovdje opisane osnove vrste napada. U daljnjem tekstu opisani su DDoS (eng. Distrubuted Denial-of-Service) napadi koji su modifikacije već navedenih napada. Većina prije opisanih napada se može pokrenuti u inačici koja uključuje više sustava koji napadaju simultano.

DDoS

Distribuirani napad uskraćivanja usluga (eng. DDoS Distrubuted Denial-of-Service) nastaje kada više (prethodno) kompromitiranih sustava, koji se zbirno nazivaju *botnet*, poplavljuje resurse ciljanih sustava, obično jednog ili više web poslužitelja. DoS napadi se temelje na znatnoj količini podataka kojima se preplavljuje žrtva.Oni se najčešće izvode kao DDoS (eng. Distrubuted Denial-of-Service)

napadi. Težište pri tome je da više sustava nadvlada jednog. Možemo ih podijeliti u dvije osnovne skupine:

- direktne DDoS napade i
- reflektirane DDoS napade.

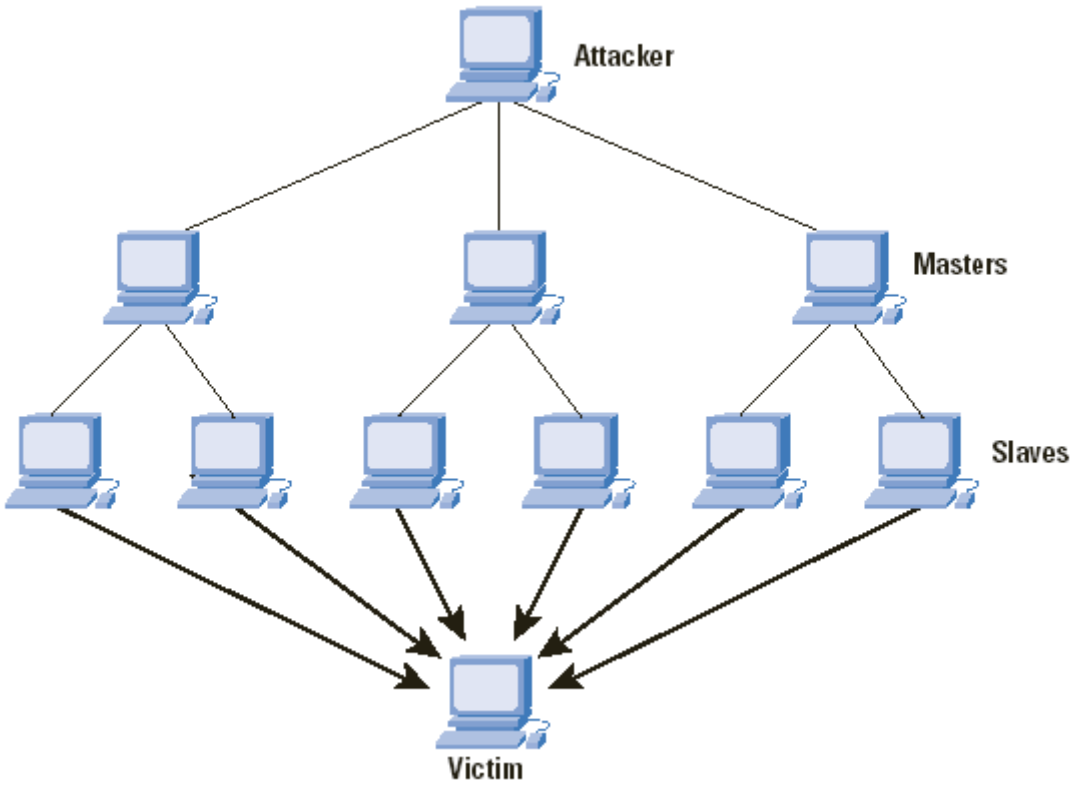
Priprema za DDoS napade

Za izvođenje DDoS napada je potreban velik broj računala koja su spremna izvršiti napad sinkronizirano pod komandom napadača. Takav sustav računala se ne gradi preko noći, te postoje mnoge tehnike kojima vješti kriminalci zauzimaju sustave drugih korisnika. Najčešće korišteni među njima su trojanski konji i virusi koji se propagiraju od sustava do sustava, te aplikacije s poznatim propustima koje napadači koriste za dobivanje administratorskih prava na sustavu. Dodavanjem novih računala povećava se brojnostbotneta, te senapadač koristi tim novim računalimada bi nastavio napadati i tragati za drugim nezaštićenim sustavima. Povećanjem i strukturiranjem botneta napadač povećava svoju napadačku mogućnost. Potraga za ranjivim računalima se izvodi na više načina:

- Skeniranje slučajnim odabirom (eng. Random scanning) – uređaj na kojem je pokrenut zlonamjerni kod proizvoljno odabire neku IP adresu iz zadanog adresnog prostora 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 računala.
- 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

DDoS napad

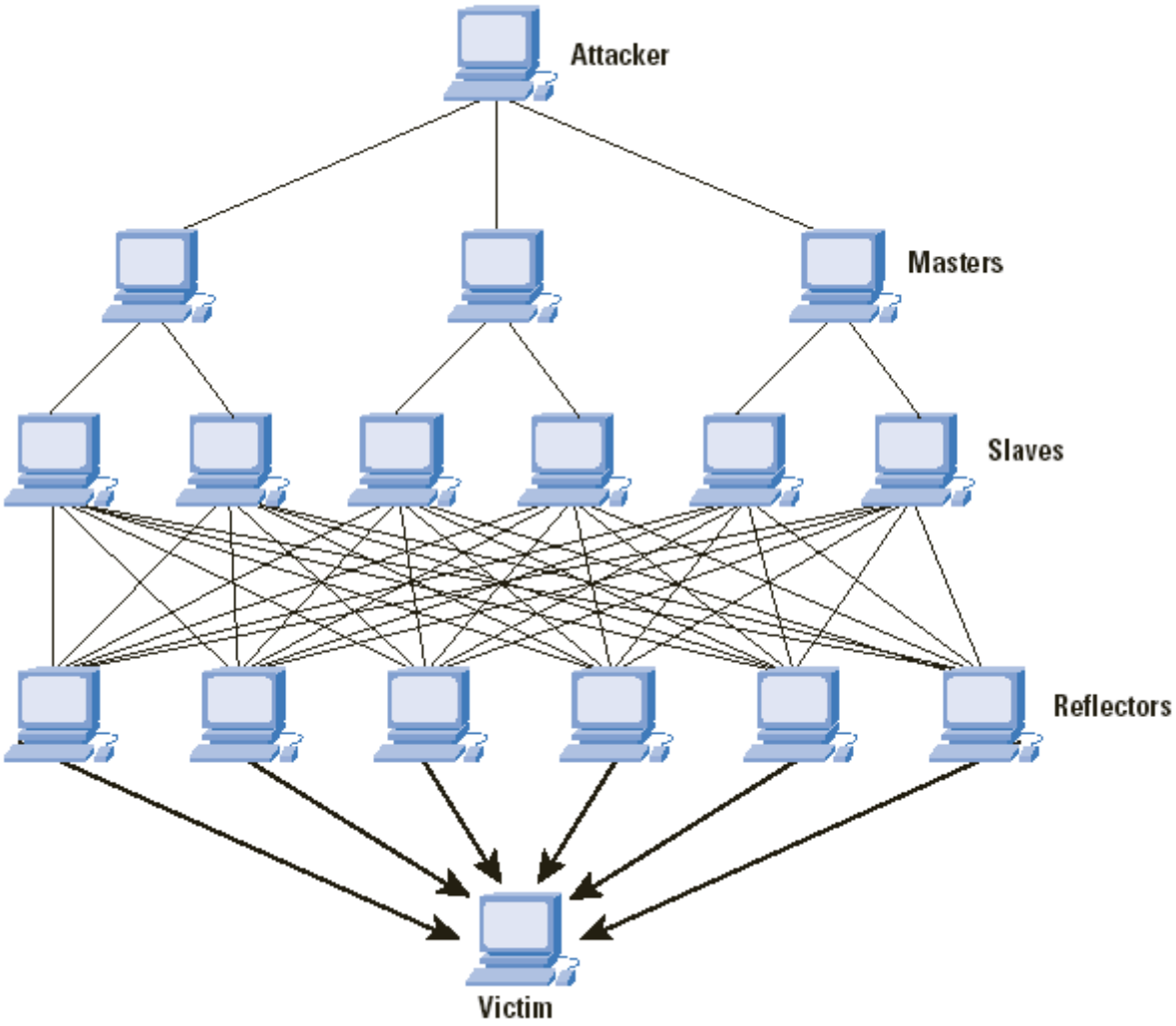
Nakon što je poprimio dovoljne razmjere botnet se strukturira tako da napadač komunicira samo s manjim brojem računala, pod nazivom gospodari, (eng. bot herder, master) koji kontroliraju napadačke sustave (eng. bot, zombie). To se izvodi radi jednostavnosti i radi težeg pronalaženja napadača preko IP adresa (eng. back-tracking). Slijedi primjer.



Tako strukturiran sustav je spreman za napad i jedino što je potrebno je jedna naredba od napadača. Slanjem naredbe gospodarima, oni prosljeđuju adresu mete botovima i napad počinje s više strana na zadanu metu. Nerijetko napadači iznajmljuju svoje botnetove ili ukoliko ih ne posjeduju iznajmljuju ih od drugih kriminalaca.

DRDoS

Pod ovom kraticom označavamo distributed reflected denial-of-service napade odnosno DDoS napade koji koriste druge računala izvan botneta da reflektiraju zahtjeve poslane njima prema sustavu koji treba napasti. Napad se izvodi tako da se od strane botneta šalje velik broj ICMP zahtjeva s lažiranom IP adresom izvora koja je postavljena na adresu žrtve, te se ti paketi nakon što ih obrade strojevi “reflektori“ prosljeđuju prema žrtvi. Takvim oblikom napada višestruko se povećava broj paketa i opterećenje na napadnuti stroj, te se time pospješuje efikasnost napada. Slika daje zorniji prikaz tog scenarija.



Peer-to-peer napadi

Specifičnost ovog DDoS napada je u tome što nije potreban botnet računala da bi se on izveo, nego se koriste legitimni korisnici peer-to-peer mreža. Koristeći brojne peer-to-peer (veza jedan na jedan) mreže napadači iskorištavaju ranjivost u istima za pokretanje DDoS napada na žrtvin sustav. Prilikom izvođenja napada, napadač nalaže klijentima peer-to-peer čvorišta za dijeljenje datoteka da se isključe iz svojih peer-to-peer mreža i spoje na žrtvin sustav. Kao rezultat toga, nekoliko tisuća računala pokušava se agresivno povezati na ciljano računalo. Tipični web poslužitelj može obrađivati nekoliko stotina veza u sekundi prije nego što mu performanse počnu opadati, usprkos tomu većina web poslužitelja pada gotovo odmah pri pet ili šest tisuća veza u sekundi. Prilikom peer-to-peer napada srednje veličine web stranica može biti pogođena sa oko 800.000 veza u kratkom vremenu, te iako može lako identificirati takvu vrstu napada pomoću unikatnih oznaka paketa (eng. signatures) tako veliku količinu veza se ne može filtrirati ukoliko se odjednom spoje na sustav. Ovakva ranjivost se može podrobno sanirati ukoliko se onemogući spajanje peer-to-peer mreža na priključak (port) 80.

DoS vs. DDoS

Razlika između ove dvije vrste napada je očigledna. Najopćenitije što se može definirati je da svaki napad koji uključuje više napadača koji pokušavaju postići uskraćivanje usluge se označava kao DDoS

napad. U protivnom se radi o DoS napadu. Iako se struktura samog napada razlikuje od napada do napada, većina DoS napada se izvodi kao DDoS napadi primarno zbog veće uspješnosti istih.